Міністерство освіти і науки України
Київський національний торговельно-економічний університет
Департамент кіберполіції Національної поліції України
Майкрософт Україна
Чернівецький національний університет ім. Федьковича

БЕЗПЕКА СОЦІАЛЬНО-ЕКОНОМІЧНИХ ПРОЦЕСІВ В КІБЕРПРОСТОРІ

МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

(Київ, 27 березня 2019 року)

Київ 2019

УДК 004.056
Б 53

Б 53 **Безпека** соціально-економічних процесів в кіберпросторі : матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). – Київ : Київ. нац. торг.-екон. ун-т, 2019. – 244 с.
ISBN 978-966-629-925-6

Збірник матеріалів учасників Всеукраїнської науково-практичної конференції «Безпека соціально-економічних процесів в кіберпросторі» присвячений актуальним питанням у сфері економічного, соціального, нормативно-правового, адміністративного безпечного функціонування кіберпростору, технічного забезпечення кібербезпеки, боротьби із кіберзлочинністю, захисту інформації в комп'ютерних системах і мережах.

Матеріали друкуються в авторській редакції. Відповідальність за зміст публікацій та академічну доброчесність несуть автори.

ISBN 978-966-629-925-6

ЗМІСТ

ПЕРЕДМОВА

В умовах сьогодення питання кібербезпеки як складової інформаційного захисту держави є надзвичайно актуальними для України і світової спільноти.

У матеріалах Всеукраїнської науково-практичної конференції «Безпека соціально-економічних процесів в кіберпросторі» (м. Київ, 27 березня 2019 року) висвітлено проблематику економічного, соціального, нормативно-правового, адміністративного безпечного функціонування кіберпростору, технічного забезпечення кібербезпеки, боротьби із кіберзлочинністю, захисту інформації в комп'ютерних системах і мережах.

Суттєва увага приділяється основним напрямам забезпечення кібербезпеки в Україні, інформаційним технологіям у боротьбі з кіберзлочинністю, принципам реалізації кіберзахисту на підприємстві, криптографічним методам захисту інформації.

Матеріали Всеукраїнської науково-практичної конференції «Безпека соціально-економічних процесів в кіберпросторі» будуть корисними для всіх учасників заходу і читачів, які цікавляться сучасними проблемами безпечного функціонування кіберпростору.

Ректор Київського національного
торговельно-економічного університету
доктор економічних наук, професор,
академік Національної академії педагогічних
наук України, заслужений діяч науки і техніки
України, лауреат Державної премії України
в галузі науки і техніки, лауреат Премії Кабінету
Міністрів України за розроблення і впровадження
інноваційних технологій **А. А. Мазаракі**

УДК 336

Мазаракі Анатолій Антонович
доктор економічних наук, професор, ректор
Київський національний торговельно-економічний університет
Волосович Світлана Василівна
доктор економічних наук, професор, професор кафедри фінансів
Київський національний торговельно-економічний університет

БЕЗПЕКА ЕКОСИСТЕМИ ФІНАНСОВИХ ТЕХНОЛОГІЙ

Сучасний розвиток суспільства характеризується посиленням орієнтації ринків на потреби споживача. Це спричинило появу фінансових технологій (*FinTech*), що спочатку трансформувало фінансовий ринок, а у подальшому вплинуло на перетворення бюджетно-податкової системи, систем соціального забезпечення та державного управління. Протягом останніх десятиліть розвиток Інтернету спричинив революцію у сфері зв'язку та комунікації, що стало суттєвим чинником світового економічного зростання та вагомим інструментом забезпечення сталого розвитку. З одного боку, це дало можливість підприємствам та споживачам в усьому світі отримати вигоди від ефективності, швидкості та зручності цифрових операцій та обміну інформацією, а з іншого – обумовило зростання ймовірності отримання фінансових збитків, витоку даних та репутаційних збитків через кіберзлочинні дії.

FinTech – це інноваційні технології, які використовуються фінансовими інститутами, органами державного управління, торговельними організаціями для задоволення потреб споживачів фінансових, адміністративних послуг та товарів в умовах розвитку економіки споживання [1, с. 8]. Іншими словами *FinTech* передбачає використання технологій для фінансових рішень.

Нині все частіше розглядають *FinTech* як екосистему. Це цілком логічно, оскільки системі фінансових технологій притаманні ознаки останньої, зокрема емерджентність, сукупність, гетерогенність. Є думка, що екосистема *FinTech* поєднує всіх учасників фінансового ринку, зокрема *FinTech*-стартапи, регуляторів, банки, міжнародні платіжні системи, асоціації банкірів та фінансистів, інкубаторів, акселераторів, постачальників [2]. На нашу думку, екосистема *FinTech* – це сукупність традиційних фінансових посередників, їх об'єднань, *FinTech*-компаній, компаній інфраструктури, стартапів, регуляторів, акселераторів, інкубаторів та споживачів, які взаємодіють між собою в кіберпросторі, завдяки чому зростає ефективність задоволення потреб споживачів, безпека здійснення фінансових операцій, відбувається оптимізація діяльності постачальників послуг та регуляторів.

До складу інститутів екосистеми *FinTech* належать: великі технологічні компанії, діяльність яких концентрується як виключно на наданні фінансових послуг, так і виходить за її межі; компанії, які забезпечують інфраструктуру чи технологію, що полегшує транзакції фінансових послуг; компанії, що швидко розвиваються, як правило, це стартапи, зосереджені на конкретній

інноваційній технології або процесі [3]. *FinTech* включає такі складові, як підсистема технологій у сфері платежів; підсистема технологій у сфері кредитування; підсистема технологій у сфері інвестиційної діяльності банків та ринків капіталу (*Invetment Banking/Capital Market*); підсистема у сфері особистих фінансів (*Personal Finance*); підсистема технологій у сфері інституційних фінансів (*Institutional Finance*); підсистема технологій у сфері страхування (*InsurTech*); підсистема у сфері регулятивних технологій (*RegTech*).

Ризики учасників екосистеми *FinTech* поділяють на прямі та непрямі. Перші стосуються безпосередньо користувачів фінансових технологій, а другі – пов'язані із порушенням стабільності системи в цілому, що в подальшому також має негативний вплив на користувача, оскільки в результаті їх реалізації знижується зручність використання технологій і зростає вартість послуг внаслідок здійснення заходів щодо управління ризиками. До прямих ризиків належать ринковий ризик, що передбачає негативні наслідки від істотної зміни ринкової кон'юнктури; кіберризик, що виникає внаслідок специфіки середовища фінансових технологій; технологічний ризик, що передбачає порушення безперебійності надання послуг внаслідок збоїв чи помилок у діяльності сервісу; юридичні ризики, які стосуються недостатності захисту прав споживачів. Серед непрямих ризиків функціонування фінансових технологій варто виокремити ризик застосування фінансових технологій з метою відмивання грошей та фінансування тероризму, який може призвести до криміналізації фінансового сектору, що погіршить якість фінансових послуг та створить підгрунтя для втрати коштів сумлінних споживачів. При цьому результати опитування менеджерів з ризиків фінансових послуг, проведеного *Depository Trust&Clearing Corporation* (*DTCC*), свідчать, що 70% респондентів вважають найсуттєвішим вплив кіберризику на функціонування глобальної фінансової системи [4]. Згідно із дослідженнями «*The Risk Institute»*, 28% фінансових компаній стають жертвами кібератак, ризик реалізації яких останнім часом лише зростає [5].

При наявності низки переваг та можливостей *FinTech,* подальше поширення використання інструментів фінансових технологій містить й загрози, що стосуються:

– подальшого скорочення робочих місць у фінансовому секторі;

– скорочення частки традиційних фінансових посередників на ринку;

– порушення фінансової стабільності;

– неадекватного прийняття ризиків споживачами;

– спричинення зростання фінансової волатильності;

–примусове впровадження може призвести до добровільної фінансової ексклюзивності;

– порушення конфіденційності даних;

– недостатнього захисту прав споживачів фінансових послуг.

Основними напрямами подолання цих загроз та підвищення рівня безпечності функціонування фінансового сектору при застосуванні *FinTech* є:

– розробка та затвердження національних та міжнародного регулювання сфери *FinTech;*

– виникнення нових видів страхування ризиків, що реалізовуються в сфері *FinTech*, зокрема кіберризиків;

– впровадження інструментів *RegTech*.

RegTech – це технологія, яка прагне забезпечити «прості, налаштовані, легкі для інтеграції, надійні, безпечні та економічно ефективні» регуляторні рішення [6]. Її призначення полягає у трансформаційному потенціалі щодо здатності забезпечувати моніторинг фінансових ринків у реальному часі. Еволюція нетрадиційних посередників вимагатиме подальшої еволюції *RegTech*, оскільки нині спостерігається поступове зміщення акценту з інформації типу *KYC* (знай свого клієнта) до парадигми *KYD* (знай свого розробника).

Виокремлюють такі сфери застосування *RegTech*: дотримання відповідності; управління та контроль ідентифікації; управління ризиками; нормативна звітність; моніторинг транзакцій; торгівля на фінансових ринках. Перевагами *RegTech* для продавців фінансових послуг є збільшення ефективності контролю за витратами та ризиками, вивільнення надлишкового регуляторного капіталу; надання нових можливостей для стартапів, консультаційних компаній і технологічних компаній *FinTech*.

Для регуляторів *RegTech* (*SupTech*) дозволяє розробляти інструменти безперервного моніторингу для виявлення проблем; скорочує час, необхідний для розслідування порушень дотримання вимог; сприяє розвитку систем моделювання й інкубаторів, які можуть визначити ймовірні наслідки пропонованих реформ і нових підходів.

Отже, розвиток *FinTech* вимагає необхідності балансування між дотриманням безпеки та децентралізації й забезпеченням конфіденційності і масштабованості.

Список використаних джерел:

1. Мазаракі А. FinTech у системі суспільних трансформацій / А. Мазаракі, С. Волосович //Вісник Київ. нац. торг.-екон. уні-ту. 2018. – №2. – С. 5–18.
2. ФінТех в Україні : звіт Проекту USAID «Трансформація фінансового сектору» та інноваційного парку UNIT.City. – Режим доступу : http://data.unit.city/fintech/fgt34ko67mok/fintech_in_Ukraine_2018_ua.pdf
3. What is FinTech? – Режим доступу : https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-fsi-what-is-fintech.pdf
4. Reagan J.R., Raghavan A., Thomas A. Quantifying risk: What can cyber risk management learn from the financial services industry? //Deloitte Review. 2016. Issue 19. . – Режим доступу : https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/quantifying-risk-lessons-from-financial-services-industry.html
5. Renaud Ph. Cyber resilience: Tactics to find and fix security vulnerabilities. – Режим доступу : https://www.cefpro.com/0506ri-cyber-resilience-tactics-to-find-and-fix-security-vulnerabilities/
6. What is Regtech? And why is it becoming the next big thing? – Режим доступу : https://complyadvantage.com/blog/what-is-regtech/

УДК 351.865

Демедюк Сергій Васильович
кандидат юридичних наук,
доцент кафедри програмної інженерії та кібербезпеки КНТЕУ,
генерал поліції третього рангу,
начальник Департаменту кіберполіції Національної поліції України
Чубаєвський Віталій Іванович
кандидат політичних наук,
доцент кафедри програмної інженерії та кібербезпеки КНТЕУ,
полковник поліції,
заступник начальника Департаменту кіберполіції Національної поліції України
Макоєдова Валентина Олександрівна
провідний інженер-програміст Центру тестування та моніторингу знань
Київський національний торговельно-економічний університет

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ЯК НАПРЯМ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стрімкий розвиток технологій Інтернету зумовлює появу та розвиток нових видів кіберзлочинів, які тягнуть за собою серйозні та незворотні наслідки. Величезний технічний потенціал та безмежні можливості у віртуальному просторі все частіше використовуються кіберзлочинцями для шахрайства, тероризму та для реалізації політичної мети [1].

Саме з цих причин ми повинні налагоджувати співробітництво з іншими державами, міжнародними експертними організаціями у цій сфері, а особливо воно повинно активізуватися при розроблені відповідних нормативно-правових актів і прийнятті на рівні держави міжнародних норм та стандартів.

Положенням Стратегії національної безпеки на законодавчому рівні було деталізовано пріоритети державної політики у сфері забезпечення кібербезпеки та безпеки інформаційних ресурсів, до яких віднесені: реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [2].

Розвиток безпечного, стабільного і надійного кіберпростору має полягати у підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраціУкраїни з ЄС та НАТО для посилення можливостей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кібезпросторі, які проводяться під егідою ОБСЄ [3].

На підставі статті 14 Закону [4] регламетовано засади міжнародного співробітництва у сфері кібербезпеки за такими напрямами:

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

2. Україна відповідно до міжнародних договорів може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України «Про порядок направлення підрозділів Збройних Сил України до інших держав» та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України».

3. Відповідно до законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.

У лютому 2018 року Конгрес США схвалив закон «Про співпрацю з Україною з питань кібербезпеки», що передбачає:

– забезпечення України необхідною підтримкою для забезпечення урядових комп'ютерних мереж від кібератак зокрема, мережі, що захищають критичну інфраструктуру;

– підтримку Україні для зменшення залежності від російських інформаційно-комунікаційних технологій;

– допомогу Україні розбудувати потенціал, розширити обмін інформацією про кібербезпеку та співпрацювати з міжнародними зусиллями у сфері кіберпростору;

– зусилля США щодо зміцнення спроможності України запобігати кіберінцидентам та реагувати на них;

– потенціал для нових сфер взаємної допомоги США та України у вирішенні спільних кіберзлочинів, включаючи кіберзлочинність, стійкість до ботнетів та інших автоматизованих розподілених загроз та зусилля НАТО щодо надання Україні допомоги у розробці технічних можливостей для протидії кіберзагрозам [5].

Забезпечення міжнародної безпеки в інформаційній сфері і в світовому кіберпросторі вимагає не тільки зусиль окремих країн світу, а й розробку і здійснення максимально ефективних міжнародних інструментів. Тому всі економічні і політичні ресурси з протидії загрозам міжнародної

інформаційної та кібербезпеки повинні розглядатися на найвищому світовому рівні за участю основних кібердержав. Забезпечення кібербезпеки в контексті глобальних загроз, поряд з спільними зусиллями міжнародного співтовариства, диктує важливість розробки і здійснення превентивних дієвих заходів проти кібератак і кіберзлочинів в світовому кіберпросторі [6].

Держави–члени ООН акцентували й продовжують акцентувати увагу на необхідності налагодження стійкого діалогу між країнами та запровадження дієвих механізмів протидії викликам, якими супроводжується їх діяльність у кіберпросторі. Одними з пріоритетних напрямів є: створення мирної, безпечної, стійкої й відкритої інформаційної сфери; відповідальна поведінка держав; заходи з нарощування потенціалу тощо. У результаті потребують розроблення глобальні стандарти поведінки в кіберпросторі, розширення можливостей міжнародно-правової системи в попереджені та боротьбі з кіберзлочинністю; розвиток і заохочення позитивного досвіду у сфері інформування щодо надзвичайних ситуацій, створення стандартів поведінки в кіберпросторі [7].

Системний підхід до розв'язання проблем кібербезпеки, реалізація комплексу заходів для забезпечення кіберзахисту інформаційного простору України в тісній співпраці зарубіжними партнерами дозволить суттєво підвищити рівень захисту та зменшити втрати від майбутніх кібератак, ймовірність застосування яких є достатньо високою.

Список використаних джерел:

1. Дешко Л. М., Бондарєва К. Д. Кібербезпека в Україні: національна стратегія та міжнародне співробітництво [Електронний ресурс] // Електронне наукове фахове видання «Порівняльно-аналітичне право». – 2018. - №2. – с.379-382. – Режим доступу: http://www.pap.in.ua/2_2018/112.pdf.
2. Про затвердження Стратегії національної безпеки [Електронний ресурс] : Указ Президента України від 26 травня 2015 р. № 287/2015. – Режим доступу: https://www.president.gov.ua/documents/2872015-19070.
3. Про Стратегію кібербезпеки України [Електронний ресурс]: Указ Президента України від 27 січня 2016 р. № 96/2016. – Режим доступу: https://www.president.gov.ua/documents/962016-19836.
4. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017р. №2163-VIII. Відомості Верховної Ради. 2017. №45. Ст.403.
5. Ukraine Cybersecurity Cooperation Act of 2017 [Electronic resource]. – Mode of Access : https://www.congress.gov/bill/115th-congress/house-bill/1997.
6. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки [Електронний ресурс] // Міжнародні відносини Серія «Політичні науки». – №18-19 (2018) – Режим доступу: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389/3066.
7. Шемчук В. В. Основні напрями міжнародного співробітництва у сфері кібербезпеки [Електронний ресурс]/ В. В. Шемчук // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Юридичні науки. - 2018. - Т. 29(68), № 2. - С. 125-130. - Режим доступу: http://nbuv.gov.ua/UJRN/UZTNU_law_2018_29(68)_2_24.

УДК 004.056.5:343.326 (045)

Браіловський Микола Миколайович
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка.
Хорошко Володимир Олексійович
доктор технічних наук, професор,
професор кафедри безпеки інформаційних технологій
Національний авіаційний університет.

ОСОБЛИВОСТІ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВАХ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Використання кіберпростору [1] розширює можливості людей у спілкуванні, сприяє розвитку інформаційних технологій, досліджень та інновацій, стимулює до розвитку бізнесу, створює глобальний інтерактивний ринок. При цьому, переваги сучасного кіберпростору неминуче ведуть до виникнення нових загроз людям, суспільству, національній і міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, об'єднань держав, груп та осіб.

Кібератаки стають все більш привабливим транснаціональним бізнесом. Бізнесом, який не має кордонів, немає обличчя, немає покарання, так як за часту неможливо ні відслідкувати зловмисника, ні покарати його за законом. Хакерські групи перетворюються на кібертерористичні організації.

Зважаючи, що останнім часом інформаційні технології все частіше використовуються для досягнення воєнно-політичних цілей, втручання у внутрішні справи суверенних держав та порушення суспільного порядку, здійснення актів агресії проти інших держав, здійснення деструктивного впливу на об'єкти критичної інфраструктури, то це дає можливість застосування проти нашої держави низки кібератак і кібероперацій, які можуть призвести до проблем, пов‘критичної язаних із забезпеченням безперебійного функціонування об‘єктів інфраструктури, цілісності та конфіденційності інформації, а також її збереження [2].

На сьогодні основний напрямок дій хакерських або терористичних груп у кіберсфері є блокування серверів і інтернет-ресурсів за допомогою DDoS-атак [3], а також комп'ютерні атаки, що направлені на виведення з ладу інформаційно-комунікаційних мереж і систем зв'язку за допомогою вірусів; тимчасове блокування публічних веб-сайтів за допомогою спамів; атаки на офіційні веб-сайти або сторінки у соціальних медіаорганах державної влади та комерційних організацій з метою розміщення повідомлень дискретизаційного спрямування; несанкціонований доступ у систему з метою викрадення даних або її використання в організації кібератак на інші системи (створення бот-мереж); незаконне оприлюднення персональних даних у мережі Інтернет стосовно політиків, правоохоронців чи військовослужбовців у поєднанні із прямими погрозами.

На перший погляд, може скластися думка, що це шляхи атак на великі організації, підприємства критичної інфраструктури чи урядові структури. Насправді, нема сенсу атакувати системи, які заздалегідь відомо що мають потужний захист. Зрозуміло, що невеличкі підприємства, маючи розгалужену мережу електронних зв'язків як між собою, так і з великими підприємствами є більш привабливою здобиччю. При цьому більшість персоналу таких фірм не мають навіть гадки про правила поводження при таких ситуаціях, елементарних знань у галузі захисту від кібератак.

З метою убезпечення від таких дій постає потреба у проведенні, перш за все, інформаційно-пропагандистської кампанії про значимість проблематики інформаційної та кібербезпеки, а також підвищенні компетентності фахівців різних сфер діяльності з цих питань. При цьому за доцільне вбачається фахову підготовку фахівців з інформаційної і кібербезпеки для потреб як силових структур та органів державного управління, так і виробничої та банківської сфери проводити у єдиній системі освіти України. Крім того, створити систему підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки на курсах підвищення кваліфікації.

Також необхідно створити у сфері кібербезпеки державно-приватну взаємодію. Створення умов та можливостей по обміну інформацією про кіберзагрози і координацію команд реагування на комп'ютерні надзвичайні події. Це можливо зробити завдяки створенню для громадян, представників промисловості та бізнесу консультаційні пункти по допомозі у своєчасному виявленню, попередженню та нейтралізації кіберзагроз, а при необхідності консолідації зусиль у розслідуванні їх. Для створення таких центрів необхідно залучати волонтерські організації як українські, так і закордонні, що буде сприяти покращенню міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, та невідворотності покарання за вчинення кіберзлочинів.

Список використаних джерел:

1. Закон України Про основні засади забезпечення кібербезпеки України [Електронний ресурс].- Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

2. Nikolay Brailovskyi, Valeri Kozura, Svetlana Kondakova, Volodymyr Khoroshko Analysis of the cybersecurity status of the information space // Scientific & practical cyber security journal (SPCSJ) №4. [Electronic journal]. URL: https://journal.scsa.ge/issue/december-2018/

3. Браіловський М.М. Аналіз та моделювання загроз інформації з використанням міжмережевої взаємодії на прикладі DDOS атак. /Браіловський М.М., Зінченко А.С.// Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 05-06 квітня 2018 року; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова)та ін. К.: ВПЦ «Київський університет», 2018. – 510 с. С.142-144.

УДК 004.056

Остапов Сергій Едуардович
доктор фізико-математичних наук, професор,
завідувач кафедри програмного забезпечення комп'ютерних систем
Чернівецький національний університет імені Юрія Федьковича
Валь Олександр Данилович
кандидат фізико-математичних наук, доцент,
доцент кафедри програмного забезпечення комп'ютерних систем
Чернівецький національний університет імені Юрія Федьковича
Бесага Роман Миколайович
кандидат фізико-математичних наук, доцент,
доцент кафедри оптики та видавничо-поліграфічної справи
Чернівецький національний університет імені Юрія Федьковича

КВАНТОВИЙ КОМП'ЮТИНГ ТА СУЧАСНА КРИПТОГРАФІЯ

Відомо, що сучасні засоби криптографічного захисту інформації використовуються практично всюди: у захищених протоколах https, SSL, SET тощо, для захисту цілісності інформації, у системах електронного цифрового підпису. Однак баланс, що сьогодні підтримується цими засобами захисту, може бути порушено за допомогою одного з новітніх засобів обчислень: квантового комп'ютингу.

У 2016 році NIST (Національний інститут стандартів і технологій) США опублікував документ NISTIR 8105 [1], в якому обговорювався вплив масштабованого квантового комп'ютера на загальні криптографічні алгоритми. Вказувалося, що розробка масштабованого квантового комп'ютера та використання специфічних квантових алгоритмів факторизації великих цілих чисел та пошуку в невпорядкованому масиві, здатні не тільки ускладнити життя сучасній криптографії, а й зробити цілі розділи повністю непридатними. Так, використання алгоритму факторизації П. Шора [2] на масштабованому квантовому комп'ютері загрожує зробити повністю небезпечним використання асиметричних крипто-алгоритмів, які є основою всіх сучасних систем електронного цифрового підпису.

Стосовно симетричних алгоритмів ситуація виглядає значно кращою, оскільки просте збільшення довжини ключа робить квантові атаки за допомогою алгоритму Л. Гровера [3] малоперспективними.

Те саме відноситься й до криптографічних функцій хешування: простим збільшенням довжини хеш-образу вдається значно зменшити ефективність квантових атак.

Усі вказані небезпеки відносяться до розробки масштабованого квантового комп'ютера, який на сьогодні ще не створений. Зараз ведуться розробки спеціалізованих квантових комп'ютерів, призначених для розв'язання конкретних задач. Так, Google проводить експерименти з

розпізнавання образів Google Street View за допомогою квантового комп`ютера, Lockheed Martin використовує квантовий комп'ютер для аналізу програмного забезпечення військових літаків. Однак були спроби реалізації й алгоритмів факторизації, наприклад, експерименти IBM по розкладанню чисел на прості множники. Відомі на сьогодні реалізації квантових комп'ютерів мають об'єм квантового ОЗП від 5 до 56 кубітів і призначених для виконання як елементарних квантових алгоритмів, так і моделювання фізичних об'єктів та процесів.

Окремо варто згадати розробки канадської компанії D-Wave [4], яка випускає квантові комп'ютери з ОЗП у 128 кубітів і анонсує такі з ОЗП у 1024 кубіти. І хоча наукова спільнота досить скептично відноситься до цих розробок, оскільки вони не повністю відкриті, D-Wave треба розглядати як серйозного гравця після експериментів, що довели існування в ОЗП їхніх комп'ютерів стану квантової суперпозиції та підтвердження квантового прискорення обчислень.

Що ж може протиставити цьому сучасна криптографія в частині асиметричної криптографії?

Сьогодні, як альтернатива, розглядаються алгоритми завадостійкого кодування. Вони можуть бути модифіковані таким чином, щоб замінити сучасні асиметричні криптоалгоритми. Це, зокрема, алгоритми МакЕліса, МакЕліса-Нідеррайтера та інші.

Аналіз вказаних алгоритмів демонструє їх стійкість до існуючих квантових атак та можливість порівняно простої реалізації.

Звісно, повна заміна класичних асиметричних криптоалгоритмів – це не є задачею сьогоднішнього дня, однак в недалекому майбутньому, після введення до експлуатації програмованого квантового комп'ютеру, ми повинні бути до цього готові.

Роботи, які ведуться в цьому напрямку, дозволяють зі стриманим оптимізмом дивитися в майбутню еру постквантової криптографії.

Список використаних джерел:

1. NIST Interagency Report 8105 «Report on Post-Quantum Cryptography» / [Електронний ресурс]. – Режим доступу : https://csrc.nist.gov/csrc/media/publications/nistir/8105/final/documents/nistir_8105_draft.pdf (дата звернення 11.03.2019).

2. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Foundations of Computer Science : Conference Publications. — 1994. — P. 124–134.

3. Grover L.K. A fast quantum mechanical algorithm for database search // Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC). - 1996. - P. 212-219.

4. D-Wave – The Quantum Computing Company: офіційний сайт / [Електронний ресурс]. – Режим доступу : https://www.dwavesys.com/quantum-computing (дата звернення 11.03.2019).

УДК 004.056

Звєрєв Володимир Павлович
кандидат технічних наук, старший науковий співробітник,
дійсний член Української Академії кібербезпеки,
помічник Голови Національної поліції України
Козаченко Ігор Миколайович
незалежний експерт з кіберзахисту,
дійсний член Української Академії кібербезпеки,
СОО компанії ROMAD UKRAINE LLC

РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ АНТИВІРУСНОЇ СИСТЕМИ ЗАХИСТУ ROMAD ENDPOINT DEFENSE

Найбільш поширеною загрозою сталій роботі комп'ютерних мереж і пристроїв, під'єднаних до відкритого Інтернет-ресурсу, безперечно вважається поява нових видів шкідливого програмного забезпечення (ШПЗ).

Тільки за останні два роки масштабні атаки вірусів-шифрувальників таких як WannaCry, NotPetya, Locky та BadRabbit тощо, завдали збитків компаніям та приватним особам на суму понад 53 млрд доларів США [1, 2]. При цьому класичні антивірусні програми, побудовані на процедурі перегляду великої кількості сигнатур штамів вірусів, взагалі не змогли виявити цю загрозу, а тим паче її заблокувати (нейтралізувати).

У відповідності до новітніх світових тенденцій та протистоянню новітнім тенденціям кібератак, пропонується для боротьби із даним класом кіберзагроз використовувати антивірусну систему наступного покоління (next-generation antiviruses, NGAV) ROMAD™ Endpoint Defense.

Суттєві переваги запропонованої антивірусної системи ROMAD™ Endpoint Defense у порівнянні із відомими антивірусними програмами полягає у використанні багатоступеневої детекції системних викликів.

Функціонально система складається з двох підсистем:

Multi-tier filtering system - займається фільтруванням системних викликів; Malware Genome™ database - реалізує біоінформатичні алгоритми пошуку поведінкових "ДНК" шкідливих ПЗ.

Траси системних викликів структуруються в так звані "фрейми", які підлягають опису у внутрішньому форматі ROMAD. Детектор вміє агрегувати фрейми на базі потоків даного процесу, або різних процесів операційної системи. Кожна генетична секвенція складається з одного і більше фреймів. Сукупність генетичних секвенцій утворюють Malware Genome™ [3, 4].

Таким чином, опис ШПЗ через Malware Genome™ немає схильності до поліморфізму, властивого класичним антивірусам.

Аналітики IT-ринку прогнозують подальше стрімке збільшення кількості пристроїв, які підпадають під загрозу зловмисних атак хакерів. Станом на сьогодні в світі вже налічується понад 8 млрд. пристроїв, які мають підключення до мережі Інтернет (включно із телевізорами, холодильниками, приставками ТБ, пристроями Інтернету речей (IoT),

розумний будинок тощо), а в 2021 році їх загальна кількість очікується на рівні більше ніж 25 млрд пристроїв [5]. Це все спонукає до захисту кінцевих точок новітніми рішеннями щодо блокування ШПЗ в різних його проявах, а також боротьби з атаками типу «0-дня».

Такі тенденції практично унеможливлюють ефективне використання класичних антивірусних програм і створюють сприятливі передумови запровадженню антивірусних систем наступного покоління.

Так, ROMAD™ Endpoint Defense – це: програмне забезпечення наступного покоління (Next Generation) класу Endpoint Detection and Response (NG EDR); захист кінцевої точки від кібератак, які використовують шкідливе програмне забезпечення (ШПЗ); технологічні інновації, які дозволяють проводити поведінковий аналіз 100% системних викликів у реальному часі із мінімальним навантаженням обчислювальних ресурсів; за результатом аналізу детектується та блокується деструктивна активність ШПЗ до того, як заподіяна будь-яка шкода кінцевій точці; виявлення та блокування сімейств ШПЗ, а не окремих штамів вірусів.

Такий підхід дозволяє підвищити ефективність більше ніж у мільйон раз, порівняно із традиційним антивірусним захистом, оскільки на сьогодні у світі відомо не більше 250 сімейств ШПЗ, на базі яких створено понад 750 000 000 окремих унікальних штамів ШПЗ; ефективний захист від загроз типу «0-day», - нові, досі невідомі штами ШПЗ, які не виявляються та не блокуються антивірусними програмами навіть із оновленими та актуальними базами сигнатур; реалізація принципу «пісочниці», але на більш досконалому рівні, оскільки принципово нейтралізуються усі технології кіберзлочинців, які дозволяють новому штаму ШПЗ виявити «пісочницю» та не розпочинати свої деструктивні дії (активізацію); блокування ШПЗ, яке не має файлу, або видаляє свій файл після запуску. Так, традиційний антивірусний захист аналізує тільки ШПЗ, яке має файли; автономна робота на кінцевій точці, не потрібен доступ до «хмари» для ефективного захисту від кібератак; відсутня потреба у частому оновленні генетичних секвенцій (аналог сигнатур у класичного антивірусу). Оновлення один раз на місяць або рідше; технологічні інновації захищені патентами США (US2014/0237596A1, US9372989B2) та Європейського Союзу (EP 2767923 A3).

Список використаних джерел:

1. McAfee Labs Threat Report / [Електронний ресурс]. – Режим доступу : https://www.mcafee.com/ru/resources/reports/rp-quarterly-threats-sept-2017.pdf
2. Infosecurity Group / [Електронний ресурс]. – Режим доступу : https://www.infosecurity-magazine.com/news/fedex-notpetya-cost-us-300-million/
3. AV-TEST Institute / [Електронний ресурс]. – Режим доступу : https://www.av-test.org/en/statistics/malware/
4. Digital Immunity Stay Productive, Stay Secure. / [Електронний ресурс]. – Режим доступу : https://www.digitalimmunity.com/wp-content/uploads/2018/04/EMA-NGES-2017-RR.pdf
5. Windows Anti-malware Market Share Report / [Електронний ресурс]. – Режим доступу : https://metadefender.opswat.com/reports/anti-malware-market/

УДК 044:327(075.8)(477:470+571:510:73)

Гайдук Олег Васильович
перший заступник голови громадської спілки «КІБЕРКОВЧЕР»

КІБЕРПРОСТІР ЯК ПЛОЩАДКА ТА ІНСТРУМЕНТ ВПЛИВУ НА СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОЦЕСИ

Кіберпростір охоплює область функціонування цифрових продуктів інформаційно-комунікаційних технологій, що створюють складні системи взаємодії, генерують і отримують інформацію, керують нею, а також здійснюють комунікації в умовах безлічі різних інформаційних мереж. Крім цього, він фактично являє собою загальний простір взаємодії інформаційних потоків, в якому спостерігаються явище глобалізації у всьому різноманітті її проявів. Кіберпростір не виокремлюється межами національних держав, його межі рухливі і мінливі, він розсіяний повсюди, хоча і не відображений ні на одній карті світу. З'являється новий формат соціально-економічних процесів і внутрішніх відносин, включаючи нові форми трансграничної соціалізації (через розваги, роботу, приналежність до груп інтересів тощо), що робить зв'язок із національними кордонами дедалі примарнішими [1].

В західних дослідженнях визначення поняття кіберпростору не дається напряму, у зв’язку з тлумаченням його другого складника – простір. У той час як у вітчизняній практиці простір розуміється переважно як загальне поняття, що описує певну частину буття людини, в західній літературі йде мова здебільшого про environment. Environment надає кіберпростору характеристик певного «навколишнього середовища», яке можна відчути і на яке можна вплинути повсякденною діяльністю аж до знищення.

Соціально-економічний аспект аналізу кібернетичного простору пов'язаний з вивченням всіх відповідних взаємодій, які відбуваються в цифровому середовищі, в тому числі функціонування численних віртуальних спільнот, а також нові можливості для побудови ідентичностей. Кіберпростір і реальний простір нерозривно пов'язані між собою і перетинаються в загальному потоці соціальних взаємодій. У зв'язку з цим доцільно зазначити, що нові можливості, які відкривають для людини інформаційно - комунікаційні технології дозволили фактично стерти межу між реальним світом і кіберпростором.

Визначивши кіберпростір як нове середовище існування сучасної людини, слід звернутися до ключових його характеристик. Однією з таких характеристик є його віртуальність. Сучасне вживання поняття «віртуальність» все частіше виходить за рамки області інформатики та комп'ютерної техніки. У побут увійшли такі, ще до недавнього часу нереальні терміни, як «віртуальна корпорація», «віртуальні гроші», «віртуальна демократія», «віртуальне навчання» і т.п. Віртуальна реальність, таким чином, стає максимально об'єктивною, гранично конкретною і відчутною. Віртуальність тут не виступає протилежністю дійсності. Проте, віртуальність означає те, що щось в кіберпросторі може бути зовсім не тим, чим здається.

Таким чином, кіберпростір, будучи віртуальним місцем, не є місцем в звичному сенсі, коли місце або простір для взаємодії обмежені просторово - часовими рамками.

Кіберпростір є соціальним простором, оскільки в ньому відбуваються численні соціальні інтеракції між реальними людьми, які можуть представляти себе таким же чином, як вони представлені в реальному житті, або створювати свій новий образ за допомогою використання всіляких аватарів. Мова тут йде про конструювання мережевої ідентичності, що відрізняється гнучкістю, фрагментованістю і множинністю.

Соціальні інститути в нових умовах набувають віртуальну форму, не перестаючи при цьому залишатися частиною соціальної реальності. Кіберпростір виступає в якості особливого соціального, економічного та культурного середовища, яке за допомогою якісно нових феноменів істотно змінює параметри соціальних взаємодій індивідів. Кіберпростір неоднорідний. Існує різні рівні доступу людей в залежності від місця проживання, рівня доходу, освіти, статі, віку, походження, раси, мови і т.д. Це демонструє так званий цифровий розрив, який існує в сучасному світі як на глобальному рівні, так і на рівні окремих держав. Соціальний простір є символічною структурою людської діяльності. У нормативному плані він гетерогенний. Його базовою одиницею є соціальна позиція (статус). Соціальний простір складається з двох вимірів: вертикального (ієрархія соціальних інститутів) і горизонтального (специфіка їх конкретних видів). Одним із феноменів є соціальна кібер-репутація, яка характеризує когнітивне і афективне уявлення про діяльність і поведінку соціальних індивідів, що формується на основі колективно розділеної сукупності вірувань і цінностей в процесі їх взаємодії в інтернеті з різними мережевими співтовариствами. Це багатофазний процес, в якому послідовно наступні процеси змінюють один одного: заняття цільового сегмента інтернет-простору, вибудовування зв'язку з цільовою аудиторією і створення семантичного наповнення даного конструкту.

В аксіологічному аспекті соціальна кібер-репутація есплікується через цінності соціальної та економічної ефективності, свободи інформації та відкритості комунікації. Тим самим вона визначає як параметри впізнаваності й популярності в інтернеті конкретного соціального актора, маркетингового процесу або об'єкта, так і їх унікальні ідентифікаційні характеристики. Фактично кібер-репутація, яку в інтелектуальній традиції Science and Technology Studies (STS) можна розглядати як соціальний конструкт, надає індивідам конкурентні переваги за рахунок конвертації цифрового популярності у вплив. На практиці це вплив реалізується не тільки в форматі віртуального простору, але і в реальному соціально-економічному просторі, забезпечуючи отримання індивідами не тільки символічних, але і конкретних матеріальних дивідендів.

Попри всі публічні заклики до мирного використання кіберпростору в інтересах усіх людей і держав, уряди тих самих країн, які до цього закликають, активно долучилися до гонки кіберозброєнь, відтворюючи класичну «дилему безпеки» на якісно новій основі. А це означає, що на тлі

розгортання складних і суперечливих глобальних процесів політичного, економічного та соціального розвитку кіберпростір перетворюється на простір виникнення «холодної війни v2.0.», тобто основу нового протистояння ключових геополітичних суб'єктів, яке відбуватиметься переважно в кіберпросторі [2].

Причому наразі ЄС фундаментально переосмислює кібербезпекову дійсність і переходить від розуміння кіберзагроз виключно як кіберзлочинів до військових і геополітичних трактувань цього явища. У феномені кібермогутності держави ключовим чинником є не стільки технологічна, скільки кадрова перевага – наявність достатньої кількості фахівців, які зможуть забезпечити інтереси держави в кіберпросторі. Відповідно, держави з більшою кількістю населення отримують очевидні латентні переваги у використанні потенціалу цього нового простору.

Якщо визначити, що кібервійна є крайнім проявом агресії у кіберпросторі, то ми побачимо великий спектр менш радикальної, але не менш негативної діяльності, з якою вже більше 5-ти років напряму доводиться стикатися нашій країні.

Згадаймо політичне протистояння в жовтні 2013 року – лютому 2014 року довкола підписання/не підписання тодішньою владою Угоди про асоціацію між Україною та ЄС (події Євромайдану). Це протистояння активно відбувалося в соціальних мережах, де спостерігався значний сплеск зацікавленості проблемою. З першого дня Євромайдану "невідомі особи" почали масово використовувати інструменти соцмереж з метою засмічення інформаційного поля, введення людей в оману та поширення чуток. Наприклад, у Twitter, де можна відслідковувати всі події за хештегом #євромайдан, десятки нетботів вкидали різноманітне інфосміття.

Використовувалися також механізми ускладнення традиційних комунікацій, зокрема мобільного зв'язку (через автоматичні дзвінки на телефони певних активістів чи політиків, що унеможливило використання їхніх мобільних телефонів у роботі). Було «зламано» електронні пошти, акаунти політиків у Twitter та Facebook. Зі «зламаних» сторінок масово розсилалися фейкові повідомлення, спрямовані на дезінформування суспільства. Загалом відбулася прицільна атака на ресурси та інструменти, які забезпечують комунікацію політиків із громадськістю та ЗМІ через інтернет. Постраждали й електронні ЗМІ, які були головними інформаційними майданчиками, а заразом і рушійними силами акцій протесту. Кілька днів поспіль хакерських атак зазнавали сайти «Української правди», «Главкому» та інтернет-видання «Цензор.нет». Офіційні сайти Міністерства внутрішніх справ, Кабінету Міністрів і Президента України зазнали хакерських атак [2].

Останнє на часі кіберпротистояння стосується загострення україно-російських відносин. Частково воно є наслідком тієї суспільно-політичної кризи, яка охопила українське суспільство протягом грудня 2013 року – лютого 2014 року. Внаслідок цього протистояння було сформовано загони хактивістів, які йменують себе «Кіберберкутом» (Cyberberkut – віртуальна структура, що не визнає української влади, яка сформувалася після лютого 2014 р. та «Кіберсотнею Майдану», «Анонімусами» з російською або

українською «пропискою» тощо. Діяльність «кіберберкутівців» та інших інтернет-активістів (хактивістів) аналогічного ідеологічного спрямування зводиться переважно до DDos-атак на державні установи, мас-медіа й навіть комерційні структури.

Найбільш масовою атакою цієї групи на урядові інтернет ресурси була атака, організована 3 березня 2014 року. Складнощі в роботі відчули численні (понад 100) сайти – як урядові (зокрема Верховної Ради України, Кабінету Міністрів України, РНБОУ), так і різноманітних інтернет-ЗМІ.

З боку лояльних до нової влади хакерських структур було проведено аналогічні кібератаки проти веб-сайту «Кремлін.Ру», сайтів Центробанку Росії, Міністерства іноземних справ РФ, Russia Today (RT), «Російської газети».

Разом з явними проявами кіберзброї присутні і інші її виміри, це в першу чергу маніпулювання суспільною свідомістю, використовуючи різні методи впливу на думки, вподобання людей в кіберпросторі.

Під маніпуляцією свідомістю розуміють дії, направлені на зміну психологічних установок, ціннісних орієнтацій, поведінки індивідів і аудиторій незалежно від їх бажання. Мета маніпуляції — контроль над аудиторією, її керованість. Для досягнення мети використовуються різні маніпулятивні технології: цілеспрямоване спотворення інформації (замовчування, селекція, «перекручування» і т.д.) [2].

Час працює не на самовизначення України щодо прийнятності/ не прийнятності одного із запропонованих підходів до міжнародної інформаційної кібербезпеки. Ідеться, зрештою, про стратегічний вибір напряму формування позиції країни з питань кібербезпеки та перспектив розвитку світового кіберпростору не лише на міжнародному, а й на національному рівні. Має бути сформована відповідна стратегічна «дорожня карта», що визначатиме головне: якою Україна бачить себе через 10–20 років: «неоколонією», яка постачатиме «метрополії» науковців і технології, чи країною, спроможною забезпечити суб'єктність на світовій арені. Під час її розроблення, зокрема, треба зважати на те, що неоліберальна парадигма не лише не передбачає виключного положення держави як такої на міжнародній арені, а й дедалі частіше апелює до нових геополітичних суб'єктів, якими є недержавні (позадержавні) актори у вигляді ТНК. У цій ситуації Україні варто зосередитися не стільки на обранні варіантів «або-або», скільки на обстоюванні тих стратегічних цілей щодо глобального кіберпростору, досягнення яких повністю відповідає національним інтересам України, незважаючи на те, яким, власне, підходам це відповідатиме.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України». Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата відклику 17.03.19)
2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

УДК 004.378:147

Пашорін Валерій Іванович
кандидат технічних наук,
професор кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет

ТЕРМІНОЛОГІЧНІ ТА ОСВІТНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

Однією із сучасних форм представлення знань є постійно оновлюванні тезауруси. В даному випадку будемо розглядати тезаурус як поняття, визначення і терміни спеціальної галузі знань або сфери діяльності. В освітньому процесі звернення до тезаурусу є обов'язковим, але імплементація тезаурусу важлива і для правильної корпоративної комунікації, розуміння в спілкуванні і взаємодії осіб, пов'язаних однією дисципліною чи професійними обов'язками.

Вичерпано сформульована та детермінована термінологія є перший крок, що допоможе фахівцям з кібербезпеки та захисту інформації виконувати їх головне професійне завдання – забезпечення кібербезпеки інформаційно-комунікаційної інфраструктури, тому вже на етапі підготовки таких фахівців важливо ведення та підтримка всіма суб'єктами освітнього процесу єдиного тезаурусу кібербезпеки.

Перш за все проблеми визначення термінологічної бази сфери кібербезпеки стикаються із суміжною та відносно ширшою категорією під назвою «інформаційна безпека». Таким чином постає завдання визначення відношень між категоріями «інформаційна безпека» та «кібербезпека».

Поява такого терміну як кібербезпека пов'язана з прийняттям нового явища в суспільстві, яке получило назву – кібернетичний простір, або кіберпростір. Відповідно до міжнародного стандарту, кіберпростір — це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі.

Кібербезпека – це безпека комп'ютерного та телекомунікаційного обладнання, програмного забезпечення і мереж. Тезаурус кібербезпеки інтегрований із поняттями інформаційної безпеки, комп'ютерної безпеки, безпеки додатків, мережевої безпеки, безпеки Інтернет та безпеки критичної інформаційної інфраструктури.

На сьогоднішній день під інформаційною безпекою розуміють захищеність суспільства і особистості від деструктивного інформаційного впливу (пропаганди, дезінформації, агресивної реклами, низькопробних видів мистецтва і т. п.) і тому тезаурус галузі інформаційної безпеки відображає широкий спектр суттєвих властивостей, ознак та відношень, притаманних даному специфічному виду безпеки.

Навіть в самих визначеннях, наведених тут категорій «інформаційна безпека» та «кібербезпека» продемонстровані суттєві розбіжності в сфері їх

застосування. Фахівець з інформаційної безпеки, виходячи з визначення, може навіть не розумітися в IT технологіях так, як фахівець з кібербезпеки.

Відрізнити спеціаліста з кібербезпеки від спеціаліста з інформаційної безпеки можна по сертифікації. Сертифікацій на тему кібербезпеки та інформаційної безпеки у світі величезна кількість, але є декілька найпоширеніших та найбільш популярних.

Спеціалісти з кібербезпеки:

CEH (Certified Ethical Hacker);

CISSP (Certified Information System Security Professional);

CCSP (Cisco Certified Security Professional).

Спеціалісти з інформаційної безпеки:

CISM (Certified Information Security Manager);

CISA (Certified Information Systems Auditor);

ISO 27001 Lead Implementer;

ISO 27001 Lead Auditor.

Ще один термінологічний казус в вітчизняному кіберпросторі пов'язаний з терміном хакер. Цей термін часто використовується як синонім до слова «зловмисник»: особа, яка вчиняє різного роду незаконні дії у кіберпросторі. Чи правильно це?

З початку надаємо визначення цього терміну з англомовного сектору вікіпедії:

Хакер:

1. Людина, що захоплюється дослідженням подробиць програмованих систем, вивченням питання підвищення їх можливостей, на противагу більшості користувачів, які вважають за краще обмежуватися вивченням необхідного мінімуму.

2. Хто-небудь, хто програмує з ентузіазмом, або люблячий програмувати, а не просто теоретизувати про програмування.

3. Експерт по відношенню до певної комп'ютерній програми, або той хто часто працює з нею (приклад: «хакер Unix»).

4. Експерт або ентузіаст будь-якого роду. Будь-хто може вважатися «хакером астрономії», наприклад.

5. Той, хто любить інтелектуальні випробування, які полягають в творчому подоланні або обході обмежень.

Тепер наведемо визначення терміну хакер в документі RFC -1983 Internet Users' Glossary, який розглядається як стандарт Інтернету.

«Hacker. A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular».

В цих визначеннях жодного негативного змісту до терміну хакер.

На наш погляд в тезаурус кібербезпеки перш за все в освітніх закладах необхідно ввести таке визначення терміну хакер.

Комп'ютерний хакер - це будь-який досвідчений комп'ютерний експерт, який використовує свої технічні знання для подолання проблеми.

Хакер – це оцінка кваліфікації користувача інформаційної системи. Хакер може здійснювати злочинні дії, а може їх і не здійснювати, може втручатися в роботу систем, порушувати їх нормальне функціонування, але

роботи це легально, з дозволу керівництва і не надаючи збитків компанії. В той же час легальний користувач за своєї низької кваліфікації може надати куда більше збитків із-за неграмотних дій, або не виконання політики безпеки підприємства. Статистика показує, що за некваліфікованої роботи легальних користувачів загрози для інформаційних ресурсів набагато більше.

Останнім часом ЗМІ словом «хакер» часто називають всіх мережевих зломщиків, творців комп'ютерних вірусів та інших комп'ютерних злочинців, таких як кардери, крекери, скрипт-кідді. Невизначеність в правовому полі що до цього терміну приводе в журналістських кругах вже до кольорових епітетів хакерам (як і магам). В грудні 2018 року в «Українській правді» журналісти пишуть про наявність в Україні нібито білих та чорних хакерів (саме так , а не white або black hat, як в західній пресі називають професіональних аудиторів інформаційних систем та кіберзлочинців відповідно).

Необхідно вивести з переліку дійових особ кіберпростору хакерів як особ, що негативно впливають на кібербезпеку. Таке рішення необхідно ще і для того, щоб ні у кого не виникало сумнівів при можливому доповнені стандарту вищої освіти України з спеціальності 125 Кібербезпека додатковими фаховими компетентностями для здобувачів вищої освіти. Мова йде про включення до стандарту такої фахової компетентності, наприклад як «…застосовувати методи аудиту та тесту на проникнення в інформаційні системи». Тобто, пропонується ввести в навчальні плани дисципліни, які надають знання методів так званого етичного хакінгу.

Прискорення темпів технологічного розвитку суспільства призвело до суттєвого відставання вищої освіти від зростаючих вимог ринку, як в області інформаційних технологій, так і в області кібербезпеки. ВНЗ України готують фахівців по спеціальності 125 Кібербезпека, але за різними спеціалізаціями: де спрямованість на менеджмент кібербезпеки, де на юридичні аспекти, а де на технічну підготовку. В нашому виші вибраний шлях, в рамках стандарту по спеціальності, давати посилену підготовку в напрямку програмування. Включення дисциплін з етичного хакінгу буде логічним продовженням підготовки саме таких фахівців, які добре розуміються в програмуванні. Така координація, по-перше, дозволить підняти рівень підготовки фахівців в Україні, завдяки міжнародній співпраці, а, по-друге, протидіяти кіберзлочинності спільно фахівцями з різних країн, оскільки, на відміну від реального простору, кіберпростор не має державних кордонів.

Зміна в світі парадигми підготовки фахівця з кібербезпеки від пасивного на активного захисника пов’язана з тим, що сучасні кіберзлочинці діють все більш приховано і завдають все більш серйозної шкоди. Для адекватного реагування на нові виклики і відповідності новим вимогам необхідно перевести орієнтацію освітніх програм на практичну підготовку, на вироблення у студентів вміння вирішувати реальні завдання. Фахівець з кібербезпеки повинен знати все те, що може знати і кіберзлочинець, наприклад виконувати тести на проникнення в інформаційну систему, і тільки тоді він зможе своєчасно зупинити його діяльність.

НАУКОВИЙ НАПРЯМ 1
КІБЕРБЕЗПЕКА В УКРАЇНІ:
ОСНОВНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ

SCIENTIFIC AREA 1
CYBERSECURITY IN UKRAINE:
MAIN PROVIDING DIRECTIONS

УДК 338.27+351.86

Лахно Валерій Анатолыйович
доктор технічних наук, професор,
завідувач кафедри комп'ютерних систем і мереж,
Національний університет біоресурсів і природокористування України
Малюков Володимир Павлович
доктор фізико-математичних наук, доцент,
професор кафедри комп'ютерних систем і мереж,
Національний університет біоресурсів і природокористування України
Касаткин Дмитро Юрійович
кандидат педагогічних наук, доцент,
доцент кафедри комп'ютерних систем і мереж,
Національний університет біоресурсів і природокористування України
Блозва Андрій Ігорович
кандидат педагогічних наук, доцент кафедри комп'ютерних систем і мереж,
Національний університет біоресурсів і природокористування України

ПРОБЛЕМИ ІНВЕСТУВАННЯ В КІБЕРБЕЗПЕКУ SMART CITY

Як показує практика, що для підвищення достовірності рекомендацій, наданих аналітиками (особа, яка приймає рішення – ОПР) у різних галузях, зокрема, в завданнях, що пов'язані з оцінкою інвестиційних проектів у сфері кібербезпеки (КБ) SmartCity, необхідно ширше використовувати комп'ютерні системи підтримки прийняття рішень (СППР). Запропоновано модель для розроблюваної СППР в ході процедури інвестування у проекти в сфері КБ SmartCity з урахуванням багатофакторності завдання. На відміну від існуючих підходів, модель заснована на рішенні білінійної багатокрокової гри якості з декількома термінальними поверхнями. В ході досліджень вперше розглянуто новий клас білінійних багатокрокових ігор, що описують взаємодію об'єктів в багатовимірному просторі. Це дозволяє адекватно описувати процес пошуку раціональних стратегій гравців (інвесторів) у ході інвестування в проекти в сфері КБ SmartCity. У процесі досліджень був розроблений програмний продукт «Investing in digital enterprises» в середовищі Android Studio. Модель та програмний продукт, що нами розробляється, дозволяє скоротити розбіжності даних прогнозних оцінок для інвестиційних проектів в сфері КБ SmartCity і реальної віддачі від інвестування. Також можливе вирішення завдань, пов'язаних з оптимізацією стратегій інвесторів.

Показано, що одним з найважливіших завдань, що стоять перед службами, що забезпечують розробку, створення і впровадження передових технологій КБ для Smart City, є завдання їх фінансового забезпечення проектів і залучення фінансових ресурсів ($FinR$) інвесторів. У свою чергу прийняття рішень щодо інвестування в технології КБ SmartCity має ґрунтуватися на процедурах, що дозволяють здійснювати фінансування з урахуванням всіх можливих факторів, в тому числі множинності передових

технологій в сфері захисту інформації та кібербезпеки. Це можливо, якщо будуть розроблені і впроваджені СППР або експертних систем (ЕС). Зокрема, затребувані програмні продукти для платформи Android, що дозволяють приймати раціональні рішення по вкладенню фінансових коштів на розвиток таких технологій.

Пропонована нами модель, заснована на аналізі можливостей процедури фінансування гравців в технології КБ Smart City з урахуванням їх багатофакторності, яка обумовлена їх множинністю. Модель є продовженням наших робіт [1-4] і заснована на вирішенні білінійної багатокрокової гри якості з двома термінальними поверхнями. Ми розглянули завдання в такій постановці. Є два гравці (інвестора), які керують динамічною системою в багатовимірних просторах. Система задана системою білінійних багатокрокових рівнянь із залежними рухами. Визначаються безліч стратегій (U) і (V) гравців і задаються термінальні поверхні S_0, F_0.

Мета першого гравця (далі $Inv1$) привести динамічну систему за допомогою своїх стратегій управління на термінальну поверхню, як би не діяв другий гравець (далі $Inv2$).

Мета $Inv2$ привести динамічну систему за допомогою своїх стратегій управління на термінальну поверхню F_0, як би не діяв $Inv1$.

Подальшими перспективами розвитку моделей і програмних продуктів, описаних в рамках тез, є перенесення накопиченого досвіду в реальну практику оптимізації інвестиційної політики і конкретних проектів у сфері інвестування в кібербезпеку SmartCity, а також накопичення статистичних даних для подальшої перевірки адекватності нашої моделі.

Список використаних джерел:

1. V. Lakhno, V. Malyukov, T. Bochulia, Z. Hipters, A. Kwilinski and O. Tomashevska, 2018. Model of managing of the procedure of mutual financial investing in information technologies and smart city systems. International Journal of Civil Engineering & Technology (IJCIET), Vol. 9, Iss. 8, pp. 1802-1812.
2. Malyukov, V.P. (1993). Discrete-approximation method for solving a bilinear differential game, *Cybernetics and Systems Analysis*, 29(6), pp. 879 – 888.
3. Akhmetov, B. B., Lakhno, V. A., Akhmetov, B. S., & Malyukov, V. P. (2018). The Choice of Protection Strategies During the Bilinear Quality Game On Cyber Security Financing. Bulletin of The National Academy of Sciences of the Republic of Kazakhstan, (3), pp. 6-14.
4. Lakhno, V., Malyukov, V., Parkhuts, L., Buriachok, V., Satzhanov, B., & Tabylov, A. (2018). Funding model for port information system cyber security facilities with incomplete hacker information available. Journal of Theoretical & Applied Information Technology, 96(13), pp. 4215-4225.

УДК 004.056

Звєрєв Володимир Павлович
кандидат технічних наук, старший науковий співробітник,
дійсний член Української Академії кібербезпеки,
помічник Голови Національної поліції України
Національна поліція України
Козаченко Ігор Миколайович
незалежний експерт з кіберзахисту,
дійсний член Української Академії кібербезпеки,
СОО компанії ROMAD UKRAINE LLC

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРЗАХИСТУ ЕЛЕМЕНТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ПЕРІОД ВИБОРЧОЇ КАМПАНІЇ 2014 РОКУ

З метою забезпечення електронного підрахунку голосів під час позачергових виборів Президента України у 2014 році була створена Єдина інформаційно-аналітична система «ВИБОРИ» (ЄІАС).

Топологічна структура центрального ядра ЄІАС інформаційної мережі Центральної виборчої комісії (ЦВК) представлена на малюнку 1.

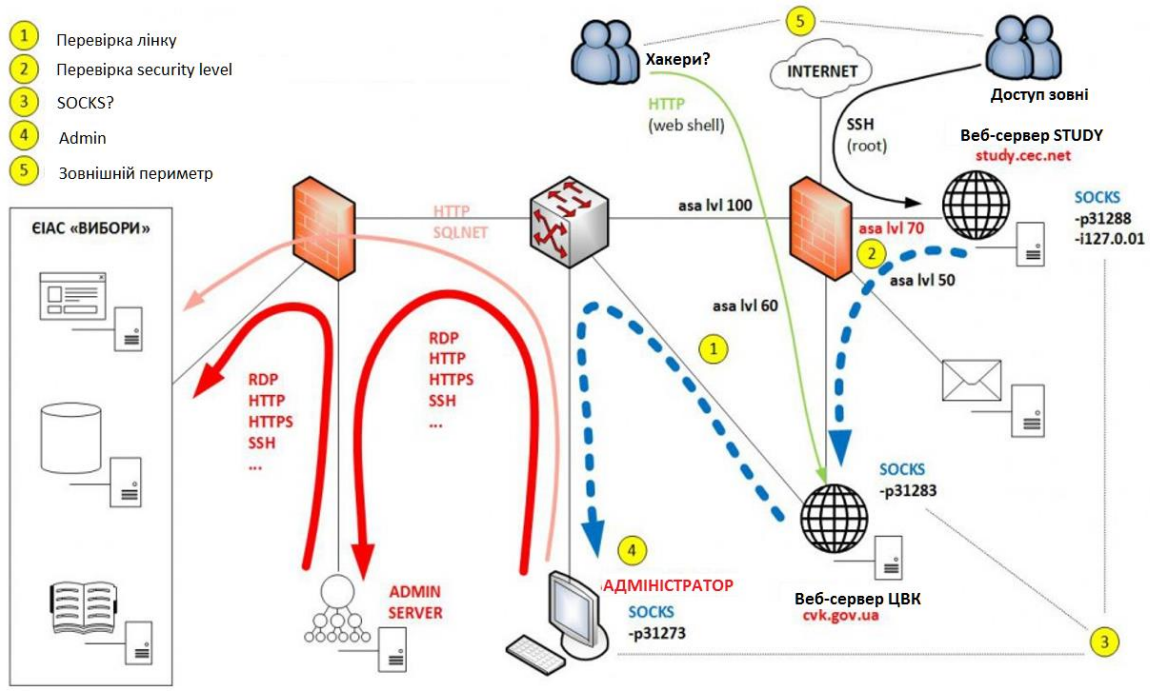

Рис. 1. Топологічна структура центрального ядра ЄІАС інформаційної мережі Центральної виборчої комісії (ЦВК)

За детальним аналізом роботи ЄІАС було виявлено наступні етапи підготовки і проведення кібератаки на серверне обладнання ЦВК:

– підготовча фаза, яка розпочалася за 6-9 місяців до дати виборів. За думкою експертів, на даному етапі було зроблено декілька спроб несанкціонованого доступу зловмисників до веб-серверу ЦВК з метою доступу до серверів адміністраторів інформаційно-телекомукаційної мережі ЦВК та здійснювалось постійне сканування веб-сайту ЦВК для інфекціювання шкідливим програмним забезпеченням;

– проактивна фаза, протягом якої на веб-сервері ЦВК невизначеним способом з'являється спеціально розроблене шкідливе програмне забезпечення «Sofacy», яке на момент несанкціонованого доступу не детектувалося відомими антивірусними засобами. Також на веб-сайті ЦВК з'являється веб-шелл – програма, яка призначена для несанкціонованого віддаленого керування веб-сервером. Створення веб-шеллу може рахуватися датою отримання зловмисниками несанкціонованого віддаленого доступу до веб-серверу ЦВК через протокол HTTP;

– фаза втручання в роботу веб-серверів ЦВК, коли зафіксовані спроби вивести з ладу серверне обладнання ЄАІС. Проведення масованих DDoS-атак (типу TCP SYN-flood) на веб-сайт cvk.gov.ua (193.138.87.26). Висвітлення в засобах масової інформації заздалегідь підготовлених неправдивих даних попередніх підрахунків голосів з так званою «картинкою Яроша».

З боку команди реагування на комп'ютерні інциденти Держспецзв'язку (CERT), спеціалістів кіберзахисту підрозділів СБУ та персоналу ЦВК, а також при належній підтримці з боку провайдерів Інтернет, які були залучені до протидії дестабілізації роботи ЦВК, було оперативно вжито адекватних заходів, які сприяли забезпеченню сталої роботи ЄАІС «ВИБОРИ».

Підтвердженням ефективної і коректної роботи ЄІАС став той факт, що кількість підрахованих бюлетенів в електронному вигляді та з «мокрими печатками» співпали з точністю до сотих часток відсотку.

Отже, висновок можна сказати, що складність проведення заходів із кіберзахисту під час позачергових виборів Президента України у 2014 році полягала у використанні зловмисниками методів так званої «гібридної війни», коли активні кібератаки підсилювались масованими «вкиданнями» недостовірної інформації через засоби масової інформації. Проте рівень підготовки фахівців з кіберзахисту та сучасна технологічна платформа дозволили забезпечити сталу роботу ЄІАС, що не дало змоги дискредитувати результати виборів.

Список використаних джерел:

1. Закон україни «Про затвердження Концепції Єдиної інформаційно-аналітичної системи «Вибори» / [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/v0016359-03 (дата звернення 12.03.2019).

УДК 343.541

Демедюк Сергій Васильович
кандидат юридичних наук,
доцент кафедри програмної інженерії та кібербезпеки КНТЕУ,
генерал поліції третього рангу,
начальник Департаменту кіберполіції Національної поліції України
Демедюк Тетяна Сергіївна
кандидат юридичних наук,
доцент кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ, доцент

ПРОТИДІЯ РОЗПОВСЮДЖЕННЮ ДИТЯЧОЇ ПОРНОГРАФІЇ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Україна є одним з лідерів у світі за розповсюдженням дитячої порнографії у мережі Інтернет. Щороку в нашій державі до кримінальної відповідальності за розповсюдження дитячої порнографії притягуються сотні осіб. Стрімкий розвиток інформаційних технологій та комп'ютерної техніки спричинив утворення принципово нових схем вчинення злочинів, пов'язаних з розповсюдженням продукції порнографічного характеру через всесвітню мережу Інтернет, що передбачено статтею 301 Кримінального кодексу України. Особливо суспільно небезпечними проявами таких відносин є втягнення до злочинних діянь у цій сфері неповнолітніх та малолітніх, які стають не тільки знаряддям злочину, а й об'єктом наруги, примушування до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру з розбещенням, зґвалтуванням, застосуванням до них різного роду насильства та сексуальної експлуатації.

Категорія злочинів, пов'язаних з дитячою порнографією, є досить специфічною, тому вимагає принципово нового підходу оперативних працівників та слідчих до їх попередження та розслідування. По-перше, великого значення для доказування обставин набуває технічна інформація, що нетипово для інших видів злочинів. Це вимагає від працівників певного рівня знань у сфері комп'ютерної техніки, засобів комунікації тощо. По-друге, ефективне здійснення оперативно-розшукової та процесуальної діяльності за справами цієї категорії передбачає проведення комплексу заходів, які ще недостатньо поширені в службовій діяльності органів розслідування (оперативна закупівля через мережу Інтернет). По-третє, у багатьох випадках діяльність злочинців виходить за межі України, тому виникає необхідність міжнародного співробітництва.

Департамент кіберполіції співпрацює з Міжнародною оперативною групою по боротьбі з дитячою порнографією ФБР США, можливості якої використовуються при документуванні протиправної діяльності транснаціональних злочинних груп. В Інтерполі створено автоматизовану базу даних зображень дітей, які стали жертвами сексуальної експлуатації в Інтернеті. Інформаційні масиви накопичують

відомості про ідентифікованих та неідентифікованих потерпілих від сексуального насильства і доступна для всіх країн - учасниць Інтерполу.

Ефективна робота оперативних і слідчих підрозділів у протидії злочинам, пов'язаним із виготовленням та розповсюдженням дитячої порнографії у всесвітній комп'ютерній мережі Інтернет вимагає встановлення осіб, причетних до діяльності того чи іншого Інтернет – ресурсу та спостереження за діями цієї особи з одночасним їх документуванням. У ході цієї роботи необхідно встановити:

- кому належить той чи інший сайт або електронна поштова скринька;
- реєстраційні дані (logs) та абонентську інформацію про особу, якій надаються послуги хостінгу, як користувача сайту;
- адресу, телефонні номери та інші реквізити власника сайту;
- IP-адресу, яку використовували для створення та поповнення змісту сайту;
- інформацію щодо змісту сайту та користування ним, тощо.

Кожен комп'ютер у мережі має свою унікальну адресу, яка називається IP-адреса (адреса Інтернет-протоколу). При реєстрації мережі в Інтернет їй виділяється мережний ідентифікатор залежно від класу. Ідентифікація ж вузлів у підмережах мережі здійснюється організацією-власником.

Коли особа підключається до Інтернет-мережі, її комп'ютер стає частиною мережі і йому надається унікальна IP-адреса. Отримання IP-адреси здійснюється при кожному підключенні, але ця адреса кожного разу має нове значення з діапазону динамічних IP-адрес провайдера, через якого здійснюється підключення.

Статичні IP-адреси, як правило, закріплені за тими вузлами мережі Інтернет, що повинні бути присутніми у мережі постійно. Це сервери, призначення яких полягає в тому, щоб обробляти запити користувачів Інтернет.

Хоча комп'ютерна система IP-адресації здається цілком прийнятною у всіх відносинах, для людини форма подачі цієї інформації вважається не зовсім зручною. Коли комп`ютеру дається команда відкрити сторінку, то вводиться URL (адреса Інтернет-ресурсу), це змушує комп`ютер звертатися за довідкою до іншого комп`ютера щоб визначити, яка IP-адреса відповідає введеному доменному імені. Цей "довідковий" комп`ютер називається сервером DNS (Domain Name System), який є службою каталогізації доменних імен. Таблиця відповідності доменних імен IP-адресам розміщається на багатьох DNS – серверах, що послідовно опитуються при пошуку того чи іншого значення.

Щоб довідатися про IP-адресу сайту, доменне ім'я якого відомо (і взагалі довідатися, чи існує така адреса), можна скористатися програмою Ping (Packet Internet or Inter-Network Groper), що входить у комплект Windows.

Отримання інформації про адресу електронної пошти суттєво відрізняється від перевірки відомостей про сайти. Дані щодо Інтернет-сайту отримати легше тому, що для постійного доступу він має статичну адресу та розташований на технічних ресурсах провайдера, які надаються клієнтам за плату. Ця послуга має назву хостінг (англ. „hosting" - хазяйнувати) -

надання провайдером власних технічних ресурсів для розміщення та роботи сайтів.

З метою перевірки адреси електронної пошти, якими користуються зловмисники, доцільно провести моніторинг із використанням пошукових систем і загальнодоступних сервісів. Подальші заходи залежать від поштової служби, якою користується фігурант, оскільки наші можливості обмежені співпрацею з українськими компаніями, наприклад, Ukr.net, Gala.net, TeNet та іншими. Без отримання дозволу суду на проведення заходів, які обмежують права та свободи громадян, можливо отримати наступну інформацію:

1. Адреса, телефонні номери та інші реквізити абонента.

2. IP-адреси, які використовувалися для створення цього облікового запису.

3. IP-адреси, які використовуються для з'єднання з цим обліковим записом.

4. Реєстраційні дані (logs) та абонентська інформація про користувача облікового запису (електронної поштової адреси).

5. Відомості про обліковий запис (електронну поштову адресу), на який пересилається повідомлення після його отримання (робиться операція “Forward”).

У випадку використання правопорушником електронної поштової адреси є велика ймовірність, що на перші два питання відповіді в провайдера не буде або інформація буде неправдивою. Це обумовлено тим, що більшість електронних поштових адрес надаються безкоштовно і користувач майже ніколи не заповнює реквізити. Останні три питання дають інформацію про осіб, які можуть надати додаткову інформацію відносно користувача електронної поштової адреси, якого необхідно встановити, інші електронні поштові адреси, які він може використовувати, та його особисті адреси.

Тут будуть отримані динамічні IP-адреси інших провайдерів, з яких здійснював свою діяльність користувач електронної поштової адреси, тому дуже важливо знати точний час стосовно кожної використаної адреси. Згідно з цією інформацією необхідно за допомогою сервісу Whois установити провайдера, який надавав послугу з використання мережі Інтернет для користувача електронної поштової адреси та направити до нього запит або отримати таку інформацію за допомогою ухвали слідчого судді. Відповідь на це запитання надасть можливість установити фактичну адресу користувача електронної поштової адреси.

Але, якщо електронна поштова адреса створена навмисно для протиправних дій, правопорушник може користуватися нею з Інтернет - клубів (кафе, орендованих квартир, готелів тощо), тому необхідно буде встановити:

1. Комп'ютер у внутрішній локальній мережі клубу (кафе або інше місце), з якого правопорушник здійснював свою діяльність.

2. Який адміністратор закладу був на зміні під час виходу правопорушника до мережі Інтернет.

3. Осіб з числа інших клієнтів, які в той час знаходились поблизу комп'ютера правопорушника.

4. Інший обслуговуючий персонал клубу (кафе, готелю тощо), який міг запам’ятати правопорушника (охоронець, бармен, прибиральниця тощо).

Зазначених осіб необхідно опитати та встановити особу правопорушника.

Зміст електронного листування особи, перелік її контактів або паролі доступу до скриньки можливо отримати виключно за ухвалою слідчого судді і в установленому законом порядку.

Найбільш ефективним способом, який дозоляє отримати первинні дані про вчинення таких злочинів, є систематичний і цілеспрямований моніторинг загальнодоступних інформаційних ресурсів.

У багатьох випадках перед органами розслідування постає задача доказування факту використання конкретного комп’ютера для доступу до інтернет - ресурсів. Така потреба, зокрема, виникає, коли для з’єднання із глобальною мережею використовувалася динамічна IP-адреса, яка могла бути надана необмеженому колу осіб (наприклад, при використанні безпровідного з’єднання Wi-Fi або при підключенні до мережі через засоби стільникового зв’язку тощо). У таких випадках слід відслідкувати MAC-адресу комп’ютера зловмисника. MAC-адреса або фізична адреса комп’ютера – це незмінний ідентифікаційний номер пристрою, за допомогою якого здійснюється з’єднання з мережею.

Слід відзначити, що при вчиненні злочинів зазначеної категорії для зашифровки схеми руху коштів зловмисниками використовуються віртуальні трансферні системи такі як «Webmoney», «E-passport», «Yandex-деньги» та інші. Для цього злочинці відкривають власні Інтернет - гаманці шляхом створення облікових записів у адміністраторів систем. Номер Інтернет-гаманця, як правило, не приховується. Він може міститися в рекламному оголошенні, на сайті Інтернет - крамниці або повідомлятися в ході спілкування з покупцями.

Номер гаманця дозволяє отримати деяку інформацію про його власника і відомості, які в подальшому можна використати в суді як докази діяльності підозрюваного.

Оператор трансферної системи, як правило, має відомості про програмне забезпечення, яким клієнт користується для здійснення операцій по гаманцям. Такі клієнтські програми є специфічними та можуть завантажуватися на комп’ютер користувача з сайтів оператора. Відповідна інформація також може бути надана оператором за запитом і матиме доказове значення після вилучення комп’ютерної техніки, яка використовувалася для вчинення злочину, та проведення комп’ютерно - технічної експертизи.

Отримана інформація у подальшому дозволить з’ясувати додаткові відомості про фігуранта: встановити його особу та місце проживання, номер мобільного телефону, комп’ютер, який використовується для з’єднання з мережею Інтернет. У деяких випадках для підтвердження сертифікатів представники трансферних систем вимагають від клієнтів надання копій документів, які підтверджують особу (найчастіше - паспорту), отже є вірогідність отримання за запитом повних паспортних даних власника Інтернет-гаманця.

Як уже зазначалося, відомості про осіб, які представляють оперативний інтерес, можливо отримати шляхом елементарного використання пошукових систем. У поле пошуку рекомендується вводити будь-які ідентифікуючі дані об'єкта: номери телефонів, гаманців, облікових записів інтернет-пейджерів, електронні та поштові адреси, прізвища або вигадані для спілкування в мережі імена, назви суб'єктів підприємницької діяльності тощо.

Серед Інтернет - ресурсів, на яких може міститися інформація, що становить оперативний інтерес, слід визначити такі: сайти, які відкрито пропонують послуги сексуального характеру за гроші або роблять це завуальовано: під виглядом масажних салонів, VIP-відпочинку, ескорт – послуг тощо; веб - сторінки з дошками оголошень незалежно від спеціалізації («куплю», «продам», «пропоную роботу» і т.д.) або регіональної спрямованості; форуми різноманітної тематики; соціальні мережі; сайти знайомств, на яких розміщуються анкети користувачів.

Щоб закріпити процесуальне значення інформації, здобутої під час проведення розшукових заходів, необхідно належним чином оформити документи про отримання та фіксацію інформації. За наявності відкритого доступу до змісту сайту, слід оформити протокол огляду в присутності понятих із застосуванням відеозапису або програм, які фіксують зображення, що виводиться на екран. У разі використання програм «SnagIt», «Camtasia» отримані відомості необхідно записати на оптичний носій без можливості перезапису (CD-R) та долучити диск до протоколу в якості додатку.

Отже, для протидії розповсюдженню дитячої порнографії, вчиненого із застосуванням інформаційних технологій, потрібно ідентифікувати комп'ютер, в якому зберігається і з якого розповсюджується продукт дитячої порнографії. В подальшому встановити осіб, які зберігають, адмініструють та розповсюджують ресурси, на яких розміщується контент з дитячою порнографією.

Список використаних джерел:

1. Кримінальний кодекс України : від 05.04.2001 зі змінами станом на 14.03.2018: [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua. – Назва з екрана.

2. Кібербезпека дітей в інтернеті: Про що мають дбати батьки, школа: [Електронний ресурс]. – Режим доступу: *womo.ua/kiberbezpeka-ditey-batki-shkola-derzhava – Назва з екрана.*

3. Конвенція Ради Європи про кіберзлочинність / Ратифіковано із застереженнями і заявами Законом України від 7 вересня 2005 року №2824-IV // Відомості Верховної Ради України. – 2006 р. – №5-6. – Ст. 71.

4. Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії : закон України від 03.04.2003 № 716-IV (716-15) [Електронний ресурс] : Законодавство України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_b09. – *Назва з екрана.*

УДК 004.056.57: 004.492

Говорущенко Тетяна Олександрівна
доктор технічних наук, доцент,
завідувач кафедри комп'ютерної інженерії та системного програмування
Хмельницький національний університет
Савенко Олег Станіславович
кандидат технічних наук, професор,
декан факультету програмування та комп'ютерних і телекомунікаційних систем
Хмельницький національний університет
Лисенко Сергій Миколайович
кандидат технічних наук, доцент,
доцент кафедри комп'ютерної інженерії та системного програмування
Хмельницький національний університет

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ В УМОВАХ ІННОВАЦІЙНОГО РОЗВИТКУ УКРАЇНИ

На сучасному етапі економічного розвитку України, коли управління інформацією стає функцією, критично важливою для бізнесу, а обсяги інформації невпинно зростають, все гостріше стоїть питання інформаційної безпеки.

На сьогодні триває кібер-війна України з Росією, під час якої Україна перетворилась на тестовий полігон для російських хакерів. Щомісяця Україна піддається кібератакам 3000-3500 разів. За останні 12 місяців кожна друга промислова компанія в світі пережила від одного до п'яти кібер-інцидентів [1]. Втрати світової економіки в результаті кібер-атак становлять 445000000000 USD. Збитки українського бізнесу, завдані кібер-атаками, складають 25000000 USD [2].

Домінуючою загрозою для промислових та критично важливих інфраструктур на сьогодні стало шкідливе програмне забезпечення (ШПЗ) – 53% кібер-інцидентів пов'язані з ШПЗ, причому біля 36% компаній піддавались таргетованим атакам [1].

Якщо підприємство працює з даними фізичних осіб, то кібер-атаки та крадіжка інформації – це фактори ризику, які завдають підприємству репутаційних та фінансових збитків. При цьому 64% підприємств не використовують спеціальних програм збору та аналізу інформації про кібер-загрози, обмежуються несистемними заходами в цій галузі. 86% підприємств визнають, що їх політика кібербезпеки не відповідає повною мірою потребам організації [1]. Основними причинами, які перешкоджають підвищенню кібербезпеки підприємств, є: недостатнє фінансування; нестача або відсутність кваліфікованих кадрів; нестача розуміння або підтримки з боку керівництва організації.

Отже, наразі *актуальною проблемою* при використанні комп'ютерних систем (КС) є надійний захист інформації від кібер-загроз і ШПЗ.

Відомі на сьогодні методи та системи [3, 4] виявлення кібер-загроз та шкідливого ПЗ неспроможні здійснювати достовірний та ефективний захист КС через недосконаліть методів, покладених в їх основу, та зростання кількості нових кібер-загроз та шкідливого ПЗ (кожні 4 секунди в світі з'являється нове, невідоме шкідливе ПЗ). Сучасні антивірусні засоби виявляють лише 46% ШПЗ.

Для підвищення достовірності виявлення кібер-загроз та ШПЗ в комп'ютерних системах було розроблено інтелектуальну систему виявлення кібер-загроз та шкідливого ПЗ, яка складається з:

– підсистеми діагностування КС на наявність троянських програм;

– підсистеми виявлення бот-мереж на основі аналізу DNS-трафіка;

Розроблена інтелектуальна система виявлення кібер-загроз та шкідливого ПЗ надає наступні переваги:

– підвищує достовірність та ефективність виявлення кібер-загроз та ШПЗ, зменшуючи рівень хибних спрацювань та обчислювальну складність процесу виявлення;

– підвищує ефективність діагностування комп'ютерних систем на наявність нових троянських програм;

– підвищує достовірність виявлення ботів відомих та невідомих бот-мереж на 8-22% в порівнянні з відомими засобами виявлення бот-мереж;

– підвищує достовірність виявлення метаморфних вірусів на 7-14%.

Розроблена інтелектуальна система може бути використана в державних установах, військових формуваннях та правоохоронних органах (зокрема, в кіберполіції), оскільки вона спрямована на забезпечення національної безпеки України в частині підвищення її кібербезпеки. При використанні в комерційних організаціях представлена система дозволяє захистити КС підприємства від кібер-загроз та шкідливого ПЗ.

Список використаних джерел:

1. Киберпреступность в мире. Состояние киберпреступности в различнх регионах мира // [Электронный ресурс]: [Веб-сайт]. – Электронные данные. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Киберпреступность_в_мире (дата обращения 21.02.2019) – Название с экрана.

2. Кибер-страхование. Современный способ защиты в эпоху технологий. // [Электронный ресурс]: [Веб-сайт]. – Электронные данные. – Режим доступа: https://13.uisgcon.org/pdf/uisgcon13-olexandra-gladyshevska+cyber-insurance.pdf (дата обращения 21.02.2019) – Название с экрана.

3. Moldavskaya A.V. Method of learning malware behavior scripts by sequential pattern mining / A.V.Moldavskaya, V.M.Ruvinskaya, E.L. Berkovich // Lecture Notes in Computer Science. – 2016. – Vol. 9653. – Pp. 196-207.

4. Komar M. Intelligent Cyber Defense System Using Artifficial Neural Network and Immune System Techniques / M. Komar, A. Sachenko, S. Bezobrazov, V. Golovko // Communications in Computer and Information Science. – 2017. – Vol. 783. – Pp. 36-55.

УДК 342.9

Шведова Ганна Леонідівна
кандидат юридичних наук, доцент,
доцент кафедри загальноправових дисциплін,
Київський національний торговельно-економічний університет

КОРУПЦІЯ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Реформування системи забезпечення кібербезпеки сьогодні стало одним із найактуальніших питань в Україні. З огляду динаміки соціальних, економічних, політичних процесів, що відбуваються у світі, сучасна українська держава опинилась в умовах, у яких питанням захисту об'єктів критичної інфраструктури має приділятися більш пильна увага. Як зазначають експерти, корупція та некомпетентність у сфері регулювання галузі інформаційної безпеки та кібербезпеки набувають в Україні критичних форм [1].

Виходячи з того, що до об'єктів критичної інфраструктури (далі - КІ) закон відносить підприємства, діяльність яких безпосередньо пов'язана з технологічними процесами, що мають велике значення для економіки, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, можна зробити висновок, що процеси, які тривають в кіберпросторі, пов'язані з безпекою цих об'єктів [2].

В зв'язку з цим слід звернути увагу на думку професора З. С. Варналія, який найнебезпечнішою інституціональною загрозою національній безпеці України вважає корупцію. Особливості корупції в Україні, на думку професора, полягають в тому, що вона не протистоїть формальній економіці, а існує в ній, слугуючи закономірним наслідком легальних статусів господарюючих суб'єктів, в тому числі об'єктів КІ. В свою чергу це створює додаткові умови для зловживань в сфері інформаційної безпеки таких структур. А корупційні відносини ґрунтуються на можливості використати будь-яке суспільне благо для тіньового обороту у власних інтересах [3, с. 60].

Слушним є зауваження Філіпа Ціммермана, творця першого програмного забезпечення для шліфування електронної пошти про те, в останні роки кібербезпека набула більшої ваги через геополітичні міркування. На думку Ф. Ціммермана, лише вмотивовані інженери, націлені на захист країни від кібернападів, сприятимуть створенню в Україні європейського центру компетенції в галузі кібербезпеки [4]. Але тут виникає ряд перешкод: нестача фінансування, інституційного забезпечення, відтік кадрів. Щодо останнього елементу - тут можна погодитись з тим, що корупція стає головною перепоною до формування інтелектуального потенціалу у боротьбі з кіберзлочинністю. Адже виховання патріотизму, відданості своїй державі зустрічає перешкоди в країнах, що розвиваються і паралізовані корупцією.

Цинізм, що виховує корупція, заважає застосуванню фахівцями навичок кібербезпеки саме в своїй країні [4].

Постійний представник МВФ в Україні Й. Монглан оцінює втрати від корупції в 2% ВВП, про що він повідомив на Ukrainian Investment Forum 03.11.2017 р. Масштаби поширення корупції залишаються найбільшою загрозою для кібербезпеки України.

Окрім цього, справедливим є висновок про те, що сучасна криміногенна ситуація в Україні – якісно новий феномен, як за обсягами злочинних виявів, так і за ступенем їх руйнівного впливу на життєдіяльність суспільства, об'єкти критичної інфраструктури, адже протягом останніх років відбулась трансформація організованої злочинності в нашій країні, використовуються нові інформаційні засоби для здійснення протиправної діяльності [5, с. 159].

З іншого боку, кібербезпека як належний стан захищеності життєво важливих інтересів суспільства в кіберпросторі, може стати дієвим інструментом у виявленні та попередженні корупційних правопорушень.

Отже, кожна держава визначає свій перелік об'єктів критичної інформаційної інфраструктури, в тому числі зважаючи на критичність окремих секторів та важливість певних послуг для держави та безпеки її суспільства, та виявляє свої потенційні загрози для таких об'єктів. Доведено, що для нашої держави серед інших небезпек корупційні ризики створюють найсерйознішу загрозу стабільній і безпечній діяльності багатьох об'єктів критичної інфраструктури.

Список використаних джерел:

1. Кібербезпека: коли від чиновницького проекту за кілометр тхне корупцією // Офіційний веб-портал Укрінформ [Електронний ресурс]. - Режим доступу: https://www.ukrinform.ua/rubric-technology/2507505-kiberbezpeka-koli-vid-cinovnickogo-proektu-za-kilometr-thne-korupcieu.html (дата звернення: 05.03.2019)

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року // Офіційний веб-портал Верховної Ради України [Електронний ресурс]. - Режим доступу: http://zakon5.rada.gov.ua/laws/show/2163-19 (дата звернення: 04.03.2019)

3. Варналій З. С. Корупція як інституціональна загроза національній безпеці України // Реалізація державної антикорупційної політики в міжнародному вимірі [Текст]. – Матеріали ІІ міжнар. наук.-практ. конф. (Київ, 8 груд. 2017 р.) // [Редкол. В. В. Чернєй, В. В. Гусарєв, С. С. Чернявський та ін.]. - Київ : Нац. акад. внутр. справ, - 2017. – С. 59-63

4. Не до жартів. Україна може стати європейським центром з кібербезпеки // Офіційний веб-портал Економічної правди [Електронний ресурс]. - Режим доступу: https://www.epravda.com.ua/publications/2017/10/3/629730/ (дата звернення: 05.03.2019)

5. Катеринчук І. П. вступне слово / І.П. Катеринчук // Кримінальна розвідка: методологія, законодавство, зарубіжний досвід і матеріалами Міжнар. наук.-практ. конф., Одеса, 29 квітн. 2016 р.). – Одеса: ОДУВС, 2016. – 184 с.

УДК 004.056.53

Біленький Андрій Леонідович
викладач
Гусятинський коледж Тернопільського національного технічного університету імені Івана Пулюя

ЦИФРОВА БЕЗПЕКА РОЗУМНОГО МІСТА

Smart city (розумне місто) – це місто, яке об’єднує сучасні методи керування процесами комплексного функціонування міста, метою яких є покращення рівня життя пересічних громадян. Збільшення міського населення призводить до необхідності використання сучасних підходів управління, використання новітніх інформаційних технологій – платформ та методів для інтелектуального розвитку міста, але є і зворотна сторона такого розвитку.

З точки зору мешканців міста, переваги Smart city полягають в ефективному управлінні послугами житлово-комунального господарства, швидкому реагуванні на екстрені виклики, покращенню екологічних показників тощо. Водночас самі громадяни стурбовані тим, чи забезпечений належний рівень захисту їхніх персональних даних, які передаються по відкритих каналах зв’язку, особливо безпровідними мережами.

Процес організації інформаційної безпеки міста є складним, оскільки передбачає високу взаємопов’язаність таких складових, як: дані, технології, додатки та інфраструктура.

Міська інфраструктура, наприклад, постачання електроенергії, води, управління світлофорами, та інші, стикаються з багатьма кіберзагрозами, в тому числі:

– системи відеоспостереження: у багатьох великих містах встановлені приватні та публічні камери відеоспостереження, звернення до яких здійснюється за допомогою імені користувача та паролю. Наявність доступу до них призводить до ймовірних порушень конфіденційності приватного життя або шпигунських дій зі сторони іноземних держав чи організацій.

– мережі зв’язку: комп’ютерний зв'язок і системи обміну інформацією між державними структурами, бізнесом чи мешканцями розумного міста здійснюється за допомогою таких комунікаційних технологій, як WiFi, 4G, RFID, GSM, кожна з яких має певні проблеми безпеки, які необхідно враховувати під час їх впровадження;

– системи управління транспортом: такі системи стикаються з найбільш критичними проблемами, оскільки вони призводять до катастроф, особливо коли трапляються в системах повітряного руху або в системах управління поїздами. Більше того, вони супроводжуються довготривалими та масштабними заторами, спричиненні, шляхом злому систем керування світлофорами [1].

Інтелектуальні міста мають справу з величезними обсягами даних у режимі реального часу та пов'язаних з ними технологій, тому необхідно

підтримувати захист даних, в тому числі і персональних [2]. Загрози, які стосуються конфіденційності, можна класифікувати наступним чином :

1. Комунікації (людино-машинна та машино-машина взаємодії):

1.1. Витік інформації – несанкціоноване зняття чи доступ до конфіденційної інформації з каналів зв'язку [3].

1.2. Атака на відмову в обслуговуванні (англ. DoS attack) – дестабілізація віддаленої системи, приведення її у неробочий стан ;

1.3. Атака «людина посередині» (англ. Man in the middle) – ситуація, коли криптоаналітик (атакувальник) здатний читати та видозмінювати на свій розсуд повідомлення, якими обмінюються кореспонденти, причому жоден з останніх не може здогадатися про його присутність в каналі;

1.4. Атака сторонніми каналами (англ. side channel attack) – використання будь-якої інформації про фізичні процеси у пристрої, такі як диференційній аналіз енерговикористання .

2. Комерційна діяльність (Банківська сфера, Е-комерція):

2.1. Фíшинг (англ. Phishing) – отримання конфіденційної інформації (паролі, номери банківських карток і т.і.) обманним шляхом [1];

2.2. Підміна (англ. spoofing) – змушення жертви відправляти трафік не легітимному одержувачу безпосередньо, а атакуючому, який потім вже ретранслює трафік далі. При цьому атакуючий отримує можливість модифікації трафіку або, як мінімум, перегляду [4];

2.3. Атака на цілісність даних – спотворення, зміна або знищення даних.

На сьогодні актуальність проблеми кібербезпеки в розумних містах не викликає жодних сумнів. Продумана організація цифрової інфраструктури міста та захисту її елементів спростить і впровадження нових проектів. Але при цьому, їх безпека також повинна бути ретельно спланована, реалізована і протестована. Особливо це важливо, коли мова йде про об'єкти критичної інфраструктури або персональні дані громадян.

Список використаних джерел:

1. Lo'ai AT, Bakheder W, Song H. A mobile cloud computing model using the cloudlet scheme for big data applications. InConnected Health: Applications, Systems and Engineering Technologies (CHASE), 2016 IEEE First International Conference on 2016 Jun 27 (pp. 73-77). IEEE.

2. Ijaz, Sidra, Munam Ali Shah, Abid Khan, and Mansoor Ahmed. "Smart Cities: A Survey on Security Concerns." INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS 7, no. 2 (2016): 612-625.

3. Cédric, LÉVY-BENCHETON, Eleni DARRA, Daniel Bachlechner, Michael Friedewald, Timothy MITCHENER-NISSEN, Monica LAGAZIO, and K. U. N. G. Antonio. "Cyber Security for Smart Cities-an Architecture Model for Public Transport. pdf." (2015).

4. Oliveira LM, Rodrigues JJ, Sousa AF, Lloret J. Denial of service mitigation approach for IPv6- enabled smart object networks. Concurrency and Computation: Practice and Experience. 2013 Jan 1;25(1):129-42

УДК 004.056

Козік Олександр Іванович
викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Гаврилюк Яна Миколаївна
студентка 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

АКТУАЛЬНІСТЬ КІБЕРТЕРОРИЗМУ

Кібертероризм – використання комп'ютерних та телекомунікаційних технологій (насамперед, інтернету) в терористичних цілях. Головну тактику кібертероризму можна охарактеризувати таким чином: кіберзлочин повинен мати досить небезпечні наслідки, стати широко відомим, отримати великий суспільний резонанс і створити атмосферу загрози повторення акту без вказівки конкретного об'єкта. Що стосується природи кібертероризму, то він якісно відрізняється від загальноприйнятого поняття тероризму, зберігаючи лише стержень цього явища і ознаки. Наприклад, акти, спрямовані на залякування з метою досягнення або завдання шкоди комп'ютерним мережам, особливо персональним комп'ютерам, підключеним до Інтернету, за допомогою таких засобів, як комп'ютерні віруси, а також з метою політичних результатів.

Основною формою кібертероризму є інформаційна атака на апаратуру передачі даних, комп'ютерну інформацію, обчислювальні системи та інші складові інформаційної інфраструктури. Така атака дозволяє проникати в систему, що атакується, перехоплювати управління або придушувати кошти мережевого інформаційного обміну, здійснювати інші деструктивні дії. Ефективність форм і методів кібертероризму залежить від особливостей інформаційної інфраструктури і ступеня її захищеності.

За даними соціологічних опитувань на поширення кібертероризму нині активно впливають[1]:

– темпи комп’ютеризації та стрімке збільшення кількості інтернет-користувачів;

– високий потенціал і професійний рівень українських програмістів;

– здатність молодої аудиторії швидко опановувати технічні новинки, про які ще вчора вони не мали жодного уявлення.

До основних чинників, що формують джерела таких загроз, експерти відносять:

– недостатню пропускну здатність і надійність каналів зв’язку, комунікаційного обладнання;

– перехоплення електронної пошти, паролів і файлів за допомогою легкодоступних для зацікавлених користувачів програмно-технічних засобів;

– розширення можливостей для негативного інформаційного впливу на людину, суспільство та державу за допомогою нових комп'ютерно-телекомунікаційних засобів і технологій, що постійно розвиваються.

За таких умов напрямком для керівництва України є організація взаємодії та координації зусиль правоохоронних органів, спецслужб і судових органів, передусім СБ та Служби зовнішньої розвідки України, ДССЗЗІ та МВС України, які мають на меті здійснення заходів із кіберзахисту власної ІТ-інфраструктури, забезпечення безпеки національного інформаційного простору, а також активну протидію внутрішнім і зовнішнім кібернетичним загрозам. З дня на день стає все важче протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем та мереж, а також порушенню функціонування об'єктів нападу (інформації, що циркулює та обробляється в ІТС, баз даних та програмного забезпечення, призначеного для обробки зібраної інформації тощо) на тлі інтенсифікації діяльності кіберзлочинців. Наступні чинники стають на заваді істотного поліпшення ситуації [2]:

- складність організації захисту міжмережної взаємодії;
- відсутність адекватного захисту даних у більшості із сучасних мережевих протоколів;
- наявність помилок у загальному та спеціальному ПЗ, ОС та утилітах, що відкрито розповсюджуються мережею;
- наявність помилок у конфігурації систем і засобів забезпечення безпеки, а іноді й повне ігнорування необхідності їх упровадження.

Даними чинниками пояснюється ефективність кібератак, оскільки деякі напади досягають очікуваного результату. Також надзвичайно актуально вирішення завдань щодо виявлення кібертероризму та запобігання негативним наслідкам. Вирішення проблеми кібертероризму є важливим при міжнародній інформаційній безпеці. Головні кроки, що сприятимуть покращенню кібербезпеки, полягають у вивченні слабких місць прикладних програм, застосуванні крім системного адміністрування систем розпізнавання атак (IDS-технологій) додаткового ПЗ, що дасть змогу відстежувати всі пакети, які проходять через певний мережний інтерфейс, використовувати евристичні механізми захисту та антивірусні програми, аналізувати спеціальні аналітичні додатки із застосуванням мережних лог-файлів та лог-файлів операційних систем.

Список використаних джерел:

1. Ендрю Конрі-Мюррей. Політика безпеки в часи терору. – [Електронний ресурс]. – Режим доступу: http://www.osp.ru/lan/2002/02/083.htm.
2. Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризму. Довідковий посібник. – СПб.: БХВ – Петербург; Арліт 2002. – 496 с.
3. Юрій Травников. Злочини в Паутині: Кордони без замків. − [Електронний ресурс]. – Режим доступу: http://www.pl-computers.ru/article.cfm?Id=742&Page.

УДК 519.7-004.65

Гончар Сергій Феодосійович
кандидат технічних наук, учений секретар
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
Комаров Максим Юрійович
аспірант
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

МЕТОДИКА ОЦІНКИ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Функціонування об'єктів критичної інфраструктури в такому специфічному середовищі, як кіберпростір, пов'язане з уразливістю і загрозами і вимагає розробки нового інструментарію забезпечення стійкості в умовах комп'ютерних атак. Управління стійкістю функціонування об'єктами критичної інфраструктури ґрунтується на знаннях про стан об'єктів управління, стан середовища функціонування і про впливи, які відбуваються. Невід'ємним елементом таких систем управління є низка підсистем підтримки прийняття рішень. Можливості системи управління залежать від здатності підсистеми підтримки прийняття рішень забезпечити особу, що приймає рішення, якісно збалансованою інформацією, яка характеризує реальні і прогнозовані стани об'єктів критичної інфраструктури та запропонувати обґрунтований вибір дій для досягнення мети.

Високий ступінь автоматизації управління і глобалізації інформаційних систем через інформаційно-телекомунікаційні системи загального користування привело до формування глобального інформаційного суспільства і нового середовища його функціонування - кіберпростору, що ставить об'єкти критичної інфраструктури в залежність від степеню захищеності. Кібернетичне протиборство – різновид боротьби, в ході якої здійснюється кібернетичний вплив на апаратно-програмні комплекси автоматизованих систем противника, спрямований на порушення їх нормального функціонування.

Аналіз відкритих джерел, присвячених забезпеченню безпеки об'єктів критичної інфраструктури, надійності і стійкості функціонування автоматизованих систем об'єктів критичної інфраструктури свідчить про те, що в них практично не розглядаються питання, пов'язані з розробкою:

- моделей і методів побудови системи оцінки стану об'єктів критичної інфраструктури;
- науково-методичного апарату побудови автоматизованих систем збору та приведення до єдиного виду інформації, що характеризує стан критичної інфраструктури в умовах деструктивних інформаційних впливів;
- моделей і методів адаптивного управління критичною інфраструктурою, які враховують поточний і прогнозований стан об'єктів критичної інфраструктури в умовах деструктивних інформаційних впливів.

Таким чином, існує нагальна необхідність у розробці заходів щодо забезпечення кіберстійкості об’єктів критичної інфраструктури [1]. Пропонується методика оцінки кіберстійкості об’єктів критичної інфраструктури, що включає в себе наступні етапи:

1. Оцінка кіберстійкості кожного об'єкта критичної інфраструктури:

- оцінка одноланкового об'єкта КІ. Рівень кіберстійкості визначається, як ймовірність виходу з ладу певного елемента в умовах деструктивних інформаційних впливів. Здійснюється оцінка коефіцієнта пов'язаності заданого елемента і його внесок в цільову функцію об'єкта критичної інфраструктури;

- оцінка багатоланкового об'єкта критичної інфраструктури. Рівень кіберстійкості визначається, як ймовірність виходу з ладу певного одноланкового об'єкта критичної інфраструктури в умовах реалізації деструктивних інформаційних впливів. Оцінюється коефіцієнт пов'язаності заданого одноланкового об'єкта критичної інфраструктури та його внесок в цільову функцію багатоланкового об'єкта критичної інфраструктури.

2. Оцінка кіберстійкості взаємодіючих об'єктів критичної інфраструктури.

Рівень кіберстійкості визначається, як ймовірність виходу з ладу певного багатоланкового об'єкта критичної інфраструктури в умовах реалізації деструктивних інформаційних впливів. Оцінюється коефіцієнт пов'язаності заданого багатоланкового об'єкта критичної інфраструктури та його внесок у цільову функцію багатоланкового об'єкта критичної інфраструктури.

3. Оцінка кіберстійкості критичної інфраструктури через суму стійкості її елементів з урахуванням їх коефіцієнта пов'язаності.

Запропонована методика внаслідок декомпозиції критичної інфраструктури на окремі об'єкти з урахуванням коефіцієнтів зв′язаності і ступеня важливості функцій, які виконуються в даний момент, дозволяє здійснити оцінку стану захищеності критичної інфраструктури відповідно до заданого рівня якості. Це дозволяє однозначно дати оцінку стану захищеності критичної інфраструктури від деструктивних інформаційних впливів.

Новизна запропонованої методики полягає в оцінці складних технічних систем, які мають високий ступінь критичності. Практична значимість розробленої методики полягає в можливості її застосування для підвищення ефективності управління КІ, а також для обґрунтування нових методів і засобів протиборства в кіберпросторі. Дану методику можна використовувати при розробці концептуальних рішень при побудові систем захисту інформації об’єктів КІ, а також при плануванні заходів із забезпечення безпеки інформації, що обробляється в спеціалізованих ІТС.

Список використаних джерел:

1. Гончар С.Ф. Методологічні засади розробки та впровадження систем захисту інформації на об’єктах критичної інфраструктури / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. // Спеціальні телекомунікаційні системи та захист інформації. – 2014. - №1(25). С. 158-163.

УДК 004.6

Жирова Тетяна Олександрівна
кандидат педагогічних наук, старший викладач,
старший викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Гамалій Богдан Сергійович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ШЛЯХИ ЗЛОМУ БАЗ ДАНИХ

Нині галузь ІТ, і програмування БД зокрема, продовжують стрімко розвиватися. Проте, з розвитком ІТ, все гостріше стоїть питання безпеки ПЗ та БД, якими оперують ІС. Одна з найбільш актуальних проблеми сучасних баз даних, написаних за допомогою SQL – це SQL-injection.

SQL ін'єкція – один з поширених способів злому сайтів та програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду.

Перед самою атакою зловмисник вивчає поведінку скриптів сервера при маніпуляції вхідними параметрами з метою виявлення їх аномальної поведінки. Маніпуляція відбувається всіма можливими параметрами:

– даними, переданими через методи post і get;

– значеннями (http-cookie);

– http_referer (для скриптів);

– auth_user та auth_password (при використанні аутентифікації).

Як правило, маніпуляція зводиться до підстановки в параметри символу одинарної (рідше подвійний або зворотної) лапки.

Аномальною поведінкою вважається будь-яка поведінка, при якій сторінки, одержувані до і після підстановки лапок, розрізняються (і при цьому немає повідомлення про неправильний формат параметрів).

Найчастіші приклади аномальної поведінки:

– виводиться повідомлення про різні помилки;

– при запиті даних (наприклад, новини або списку продукції), дані про які здійснювався запит не виводяться взагалі, хоча сторінка відображається і т.д.

Слід враховувати, що відомі випадки, коли повідомлення про помилки, в силу специфіки розмітки сторінки, не видно в браузері, хоча і присутні в її HTML-коді.

Впровадження SQL, залежно від типу СУБД та умов впровадження, може дати можливість атакуючому виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів

та виконання довільних команд на сервері. Атака типу впровадження SQL може бути можлива за некоректної обробки вхідних даних, що використовуються в SQL-запитах, поділяється на кілька типів:

1. UNION query SQL injection. Класичний варіант впровадження SQL-коду, коли в уразливий параметр передається вираз, який починається з «UNION ALL SELECT». Ця техніка працює, коли веб-додатки напряму повертають результат вводу команди SELECT на сторінку: з використанням циклу for або схожим способом, так що кожен запис отриманої з БД вибірки послідовно виводиться на сторінку.

2. Error-based SQL injection. Цей спосіб базується на виведенні інформації в тексті помилки виконання запиту. Для цього потрібно прямо виводити текст помилки на саму сторінку. Нажаль цим «грішить» значна частина починаючих розробників.

3. Stacked queries SQL injection. Цей прийом, в основному, використовується для впровадження SQL-команд, відмінних від SELECT, наприклад, для маніпуляції даними (за допомогою INSERT або DELETE). Примітним є те, що техніка потенційно може привести до можливості читання/запису з файлової системи, а також виконанню команд в ОС.

4. Boolean-based blind SQL injection. Реалізація так званої «сліпої ін’єкції»: дані з бази даних у «чистому» вигляді уразливим веб-додатком не повертаються. Цей прийом також іноді називають дедуктивним.

5. Time-based blind SQL injection. Повністю сліпа ін’єкція. Як і в минулому прикладі «гра» проводиться з уразливим параметром. Але до нього додається підзапит, який призводить до паузи роботи DBMS на певну кількість секунд (наприклад, за допомогою команд SLEEP() або BENCHMARK()). Використовуючи цю специфіку, хакер може посимвольно вилучити інформацію з бази даних, порівнюючи час відповіді на оригінальне питання й на запит з впровадженим кодом. Також тут використовується алгоритм бінарного пошуку. Крім того, використовується спеціальний метод верифікації даних, щоб зменшити ймовірність неправильного вилучення символу через нестабільне з’єднання.

Якщо сайт було зламано, то слід врахувати, що використовуючи інформацію в своїх цілях, хакери залишають так звані backdoors – приховані точки входу. Це можуть бути файли з будь-яким розширенням, навіть jpg, але в них буде закодовано php-код для проникнення в систему. В наш час існує багато антивірусів, програм, які сканують файлову систему сайту на предмет підозрілих файлів.

Список використаних джерел:

1. WASC Threat Classification — SQL Injection Entry, by the Web Application Security Consortium (дата звернення 11.03.19р.)
2. «Why SQL Injection Won't Go Away». Stuart Thomas. (дата звернення 11.03.19р.)

УДК 004.77

Пашорін Валерій Іванович
кандидат технічних наук,
професор кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Залевський Богдан Павлович
Студент ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ПРОБЛЕМИ АНОНІМНОСТІ В ІНТЕРНЕТІ

Мережа інтернет без сумнівну прокралася в кожний аспект нашого життя. Правоохоронні органи цивілізованих країн докладають багато зусиль щоб наше користування мережею було якомога безпечнішим а його сегменти дотримувалися законів та правових норма як на рівні однієї країни, так і на рівні міжнародних домовленостей та правових актів. Кожного дня ми перевіряємо пошту, ведемо активну переписку в соціальних мережах, переглядаємо новини чи навіть ведемо власний бізнес. На жаль інтернет не тільки покращує зручність нашого повсякденного життя але і веде за собою низку певних негативних ефектів які багато людей навіть не помічають. Справа у тому що користувачі не помітили як вже самі віддали майже усю свою персональну інформацію, особисті данні та наші уподобання соціальним мережам чи рекламних агентам. Прикладами таких речей можуть бути: фотографії, дані банківських карток та дані банківського акаунта, персональні дані, що дозволяють встановити особистість, дані про акаунти, пов'язані з соціальними мережами та платіжними системами, ділова електронна пошта, історія браузера та інше. Одним із шляхів захисту цих активів є використання такого механізму безпеки існування в кіберпросторі, як анонімність.

Слово «анонімний» використовується в реальному житті для опису ситуацій де ім’я особи невідоме. Прикладом анонімності є таємне голосування (наприклад в Україні наймасштабнішим застосуванням таємного голосування є президентські вибори), таємниця листування та захист свідків.

З одного боку багато хто може стверджувати що «законослухняному громадянину немає чого боятися». З іншого боку такий висновок роблять люди які часто не розуміються на структурі інтернету. Дотримання анонімності важливе не тільки для людей, що бояться правоохоронних органів, але і для звичайного користувача, того ж самого «законослухняного громадянина». Уже давно не секрет що реклама в вікнах браузера відображається на основі наших пошукових запитів. Самі пошукові запити фільтруються як на рівні пошукових систем, так і на рівні провайдерів. Провайдерам чи адміністраторам мережі нічого не заважає продавати бази даних клієнтів інтернет магазинам чи навіть зловмисникам [1].

У 2018 році, Американська газета The New York Times і британське видання The Guardian написали про те, що компанія Cambridge Analytica зібрала і проаналізувала дані 50 млн користувачів Facebook без їхнього відома. Ці дані потім використовувалися для створення програми, здатної оцінювати переваги виборців і впливати на їхній вибір під час голосування [2]. Здавалося б люди самі віддали мережі свою приватну інформацію, чим і допомогли у розробці вищезгаданої програми виборців. Але саме найбільша у світі соціальна мережа змогла допустити витік такої конфіденційної інформації.

Не дивно що хвилюючись за безпеку своїх даних, боячись переслідувань чи виступаючи проти цензурування, люди і починають використовувати різні способи анонімізації та обходу. Найпростішим способом залишатися анонімним є використання численних VPN-сервісів, мереж що створюються поверх інших мереж, які мають менший рівень довіри. Більш захищеними є цілі анонімні мережі Darknet на прикладі Tor (The Onion router), I2P (Invisible Internet Project), Freenet чи GNUnet, використовуючи зазвичай peer-to-peer з'єднання.

Тут ми і маємо негативні наслідки анонімізації. Підключення до даркнету, чи використання інших способів анонімізації, може бути використано як для забезпечення позитивних правових аспектів, як недоторканості приватного життя чи захисту від тоталітарних систем правління, так і для розповсюдження заборонених законом чи авторським правом об'єктів, та більш серйозних кіберзлочинів [3].

Найвідомішим борцем з анонімністю поки залишається Китай. Там забороняють VPN, Tor та інші засоби шифрування і вимагають розкривати свою особистість для будь-якої активності в інтернеті. Також Російський Роскомнадзор вже підтримав ідею заборони анонімайзерів, та намагається призупинити поширення подібної по суті інформації про способи обходу заблокованих сайтів.

Але на жаль ми і досі не маємо остаточних висновків щодо анонімності в мережі, і хоча з одного боку це захищає права людини, з іншого ми і досі майже в більшості випадків безпорадні проти кіберзлочинів пов'язаних з цим.

Як висновок слід зазначити, що розкриття інформації та деанонімізація можуть привести до ряду наслідків: від втручання в приватне життя до навіть загрози самому життю. Рівень приватності та анонімності, який потрібен, прямо пропорційний рівню безпеки.

Список використаних джерел:

1. MIT UA. Анонімність в інтернеті. Стаття від 05.02.2018. URL: https://www.mit-net.com.ua/анонімність-в-інтерн/.
2. New York Times. Facebook Security Breach Exposes Accounts of 50 Million Users. URL: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
3. UA Crypto. Що таке DarkNet і як до нього потрапити. URL: https://uacrypto.top/blog/darknet

УДК 004.49

Жирова Тетяна Олександрівна
кандидат педагогічних наук, старший викладач,
старший викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Маркевич Богдан Степанович
студент 4 курсу 6 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ОГЛЯД СУЧАСНИХ ПРОБЛЕМ КІБЕРЗЛОЧИННОСТІ

Використання Інтернет має низку позитивних переваг та небезпечене використання Інтернету призводить до негативних наслідків. Розвиток глобальних систем призвів до багатократного збільшення кількості користувачів і збільшенню кількості атак на комп'ютери підключені до мережі Інтернет. Тому при підключенні до мережі Інтернет необхідно потурбуватись про забезпечення інформаційної безпеки підключених локальних чи корпоративних мереж.

Через Інтернет порушник може:

– проникнути до внутрішньої мережі підприємства та отримати несанкціонований доступ до конфіденційної інформації;

– незаконно скопіювати важливу і цінну для підприємства інформацію;

– отримати паролі, адреси серверів і навіть їх зміст;

– заходити до інформаційної системи підприємства під іменем користувача, раніше зареєстрованого і т.д.

З допомогою отриманої правопорушниками інформації може бути серйозно підірвана конкурентоспроможність підприємства і довіра клієнтів до нього.

Однією з актуальних тем у сфері кібербезпеки є вдосконалення систем безпеки, що захищають IT-системи від атак з вимогами. У деяких країнах знову з'являються повідомлення про кіберзлочинців з *Ransomware*. Ці віруси поширюються електронною поштою, яка автоматично відправляє себе з заражених облікових записів електронної пошти і розсилає інфіковані електронні листи всім контактам електронної пошти вірусної поштової скриньки**,** інфікованої вірусом. Вірус є дуже небезпечним**,** оскільки після відкриття підробленої електронної пошти вірус встановлюється глибоко в комп'ютер і шифрує доступ до дисків, блокуючи доступ до вмісту дисків.

Аналіз банківських троянів полягає у дослідженні методів кіберзлочинності у сфері зараження інформаційних систем банку, як тих, які є внутрішньобанківськими, так і тих, які обслуговують клієнтів банку як частину інтернет-мобільного банкінгу. Аналіз атак кіберзлочинців, наприклад, популярних в останні роки вірус-троян типу вимагання, який

після шифрування комп’ютерів шифрує дані дисків. Крім того, інші типи троянських коней використовуються для крадіжки конфіденційних даних, особистих клієнтів або розкрадання коштів з банківських рахунків клієнтів, вимагання кредитів тощо.

Після аналізу методів, що використовуються кіберзлочинцями, банки зміцнюють системи безпеки, захищають банківські системи від цих атак, поліпшують безпеку та інструменти авторизації клієнтів онлайн-банкінгу. Крім того, наступним кроком є вдосконалення процесу управління ризиками ІТ-систем. Крім того, атаки на комп’ютерні злочини на електронних банківських системах, ймовірно, набагато більше, ніж надає офіційна статистика, оскільки банки не похвалилися цими подіями, якщо їм не потрібно. Це пояснюється тим, що багато з цих атак на кіберзлочинність є неефективними або мають відносно низькі витрати, а виявлені прогалини в системі електронного банкінгу швидко відновлюються. Однак, якщо клієнти банку знали всі ці події кіберзлочинців, це може знизити рівень довіри до банків. Тоді клієнти банку могли б почати виводити банківські депозити з банків в масовому масштабі, тоді серйозною проблемою для банків з'явилося б пов'язане з різким зростанням рівня ризику ліквідності.

Ще однією з актуальних тем у сфері кібербезпеки є аналіз систем безпеки, розроблених в порталах соціальних медіа. На жаль, незважаючи на запевнення компаній, які працюють на порталах соціальних медіа, інформація, що міститься на цих веб-сайтах, не завжди повністю захищена від діяльності кіберзлочинців. Крім того, для того, щоб обробляти їх для маркетингових цілей, слід додати питання про завантаження даних великих компаній з порталів соціальних медіа. Питання конфіденційності в соціальних мережах є дуже важливим і стосується безпеки особистої інформації. Конфіденційність знаходиться під загрозою з точки зору інформації, розміщеної на порталах соціальних медіа.

Список використаних джерел:

1. Корченко О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О.Г. Корченко, В. Л. Бурячок, С.О. Гнатюк // Безпека інформації. – 2013. – Т. 19, № 1.
2. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О.О. Тихомиров, О.С. Лєнков // Зб. наук. праць Військового ін-ту КНУ ім. Тараса Шевченка. – К.: ВІКНУ, 2011.— Вип. 30.
3. Словник термінів із кібербезпеки / За заг. ред. О.В. Копана, Є.Д. Скулиша — К.: ВБ «Аванпост-Прим», 2012.
4. Масштаби кібератак будуть тільки збільшуватися. – Режим доступу: https://tyzhden.ua/News/192282 (дата звернення 12.03.19р.)
5. Україна готується до «розумних» вірусів та кібератак майбутнього. Режим доступу: https://innovationhouse.org.ua/statti/ukrayna-gotovytsya-k-umnym-vyrusam-y-kyberatakam-budushhego/ (дата звернення 12.03.19р.)

УДК 355/359.07

Криворучко Олена Володимірівна
доктор технічних наук, професор,
завідувач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Опенько Павло Вікторович
кандидат технічних наук, начальник науково-дослідної лабораторії інституту авіації та протиповітряної оборони
Національний університет оборони України імені Івана Черняховського
Опенько Дар'я Павлівна
студентка 4 курсу ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ОГЛЯД СУЧАСНИХ ТЕНДЕНЦІЙ БОРОТЬБИ У КІБЕРПРОСТОРІ

Події кінця XX – початку XXI сторіччя проходять на фоні трансформації суспільства від постіндустріального до інформаційного. В світі відбувається бурхливий розвиток інформаційних технологій та їх проникнення у всі сфери діяльності людини: соціальну, економічну, політичну, воєнну тощо. До основних характерних рис процесу інформатизації суспільства на сучасному етапі відносяться глобалізація та інтенсифікація інформаційних процесів, зміна сучасної картини світу.

Завдяки революції в області інформатизації і комунікацій відбуваються значні зміни у військовій справі. Поширився континуум вимірів, в яких може вестися збройна боротьба – сьогодні можна констатувати, що вона ведеться не тільки в традиційних вимірах "простір – час", але і в "інформаційному вимірі".

У сучасних умовах інформаційна інфраструктура держави набуває статусу критичної (життєво важливої для існування) з усіма від цього похідними: вона стає об'єктом першого удару і потребує для свого захисту збалансованої державної політики в інформаційному просторі. До критичної інформаційної інфраструктури належать, в першу чергу, економіка, транспорт, енергетика, фінансова система, системи управління структур, що забезпечують безпеку та оборону держави тощо. Системи управління, канали зв'язку, системи навігації, розвідки, банківські системи та інші елементи інформаційного середовища потребують захисту від відповідних впливів.

Аналіз подій, що розгортаються в інформаційному просторі розвинутих у воєнному відношенні країн світу, дозволяє відзначити наступні тенденції:

по-перше, глобальна інформатизація військових формувань та створення високоінтегрованих систем управління призводить до глобалізації об'єктів інформаційного впливу, розвитку відповідно до цього форм і способів ведення інформаційного протиборства;

по-друге, наявність великої імовірності майбутніх конфліктів у інформаційному просторі, при чому конфліктів, в яких будуть брати участь

не поодинокі угруповання хакерів, а спеціально створені і призначені для цього державні, насамперед, військові структури та формування;

по-трете, можливість переносу тероризму в площину інформатизації. У силу нерівномірного розвитку інформаційного простору у різних країн деякі держави, імовірно, або окремі терористичні угруповання можуть вдатись до будь-яких заходів для нейтралізації домінування більш розвинутих країн саме через інформаційний простір;

по-четверте, використання світової мережі Інтернет та електронних засобів масового інформування для маніпулювання свідомістю як світової громади, так й населення окремої країни; зміщення і перенос, для цього, центру тяжіння у масовому інформуванні в бік електронних засобів;

по-п’яте, виділення інформаційного забезпечення в самостійний вид стратегічного (оперативного) забезпечення бойових дій і формування відповідних військових структур для здійснення інформаційного протиборства і управління ним.

Таким чином, в умовах сьогодення, коли суспільство практично повністю залежить від застосування інформаційних технологій, полем інформаційної битви стають комп’ютерні мережі, а метою й завданнями – порушення функціонування ключових військових, промислових й адміністративних об’єктів, а також здійснення інформаційно-психологічного впливу на населення та військові формування держави.

Наявність розглянутих тенденцій боротьби в кіберпросторі в умовах ведення інформаційної війни проти України та відсутності цілісної комунікативної політики держави, недостатнього рівня медіа-культури суспільства є вихідними даними для формування державної політики в інформаційному та кіберпросторі, реалізація якої дозволить мінімізувати уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак; негативні наслідки впливу на систему управління безпекою критичної інфраструктури і систем життєзабезпечення, систему охорони державної таємниці та інших видів інформації з обмеженим доступом.

Список використаних джерел:

1. Указ Президента України від 26 травня 2015 року №287/2015 Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України”.
2. Мак-Клар Стюарт, Джоел Скембрей, Джордж Курц. Секреты хакеров. Безопасность сетей – готовые решения, 3-е изд.: Пер. с англ. – М.: Издательский дом “Вильямс”, 2002. – 736 с.
3. Коул Эрик. Руководство по защите от хакеров. :Пер. с англ. – М.: Издательский дом “Вильямс”, 2002. – 640 с.
4. Мак-Клар Стюарт, Шаумил Шах, Шрирай Шах. Хакинг в Web: атаки и защита : Пер. с англ. – М.: Издательский дом “Вильямс”, 2003. – 384 с.
5. Пермяков О.Ю., Сбітнєв А.І. Інформаційні технології і сучасна збройна боротьба. – Луганськ: Знання, 2008. – 204 с.

УДК 004.031.43

Цюцюра Микола Миколайович
кандидат технічних наук,
доцент кафедри інформаційних технологій
Київський національний університет будівництва та архітектури
Мосійчук Євген Володимирович
студент 4 курсу 7 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

КІБЕРБЕЗПЕКА У СФЕРІ ІНТЕРНЕТ-БАНКІНГУ

Фінансові дані – один із найпопулярніших об’єктів атак кіберзлочинців в інформаційному просторі. Найбільш цінні для зловмисників дані, використання яких спрямовані на отримання грошового прибутку, перебувають у розпорядженні фінансових організацій. Через це банківські установи завжди були мішенню для кібернетичних атак на всіх рівнях IT-інфраструктури.

З кожним роком в Україні збільшується кількість кібератак, пов’язаних з отриманням фінансових даних і подальшим використанням їх у власних цілях кіберзлочинців. При цьому близько половини українських банків і платіжних систем (48%) вважає за краще боротися з наслідками кібератак, а не інвестувати кошти у засоби для покращення рівня захисту даних і рахунків своїх клієнтів.

Згідно інформації Національного банку України, найбільш розповсюдженими видами кіберзлочинів в банківській системі України є:

1. Банкоматне шахрайство:

– скіминг – крадіжка даних карти за допомогою спеціального пристрою, що зчитує (скімера);

– використання «білого пластику» для «копіювання» (підробки) платіжної картки та в подальшому зняття готівки в банкоматах;

2. Махінації в торговельно-сервісних мережах:

– «клонування» реквізитів платіжних карток із застосуванням технічних засобів;

– транзакції без проведення авторизації на суму меншу встановленого ліміту;

3. Махінації в онлайн просторі:

– підробка даних платіжних карток;

– здійснення транзакцій, використовуючи викрадені дані платіжних карток;

– написання програмного забезпечення для крадіжки реквізитів платіжних карток (перехоплення трафіку, створення підробних WEB-сайтів, поширення троянських програм та вірусів).

4. Махінації у системах дистанційного банківського обслуговування (надалі – ДБО):

– написання троянських програм та комп'ютерних вірусів для прихованого перехоплення контролю над комп'ютером клієнта з встановленим програмним забезпеченням ДБО;

– отримання платежів через міжнародну систему SWIFT від закордонних відправників внаслідок втручання у роботу комп'ютерів та систем ДБО клієнтів закордонних банківських установ.

У сучасних умовах фінансовим компаніям необхідно використовувати комплекс програмних і апаратних засобів, які б дозволили забезпечити високий рівень захищеності інфраструктури із збереженням достатньої ефективності бізнес-процесів. Для запобігання атакам ефективними є методи соціальної інженерії – це регулярне інструктування всіх співробітників компанії безпечній роботі в інтернет-мережі та інформування їх про існуючі види загроз. Користування послугами сторонніх компаній, які спеціалізуються на захисті даних від DDoS-атак, підключившись до хмарних сервісів організації. Сайтам, яким найбільше загрожують кібератаки, варто піклуватися про рівень захищеності своїх систем. Варто згадати, що найнебезпечніші сайти розроблені на мові PHP, так як 75% з них містять критичні вразливості. Більш захищеними виявилися веб-ресурси на ASP.NET (55%) та Java (70%) (згідно інформації компанії Positive Technologies). Адміністратори корпоративної мережі організації мають контролювати, які веб-сайти їх співробітники відвідують і якими програмними забезпеченнями користуються. Зовнішні ресурси повинні мати дійсні SSL сертифікати.

На даному етапі розвитку сфери інтернет-банкінгу в Україні, системи захисту не досить розвинуті та захищені від кібератак. Для забезпечення уникнення усіляких ризиків, службам безпеки банків необхідно захистити не тільки бази даних і робоче обладнання персоналу, а також і комп'ютерні мережі, термінали працівників фронт-офісу та банкомати від дій кіберзлочинців. Основною ціллю українських спеціалістів з кібербезпеки має стати захист своїх клієнтів, адже зарубіжні конкуренти в XXI столітті задають високу планку у цій сфері.

Список використаних джерел:

1. Карчевський М. В. Комп'ютерна інформація, як предмет злочину в сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку / М. В. Карчевський. // Боротьба зі злочинами у сфері комп'ютерної інформації : проблеми та шляхи їх вирішення. – 2012. – С. 61–64.

2. Чуб О. О. Розвиток Інтернет-банкінгу в глобальному середовищі / О. О. Чуб. // Вісник Української академії банківської справи. – 2009. – С. 62– 67.

3. P. Mell and T. Grance, The NIST definition of cloud computing, National Institute of Standards and Technology, U.S. Department of Commerce, 2014 – 100 с.

УДК 004.05

Жирова Тетяна Олександрівна
кандидат педагогічних наук, старший викладач,
старший викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Королік Марина Олегівна
студентка 3 курсу 1 групи ФОАІС,
напрям підготовки «Економічна кібернетика»
Київський національний торговельно-економічний університет
Ришко Юлія Михайлівна
студентка 3 курсу 1 групи ФОАІС,
напрям підготовки «Економічна кібернетика»
Київський національний торговельно-економічний університет

ТЕСТУВАННЯ БЕЗПЕКИ WEB-ПРОГРАМ

Число компаній, які застосовують веб-технології для підвищення продуктивності роботи і залучення нових клієнтів, зростає з кожним роком. Безсумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберзагроз. Так, компанія Symantec в своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зломі веб-сайтів зазвичай використовують вразливості веб-додатків, що працюють на сервері або експлуатують деякі вразливості операційної системи, на якій працюють ці додатки. Наприклад, за допомогою атак типу XSS хакер може перенаправити запити користувачів на шкідливі веб-сторінки, а за допомогою SQL-ін'єкцій – витягувати з баз даних сайту різну конфіденційну інформацію. Тому тестування безпеки потрібне для додатків найрізноманітніших сфер застосування. Це можуть бути звичайні веб– додатки; додатки з важливою комерційною або персональною інформацією, що підлягає захисту; різні платіжні системи, де ризик втрати інформації може оцінюватися в значні суми; додатки з підвищеними вимогами до цілісності; а також популярні і широко використовувані зараз соціальні мережі.

На сьогодні найбільш поширеними видами вразливості в безпеці програмного забезпечення є такі. XSS (Cross-Site Scripting) - це вид вразливості програмного забезпечення (Web додатків), при якій, на генерованій сервером сторінці, виконуються шкідливі скрипти, з метою атаки клієнта. XSRF / CSRF (Request Forgery) - це вид вразливості, що дозволяє використовувати недоліки HTTP протоколу, при цьому зловмисники працюють за такою схемою: посилання на шкідливий сайт встановлюється на сторінці, що користується довірою у користувача, при переході за шкідливим посиланням виконується скрипт, який зберігає особисті дані користувача (паролі, платіжні дані і т.д.), або відправляє СПАМ повідомлення від особи користувача, або змінює доступ до облікового запису користувача, для отримання повного контролю над нею. Code injections (SQL, PHP, ASP і т.д.) -

це вид вразливості, при якому стає можливо здійснити запуск виконуваного коду з метою отримання доступу до системних ресурсів, несанкціонованого доступу до даних або виведення системи з ладу. Server-Side Includes (SSI) Injection - це вид вразливості, що використовує вставку серверних команд в HTML код або запуск їх безпосередньо з сервера. Authorization Bypass - це вид вразливості, при якому можливо отримати несанкціонований доступ до облікового запису або документам іншого користувача.

У загальному випадку, тестування – це процес перевірки заявлених до продукту вимог і реально реалізованої функціональності, який здійснюється шляхом спостереження за його роботою в штучно створених ситуаціях, на обмеженому наборі тестів, обраних певним чином. Тому тестування безпеки, як і будь-який інший вид тестування, проводиться на основі поставлених вимог.

Основними методами тестування безпеки є:

1. Code review – перегляд вихідного коду програми. Як правило, перегляд виконується кваліфікованим розробником. Тестувальник , у свою чергу, може використовувати утиліти для статичного і динамічного аналізу: RATS, cppcheck та ін.. Даний метод дозволяє виявити уразливості в коді ще на етапі реалізації проекту.

2. Fuzz – тестування – це ще один метод тестування безпеки. Суть даного методу тестування полягає в тому, що на вхід програми подаються свідомо невірні, непередбачені або випадкові дані. Таким чином, ми вивчаємо поведінку програми при використанні самих різних вхідних даних. При застосуванні фаззінга – тестування можна виявити помилки обробки вхідних даних, витоку пам’яті, невірні коди помилок. Існує ряд програмних засобів для проведення фаззінга тестування – Skyfish, SPIKE Proxy, OWASP WSFuzzer (Soap).

3. Тестування на проникнення (penetration testing). Даний метод дозволяє проводити тестування, взаємодіючи з додатком виключно з користувацької сторони. Тестувальник може використовувати як автоматичні сканери безпеки, такі як skipfish або wapiti, так і аналізатори мережі. Важливим аспектом при тестуванні на проникненні є ручне (дослідне) тестування – адже програмні засоби не завжди можуть виявити всі уразливості в безпеці.

Безумовно, провівши повний цикл тестування безпеки, не можна бути на 100% впевненим, що система є абсолютно безпечною. Однак те , що відсоток несанкціонованих проникнень, крадіжок інформації і втрат даних буде в рази меншим, ніж у тих хто не проводив тестування безпеки, гарантовано.

Список використаних джерел:

1. Whittaker, James A. How to Break Web Software: Functional and Security Testing of Web Applications and Web Services / James Whittaker & Mike Andrews − Addison-Wesley Professional, 2006.
2. Whittaker, James A. How to Break Software Security / James Whittaker & Hugh Thompson − Addison-Wesley, 2003.

УДК 004

Цюцюра Микола Ігорович
кандидат технічних наук,
доцент кафедри інформаційних технологій
Київський національний університет будівництва і архітектури
Моспан Олександр Вікторович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЇЇ ЗАБЕЗПЕЧЕННЯ У СОЦІАЛЬНИХ МЕРЕЖАХ

Життя сучасних людей в еру інформаційного суспільства не можна уявити без Інтернету. Сьогодні – це частина нашого повсякденного життя. Це одночасно середовище для розваг, спілкування та навчання. За допомогою Інтернету стало можливим робити покупки та оплачувати послуги [1].

Також, для багатьох людей – це спосіб заробітку. Проте найбільшою цінністю в мережі є сама інформація. Великою перевагою Інтернету можна назвати його всеохопність, тобто об’єднання людей і ресурсів [2].

Досить тісним є зв'язок Інтернету з освітнім процесом. Інформація, яка необхідна людині, що навчається, може міститись не тільки у підручниках, збірниках, журналах, а й у електронному вигляді в мережі.

Часто Інтернет використовують для спілкування в соціальних мережах. Соціальні мережі все глибше проникають у життя користувачів. Але поряд з перевагами віртуального спілкування є небезпека заволодіння приватною інформацією зловмисниками для використання її в неправомірних цілях.

Мета даної роботи - розглянути всі можливі небезпеки у соціальних мережах та шляхи їх подолання. Спеціалісти у галузі кібербезпеки виділяють найбільш типові загрози, серед яких: маніпуляція, ЗПЗ (зловмисне програмне забезпечення), мережеві та комп’ютерні атаки, дезінформування, фармінг, фішинг тощо. Зловмисники використовують всі види обману для отримання доступу до особистої інформації користувача мережі та її використання. Однією з яких є фішинг.

Фішинг – це схема, за якої хакери змушують користувачів передавати конфіденційну інформацію. Цей вид шахрайства заснований на довірі та заволодінні злочинцем аккаунтом іншого користувача. Він зазвичай передбачає надсилання користувачу соціальної мережі повідомлення, яке ніби походить із довіреного джерела, наприклад від знайомого з проханням позичити електронних грошей, скачати контент або перейти за посиланням. Людина не може точно знати, хто відправив їй повідомлення – друг чи шахрай, який заволодів його сторінкою, і, як правило, вона, не замислюючись про це, виконує прохання.

Досить поширеним явищем у мережі є випадки, коли у повідомленні може бути посилання на віруси, черв'яки, троянські програми Ці небезпечні програми створені для зараження комп'ютера з метою його пошкодження, викрадення особистої інформації, шпигунства чи показу реклами.

Найбільш простий спосіб захистити свій комп'ютер від мережевих атак - встановити на нього та належним чином налаштувати антивірусне програмне забезпечення та міжмережевий екран.

Фармінг – це перенаправлення жертви за помилковою адресою, наприклад це імітація сторінки авторизації в соціальну мережу з метою заволодіння логіном та паролем від облікового запису. Аби не потрапити у цю пастку необхідно уважно дивитися, за якими посиланнями та сторінками здійснюється перехід та використовувати механізм двофакторної аутентифікації в соцмережі.

Отже, для захисту від загроз необхідно мати на увазі наступне:

– Потрібно реєструватися тільки в тих соцмережах, які викликають довіру та пропонують надійні механізми аутентифікації і розмежування доступу до особистої інформації користувача.

– Слід пам'ятати, що будь-яка інформація, розміщена в Інтернеті, з великою імовірністю залишається там назавжди, навіть в разі її видалення автором, адже може бути збережена або поширена іншими користувачами.

– Особливу увагу слід приділяти посиланням, які надходять від інших користувачів – вони можуть бути частиною фішингової чи фармінгової атаки.

В роботі проведений аналіз найбільш поширених загроз для користувачів соціальних мереж.

Якщо дотримуватися рекомендацій щодо поведінки у мережі Інтернет, можна зменшити ймовірність потрапити до пастки зловмисників та втратити конфіденційну інформацію.

Список використаних джерел:

1. Управління боротьби з кіберзлочинністю // Міністерство внутрішніх справ України [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/ publish/article/544754

2. Про Доктрину інформаційної безпеки України : Указ Президента України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009

3. Gladius Partners with Remme to Tackle Enterprise Cybersecurity. [Електронний ресурс]. URL: https://medium.com/gladius-blog/gladius-partners-with-remme-to-tackle-enterprise-cybersecurity-b1d12c288fa6

4. Закон України «Про основні засади забезпечення кібербезпеки України». Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата відклику 17.03.19)

5. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

УДК 351

Олексюк Лілія Віталіївна
кандидат наук з державного управління, старший викладач,
старший викладач кафедри публічного управління та адміністрування
Київський національний торгово-економічний університет

КІБЕРГІГІЄНА ОСОБИ – ОСНОВА КІБЕРБЕЗПЕКИ УКРАЇНИ

Останнім часом діти отримують доступ до смартфонів та інших електронних пристроїв раніше, ніж навчаються ходити і говорити. Важко уявити сім'ю, у якої відсутній хоча б один пристрій із доступом до мережі Інтернет. За різними оцінками (Державної служби статистики України, Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, Інтернет-асоціації), абонентами мережі Інтернет в Україні є від 19 до 24 млн. осіб. Кількість абонентів мережі Інтернет, що не досягли повноліття, за офіційною статистикою встановити неможливо, оскільки жодним державним органом такі дані не збираються і не обробляються. Масштаб проблеми можна визначити тільки методом апроксимації - якщо близько 70 % сімей мають доступ до мережі Інтернет, а за офіційною статистикою в Україні близько 6,5 млн сімей з дітьми[0] , то до мережі Інтернет мають доступ близько 4,5 млн. дітей. Усне опитування, проведене автором у приватному навчальному закладі Київській філії Міжнародної Комп'ютерної Академії «ШАГ» у 2016 році, серед дітей віком від 7 до 15 років, показало повну відсутність знань і вмінь цифрової гігієні при майже 100% реєстрації та використанні для спілкування дітьми хоча б однієї соціальної мережі. При цьому ці діти є мешканцями Києва чи приміських населених пунктів, мають повний необмежений доступ до мережі Інтернет і навчаються у кращих школах Києва, інформатика у яких у більшості була з 1 класу. Огляд підручників з інформатики [0], розміщених у вільному доступі, показав, що тематиці Інтернет приділяється 1 чи 2 теми за весь курс.

Не набагато краща ситуація із дорослим населенням, яке не знає своїх цифрових прав, обов'язків і часто самі сприяють проведенню шахрайських дій у цифровому середовищі. Досвід проведення семінарських і лекційних занять із теми доступу до публічної інформації та цифрової економіки, доводить необхідність проведення широкої роз'яснювальної кампанії серед дорослих і дітей з питання захисту власних даних, заходів із інформаційної та кібербезпеки. Якщо знання і навички щодо особистої гігієни, санітарних норм тощо дорослі здатні передати дітям, оскільки мають самі ці навички, то навички цифрової гігієни необхідно набувати одночасно і дорослим, і дітям (довідково – мережа Інтернет у такому вигляді, як ми її зараз бачимо, існує в Україні лише із 1995 року, отже навички щодо поведінки і мережі може передавати обмежена кількість осіб).

Статистика свідчить, що у 2016 році кіберзлочини зайняли 2 місце з усіх зареєстрованих злочинів в світі. В Україні кількість зареєстрованих злочинів, що можуть кваліфікуватись як кіберзлочини, за даними

Національної поліції щорічно збільшується на 2,5 тисячі. За 2017 рік хакери викрали понад 16,7 млрд. дол. США по всьому світу. Крім того, персональні дані щонайменше 40 млн. людей були викрадені різними угрупуваннями. Тому питання кібербезпеки людини є надзвичайно актуальним на сьогодні.

Ситуація ускладнена тим, що загального визначення кіберзлочинів не існує ні в національному законодавстві, ні в міжнародному. Це призводить до відсутності єдиного підходу до визначення підстав віднесення протиправних діянь до таких злочинів, розробки спільних заходів щодо їх ліквідації та розробки превентивних заходів.

Європейське законодавство за останні п’ять років посилило відповідальність стосовно обробки персональних даних та захисту конфіденційності у різних сферах [0, 0]. Україна поки що розробляє тільки проекти таких документів.

Аналіз діючих стратегічних документів держави та проектів, що розробляються [0, 0], а саме відсутність в них заходів і відповідальних органів за реалізацію політики у сфері цифрової економіки, розвитку цифрових навичок і цифрової гігієни, доводить необхідність розробки окремої стратегії із розвитку цифрових навичок населення та плану її реалізації якнайшвидше. Інакше відставання населення у даному питанні призведе до відставання країни, яке надолужити буде вкрай важко. Цифровий розрив сьогодні приводить до іншого поділу країн на рівні, що в цілому негативно позначиться місці України у світі і призведе до неможливості потрапити із третього світу у перший.

Список використаних джерел:

1. Сім'я та демографічна політика http://www.sport.gov.ua/index/ua/material/44
2. ЕЛЕКТРОННІ ПІДРУЧНИКИ [Електронний ресурс].– Режим доступу: https://mon.gov.ua/ua/osvita/zagalna-serednya-osvita/pidruchniki/elektronni-pidruchniki/elektronni-pidruchniki-dlya-2-klasu/pidruchniki-dlya-2-klasu-shkil-z-ukrayinskoyu-movoyu-navchannya
3. Regulations Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
4. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс].– Режим доступу: http://zakon3.rada.gov.ua/laws/show/96/2016
5. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки [Електронний ресурс].– Режим доступу:https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80
6. Proposal for a Regulation on Privacy and Electronic Communications [Електронний ресурс] – Режим доступу: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

УДК 374.73

Палагута Катерина Олексіївна
кандидат економічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Радько Максим Андрійович
студент 4 курсу 7 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ПРОБЛЕМА КРАДІЖКИ ПЕРСОНАЛЬНИХ ДАНИХ В ІГРОВІЙ ІНДУСТРІЇ. ЗАХИСТ ОБЛІКОВОГО ЗАПИСУ В STEAM

На теперішній час ігрова індустрія бурхливо розвивається. Ринок відеоігор у світі досяг $161 мільярдів, грають у комп'ютерні ігри близько 2,3 мільярдів осіб. У 2018 році Україна потрапила у 50 країн з найвищими доходами індустрії відеоігор. По оцінці експертів в Україні з 26 мільйонів інтернет-користувачів 14,2 мільйона грають у комп'ютерні ігри. У 2018 році українці витратили по різних оцінках від $161 до $161 мільйонів на відеогри. У порівнянні з іншими країнами ринок відеоігор України не є дуже міським, однак він стрімко розвивається. Україна також активно задіяна у розробці відеоігор. Більше 70 українських компаній спеціалізуються на розробці комп'ютерних ігор, біля 20000 розробників задіяні у цій сфері. Все це свідчить про актуальність досліджень різноманітних аспектів діяльності ігрової індустрії.

Досить популярним в Україні є сервіс компанії Valve Steam. Корпорація Valve є відомим у світі розробником відеоігор, а також спеціалізується на цифровій дистрибуції. Сервіс Steam надає послуги цифрової дистрибуції, багатокористувацьких ігор і спілкування гравців. Через Steam поширюється близько 23000 продуктів, кількість активних користувачів перевищує 125 мільйонів, щодня сервісом у середньому користуються 14 мільйонів осіб. По оцінці експертів сервіс Steam охоплює 70 % ринку цифрової дистрибуції відеоігор у світі.

9 грудня 2018 р. компанія Valve обмежила обмін предметами в сервісі Steam для користувачів, які не використовують двоетапну перевірку через мобільний додаток. Щоб донести до геймерів важливість застосування цього методу, компанія привела тривожну статистику злому облікових записів і докладніше розповіла про причини свого рішення. З'ясувалося, що щомісяця в руки зловмисників потрапляють близько 77 тис. аккаунтів, і кількість зломів продовжує зростати.

«Крадіжки облікових записів Steam відбуваються з моменту появи сервісу, але після запуску торгового майданчика важливість цієї проблеми

багаторазово посилилася, - написав представник Valve в Steam Community. - Зараз злом аккаунтів - найчастіша скарга користувачів »

«Крадіжка віртуальних товарів в Steam стала справжнім бізнесом для умілих хакерів, - продовжив співробітник. - Практично всі активні облікові записи Steam [в лютому їх налічувалося приблизно 125 млн] Так чи інакше залучені в економічну систему сервісу: їх власники продають і купують колекційні картки і предмети. Тому майже кожен аккаунт коштує витрачених хакером зусиль. За великим рахунком, метою зловмисників є кожний обліковий запис Steam». «Злом аккаунтів став звичайною справою», - додав він.

Існує два варіанти викрадення інформації:

1) За допомогою програми, яка відсилає з Вашого комп'ютера інформацію зловмисникові. Говорячи простіше - це вірус (шпигун, кейлогер, троян та інші).

2) Користувач добровільно передає інформацію.

Зазвичай таким способом є фішингові сайти. Це саме ті сайти, які мають ідентичний вигляд оригінального сайту, але з іншою адресою (доменом). Адреса буває дуже схожою на адресу необхідного вам сайту, але візуально його можна прийняти за справжній. Відмінність може бути в одній букві по типу: mn, nn, mm або nm від повної адреси.

Треба пам'ятати, що на 99.99% захист аккаунта залежить від самого користувача. Якщо користувач не бажає бути обережним і уважним, то такого користувача не врятує жоден захист і ніякі поради не допоможуть.

Щоб захистити свій обліковий запис Steam доцільно використовувати Steam Guard. Steam Guard - це додатковий рівень безпеки, який може бути використаний на ваш обліковий запис Steam. Перший рівень безпеки - ваші облікові дані: логін аккаунта і пароль. Активована функція Steam Guard ускладнить доступ до аккаунту для сторонніх осіб. Якщо на акаунті активована функція Steam Guard, для входу в нього з неавторизованого пристрою буде потрібно спеціальний код доступу. Залежно від ваших налаштувань Steam Guard, код доступу ви отримаєте або в повідомленні, надісланому на контактну адресу електронної пошти, або через мобільний додаток Steam.

Список використаних джерел:

1. Сообщество Steam – Керівництво [Електронний ресурс]. - Режим доступу: https://bit.ly/2SoaMiT
2. Steam Guard – Account Recovery [Електронний ресурс]. - Режим доступу: https://bit.ly/2SqPjpD
3. Дорослі забави. Скільки заробляє ігрова індустрія України [Електронний ресурс]. - Режим доступу: https://ubr.ua/ukraine-and-world/technology/vzroslye-zabavy-skolko-zarabatyvaet-ihrovaja-industrija-ukrainy-3879337
4. У 2018 році українці витратили на відеоігри майже $ 180 млн [Електронний ресурс]. - Режим доступу: https://ain.ua/2019/01/25/180-mln-na-videoigry

УДК 374.73

Козік Олександр Іванович
викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Сябренко Микола Євгенович
студент 4 курсу 7 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

СТАН КІБЕРБЕЗПЕКИ В УКРАЇНСЬКОМУ ІНТЕРНЕТ-ПРОСТОРІ

Безпекою кіберпростору займатися потрібно спільно, безглуздо вирішувати це питання в межах однієї країни. Тісна співпраця з партнерами і союзниками в цій області абсолютно необхідно. Ми повинні розробити електронну вакцину, яка буде боротися з маніпуляцією громадською думкою в демократичних країнах. Європейська кіберзахист і кібербезпека повинні бути перебудовані. Не варто чекати, поки трапиться 11 вересня в кіберпросторі. Ми повинні підготувати відповідь для тих, хто хоче підірвати нашу демократію зсередини [1].

Основний тренд кібербезпеки - поворот з боку технологій в сторону додатків. Гарна ідея Hacken - з'єднати безпеку і блокчейн, тому що за великим рахунком блокчейн - це технологія довіри, що захищає інформацію та дані. Крім блокчейна, є ще машинне навчання, штучний інтелект і інші технології. Тобто основний тренд - інтеграція різних технологій для створення real-life applications. Але повинен зайти великий і чистий капітал і допомогти впровадити ці технології. Це повинно відбутися в найближчі 2-3 роки [1].

Українські користувачі у високій мірі схильні до заражень через старе програмне забезпечення і піратські копії програм. Показово також, що 17% всіх заражень припадає на користувачів, що працюють із застарілою операційною системо.

Нерідко спамери для розсилки «нігерійських листів» спекулюють на темі політичної ситуації в Україні або ж розсилають листи від імені «російських наречених»: дівчат з Росії і України, які скаржаться на свою нелегку долю і просять перевести на їх рахунки деяку суму.

Україна посіла п'яте місце в світі (і перше в Європі) за ризиками зіткнення з веб-погрозами в третьому кварталі 2018 року. За даними, KasperskySecurityNetwork за липень-вересень 2018 року третина (33,7%) українських користувачів мережі зіткнулися з погрозами, що розповсюджуються через інтернет [2].

За тим же показником, за період з січня по вересень 2018 Україна займає третю сходинку рейтингу країн з найбільшим ризиком зараження через інтернет: 35,7% користувачів зіткнулися з веб-погрозами за звітний період.

За результатами другого кварталу 2018 року, Україна опинилася на 9 сходинці рейтингу країн з найбільшим ризиком зараження мобільними зловредів (8,39%). Досить високий для українців і ризик зіткнення з локальними погрозами (54,5%). Сюди потрапляють об'єкти, які проникли на комп'ютери шляхом зараження файлів або знімних носіїв або спочатку потрапили на комп'ютер не в відкритому вигляді (наприклад, програми в складі складних інсталяторів, зашифровані файли і т.д.). За цим показником країна займає передостанню сходинку в топ-20 по світу, але перше в Європі [2].

В Україні було відзначено велику кількість спрацьовувань антивірусу на програми-вимагачі і шифрувальники - шкідливі програми, мета яких - заблокувати пристрій або браузер або зашифрувати файли користувача, зробивши їх недоступними без спеціального ключа, за який потрібно заплатити викуп.

Серед жертв Turla - однієї з найскладніших кібершпигунских компаній, яка діє вже більше 8 років, були виявлені комп'ютери українських чиновників. Угруповання, яке стоїть за Turla, заразила сотні комп'ютерів більш ніж в 45 країнах світу, що належать, зокрема, державним установам, посольствам, військовим, дослідницьким центрам і фармацевтичним компаніям. Метою кіберзлочинців є збір необхідних або конфіденційних даних з комп'ютера жертви.

Також українці були серед жертв таких компаній, як CosmicDuke, MiniDuke, Agent.btz, EpicTurla, TeamSpy, BlackEnergy і RedOctober.

Сучасні атаки практично не можна запобігти, тому зараз не менше зусиль потрібно направляти на підготовку команд реагування на інциденти.

Кіберзлочинці – це не одинаки, це добре підготовлені, добре мотивовані і добре фінансовані організації.

Вся інформація, яку ви знаєте про свою мережі і техніці – ніщо, якщо ви не знаєте, хто вам протистоїть. Тому вам потрібно встати на місце хакера і зрозуміти, що йому може бути цікаво в вашої компанії і як він може це отримати.

Головне порушення кібербезпеки сьогодні - це відсутність комплексного підходу (люди, системи, процеси), ігнорування питань кібербезпеки з боку CEO, зайва впевненість у безпеці [1].

Раніше зловмисники атакували для шантажу або заволодіння грошовими коштами, сьогодні це використання інфраструктури жертви для атаки на третіх осіб, маніпулювання виборами або техногенні катастрофи [2].

Список використаних джерел

1. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture, National Institute of Standards and Technology, U.S. Department of Commerce , 2015 –28c.
2. P. Mell and T. Grance, The NIST definition of cloud computing, National Institute of Standards and Technology, U.S. Department of Commerce, 2014 – 100 c.

УДК 004.056.52

Котенко Наталія Олексіївна
кандидат педагогічних наук, старший викладач,
старший викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Гамалій Любомир Сергійович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ЗАГАЛЬНА СТРУКТУРА СИСТЕМИ ПРОГРАМНОГО ЗАХИСТУ МЕРЕЖЕВИХ РЕСУРСІВ

Відомо, що інформація про стан TCP/IP портів є основою мережевої безпеки. Побудова мережевого профілю та створення інструментальних засобів для розпізнавання мережевого трафіку дозволяє більш ефективно розпізнавати неавторизованих користувачів.

Мережеві порти – це точки входу до машини, під'єднаної до Інтернету. Служба, яка прослуховує порт, може отримувати дані від клієнтської програми, обробляти її і відправляти відповідь назад. Шкідливі клієнти можуть іноді використовувати уразливості коду сервера, щоб отримати доступ до конфіденційних даних або віддалено виконувати шкідливий код на машині. Ось чому тестування для всіх портів необхідно для того, щоб досягти найвищого рівня перевірки безпеки [3].

Сканування портів, як правило, здійснюється на початковому етапі тесту на проникнення, щоб виявити всі точки входу в мережу.

Сканери портів є одними з найбільш корисних інструментів, для забезпечення безпеки в будь-якій віддаленій або локальній мережі. Виділяють такі п'ять найпопулярніших сканерів портів:

– Nmap;
– Unicornscan;
– Angry IP Scan;
– Netcat;
– Zenmap [1].

Сканер портів перераховані у порядку їх популярності. Найбільш популярним вважається Nmap.

nmap, «Network Mapper» - безкоштовне відкрите програмне забезпечення для дослідження та аудиту безпеки мереж та виявлення активних мережевих сервісів. З часу публікації в 1997 став стандартом в галузі інформаційної безпеки. Автор програми, Гордон Ліон, відоміший як Fyodor, після релізу версії 5.0 назвав це найбільшим розвитком застосунку починаючи з 1997, коли сирцеві коди вперше були оприлюднені в журналі Phrack.

Nmap використовує безліч різних методів сканування, таких як UDP, TCP (connect), TCP SYN (напіввідкрите), FTP -proxy (прорив через ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN- і NULL-сканування. Nmap також підтримує великий набір додаткових можливостей.

Advanced Port Scanner – це безкоштовний сканер портів, що дозволяє швидко знайти всі відкриті порти на комп'ютерах мережі і визначити програми, що працюють на цих портах. Програма має зручний інтерфейс і багату функціональність [2].

Розглянемо програмну систему сканування доступних портів під назвою «*Scanner of ports availability*», або скорочено «*SPA*». Програма виконує сканування портів, використовуючи введені користувачем мережеві адреси та реалізує вивід отриманих результатів у формі звіту, що зберігається в *.txt* або *.json* файлі.

Алгоритмічна модель роботи програмної системи полягає у наступному:

1. Вказується файл зі скінченною кількістю мережевих адрес. Також вказується нижній поріг та верхній поріг сканування портів.

2. За допомогою програмного інтерфейсу створюється з'єднання для кожної з адрес.

3. Перевіряється доступність портів від нижнього порогу до верхнього для кожної з мережевих адрес.

4. Весь звіт виводиться у файл, який розташовується у поточній папці програмної системи і називається «*Ports.txt*» або «*Ports.json*». Файл звіту містить таблицю для запису даних з обов'язковими полями «*IP Адреса*», «*Номер та Стан порту*».

Головним недоліком, який виявлено при тестуванні програмної системи, є вразливість відкритих портів під час сканування, та відсутність можливості закрити їх під час роботи програмної системи.

Зрозуміло, що кожен відкритий мережевий порт пов'язується з додатком, який прослуховує мережу. Таким чином, поверхню атаки кожного сервера, який підключено до мережі, можливо зменшити шляхом відключення необов'язкових мережевих служб та додатків.

Список використаних джерел:

1. SecurityTrails. Режим доступу: https://securitytrails.com/blog/best-port-scanners (дата звернення: 21.03.2018)
2. Advanced Port Scanner. Режим доступу: https://www.advanced-port-scanner.com/ru/ (дата звернення: 21.03.2018)
3. Сканування TCP-порту за допомогою Nmap. Режим доступу: https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap (дата звернення: 21.03.2018)
4. Nmap Network Scanning. https://nmap.org/book/port-scanning.html
5. Wikipedia. Режим доступу: https://uk.wikipedia.org/wiki/Nmap (дата звернення: 21.03.2018)

УДК 004.49

Харченко Олександр Анатолійович
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Старичок Петро Олександрович
студент 4 курсу 7 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

КІБЕРБЕЗПЕКА В УКРАЇНІ: ОСНОВНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ

Складність світу, у якому ми живемо, вимагає від країн постійного вдосконалення нормативної бази, щоб відповідати тим викликам, які висуває швидкий технологічний розвиток.

Українські користувачі мають великий ризик до зараження через те, що невчасно оновлюють програмне забезпечення або користуються піратськими копіями програм. Також встановлено, що 17% всіх заражень вірусами припадає на користувачів, що використовують застарілу операційну систему Windows XP,оновлення якої припинено. Часто спамери користуються темою політичної ситуації в Україні для розсилки листів, також вони надсилають листи від закордонних мешканців, котрі скаржаться на свій скрутний фінансовий стан і просять перевести гроші на їх рахунок.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «Кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі»

За підсумками другого кварталу 2017 року Україна знаходилась на 5 місці в світі та на першому місці в Європі за ризиком щодо веб-загроз. Користуючись даними Kaspersky Security Network за липень-вересень 2017 року, третина (33,7%) користувачів всесвітньої павутини з України зіткнулися з погрозами, котрі було розповсюджено саме через мережу Інтернет. За період з січня по вересень 2018 року ці показники практично не змінились. Україна на третьому місці у рейтингу країн з найбільшим ризиком щодо зараження через мережу Інтернет: 36.6% користувачів зітктнулись з веб-загрозами за звітний період.

За результатами другого кварталу 2018 року, Україна знаходилась на 9 місці у рейтингу серед країн, котрі найбільше були заражені мобільними вірусами (8,38%). Поширеним для українців являється ризик зіткнення з локальними загрозами (54,5%). Сюди відносять об'єкти, котрі потрапили на комп'ютери шляхом зараження файлів або знімних носіїв, або спочатку були переміщені на комп'ютер в не відкритому вигляді (наприклад, програми які

входили до складу інших інсталяторів, або зашифровані файли і т.д.). За даними показниками Україна займає передостанню сходинку в ТОП-20 в світі.

В Україні було визначено, що занадто часто спрацьовують антивірусні програми на програми-вимагачі і шифрувальні шкідливі програми, мета яких заблокувати пристрій або браузер, або зашифрувати файли користувача, таким чином зробивши їх недоступними без спеціального ключа, за який потрібно заплатити.

Всі погоджуються, що кількість кібератак зростає з кожним днем. До 2008 року фінансування кібербезпеки здійснювалося за залишковим принципом. На сьогодні найбільш розповсюджені програми містять ген кібербезпеки в кожному процесі і в кожному пристрої, оскільки навіть кавоварка може підлягати зараженню вірусами та кібератакам, що звісно несе загрозу.

Жертвою стала і загальновідома Turla – одна з найскладніших кібершпигунських компаній, та котра діє ринку вже більше ніж одинадцять років. Угруповання, яке стоїть за Turla, вразило сотні тисяч комп'ютерів, у більше аніж в 45 країнах усього світу, котрі належать державним установам, посольствам, військовим, дослідницьким центрам і фармацевтичним компаніям. Мета кіберзлочинців полягає в зборі необхідної або конфіденційної інформації з комп'ютерів жертв.

Проблема кібербезпеки це – проблема не професійна та не технологічна, а проблема спецслужб, які повинні забезпечувати безпеку роботи підприємств.

Також українці були жертвами таких кампаній, як CosmicDuke, MiniDuke, Agent.btz, Epic Turla, TeamSpy, BlackEnergy і Red October.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII
2. Деньга С.М. Захист інформації в комп’ютерних інформаційних системах бухгалтерського обліку [Текст] / С.М. Деньга, Ю.О. Верига // Бухгалтерський облік і аудит. – 2004. – № 5. – С. 59-65.
3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека» / О.А. Баранов // Правова інформатика. – № 2(42). – 2014. – С. 54-62.
4. Бутузов В. М. Протидія комп’ютерній злочинності в Україні (системноструктурний аналіз) : [монографія] / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.
5. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 лип. 2009 р. № 514/2009 // Офіц. вісник України. – 2009. – № 52. – Ст. 1783. – С. 7. – 20 лип.
6. Про кіберзлочинність : Конвенція Ради Європи // Офіц. вісник України. – 2007. – № 65. – Ст. 2535. – С. 107. – Код акту 40846/2007. – 10 верес.
7. Решетов Ю. А. Борьба с международными преступлениями против мира и безопасности / Ю. А. Решетов. – М.: Междунар. отношения, 1983. – 224 с.

УДК 004.056.53

Степашкіна Катерина Володимирівна
викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Шабельник Ілля Ярославович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ПРОБЛЕМАТИКА КІБЕРБЕЗПЕКИ В УКРАЇНІ

Проблематика кібербезпеки являє собою проблеми зв'язані з такими поняттями як: кіберзлочин, кіберзлочинець, кіберпростір, кіберзахист. У сучасному світі ці поняття є дуже важливими, тому що кожен день ми стикаємося із необхідністю використання інформаційних технологій. Кожного дня ми заходимо на велику кількість веб-сторінок і на більшості з них надаємо персональні дані про себе. Постає питання наскільки захищені наші персональні дані? Чи є можливість захистити себе в мережевому просторі?

На жаль в нашій країні з цими питаннями виникають складнощі, при аналізі нашого законодавства було визначено, що такі поняття: кіберпростір, кіберзлочинець, кіберзахист та кіберзлочин досих пір не визначені. Ці поняття для України дуже поверхневі і щоб мати змогу захистити свої персональні дані, нашому законодавству потрібно поглибитися у вирішення даних проблем.

Кіберзахист залежить не тільки від держави, але від самих нас. Оскільки більшість людей легковажно і не дуже обережно відносяться до даного питання, це стосується тих випадків коли людина реєструється на сайтах, які їм невідомі, тим самим віддаючи персональні дані зловмиснику, а про платежі в мережі, всі ми хочемо купити речі якомога дешевше і тому частіше всього ми потрапляємо у пастку людей, які розробили сайт з «дешевими» речами. Купляючи речі на цих сайтах ми переводимо деяку суму грошей на банківський рахунок зловмисника. Це один із прикладів, а таких прикладів можливо навести тисячі. А також підключення до Free Wi-fi в публічних місцях, через відкритий wi-fi зловмисник може отримати доступ до ваших даних.

В наш час за допомогою програми «Вимагач» вимагають у людей гроші шляхом блокування їхнього доступу до файлів, до самої операційної системи, тощо. З необережності користування інтернетом люди скачують файли і разом з цими файлами шкідливе програмне забезпечення. При активації файлу на екран комп'ютера блокується и з'являється напис, на якому вимагачі просять людей перевести певну суму коштів на їхній рахунок за відведений час. У випадку непокори, людині блокується операційна система або знищуються файли, які були заблоковані. Перше що необхідно зробити -

зателефонувати стільниковому оператору чий номер зазначений в повідомленні. Сказати, що ваш комп'ютер заблокований вірусом «здирником» і попросити їх назвати вам код, продиктувавши номер на який потрібно відправка повідомлення. Паралельно цим діям можна спробувати дізнатися код за номером. Друге - вставити завантажувальний диск вашого антивіруса в дисковод і перезавантажити комп'ютер. Після цієї процедури з'являється якийсь доступ до операційної системи. Далі ставите ваш комп'ютер на повну перевірку антивірусом. Третє - лікування системи за допомогою диска Live CD або Live USB. За допомогою цього диска або флешки ви завжди зможете завантажити систему в не залежності від типу «вимагача» та інших вірусів, які блокують ті чи інші дії комп'ютера.

Щоб не стати жертвою в сфері банківського сектору достатньо притримуватися правил безпеки користування банківськими (платіжними) картками. Ніколи не давати свої картки знайомим та незнайомим людям, тому що вони можуть переписати, сфотографувати номер вашої картки та використовувати її в подальшому. Також не носити з собою PIN code записаний на листку бумаги або ще десь, краще таку інформацію пам’ятати і за можливістю змінювати пароль якомога частіше. В сучасному світі розроблено багато пристроїв для викрадення даних з карток. На превеликий жаль ці пристрої для зчитування встановлюються на банкоматах. В цих пристроях є все що потрібно зловмиснику чіп зчитування, чіп передачі даних карток та можливість передачі викрадених даних на мобільний номер у вигляді смс або на електрону пошту зловмисника. А також встановлюється пристрій на клавіатуру банкомату і при введені паролю користувачем, пристрій зчитує натиснуті кнопки і передає інформацію також по смс розсилці або на пошту. Але дану проблему з пристроями повинні вирішувати власники банкоматів.

Кіберзлочинність постійно розвивається, розробляються нові пристрої і покращуються методи впровадження цих пристроїв. На жаль протидія новим методам середня, але все ж таки вона є. Отже, кожна людина задля власної безпеки повинна бути пильна і більш обережніше ставитися до надання даних і інформації про свої платіжні картки. А також зі сторони законодавства виділення коштів на пристрої та кваліфікованих працівників задля забезпечення нашої з вами безпеки у мережі.

Список використаних джерел:

1. Що таке кібербезпека [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html (дата звернення 16.03.2019)
2. Про боротьбу з тероризмом [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://zakon1.rada.gov.ua/laws/show/638-15 (дата звернення 04.03.2019)
3. Про Стратегію національної безпеки України [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://zakon4.rada.gov.ua/laws/show/105/2007 (дата звернення 04.03.2019)

УДК 343:1

Юскович-Жуковська Валентина Іванівна
кандидат технічних наук, доцент,
декан факультету кібернетики
Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука

ПРИНЦИПИ ЗАХИЩЕНОСТІ КІБЕРПРОСТОРУ УКРАЇНИ

На сучасному етапі розвитку інформаційного суспільства існуючі об'єкти набувають альтернативної, електронної форми, практично зі всіх комп'ютерів світу здійснюється обмін гігантським потоком електронної інформації та знаннями. Глобальна комп'ютерна мережа Інтернет надає безмежний спектр інформаційних послуг, формується цифровий ринок інформації та знань.

Основною цінністю мережі Інтернет є інформація. Але інформація може зазнавати випадкових або навмисних втручань, в результаті чого існує ризик її незаконного використання або знищення.

Тому на сьогодні актуальним являється забезпечення безпеки всіх транзакцій, проведених через мережу Інтернет та збереження в ній цілісності електронних даних. Проблема безпеки зберігання інформації, протиправне втручання в інформаційні процеси, вважається однією з першочергових задач у сфері новітніх інформаційних технологій.

На сьогодні найбільш складною залишається проблема правового врегулювання функціонування цифрового простору у світовій мережі Інтернет. У 2017 році в нашій країні був прийнятий Закон «Про основні засади забезпечення кібербезпеки України». Цей Закон визначив поняття кіберпростору, як віртуального простору, як середовища, що утворене в результаті функціонування комунікаційних систем та забезпечення передачі електронних даних з використанням мережі Інтернет [1].

Безпека кіберпростору являється пріоритетним напрямком державної політики у сфері розвитку цифрового електронного простору та становлення інформаційного суспільства в Україні. Під кібербезпекою розуміється захищеність кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація загроз у кіберпросторі. Сфера кібербезпеки визначена цим Законом як складова національної безпеки України.

Об'єктами кіберзахисту, зокрема, є:

- комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси;
- об'єкти критичної інформаційної інфраструктури, затверджені КабМіном.

Забезпечення кібербезпеки в Україні грунтується на принципах:

- відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

- державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту;

- міжнародного співробітництва з метою недопущення використання кіберпростору у протиправних цілях.

Організаційно-правовий аспект передбачає створення системи колективної відповідальності за безпеку інформації у кіберпросторі. Основою оцінки безпеки у кіберпросторі став міжнародний стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій так Стратегія кібербезпеки України [2].

В мережі Інтернет зростає кількість потужних кібератак, поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконного фінансування операцій, крадіжок та шахрайства. Кіберзлочинність стає транснаціональною та здатною завдати значної шкоди інтересам суспільства, особи та держави.

Розвиток безпечного, стабільного і надійного кіберпростору в Україні визначається наступними основними принципами:

- розвитком кіберпростору в Україні у відповідності до міжнародних стандартів, стандартів ЄС та НАТО, що відповідають національним інтересам України;

- поглибленням співпраці у заходах зі зміцнення системи захисту інформації у кіберпросторі, що проводяться під егідою ОБСЄ;

- впровадженням організаційно-технічної моделі національної системи кібербезпеки для оперативного реагування на кібератаки у кіберпросторі.

Згідно із Законом «Про основні засади забезпечення кібербезпеки України» впровадження організаційно-технічної моделі кіберзахисту, як складової національної системи кібербезпеки, здійснюється Державним центром кіберзахисту та протидії кіберзагрозам. Ядром цієї моделі, центром управління, аналізу та оперативного реагування на кіберзагрози є Центр реагування на кіберзагрози Держспецзв'язку, відкриття якого відбулося у лютому 2018 р. Технологічна та аналітична системи Центру створені на базі найновітніших досягнень провідних ІТ-компаній світу, розроблені на рівні кращих світових аналогів та являються одними з найпотужніших систем в Європі [3].

Дослідження проблеми захищеності кіберпростору України дозволяє зробити висновки про те, що для забезпечення безпеки необхідний комплекс заходів, інфраструктур, технічних засобів, програмного забезпечення та організаційно-юридичних процедур, спрямованих на виявлення, нейтралізацію та запобігання кіберпорушенням у кіберпросторі.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України», із змінами, внесеними від 21.06.2018 р. №2469-VIII.

2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 р. №96/2016.

3. Електронний ресурс: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=286338&cat_id=284576. Загол. з екрану.

UDC 004.056.5:336

Hnatchenko Dmytro
Assistant of the Department of Program Engineering and Cybersecurity
Kyiv National University of Trade and Economics
Korkosh Maksym
3rd year student of group 6 of FAAIS,
Direction of preparation 6.050103 «Software Engineering»
Kyiv National University of Trade and Economics

MAIN OBJECTIVES OF CYBERSECURITY OF UKRAINE'S BANKING SYSTEM

The issue of cybersecurity in the modern world has become very relevant in all spheres of human activity. Last years, the situation in Ukraine in the field of cybersecurity was extremely complicated, the number of cybernetic attacks on state information resources has increased. In June 2017, Ukraine suffered a cyberattack with the «Petya.A» virus, which inflicted damage to critical infrastructure objects by almost half a billion dollars. Cyberattack shocked the society, since it overcame a large number of facilities, such as: Ukrzaliznytsia, international airports «Kyiv» and «Borispol», Ukrposhta, Kyiv Metro, Chornobyl Nuclear Power Plant, «Oshchadbank» and «Ukrgasbank» banking institutions, and others. Despite the fact, that the cyberattack did not cause irreparable damage, it became clear how effective the weapon is in the hands of enemies, which can paralyze the whole country, so the issue of cybersecurity of the banking system and the whole country in general is extremely important.

In conditions of a significant dependence of banking on the reliability of information technologies that it uses, ensuring information security becomes one of the fundamental principles of banking system's existence. An important feature of the work of each bank is modern digital business technologies using. Automatic banking systems, Internet and SMS banking, mobile billing, cloud technologies and sophisticated cybersecurity systems are all new realities of the banking sector.

In accordance with the Law of Ukraine "On the National Bank of Ukraine" [4], the National Bank of Ukraine (NBU): defines the directions of development of modern electronic banking technologies; creates and ensures the reliable and effective functioning, development of payment and accounting systems created by them; establishes rules for the protection of information for banks; controls the creation of payment instruments, banking automation systems and bank information protection tools; determines the procedure, requirements and measures for ensuring cyber- and information security in the banking system of Ukraine, and controls their implementation.

The NBU has a separate structural subdivision - the Department of Security, one of the main functions of which is: the development and implementation of the NBU's information security strategy and policy and the introduction of technologies in providing effective and targeted information security in the

information infrastructure of the NBU and the banking system of Ukraine [5], which uses advanced cybersecurity systems: Intrusion Prevention System, Wireless Intrusion Protection System, Security information and event management, Vulnerability Scanner, Secure Web Gateway, Network firewall. This ensures the functioning of cybersecurity system in Ukraine's banking system.

In order to introduce a legal mechanism taking into account international standards on information security, generally accepted in international practice of ensuring information security and cybersecurity, was adopted the «Provisions on the organization of measures for the provision of information security in the banking system of Ukraine»[6], which establishes:

1) the requirements to information systems of the bank interacting with the NBU information systems, taking into account the directions of the development of cryptographic protection of information in the information systems of the National Bank;

2) mandatory minimum requirements for the organization of measures for the provision of information security and cybersecurity;

3) principles of information security management.

Reliable functioning of the banking system, its protection against potential cyberattacks is an important component of the state. Almost all cybercrimes lead to information leakage and significant financial losses, impairment of reputation, and ultimately a loss of public confidence in the banking system in general. Therefore, the issue of cybersecurity of Ukraine's banking system is important, to determine the main directions of counteraction to cybercrime, to regulate relations between state bodies and private organizations and to consolidate it at the legislative level.

References:

1. Pacer M. Cybercrime – A Threat to the Banking System / M. Paters // Bulletin of the National Bank of Ukraine: An Analytical Scientific and Practical Edition. – Kyiv: National Bank of Ukraine, 2015. – No. 4. – P. 55-58.
2. Dioritsa I. Administrative-legal regulation of cybersecurity in Ukraine: diss. ... doctor jur. Sciences: 12.00.07 / Igor Dioritsa – Zaporozhye, 2018. – 521 p.
3. The Law of Ukraine «On the Basic Principles of Cybersecurity Protection of Ukraine» of 10.05.2017 / [Electronic Resource]. – Mode of access: https://zakon.rada.gov.ua/laws/show/2163-19 (application date 10.03.2019).
4. Law of Ukraine «On the National Bank of Ukraine» / Bulletin of the Verkhovna Rada of Ukraine (BPD). – 1999. – No. 29. – 238 p.
5. The main functions of the structural units of the central office of the National Bank of Ukraine / [Electronic resource]. – Access mode : https://bank.gov.ua/doccatalog/document?id=24604231 (application date 12.03.2019).
6. Regulation on the organization of measures to ensure information security in the banking system of Ukraine, approved by the Resolution of the Board of the National Bank of Ukraine dated 09/28/2017, No. 95 / [Electronic resource]. – Mode of access : http://zakon2.rada.gov.ua/laws/show/v0095500-17 (application date 12.03.2019).

UDC 004.056

Palahuta Kateryna
Ph.D. in Economics, Associate Professor
Kyiv National University of Trade and Economics
Gorbachov Pavlo
Student of the Faculty of International Trade and Law
Kyiv National University of Trade and Economics

CYBERSECURITY IN NATIONAL AND INTERNATIONAL LEGISLATION

New technologies, electronic services have become an integral part of our daily life. Nowadays, cybersecurity is a prerequisite for the development of the information society. In modern conditions, cybersecurity issues go beyond the level of information protection on a separate computer facility to the level of creation of a unified cyber security system as an integral part of the information and national security of each state.

On the world stage, the policy of information security in a particular state is ensured by adopting Cybersecurity Strategies. The first cybersecurity strategy appeared in 2003 in the United States. After that, similar Strategies and plans of activities on security in the virtual space spread throughout Europe. A list of all national Cybersecurity Strategies of the European Union members and some other non-member countries was published by the European Network and Information Security Agency – ENISA.

On May 4, 2008, at a meeting of the NATO Council in Brussels, a Memorandum of Understanding was signed on the creation of a NATO cyber defense center in Tallinn, later called the NATO Cooperative Cyber Defense Center of Excellence. The purpose of creating this center is to enhance the security alliance in cyberspace, including research and development of new ways to protect information, including the identification of harmful effects on the information systems of member countries, the assessment of damage, restoration of their efficiency, and timely adoption measures to prevent cyber attacks, legal support for NATO's cyber defense activities, the study, synthesis and dissemination of experience in the field of Information security, educational and methodological work and training of specialists in the field of protection and security of information of member countries.

The center pays special attention to conducting research in the cyber sphere, the main areas of which are the development of concepts and strategies for ensuring security in cyberspace, as well as concepts of conducting cyber operations (offensive, defensive, operational) both within NATO and in individual member countries, security solutions for digital computing systems of the Alliance and member countries, the detection and elimination of the effects of cyber attacks, the development of methods for determining greetings from the outside.

At the same time, recently, the first cybersecurity law in the European Union, which is called the "Network and Information Security Directive", was approved by the EU member states and deputies of the European Parliament. The Network

and Information Systems Security Directive (NIS Directive) was adopted by the European Parliament on July 6, 2016. The NIS Directive provides for legal measures to increase the overall level of cybersecurity in the European Union, providing cooperation between all member states, by creating a collaboration group, in order to support and facilitate strategic cooperation and information sharing between member states, as well as a security culture in all sectors, which are vital for the economy and society, such as energy, transport, water supply, banking, infrastructure of the market, health and digital infrastructure.

In October 2017, the Verkhovna Rada adopted a law "On the Basic Principles for the Cybersecurity of Ukraine". The document defines the basis for ensuring the protection of Ukraine's national interests in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity, as well as the powers of state bodies in this area, the basic principles of coordination of their activities in providing cyber security. The law has expanded and supplemented the provisions of the Cybersecurity Strategy of Ukraine, approved by the President's decree in 2016. The purpose of the strategy was to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state. At the same time, the bulk of the provisions of the strategy concerns the sphere of national defense and does not affect business. The strategy became a confirmation of Ukraine's course on European integration, the beginning of which was the signing and ratification by Ukraine of the Convention on Cybersecurity. The member states of the Council of Europe and some other signatory states have undertaken to take common and individual country measures to prevent the occurrence of criminal offenses in the digital world.

As international experience shows, national cybersecurity strategy is a tool for improving and enhancing the security level of national information infrastructure and services, showing the various areas of national interests and priorities that should be achieved at certain time intervals.

References:

1. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union/ [Електронний ресурс]/Режим доступу: http://data.europa.eu/eli/dir/2016/1148/oj

2. Закон України “Про основні засади забезпечення кіберпростору України”/ [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

3. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"/ [Електронний ресурс]/Режим доступу: https://zakon5.rada.gov.ua/laws/show/96/ 2016#n11

4. Cybersecurity 2018 – The Year in Preview: International Law and Cyber Warfare // [Electronic resource]. – Access mode: https://www.securityprivacyandthelaw.com /2017/12/cybersecurity-2018-the-year-in-preview-international-law-and-cyber-warfare/

УДК 004.056:316.77

Половенко Людмила Петрівна
кандидат педагогічних наук, доцент,
доцент кафедри економічної кібернетики та інформаційних систем
Вінницького торговельно-економічного інституту КНТЕУ

КІБЕРЗАГРОЗИ У КОНТЕКСТІ ІНТЕРАКТИВНОЇ ОСВІТИ

Стрімкий розвиток новітніх інформаційно-комунікаційних технологій спричинив глибокі системні перетворення в освітньому просторі, змінивши характер усталених освітніх практик. Перенесення значного обсягу навчального матеріалу у кіберпростір, блискавичне поширення мережевої освіти, поява відкритих освітніх ресурсів, он-лайн курсів, дистанційного навчання суттєво вплинули на традиційні університетські студії. Електронне навчання стало невід'ємним елементом сучасної освіти.

Основною перевагою освіти у кіберпросторі є «необмежені можливості створення і масового споживання знань» [1]. Поліджерельність інформації, багатоканальність формування знань, колективна взаємодія учасників навчального процесу передбачають створення розгалуженої мережі надійних джерел інформації та зв'язків.

Водночас виникає ряд нових загроз, притаманних он-лайн простору: «слабкість контролю за герменевтично-дискурсивною діяльністю учасників електронного навчання, яка охоплює складні когнітивні процеси … перетворення інформації в знання й суб'єктні смисли» [1]; небезпека споживацького ставлення до навчальної інформації, транслювання в монологічній формі масивів інформації без належного суб'єктного її осмислення й інтерпретації; відсутність глибини розуміння, поверхове сприйняття інформації; недостатнє нормативно-правове регулювання кіберпростору, зокрема в сфері захисту авторських прав; маніпулювання свідомістю та дезінтеграція; спотворення правди для маніпуляції інформацією; випадки шахрайського «флешмобу» (нерідко під виглядом психотренінгів та освітніх курсів працюють сектантські організації, які зомбують слухачів та вимагають з них кошти); застосування технологічного інструментарію цілеспрямованого соціально-психологічного впливу за допомогою «кліпової культури», породженої неконтрольованим і дуже швидким потоком фактів [2] тощо.

Одним із способів адаптації в перенасиченому інформаційному просторі виступає формування нового різновиду мислення – мережево-віртуального. Для нього характерна висока швидкість переключення, перезавантаження інформації, калейдоскопічність, фрагментарність, алогічність, велика розрізненість інформаційних потоків. Сучасна інтернет-мережа виступає основою створення «кліповості», що дозволяє значно простіше та швидше формувати нові образи. У таких випадках частіше йдеться не стільки про мислення, скільки про сприйняття образної інформації, яка, в свою чергу, здійснює комплексний вплив на свідомість людини через зображення та звук.

В процесі відображення великої кількості властивостей об’єктів без врахування конкретних зв’язків між ними, без часової прив’язки, у вигляді уривків інформації та осколків вражень, відбувається створення мозаїчної, еклектичної картини світу, в якій відсутній певний варіант системності та цілісності. Неоднорідність та неузгодженість інформаційних потоків не дають змоги формувати цілісну картину про об’єкти дослідження і, відповідно, прогнозувати поведінку системи, знаходити шляхи оптимізації та вирішення ряду проблем, що виникають. Хаос сприймання, невизначеність смислів, міфологеми переконань, ілюзії уявлень, неупередженість, помилковість зрештою призводять до маніпулювання свідомістю, цілеспрямованої дезінформації.

Варто зазначити, що процедура створення штучної «кліповості» в інформаційно-комунікативному просторі побудована не тільки на варіаціях мозаїчності картини світу, але й на викривленні та спотворенні властивостей символу (інформаційна компресія, прецедентність, конвенціональність, аттрактивність, адаптивність, інтеграційний потенціал, проактивність, ретроактивність [3]), застосуванні маніпулятивних технологій цілеспрямованого інформаційно-психологічного впливу. Якщо ж аналізувати роботу в інформаційно-комунікативному просторі сьогодення, то спочатку відбувається збір інформації, який є фундаментальним елементом для подальшого сортування, відбору, систематизації тощо. І тут зростає роль педагога як координатора у подальшій трансформації «кліпового» сприйняття у концептуальне мислення, формуванні вміння протидіяти негативним впливам аудіовізуальних маніпулятивних технологій, які сприяють побудові простору без традиційних просторово-часових характеристик, щоб не втратити відчуття фізичного середовища та налагодити ефективну взаємодію в ньому.

В процесі модернізації системи навчання, ефективним є комплексне поєднання традиційних університетських студій та сучасних інтерактивних освітніх технологій, електронного навчання з урахуванням кіберзагроз мережевого глобального суспільства.

Список використаних джерел:

1.Тимошенко Ю. Онлайн-освіта: продуктивні смисли для модернізації традиційних університетських студій. Наукові записки [Кіровоградського державного педагогічного університету імені Володимира Винниченка]. Сер. : Педагогічні науки. Випуск 147. 2016. С. 235-241. URL: http://nbuv.gov.ua/UJRN/Nz_p_2016_147_61

2. Чаплан Я.В., Чуйко Г.В. Кліпова хаотичність як маніпулятивна технологія соціально-психологічного впливу в кіберпросторі. Psychological journal. 2018. №3 (13). С. 21-40. URL: https://doi.org/10.31108/2018vol13iss3

3. Бутиріна М. Символ як інструмент прикладних соціально-психологічних комунікаційних технологій. Учёные записки Таврического национального университета им. В.И.Вернадского. Серия: Филология. Социальные коммуникации. 2011. Т. 24 (63). – С.396-401.

УДК 38/27+351.824.11

Олійник Даниїла Іллівна
доктор економічних наук, професор, головний науковий співробітник
відділу економічної стратегії та економічної безпеки
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Ніжний Даниїл Артемович
Студент
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Світ нині переживає складні, тектонічні трансформації масштабного характеру в яких зароджується новий технологічний уклад. Сутність таких цифрових трансформацій полягає у створенні абсолютно нової цифрової реальності, яка зростає безпрецедентними темпами. Цифрова трансформація на основі інноваційних технологій набуває нового виміру в глобальному масштабі і є достатньою підставою для формування єдиних підходів до оцінювання можливих ризиків щодо критичної інфраструктури як системи, яка має важливе значення для підтримки життєво важливих соціальних функцій.

В міжнародній практиці захист критичної інфраструктури стосується готовності та реагування країни на серйозні інциденти на основі впровадження стандартів. Так, в США здатність запобігати, виявляти, реагувати та управляти результатами на кібер–атаки щодо критичної інфраструктури регламентована стандартами Національного інституту стандартів і технологій (*National Institute of Standards and Technology, NIST*). Європейська програма захисту критичної інфраструктури *(European Programme for Critical Infrastructure Protection, EPCIP*) відповідно до директиви [2] описує створення стандартизованого класу активів цифрової критичної інфраструктури. Під поняттям «цифровізація» розуміється створення потоків інформації на основі цифрових активів внаслідок насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного середовища, тобто створює кіберфізичний простір. Відповідно до Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки [1] основна мета цифровізації полягає у досягненні цифрової трансформації існуючих та створенні нових галузей економіки, а також трансформації сфер життєдіяльності у нові більш ефективні та сучасні.

Проте, взаємозв'язані компоненти системи створюють системні ризики і потребують узгодження технічних аспектів для підтримки поточної

діяльності та захисту критичної інфраструктури в цифровій економіці. Підвищення надійності та ефективності функціонування критичної інфраструктури реалізується шляхом впровадження ризик-орієнтованого управління на базі цифрових технологій, і в першу чергу, технологій промислового Інтернету речей *(Industrial Internet of Things, IIoT)*. Тому цифровізація вимагає, в першу чергу, забезпечення горизонтальної та вертикальної інтеграції потоків інформації на основі системних стандартів шляхом формування загального словникового запасу та єдиної мови й простору спілкування інформаційних та експертних систем для всіх учасників галузевих процесів.

Обмеження ризиків в міжнародній практиці визначається через призму функціональної безпеки електричних та електронних пристроїв та систем на основі стандартів функціональної безпеки. Оцінка відповідності для тестування та сертифікації електротехнічного обладнання та його компонентів здійснюється відповідно до схем оцінювання безпеки, якості, ефективності на основі стандартів Міжнародної електротехнічної комісії *(International Electrotechnical Commission, IEC)*. Такий підхід, що ґрунтується на оцінці потенційного внутрішнього ризику, або можливих зовнішніх загроз є цілісним і поєднує стандарти з тестуванням та різними видами сертифікації (оцінки відповідності) відповідно до різних рівнів ризику. До таких нормативних документів *IEC* нині віднесені стандарти щодо:

- вимог функціональної безпеки (*IEC 61800-5-2:2007 Adjustable speed electrical power drive systems - Part 5-2: Safety requirements – Functional*);

- низьковольтної апаратури розподілу та управління (*IEC 60947-6-1:2005+AMD1:2013 CSV Consolidated version Low-voltage switchgear and controlgear - Part 6-1: Multiple functionequipment*);

- вимог до пристроїв безконтактного зв'язку з певною поведінкою в умовах несправностей (*IEC 60947-5-3:2013 Low-voltage switchgear and controlgear - Part 5-3: Control circuit devices and switching elements - Requirements for proximity devices with defined behaviour under fault conditions*) та ін.

Найбільш ефективні засоби захисту функціонування критичної інфраструктури залежать від впровадження «горизонтальних» та «вертикальних» стандартів. *Горизонтальні стандарти* є загальними і гнучкими, в той час, як вертикальні стандарти регламентують специфічні потреби. Так, наприклад, серія стандартів *ISO/IEC 27000* допомагає захистити інформаційні системи, забезпечує отримання даних у віртуальному середовищі та слугує горизонтальною основою для порівняльного аналізу. Стандарти серії *IEC 62443* є іншою серією горизонтальних стандартів, які призначені для збереження ІТ-систем у реальному середовищі і можуть бути застосовані до об'єктів критичної інфраструктури, таких як енергетичні підприємства або атомні електростанції, а також об’єктів сфери охорони здоров'я та транспорту. *Вертикальні стандарти* слугують доповненням до горизонтальних стандартів і призначені для задоволення потреб конкретних секторів. Так, приміром, існують вертикальні стандарти, що охоплюють

специфічні потреби безпеки ядерного сектора, промислових мереж зв'язку, промислової автоматизації та морської галузі, які адаптують стандарти системи управління інформаційною безпекою *ISO/IEC 27001[3]* та *ISO/IEC 27002* [4] до контексту ядерної безпеки та кореспондуються з серією стандартів щодо безпеки для промислової автоматизації та систем управління *IEC 62443[5]*. В той час, як стандарти серії *IEC 62645* регламентують системи вимірювання та контролю атомних електростанцій та вимоги до програм безпеки для комп'ютерних систем стосовно захисту інформації та систем управління на базі мікропроцесорів. Інший стандарт *IEC 62859* [7] встановлює вимоги до координації безпеки та кібербезпеки атомних електростанцій і формує основу для управління взаємодією між безпекою та кібербезпекою.

Таким чином *IEC* та Міжнародна організація зі стандартизації (*International Organization for Standardization, ISO)* формують нині довідкову архітектуру, яка включає в себе численні стандарти щодо безпеки критичної інфраструктури. Міжнародні стандарти виступають у вигляді технологічної платформи для інновацій з новими цифровими технологіями та рішеннями і слугують ключовими інструментами для захисту критичної інфраструктури. В Україні однією з платформ обміну технологічною інформацією стосовно кібератак є система *MISP-UA*, яка спрямована на налагодження прямої взаємодії з бізнесом в режимі онлайн в питаннях підвищення рівня кібербезпеки та загальної культури кіберзахисту. Розробниками міжнародних стандартів, які захищають певні домени та забезпечують безпеку промисловості та критично важливих об'єктів інфраструктури виступають технічні комітети стандартизації (*Technical Committees, TC*):

- *IEC TC 57 :* Енергетичні системи управління та пов'язаний з ними обмін інформацією (стандарти серії *IEC 61850* та *IEC 60870*);
- *IEC TC 65* : Вимірювання, контроль та автоматизація промислових процесів (стандарти серії *IEC 62443*);
- *IEC TC 80* : Морське навігаційне обладнання та системи радіозв'язку (стандарти серії *IEC 61162*) та ін.

Міжнародні стандарти *IEC* та *ISO* все частіше гармонізуються державами, що призводить до посилення загальної безпеки, проте не повністю відповідають на потреби окремих організацій. Підхід, що ґрунтується на оцінці ризику, є більш ефективним, особливо якщо він базується на оцінці існуючих або потенційних внутрішніх вразливостей та виявлених або можливих зовнішніх загроз. Такий нейтральний підхід передбачає різні види оцінки відповідності і застосовується як частина цілісного системного підходу, який поєднує стандарти з тестуванням та сертифікацією (оцінкою відповідності). Системний підхід відображає інтерактивний характер та взаємозалежність зовнішніх та внутрішніх факторів і базується на основній ідеї про те, що окремі стандарти дійсно ефективні, коли вони становлять частину цілісної стратегії, що є важливою

складовою будь-якої стратегії кіберзахисту, зокрема, критичної інфраструктури.

Приміром, відповідно до серії стандартів *IEC 62443* для кібербезпеки сектору промислової автоматизації надається стандартизована форма тестування та сертифікації. Таким чином, *IEC* забезпечує структуру, яка включає в себе численні стандарти, що охоплюють різні операційні технології та технології *IoT*. Понад 200 розроблених нині *IEC* стандартів з кібербезпеки дозволяють організаціям підвищувати стійкість перед швидкозростаючими загрозами безпеки мереж.

В той же час спостерігається зростання кількості кібератак на об'єкти критичної інфраструктури. Низка потужних та складних кібератак на комп'ютерні мережі енергетичного, банківського, транспортного секторів, галузі зв'язку, які відбулись з початку 2014 року, вкотре засвідчили, що кібератаки використовуються як інструмент геополітичного впливу. Протидія цьому потребує не тільки зусиль на національному рівні, але й відпрацювання дієвих механізмів нормативного забезпечення захисту критичної інфраструктури

Список використаних джерел:

1. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки : розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/67-2018-%D1%80/page
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/eli/dir/2016/1148/oj
3. ISO/IEC 27000 Information security management systems [Електронний ресурс]. – Режим доступу : https://www.iso.org/isoiec-27001-information-security.html
4. ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls [Електронний ресурс]. – Режим доступу : https://www.iso.org/ru/standard/54533.html
5. IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements [Електронний ресурс]. – Режим доступу : https://webstore.iec.ch/publication/33615
6. IEC 62645:2014 Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems[Електронний ресурс]. – Режим доступу : https://webstore.iec.ch/publication/7311
7. Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity [Електронний ресурс]. – Режим доступу : https://webstore.iec.ch/publication/26131
8. Національний інститут стратегічних досліджень - Щодо створення державної системи захисту критичної інфраструктури. Аналітична записка [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/2490/

УДК 004.056.52

Максимів Тарас Борисович
аспірант
ТНТУ ім. Івана Пулюя, Україна

ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕДИЧНИХ ЗАКЛАДАХ

Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку. Відомо дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку зовнішніх порушників, так і з боку внутрішніх порушників.

Радикальне вирішення проблем захисту електронної інформації може бути отримано тільки на базі використання криптографічних методів, які дозволяють вирішувати найважливіші проблеми захищеної автоматизованої обробки та передачі даних. При цьому сучасні швидкісні методи криптографічного перетворення дозволяють зберегти вихідну продуктивність автоматизованих систем. Криптографічні перетворення даних є найбільш ефективним засобом забезпечення конфіденційності даних, їхньої цілісності і справжності. Тільки їх використання в сукупності з необхідними технічними та організаційними заходами можуть забезпечити захист від широкого спектру потенційних загроз.

Проблеми, що виникають з безпекою передачі інформації при роботі в комп'ютерних мережах, можна розділити на три основні типи:

– Перехоплення інформації - цілісність інформації зберігається, але її конфіденційність порушена;

– Модифікація інформації – вихідне повідомлення змінюється або повністю підміняється іншим і відсилається адресату;

– Підміна авторства інформації.

Підходи до побудови системи захисту персональних даних у всьому світі є стандартними і практично завжди включають такі етапи як обстеження, класифікація ІСПДн, формування вимог до системи захисту ІСПДн, проектування, введення в дію засобів захисту, атестація. Недостатній рівень автоматизації медичних установ впливає на захист персональних даних.

Перша особливість проектів по захисту персональних даних в медичних установах полягає в необхідності більш детального аналізу бізнес-процесів установи на предмет виявлення наявності або відсутності ознак обробки персональних даних.

Інформація в багатьох установах може зберігатися на паперових носіях; окремі лікарі можуть вести облік пацієнтів у Microsoft Word, при передачі даних по страховим програмам до тепер використовується Excel, в таких установах можуть використовуватися самописні програми.

Більше половини форм облікових та звітних документів типового лікувального закладу містять персональні дані. Належить докладніше аналізувати функціональну структуру лікувального закладу та схеми взаємодії його підрозділів, а також взаємодію з зовнішніми організаціями. При реалізації проектів з захисту персональних даних всі процеси взаємодії повинні бути регульовані та застосовуватися засоби забезпечення безпеки при передачі даних.

Друга галузева особливість захисту персональних даних у медичних установах полягає в тому, що дані обробляються в таких установах зазвичай відносять до найвищої категорії захисту, тому і вимоги до таких систем є найжорстокіші. Щоб мінімізувати витрати на побудову системи захисту персональних даних в медичних установах зазвичай застосовують диференціювання вимог. Диференціація вимог означає управління доступом даними. Наприклад, далеко не всім користувачам у процесі виконання службових обов'язків потрібні всі дані по пацієнтам: реєстраційні, фінансові, медичні.

Також зазвичай вводять можливість використання певних кодів-ідентифікаторів. Наприклад, при передачі даних по каналам зв'язку (в розподілених системах, або в інші організації) можуть передаватися тільки не всі дані, а тільки частина. При цьому прив’язка до конкретної особи може здійснюватися не за ПІБ особи, а за якимось ідентифікатором. У такому випадку перехват даних в каналі зв'язку не дозволить ідентифікувати за даними конкретну особу, а це в свою чергу дозволить зняти досить серйозні (витратні) вимоги щодо криптографічного захисту.

І третя можливість це використання вбудованих в прикладні інформаційні системи засобів, що забезпечують захист персональних даних. Це дозволяє знизити витрати на придбання додаткових засобів захисту. Необхідно врахувати, що такі засоби в більшості медичних інформаційних систем розробники реалізують, але вони найчастіше не задовольняють вимогам.

Будь-який розгляд клінічних даних як суспільного блага викликає питання щодо безпеки в цілому та безпеки окремих записів пацієнтів. Підтримання конфіденційності записів даних має першорядне значення.

Список використаних джерел

1. Разграничение доступа [Електронний ресурс]/Sernam. – Режим доступу: URL: http://sernam.ru/ss_24.php.

2. Проблеми захисту інформації в комп`ютерних мережах [Електронний ресурс]/ Ua-Referat. – Режим доступу: URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5101/1/AUConferenceCyberSecurity_November2016_p79.pdf

УДК 34.096

Любохинець Лариса Сергіївна
кандидат економічних наук, доцент,
завідувач кафедри економічної теорії
Хмельницький національний університет
Мейш Алла Василівна
кандидат економічних наук,
доцент кафедри економічної теорії
Хмельницький національний університет

ФАКТОРИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КРИТЕРІЇ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В СУЧАСНОМУ КІБЕРПРОСТОРІ

В сучасному глобалізованому суспільстві інформація стала чинником зростання вразливості суспільних процесів, дезорганізації державного управління, умовою виникнення великомасштабних аварій, військових конфліктів, стихійних лих. Сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері визначають як загрози інформаційній безпеці, які носять комплексний характер і в загальному вигляді включають загрози безпеці інформації та інформаційної інфраструктури, безпеці суб'єктів інформаційної сфери й соціальних зв'язків. Кожній із загроз безпеці в різних сферах інформаційного життя необхідно протиставити певні заходи, способи, методи їх нейтралізації, захисту інформаційного ресурсу, баз даних, національного інформаційного простору. Фактори загроз інформаційній безпеці поділяють за видовою ознакою на політичні, економічні та організаційно-технічні.

З метою захисту інформації від несанкціонованого доступу, створення захисних систем та оцінки ступеня захищеності використовують систему критеріїв захищеності інформації. Для характеристики основних критеріїв інформаційної безпеки досить часто застосовують модель тріади CIA: конфіденційності, цілісності та доступності. При цьому забезпечення доступності, цілісності та конфіденційності кіберпростору стало однією з глобальних проблем XXI століття та метою ефективного функціонування держави, економіки та суспільства в цілому.

Наряду з моделлю CIA для характеристики критеріїв інформаційної безпеки використовують такі фактори, як апелювання (можливість доведення авторства конкретної особи), підзвітність (можливість фіксації діяльності користувачів інформаційної системи), достовірність (ступінь об'єктивного, точного відображення подій та фактів, що мали місце в визначений період часу), автентичність (гарантування ідентичності заявленим суб'єктам або ресурсам).

Отже, забезпечення інформаційної безпеки сьогодні вимагає пошуку перспективних шляхів тісної взаємодії й координації державних та недержавних структур у системі національної безпеки, посилення контролю та стратегії забезпечення інформаційної безпеки.

УДК 657:004.056

Гнатченко Тетяна Олександрівна
програміст бази даних ERP-системи
ДП «Профітрейд»
Палій Марія Олегівна
студентка 3 курсу 6 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБЛІКОВОЇ ІНФОРМАЦІЇ

Протягом останніх років все ширше використання перспективних інформаційних технологій зумовило не лише численні переваги, а й цілу низку проблем. Істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових форм кібератак.

Гарантування максимально стабільного ефективного функціонування та розвитку будь-якого підприємства є основним завданням безпеки його економічної інформації. Сьогодні більшість суб'єктів господарювання використовують комп'ютеризовану форму ведення бухгалтерського обліку, яка передбачає використання спеціалізованого програмного забезпечення та технічних засобів, тому головним пріоритетом захисту облікової інформації на підприємстві є розроблення заходів, спрямованих на збереження інформації, що міститься у комп'ютерних базах підприємства.

Питання кібербезпеки мають бути у порядку денному кожного підприємства незалежно від його масштабів, рівня складності і характеру комерційної діяльності, а також усвідомлені усіма співробітниками підприємства.

У визначення «кібербезпека» за основу покладаємо розуміння поняття «безпека», що означає стан, коли кому-небудь або чому-небудь ніщо не загрожує [1]. Таким чином, кібербезпека на підприємстві - це стан, за якого забезпечуються принципи доступності, цілісності та конфіденційності даних, що обертаються в інформаційних системах.

Власник підприємства особисто визначає склад цінної інформації, відповідні способи та засоби захисту. Система захисту інформації повинна бути багаторівневою з ієрархічним доступом до інформації, конкретизованою і прив'язаною до специфіки підприємства щодо методів та засобів захисту, відкритою для постійного оновлення, надійною як у звичайних, так і в екстремальних ситуаціях, не повинна створювати співробітникам підприємства незручностей у роботі [2].

У системі інформаційної безпеки облікових даних підприємства кібербезпека забезпечується завдяки регламентації: доступу до електронних документів з використанням персональних паролів; спеціальних засобів і продуктів програмного захисту (спеціалізоване програмне забезпечення);

криптографічних методів захисту інформації (шифрування тексту під час пересилки електронною поштою тощо).

Виходячи з ключового правила ведення обліку «кожний господарський факт має бути зафіксований у документі», очевидно, що кіберзахист облікової інформації реалізується через формування документообігу і використання в обробленні та зберіганні документів технологічної системи, що забезпечує захищеність інформації на будь-якому пристрої чи носії. Таким чином, також уможливлюється контроль конфіденційності на різних етапах обробки даних обліку на підприємстві.

На жаль, не завжди керівництво приділяє достатньо уваги захисту облікової інформації від кібератак. Проте, останні події, які відбулися в Україні в умовах ведення гібридної війни, засвідчили високий рівень інформаційних загроз.

Так, для підприємств, які обрали для подачі звітності веб-сервіс «СОТА», представлений розробниками програми «M.E.Doc», наслідки кібератаки з використанням вірусу «Petya.A» були набагато складнішими, ніж для тих, хто надав перевагу власне програмі «M.E.Doc». Якщо на підприємстві використовувалося офф-лайн програмне забезпечення, то за умови відключення від мережі Інтернет була можливість працювати в програмному забезпеченні на основі створених попередньо архівів. Якщо ж використовувалося он-лайн програмне забезпечення, то можливість подальшої роботи в програмі до тих пір, поки не будуть усунуті наслідки кібератаки, неможливе. За такої ситуації в умовах підвищеного рівня кібератак використання веб-сервісів в Україні не є виправданим [3].

Отже, завдання організації кіберзахисту і безпеки даних бухгалтерії полягає у забезпеченні комплексу організаційних, технічних, правових та кадрових заходів. Головне місце у забезпеченні кібербезпеки посідають засоби захисту у вигляді програм або пакетів програм, що розширюють можливості стандартних операційних систем, а також систем керування базами даних. Рекомендується утриматися від використання хмарного програмного забезпечення для ведення обліку та подання звітності, а віддавати перевагу програмам та базам даних, що встановлюються безпосередньо на робочі пристрої і мають відповідну систему контролю доступу до облікової інформації.

Список використаних джерел:

1. Клименко В. Внутрішні загрози інформаційній безпеці організації / В. Клименко // Вісник НБУ. – 2008. – № 5. – С. 62-63.
2. Шпак В. А. Організація захисту облікової інформації / В. А. Шпак // Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. - 2015. - № 2. - С. 181-187.
3. Грабчук І.Л. Організація захисту облікової інформації в умовах гібридної війни / І.Л. Грабчук // Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу. – 2018. - № 3 (41). – С. 20-24.

УДК 004.056

Фомічова Наталя Вікторівна
Торговельно-економічний коледж Київського національного торговельно-економічного університету

СПЕЦИФІКА ЗАХИСТУ ІНФОРМАЦІЇ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Однією з невід'ємних складових управління сучасним підприємством є управління інформаційною безпекою. Забезпечення інформаційної безпеки є стратегічним завданням будь-якого підприємства, компанії.

Під інформаційною безпекою розуміють захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати збитків суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації та інфраструктури, що їх підтримує [1].

Для реалізації інформаційної безпеки необхідно використовувати захист інформації – комплекс різних заходів, що забезпечують цілісність, конфіденційність та доступність інформації. Система заходів захисту інформації має бути спрямована не тільки на подолання загроз та ризиків, але й передбачати та запобігати їх настання.

Характерною ознакою сучасних закладів вищої освіти є наявність високотехнологічного обладнання, створення глобальних інформаційно-комунікаційних мереж, що дозволяють використовувати різні інформаційні ресурси в освітньому процесі. Основними ризиками при використанні інформаційних ресурсів закладів вищої освіти варто відзначити такі: неконтрольований доступ до інформаційних ресурсів, низька захищеність від внутрішніх та зовнішніх загроз, незаконне копіювання інформації, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних в інформаційних системах, викрадення інформації з бібліотек, архівів, баз даних, перехоплення інформації в технічних каналах її витоку [3].

Зважаючи на вищевикладене, особливої актуальності набуває питання удосконалення управління інформаційними ризиками при використанні інформаційних ресурсів, аналіз та дослідження загроз інформаційної безпеки закладу вищої освіти, виявлення порушників інформаційної безпеки та застосування запобіжних заходів з метою попередження порушень цілісності, доступності та конфіденційності інформації.

Типовими категоріями порушників інформаційної безпеки закладів вищої освіти є особи, що приймають активну участь у життєдіяльності закладу, а саме студенти, співробітники, відвідувачі, хакер та групи хакерів, конкуренти, злочинні угрупування та організації [3].

Студенти є найбільш вагомою частиною закладу вищої освіти, тому спостереження за їх поведінкою, мотивами діяльності, тактикою дозволяє попередити ризики кібербезпеки. Серед можливих загроз з боку студентів

можна виділити такі: зараження вірусами мережі, блокування мережі, неконтрольований вихід в Інтернет, нецільове використання інформаційних ресурсів, підробка екзаменаційно-залікових відомостей, залікових книжок, наявність плагіату в курсових та дипломних роботах.

Основними загрозами з боку співробітників закладу вищої освіти є розголошення службової таємниці, що може призвести до зниження іміджу або нанести шкоду діяльності закладу вищої освіти; недбалість, халатність і безвідповідальність співробітників, ненавмисні помилки при використанні цифрових технологій у зв'язку з низькою кваліфікацією, слабоконтрольований вихід в Інтернет, який можна регулювати шляхом встановлення певних обмежень доступу.

Відвідувачі не мають прямого доступу до інформаційних ресурсів закладів вищої освіти, тому їх можливості обмежені, проте загрози можливі при безвідповідальному ставленні співробітників закладу до захисту інформаційних ресурсів.

Хакер та групи хакерів використовують стандартні або власно розроблені програми отримання доступу до конфіденційної інформації, до серверів, систем адміністрування, управління інформаційною системою. Такі дії приводять до пошкодження цілісності мережі, призупинення освітнього процесу, потужних атак з повним виводом з ладу інформаційних систем закладу, що завдає певних матеріальних збитків.

Конкуренти мають на меті отримання інформації про комерційну таємницю, про функціонування інформаційної системи закладу вищої освіти як за допомогою використання власних потужних цифрових засобів, так і шляхом підкупу співробітників закладу вищої освіти.

Злочинні угрупування та організації представляють серйозну загрозу не тільки для інформаційної системи, а й для закладу вищої освіти в цілому. Такі угрупування найчастіше використовують соціальні мережі для залучення молоді та мають суттєвий вплив на їх свідомість.

Отже, своєчасне виявлення загроз та порушників інформаційної безпеки дозволяють побудувати таку систему управління інформаційними ризиками та захисту інформації в закладах вищої освіти, яка зможе захищати не тільки інтереси студентів, науково-педагогічних працівників закладу вищої освіти, а і національних інтересів країни.

Список використаних джерел:

1. Ахрамович В.М. Адміністративний рівень інформаційної безпеки // Сучасний захист інформації. - №1, 2017, с. 10-14
2. Доктрина інформаційної безпеки України, затверджена наказом Президента України від 25 лютого 2017 № 47/2017 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/47/2017#n12
3. Ільїн О.О. Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки // Ільїн О.О., Сєрих С.О., Вишнівський В.В. Сучасний захист інформації.- №1, 2017, с.66-72.

НАУКОВИЙ НАПРЯМ 2
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

SCIENTIFIC AREA 2
INFORMATION TECHNOLOGIES OF
THE STRUGGLE WITH CYBERCRIME

УДК 004.056

Чубаєвський Віталій Іванович
кандидат політичних наук,
доцент кафедри програмної інженерії та кібербезпеки КНТЕУ,
полковник поліції,
заступник начальника Департаменту кіберполіції Національної поліції України
Семенюк Дмитро Володимирович
начальник відділу кібербезпеки управління протидії злочинам у сфері інформаційної безпеки Департаменту кіберполіції національної поліції України, підполковник поліції

ВИКОРИСТАННЯ КОМПЛЕКСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВІЗУАЛІЗАЦІЇ ЗВ'ЯЗКІВ ОБ'ЄКТІВ АНАЛІЗУ ЗНАЧНИХ МАСИВІВ ІНФОРМАЦІЙНИХ ДАНИХ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ З ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На сьогоднішній день у нашому житті практично не залишилось галузей в суспільстві, де не використовуються інформаційні технології, комп'ютеризовані комплекси тощо. Всі ці системи оперують певними масивами даних, які рано чи пізно виникає необхідність аналізувати. І якщо у деяких сферах (фінансового, технічного характеру тощо) існують такі механізми, якими хоча б частково можна автоматизувати аналіз інформації, то в частині кримінального аналізу таких механізмів обмаль.

У рамках наданих повноважень працівники поліції здобувають достатній масив даних, що містить інформацію про злочинну діяльність як окремих суб'єктів, так і організованих злочинних груп. У зв'язку з цим, надважливим на сьогодні є застосування аналітичних інструментів, які б надали можливість оперативно опрацьовувати високооб'ємні дані, а також виконувати автоматизовані аналітичні функції. Одним із таких інструментів є кримінальний аналіз. Кримінальний аналіз – встановлення та передбачення зв'язків між даними про злочинну діяльність та іншими, потенційно з ними пов'язаними даними з метою їх використання у розробленні тактичних та стратегічних засад з протидії злочинності.

Кримінальний аналіз, можна розглядати як специфічний вид інформаційно-аналітичної діяльності, яка полягає в ідентифікації і якомога точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються злочину, та будь-якими іншими даними, отриманими з різних джерел, і їх використанням в інтересах ведення оперативно-розшукової діяльності, досудового розслідування та їх аналітичної підтримки [1].

У ході кримінального аналізу забезпечується цілеспрямоване збирання/здобування, упорядкування, фіксація, аналіз та оцінка кримінальної інформації, її представлення (візуалізація), передача та реалізація. У країнах

Європейського Союзу, США та інших країнах світу провадження кримінального аналізу є загальнообов'язковим для всіх правоохоронних органів та відіграє досить вагоме значення у попередженні та розкритті злочинів. Його зміст, правила та процедура чітко визначено та врегульовано у правовому відношенні. Це, зокрема стосується ведення оперативно-розшукової діяльності, слідства та розгляду кримінальних справ у суді.

Відповідно кримінальним аналізом займаються і такі міжнародні структури як Інтерпол та Європол. Кримінальний аналіз в сфері протидії кіберзлочинності досить складний процес[3]. Деякі з цих завдань вирішуються з використанням програмного забезпечення обробки електронних таблиць, інші можна реалізувати за допомогою графічних редакторів, треті – використовуючи спеціалізоване програмне забезпечення. Враховуючи великі об'єми інформації, на все це необхідно витратити велику кількість часу, до того ж результати, отримані з різних програм матимуть різні формати, дані з яких потім дуже складно аналізувати та приводити до одного цілого.

На сьогодні одним з найкращих аналітичних продуктів є програмне забезпечення, яке дозволяє опрацьовувати великі об'єми розрізненої інформації та видавати результат у наглядному вигляді в найкоротший термін. Спеціалізовані візуальні аналітичні середовища, які дозволяють максимально ефективно використовувати величезні обсяги інформації, накопичені державними службами та підприємствами, дозволяють аналітикам швидко зіставляти, аналізувати і наочно представляти дані з різних джерел, скорочуючи час на пошук важливої інформації в складних даних. Таке програмне забезпечення надає актуальні і дієві аналітичні засоби що допомагають виявляти, передбачати, запобігати і припиняти злочинну, транскордонну і міжрегіональну резонансну діяльність.

Отже, за допомогою комплексного програмного забезпечення для візуалізації зв'язків об'єктів аналізу можна:

- швидко систематизувати розрізнені дані в єдине узгоджене подання.
- визначити ключових осіб, подій, зв'язків і закономірностей, які не завжди можна виявити іншими способами.
- отримати розуміння структури, ієрархії і способів дій злочинних організацій.

Список використанихджерел:

1. Закон України «Про основні засади забезпеченнякібербезпекиУкраїни». Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/2163-19
2. PricewaterhouseCoopersЕлектронний ресурс. URL: https://www.pwc.com.ua/
3. Mobile App Security. [Електроннийресурс]. URL: https://www.arxan.com/resources/technology/mobile-app-security
4. L. Badger, D. Berstein, R. Bohn, F. de Valux, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, US government cloud computing technology roadmap volume 1: High-priority requirements to further USG agency cloud computing adoption, National Institute of Standards and Technology, U.S. Department of Commerce, 2016 – 150 c.

УДК 004.056

Леонтьєв Ігор Андрійович
Chief Cloud Solutions Architect
VISEO
Бакал Анатолій Миколайович
Microsoft MVP Office Apps and Services, Veeam Vanguard, ISO/IEC 27001 Lead Auditor Principal Technology Strategist, Elcore Group
Вовченко Єлизавета Юріївна
Microsoft Alliance Manager
VISEO

ВИКОРИСТАННЯ ХМАРНИХ СИСТЕМ УПІБ (SIEM) ДЛЯ УПРАВЛІННЯ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

Управління безпекою на підприємстві може бути нескінченною сагою. Хроніки подій показують, що кількість атак на інформаційні ресурси зростає щодня, причому збільшуються, безпосередньо, як кількість, так і складність цих атак. Саме тому системи УПІБ (Управління подіями інформаційної безпеки – Security information and event management) грають дуже важливу роль у побудові першого рівня відбиття атак на безпеку.

Команди управління безпекою завантажені вкрай великим обсягом сповіщень і витрачають занадто багато часу на виконання завдань іншого рівня, таких як створення інфраструктури та обслуговування. Як наслідок, багато легітимних загроз залишаються непоміченими.

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

- протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
- порушення встановлених регламентів збору, обробки та передачі інформації;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем;
- помилки в проектуванні інформаційних систем;
- відмова технічних засобів і збоїв програмного забезпечення в інформаційних і телекомунікаційних системах тощо [1].

Також необхідно враховувати, що загроза інформаційним системам підприємства може настати з боку наступних суб'єктів:

- працівники підприємства, що використовують своє службове становище (коли законні права за посадою використовуються для незаконних операцій з інформацією);
- працівники підприємства, що не мають права в силу своїх службових обов'язків, але здійснили несанкціонований доступ до конфіденційної інформації;
- особи, які не пов'язані з підприємством трудовою угодою (контрактом) [2].

Очікуваний недолік фахівців-професіоналів з безпеки оцінюється приблизно в 3,5 млн. до 2021року і саме він сприятиме подальшому збільшенню викликів для оперативних команд з безпеки[3]. Саме тому

виникає потреба у рішенні, яке надасть змогу існуючій команді управління безпекою побачити більш очевидні загрози та усунути відволікання.

Одним з таких рішень є Microsoft Azure Sentinel[4], яке забезпечує розумну аналітику безпеки в масштабах хмар для всього підприємства. Azure Sentinel дозволяє легко збирати дані безпеки в рамках гібридної організації – від пристроїв до користувачів, додатків, серверів будь-якої хмари. Рішення використовує силу штучного інтелекту, щоб забезпечити швидке виявлення реальних загроз і вивільнити людські ресурси від тягаря традиційних УПІБ, усуваючи необхідність витрачати час на створення, підтримку та масштабування інфраструктури.

Оскільки рішення побудовано на хмарі Azure, воно пропонує широкі масштаби та швидкість для задоволення потреб безпеки. Традиційні УПІБ системи на початку експлуатації виявляються достатньо дорогими, так як часто вимагають від організації заздалегідь сплачувати високу вартість обслуговування інфраструктури та прийому даних. З використанням Azure Sentinel попередні витрати відсутні, а оплата відбувається за фактично використовувані ресурси[5].

Також досить важливим моментом є те, що багато підприємств використовують програмний пакет Office 365 та у його рамках все частіше використовують розширені пропозиції щодо безпеки та відповідності, включені до пакету Microsoft 365. Azure Sentinel дає можливість перенести свої дані про діяльність Office 365 до Azure Sentinel.

Так, питання безпеки інформаційних ресурсів на підприємстві має стояти серед питань оперативного вирішення, а не бути чимось довготривалим і недосяжним. Виходячи з вищесказаного, можливим вирішенням цієї проблеми є використання системи Microsoft Azure Sentinel, що дозволить зменшити час перебування загроз інформаційній системі підприємства без додаткових витрат.

Список використаних джерел:

1. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування / [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf.
2. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства / [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/ Vntu/2009_19_1/pdf/64.pdf (дата звернення 11.03.2019).
3. Cybersecurity Jobs Report 2018-2021 [Електронний ресурс] // Сайт Cybersecurity Ventures. – Режим доступу: https://cybersecurityventures.com/jobs (дата звернення 12.03.2019).
4. Azure Sentinel : офіційна сторінка сервісу [Електронний ресурс] // Сайт Microsoft. – Режим доступу: https://azure.microsoft.com/en-us/services/azure-sentinel (дата звернення 12.03.2019).
5. Вихідний код сервісу Azure Sentinel [Електронний ресурс] // Сайт GitHub. – Режим доступу: https://github.com/Azure/Azure-Sentinel.

УДК 004.056.5

Терейковський Ігор Анатолійович
доктор технічних наук, професор, професор кафедри системного програмування і спеціалізованих комп'ютерних систем
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Терейковська Людмила Олексіївна
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій проектування та прикладної математик
Київський національний університет будівництва і архітектури
Терейковський Олег Ігоревич
студент
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

НЕЙРОМЕРЕЖЕВІ ТЕХНОЛОГІЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

В даний час у галузі захисту інформації одним із найдинамічніших напрямів розвитку є розробка нейромережевих засобів біометричної аутентифікації користувачів. Найбільшого поширення набули системи, що ідентифікують користувача на підставі аналізу таких біометричних ознак людини, як геометрія рук, вух, обличчя, кровоносних судин на руках або поверхні очного дна, а також шкірних покривів пальців користувача.

Базуються ці системи на унікальності та постійності означених біометричних ознак, а їх основними перевагами є зручність використання, висока точність класифікації, апробованість і низька вартість зчитувальних пристроїв. Разом з тим, практичний досвід, а також результати робіт [1, 2] вказують на необхідність суттєвої модернізації сучасних біометричних нейромережевих систем аутентифікації в напрямку зменшення ресурсоємності, збільшення точності розпізнавання, скорочення часу розробки і підвищення адаптації до багатьох особливостей сучасних інформаційних систем. При цьому результати аналізу сучасних нейромережевих рішень дозволять стверджувати, що важливим напрямком підвищення їх ефективності є адаптація структури моделі до умов використання.

Оскільки джерелом інформації є двовимірне зображення, то для розпізнавання слід використовувати згорткову нейронну мережу (ЗНМ), основу математичного забезпечення якої складають вирази [1]:

$$x_k^{(i,j)} = f\left(x_{0,k} + \sum_{s=1}^{K}\sum_{t=1}^{K} w_{k,s,t} x^{((i-1)+s,(j+t))} \right), \quad (1)$$

$$y = \max(0, x), \quad (2)$$

$$y_i = \exp(q_i) \Big/ \sum_{k=1}^{L_{out}} \exp(q_k), \quad (3)$$

де $x_k^{(i,j)}$ - вхідний сигнал (*i,j*)-го нейрону *k*-ої карти ознак, $x_{0,k}$ - зміщення нейронів *k*-ої карти ознак, K - розмір рецептивної області нейрону, $w_{k,s,t}$ - ваговий коефіцієнт (*s,t*)-го зв'язку нейрона k-ої карти ознак, x - вихід нейрону попереднього шару, y_i - вихід і-го нейрону вихідного шару, q_k - сумарний вхідний сигнал для k-го нейрону вихідного шару, L_{out} - кількість вихідних нейронів, *y* - вихідний сигнал нейрону карти ознак.

Основними конструктивними параметрами ЗНМ є розмір вхідного поля, кількість вхідних нейронів, кількість вихідних нейронів, кількість нейронів в повнозв'язному шарі, кількість шарів згортки, кількість карт ознак в кожному шарі згортки, кількість шарів підвибірки, масштабний коефіцієнт для кожного шару підвибірки, розмір ядра згортки, зміщення рецептивного поля при виконанні кожної процедури згортки, розмір карти ознак для кожного k-го шару згортки, структура зв'язків між сусідніми шарами згортки/підвибірки.

Адаптувати структурні параметри ЗНМ пропонується виходячи з того, що в системах біометричної аутентифікації процес розпізнавання геометрії біометричних ознак повинен бути максимально наближений до свого біологічного прототипу. Це дозволило запропонувати наступні принципи адаптації:

- Кількість шарів згортки повинна відповідати кількості рівнів розпізнавання відбитків пальців експертом.
- Кількість карт ознак у n-му шарі згортки має дорівнювати кількості ознак на n-му рівні розпізнавання.
- Карта ознак n-го шару, відповідна j-ій ознаці, зв'язується тільки з тими картами ознак попереднього шару, які використовуються для побудови зазначеної фігури.
- Розмір ядра згортки для n-го шару згортки повинен дорівнювати розміру ознак на n-му ієрархічному рівні.
- Використання шарів згортки не повинно спотворювати геометричні параметри ознак, що використовуються для розпізнавання.

Використавши запропоновані принципи та наведене математичне забезпечення (1-3) розроблено програмний комплекс, призначений для ідентифікації користувача по відбиткам пальців. Система розпізнавання навчалася і тестувалася на вибірці з бази FVC2000 DB1. Досягнута точність розпізнавання на рівні близько 95% відповідає кращим показникам подібних систем, що вказує на перспективність подальших досліджень у даному напрямку.

Список використаних джерел:

1. Руденко О.Г. Штучні нейронні мережі. Навч. посіб. / О.Г. Руденко, Є.В. Бодянський. – Харків: ТОВ "Компанія СМІТ", 2006. – 404 с.
2. Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації / І. Терейковський. - К. : ПоліграфКонсалтинг. - 2007. – 209 с.

УДК 004.056

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент,
доцент, кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Левша Мерседес Геннадіївна
студентка 4 курсу 7 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ЗАХИСТ ІНФОРМАЦІЇ В БАЗАХ ДАНИХ

У сучасному інформаційному суспільстві головним ресурсом є інформація. Комп'ютеризація людства виступає головною сферою автоматизації промислової, управлінської та наукової роботи, де обов'язкові збереження, обробка, отримання, передача і збір в єдине ціле всієї інформації.

Автоматизація на персональних комп'ютерах змінює стандарти переробки даних, надаючи злагоджену роботу промисловості і організацій на базі більш новітньої інформаційної технології.

Застосування персонального комп'ютера у вигляді механізму обробки інформації в різних областях людської діяльності підвищує інформаційну культуру суспільства, сприяючи без ускладнень перейти до інформаційного суспільства, де інформація є найціннішим матеріалом нарівні з фінансовими, енергетичними та іншими ресурсами.

Найсучаснішим засобом для накопичення і пошуку інформації в комп'ютерах є бази даних, що дозволяють організувати зберігання великого обсягу інформації з забезпеченням високої швидкості пошуку і оновлення.

Бази даних є сховищем спеціально організованих і логічно пов'язаних інформаційних елементів, складаються з самих даних і їх опису, являють собою сконструйовану сукупність фактів, що відносяться до певного предмету.

Як забезпечується інформаційна безпека баз даних? Системи управління базами даних стали основним інструментом, що забезпечує зберігання великих масивів інформації. З метою захисту інформації в базах даних найважливішими є наступні аспекти інформаційної безпеки:

- умови доступу (можливість отримати деяку необхідну інформаційну послугу);
- цілісність (несуперечливість інформації, її захищеність від руйнування і несанкціонованого зміни);
- конфіденційність (захист від несанкціонованого читання).

- До основних програмно-технічних заходів, застосування яких дозволить вирішити деякі з перерахованих вище проблем, відносяться:
- аутентифікація користувача і встановлення його ідентичності;
- управління доступом до баз даних;
- підтримання цілісності даних;
- захист комунікацій між клієнтом і сервером;
- відображення загроз, специфічних для СУБД.

Перевірка автентичності користувача додатків бази даних найчастіше здійснюється або через відповідні механізми операційної системи, або через певний SQL-оператор: користувач ідентифікується своїм ім'ям, а засобом аутентифікації служить пароль. Подібна система створює значні складності для повторних перевірок і виключає подібні перевірки перед кожною транзакцією.

Методи захисту баз даних: захист паролем, розмежування прав доступу до об'єктів БД, захист полів і записів таблиць БД.

Захист паролем є простий і ефективний спосіб захисту БД від несанкціонованого доступу. Паролі встановлюються користувачами або адміністраторами БД. Облік і зберігання паролів виконується самою СУБД. Зазвичай, паролі зберігаються в певних системних файлах СУБД в зашифрованому вигляді. Після введення пароля користувачу СУБД надаються всі можливості по роботі з БД.

Права доступу визначають можливість дії над об'єктом. Власник об'єкта – це користувач, який створив об'єкт, може надавати різні рівні доступу до створеного об'єкту..

Бази даних є домінуючим інструментом для зберігання структурованої інформації. Зростаючі масштаби крадіжок критично важливих даних роблять все більш актуальною необхідність в захисті баз даних.

Особливо значущим є створення системи захисту від внутрішніх зловмисників. Система захисту БД грає важливу роль в автоматизації контролю над діями користувачів, що працюють з базами даних, захисту від зовнішніх і внутрішніх загроз і підвищенні надійності функціонування баз даних.

Список використаних джерел

1. Куваєв Я.Г. Організація реляційних баз даних : навч. посіб. / Я.Г. Куваєв, О.А. Жукова, І.А. Сечкін – 2-ге вид., допов. та переробл. – Дніпро : НГУ, 2017. – 157 с..

2. Тарасов, О. В. Використання мови SQL для роботи з сучасними системами керування базами даних. Практикум з навчальної дисципліни "Організація баз даних та знань" [Текст] : навч.-практ. посіб. / О. В. Тарасов, М. Ю. Лосєв, В. В. Федько. - Харків : ХНЕУ, 2013. - 347 с.

УДК 004.056:004.89

Гнатченко Дмитро Дмитрович
асистент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Шапочка Денис Вікторович
студент 3 курсу 6 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ПЕРЕВАГИ СИСТЕМ КІБЕРЗАХИСТУ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

Завдяки розвитку інформаційних технологій та Інтернету загалом виникають проблеми, пов'язані із забезпеченням кібербезпеки користувачів. Мережа Інтернет з наукового інструментарію перетворилася на одну з головних інфраструктур інформаційної спільноти світу. Всесвітню мережу застосовують як уряди для інформування громадян, так і компанії для обміну інформації між своїми підрозділами, партнерами та клієнтами для підвищення ефективності бізнес-діяльності. Навчальні та наукові заклади використовують мережу для дистанційного навчання та як платформу для співпраці, та для швидкого обміну інформацією.

Але зі зростанням і поширенням Інтернет-мереж зростала і кількість атак. Не так давно утворився термін «кібернетичний тероризм», тобто загрози стали організованими та навіть спрямованими на ІТ-інфраструктури деяких держав. Так, захищеність Інтернет-мереж стала питанням безпеки не тільки бізнесу, але і держав. Тож, дослідження шляхів захисту від кібератак у мережі є важливим та актуальним.

За останні роки комп'ютерні та мережеві технології розвинулися, збільшилась як кількість користувачів, так і складність побудови сервісів для їх обслуговування. Але разом з розширенням систем з'явились і вразливості різного роду. Навіть фактор зростання мобільності користувачів значно ускладнює побудову сервісів та їх захист, адже це робить їх поведінку непередбачуваною, бо зі зміною точки підключення зміниться і конфігурація мережі, тоді усі зібрані раніше характеристики стануть недостовірними. Але і сама поява нових вразливостей і типів атак впливає на складність побудови сервісів.

Нинішній розвиток вказує на те, що подальшим напрямком буде створення мережі з інтелектуальними компонентами, що дозволить досягти більшої автономності та адаптивності, стане можливим, завдяки взаємодії системи захисту з цими компонентами, оцінювати кіберзагрози і обирати ефективні методи виявлення і боротьби з ними.

Як висновок, є необхідність в розробці систем виявлення і захисту, які могли б задовольнити такі вимоги:

– ефективність функціонування: висока надійність виявлення, швидкість роботи, стійкість до фальшивих виявлень;

– масштабованість: розширення або зміна конфігурації системи мають автоматично враховуватися;

– адаптивність: поява нових видів атак або зміна характеристик роботи не має призводити до необхідності перепрограмування системи [3].

Інтелектуальні інформаційні системи поділяють на групи, в залежності від концепції, на якій заснована така система, а саме: статистичний аналіз даних; засоби інтелектуалізації доступу до бази даних; евристичне вирішення завдань діагностики та прогнозування на основі застосування експертних систем; аналіз та прогнозування на основі використання нейронних мереж, а також баз знань прецедентів; програмні засоби динамічного планування на основі case-технологій тощо.

Та, як базис для створення систем кіберзахисту мереж найбільш доцільним є застосування інтелектуальних агентів, що користуються методами статистичного аналізу та теорії ігор. Досвід використання таких систем описано та обґрунтовано у багатьох роботах. Зокрема, вони є мобільнішими, що відкриває ще ряд необхідних особливостей, таких як адаптивність, автономність, аналіз зібраної інформації, розподіленість, та можливість працювати за непередбачуваних умов мережі чи при навмисній протидії системі. Така система зможе планувати протидії зловмисним діям завдяки базі стратегій, отриманій при аналітичному моделюванні взаємодії, та зібраним даним.

Вивчення інтелектуальних моделей кіберзахисту мереж дозволить чинити ефективну протидію та передбачувати можливі наслідки. Таке моделювання можливе завдяки ігровому аналізу, адже модуляція будується завдяки конфліктній взаємодії між нападниками та системою захисту. Складність таких систем викликає необхідність введення нових припущень, ідеалізації руху, аналіз динаміки, ідеалізацію керувань конфліктуючих груп, та визначення прийнятих стратегій захисту. Ці припущення є складними науковими проблемами, вирішення яких створить передумови для успішної розробки та функціонування інтелектуальних систем кіберзахисту.

Список використаних джерел:

1. Створення комплексної системи захисту інформаційних ресурсів у національній ґрід-інфраструктурі України / А.Г. Загородній, О.М. Боровська, С.Я. Свістунов, І.П. Сініцин, Є.С. Родін – К. : «Видавництво «Сталь», 2014. – 374 с.

2. ISO/IEC 27032:2012 Information technology.Security techniques – Guidelines for cybersecurity / [Електронний ресурс]. – Режим доступу : http://www.iso27001security.com/html/27032.html (дата звернення 10.03.2019).

3. Комплексний підхід до побудови системи кіберзахисту критичної інформаційної інфраструктури держави / І.П. Сініцин, П.П. Ігнатенко, О.О. Слабоспицька, О.В. Артеменко // Проблеми програмування. – 2017. – № 3. – С. 128-148.

УДК 004.056.53

Рассамакін Володимир Якович
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Цьомка Олександр Олександрович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ АПАРАТНИМ ТОКЕНОМ З ПІДТРИМКОЮ СТАНДАРТУ FIDO U2F

В роботі проаналізовані переваги стандартизованої технології U2F як основного методу двофакторної автентифікації.

Двофакторна автентифікація у навіть необізнаних з технологіями ІБ користувачів, асоціює з одноразовим смс-паролем.

Зломи акаунтів соціальних мереж, пошти та інших сервісів - не новина, і часто пов'язані з фінансовими або репутаційними втратами, бо, як правило, зламані облікові записи захищені тільки простим, може і не простим, але все одно одним паролем, без другого фактору автентифікації. Популяризація ж другого чинника в принципі і U2F зокрема призводить до підвищення загального рівня комп'ютерної грамотності та безпеки.

У 2013 році був організований альянс FIDO (Fast IDentity Online) для того, щоб адресувати проблеми легкої і безпечної автентифікації в інтернеті. На даний момент FIDO має більше трьохсот асоціативних членів і тридцять членів правління. У список членів правління входять такі компанії як Google, Yubico, Microsoft, Visa, Mastercard, American Express, Paypal і інші.

Розроблений альянсом FIDO протокол U2F набирає популярність серед інтернет-компаній і показує, що двофакторна автентифікація - не тільки безпечна, але доступна і проста, а головне, зрозуміла для користувача.

Мінусом є те, що користувач повинен сам подбати про посилення рівня автентифікації в своїх улюблених сервісах, а саме, придбати собі апаратний токен, а сервіси, в свою чергу, повинні заздалегідь підтримувати U2F.

Таких сервісів вже досить багато, і список їх постійно збільшується. Спочатку стандарт U2F підтримували Google (gmail, youtube, etc), Dropbox, Github. Зараз приєдналися Facebook, Salesforce, Bitbucket, Dashlane і інші сервіси і компанії.

Якщо сам сервіс не надав можливість прив'язати U2F-ключ в якості автентифікатора, можливо, це можна здійснити через провайдерів

двофакторної автентифікації, наприклад, «duo security», причому доступ можна буде налаштувати не тільки в web-додатки. Строго кажучи, такі хмарні платформи в якості автентифікатора використовують не тільки U2F, та їх можливості набагато ширше.

Так всі співробітники з Google цим успішно і з задоволенням користуються.. На початку 2017 року всі працівники корпорації перейшли на цей спосіб автентифікації своїх акаунтів. Як підсумок – за згаданий рік не відбулося жодної крадіжки особистої інформації.

Один недолік пов'язаний зі смартфонами. Щоб увійти в обліковий запис на ньому, необхідний ключ з Bluetooth або NFC, який коштує трохи дорожче.

Веб-додаток за допомогою браузера контактує з U2F пристроєм за допомогою JavaScript API. Мобільний додаток так само має «спілкуватися» з пристроєм за допомогою API, при побудові якого використовується поняття web origin. Для можливості роботи з різними API вирішено використовувати фасети (facets). Наприклад, додаток Example може мати реалізацію під Android, IOS або веб-додаток. Все це фасети додатки Example.

Facet ID - це ідентифікатор (URI), який призначається для виконання додатку конкретної платформи:

– для веб-додатків визначено в RFC 6454;

– для Android додатків - це URI android: apk-key-hash: <hash-ofapk-signing-cert>;

– для IOS додатків - це URI ios: bundle-id: <ios-bundle-id-of-app>.

AppID - це URL, який вказує на JSON файл, який містить список дозволених facet IDs. AppID є частиною переданих даних при реєстрації і автентифікації, тому для успішного їх проходження потрібно, щоб facet ID був дозволений в списку, що містить facet IDs, пов'язаному з цим AppID.

Можна заключити, що U2F це добре продумана, сильна, відкрита і стандартизована технологія. Вона була успішно протестована співробітниками Google, які на даний момент використовують U2F в якості основного методу двофакторної автентифікації.

Список використаних джерел:

1. Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.: ил. — (Серия «Библиотека программиста»).

2. Скабцов Н. С42 Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.: ил. — (Серия «Библиотека программиста»).

3. Исаев А.Б. Современные технические методы и средства защиты информации: Учеб. пособие. – М.: РУДН, 2008. – 253 с.: ил.

4. Защита информации в компьютерных системах / под ред. д-ра экон. наук Е.В. Стельмашонок, канд. физ.-мат. наук И.Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2017. – 163 с.

УДК 004.056

Цензура Микола Олександрович
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Струк Владислав Сергійович
студент 4 курсу 7 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

РОЗРОБКА МОБІЛЬНИХ ДОДАТКІВ ТА ЇХ ЗАХИСТ

Вже минули часи, коли ноутбук міг важити більше ніж дев'ять кілограмів, наразі ноутбук, смартфон та розумний годинник можуть важити не більше трьох кілограмів, що дає змогу все більшій кількості людей ознайомитись з подібною електронікою.

Сучасні мобільні додатки працюють на різноманітних операційних системах роздрібнюючи ринок користувачів на групи. Велика кількість груп ускладнює розробку програмного забезпечення так як для кожної платформи або груп платформ існує окремі редактори часто маючи різні мови програмування. Зараз існують багато двигунів для розробки кросплатформного програмного забезпечення.

Сучасне програмне забезпечення для мобільних додатків характеризується кросплатформеностю, що забезпечує коректне виконання програми на будь якій апаратній платформі. До плюсів такого підходу можна віднести економічну ефективність, охоплення більшої кількості аудиторії.

Проте кросплатформна розробка як і все інше має і негативні сторони: негативний користувацький досвід, обмеження систем, швидкодія коду та ускладнення логіки додатку.

Для створення кросплатформних мобільних додатків існують спеціальні інструменти та двигуни. В нашій програмі для спрощення процесу розробки була застосована відносно проста мова програмування Lua. Мова Lua з самого початку позиціонувалась як кросплатформова скриптова мова програмування. Оскільки Lua мала на меті бути загальнодоступною мовою розширення, то розробники зосереджувалися на підвищенні швидкості, портативності, розширюваності, та простоті у використанні.

Для програмування мовою Lua можна використовувати як мінімум два рідних середовища: ZeroBrane Studio - багатоплатформне середовище розробки або Decoda – середовище розробки під операційну систему Windows. Завдяки своїй популярності її також підтримують декілька універсальних IDE до списку котрих входять Eclipse та IntellJ IDEA. Також Lua активно використовується у кросплатформних ігрових двигунах. На даний момент Lua входить у топ 20 мов програмування, що вказує на надійність, потужність та великий спектр можливостей мови не зважаючи на її відносну простоту, та легкість освоєння.

У рамках проекту використовується середовища для розробки кросплатформного додатку Corona SDK. Як вказано у назві, Corona SDK це набір засобів розробки, утиліт та документації (software development kit), що дозволяє програмістам створювати програмне забезпечення.

Corona використовує інтегровану мову програмування Lua, а вершиною всього стає C++ та OpenGL для побудови графічних інтерфейсів додатків. За допомогою Corona Simulator додаток створюється безпосередньо з Corona Simulator. Corona Native в свою чергу дає можливість інтегрувати написаний на Lua код та активи у проекти виконані у Xcode або Android Studio для створення власного додатку та включення своїх функцій.

При розробці мобільного додатку слід враховувати, що дані, якими оперує цей додаток, можуть представляти певний інтерес для третіх осіб. Ступінь цінності цих даних варіюється в широких межах, проте, навіть найбільш проста приватна інформація, наприклад, пароль входу в додаток, вимагає опрацювання її захисту.

Сучасні смартфони та планшети містять в собі цілком дорослий функціонал, аналогічний такому у своїх «старших братів». Віддалене адміністрування, підтримка VPN, браузери java-script, синхронізація пошти, заміток, обмін файлами. Все це дуже зручно, проте ринок засобів захисту для подібних пристроїв розвинений ще слабо. Основні проблеми безпеки пов'язані з різноманіттям ОС для мобільних пристроїв, а також, як і кількістю їх версій в одному сімействі.

Основні види атак на мобільний додаток:

• декомпіляція файлу програми (.ipa-файли для Apple iOS і .apk-файли для Google Android) і розбір локально збережених даних;

• перехоплення даних, переданих по мережі (MITM-атаки). Більшість мобільних додатків є клієнт-серверними, отже, постійно передають і приймають великі обсяги інформації. І хоча сучасна мобільна бізнес-процеси активно завершують перехід на HTTPS-протокол спілкування, тим не менш, це не забезпечує повну безпеку;

• рутованія пристрою і атака на додаток і алгоритми які в ньому застосовуються через зовнішні налагоджувальні інструменти.

Перелік основних вразливостей: використання незахищених локальних сховищ; ігнорування факту наявності рутованних або заражених пристроїв; зберігання даних в захищених сховищах, але у відкритому вигляді; переведення частини функціоналу під вбудовані веб-движки.

Список використаних джерел:

1. Ian Dees. Lua // Seven More Languages in Seven Weeks. Languages That Are Shaping the Future / Bruce Tate, Fred Daoud, Jack Moffitt, Ian Dees. — The Pragmatic Bookshelf, 2015. — С. 1—48. — 320 с. — ISBN 978-1941222157.

2. Роберто Иерузалимски. Программирование на языке Lua. — 3-е изд.. — ДМК, 2014. — ISBN 9785940747673. (оригинал: Roberto Ierusalimschy. Programming in Lua. — 3-nd ed. — 2012. — ISBN 9788590379850.)

3. Mário Kašuba. Lua Game Development Cookbook. — Packt Publishing, 2015. — 402 с. — ISBN 978-1849515504.

УДК 374.73

Цюцюра Світлана Володимирівна
доктор технічних наук, професор,
завідувач кафедри інформаційних технологій
Київський національний університет будівництва і архітектури
Ткешелашвілі Давід Леванович
студент 4 курсу 7 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В ІНТЕРНЕТІ

Інформаційна безпека в мережах містить у собі широке коло проблем. Для успішності бізнесу інформаційна безпека має основоположне значення.

Перший напрямок – це забезпечення цілісності даних. Сьогодні вся комерційна інформація, бухгалтерські дані, фінансова звітність, клієнтські бази, договору, новаторські ідеї співробітників фірми, плани і стратегія її розвитку, зберігаються в локальній інформаційно-комп'ютерної мережі.

Далеко не завжди і не всі документи дублюються на паперових носіях, бо обсяг інформації дуже великий. В таких умовах інформаційна безпека передбачає систему заходів, які покликані забезпечити надійний захист серверів і робочих станцій від збоїв та несправностей, що ведуть до знищення інформації або її часткову втрату. Серйозний підхід до даного питання означає, що інформаційна безпека повинна базуватися на професійному аудиті всій IT- інфраструктури фірми.

До пошкодження даних призводить некоректна робота систем архівації, мережевого і прикладного програмного забезпечення.

Наступне найважливіше завдання - забезпечення конфіденційності інформації. Захист комерційних секретів безпосередньо впливає на конкурентоспроможність фірми і її стійкість на ринку. Тут інформаційна безпека і захист мереж стикається із зовнішніми і внутрішніми навмисними погрозами, спрямованими на розкрадання даних.

Хакери, промислове шпигунство і витік інформації з вини власних співробітників становлять найбільшу загрозу. Спокуса продати цінну комерційну інформацію великий не тільки у співробітників, що звільняються, а й у тих, амбіції яких на робочому місці незадоволені. В даному випадку, інформаційна безпека вживає превентивних заходів, спрямовані на контроль інсайдерів і багатоступеневий захист серверів від хакерських атак.

Тому заходи з протидії несанкціонованому доступу повинні бути спрямовані на досягнення двох цілей:

– Створювати умови, коли випадкові або навмисні дії, що призводять до втрати даних, стають неможливі. Інформаційна безпека вирішує цю проблему

шляхом створення системи аутентифікації і авторизації користувачів, поділу прав доступу до інформації та контролю доступу.

– Також важливо створити систему, при якій співробітники або зловмисники не змогли б приховати вчинених дій. Тут на допомогу фахівця з ІБ приходить система контролю подій безпеки, аудит доступу до файлів і папок.

Ефективними засобами захисту, як від зовнішніх загроз, так і від внутрішніх, є також: введення системи паролів користувачів, застосування для особливо важливої інформації криптографічних методів захисту (шифрування), обмеження доступу в приміщення, застосування індивідуальних цифрових ключів і смарт-карт, використання міжмережевих екранів, установка систем захисту від витоків інформації через електронну пошту, FTP-сервери і Інтернет-месенджери, захист інформації від копіювання.

Інформаційна безпека мережі передбачає також захист від атак ззовні, спрямованих на припинення працездатності серверів, комп'ютерів або компонентів мережі. Йдеться про DDos-атак, спробах підбору паролів (bruteforce-атаки). Для захисту від подібних загроз інформаційна безпека вимагає застосування спеціального програмного забезпечення – міжмережевих екранів і систем проактивного захисту.

І найголовніше, для чого потрібна інформаційна безпека - це доступність інформації для легітимних користувачів. Всі заходи забезпечення інформаційної безпеки не приносять користі, якщо вони ускладнюють роботу легітимних користувачів або блокують її. Тут на перший план виходить надійно працює аутентифікація і грамотно реалізований поділ прав користувачів.

Список використаних джерел:

1. Безопасность в интернете: готовы ли пользователи противостоять киберугрозам? [Електронний ресурс]. - Режим доступа: https://habr.com/ru/company/mailru/blog/252091/

2. Безпека електронної пошти [Електронний ресурс]. - Режим доступу: https://zillya.ua/bezpeka-elektronno-poshti

3. Інформаційна безпека підприємства [Електронний ресурс]. - Режим доступу: https://stud.com.ua/21678/ekonomika/informatsiyna_bezpeka_pidpriyemstva

4. Методи захисту від комп’ютерних вірусів [Електронний ресурс]. - Режим доступу: -https://computerbook.jimdo.com/довідник-студента/інформація-студентам/безпека-в-мережі-інтернет-та-при-роботі-з-пк/

5. Интернет-безопасность: самые распространенные ошибки и как их избежать [Електронний ресурс]. - Режим доступу: https://le-vpn.com/ru/internet-security-mistakes/

УДК 374.73

Козік Олександр Іванович
викладач кафедри інформаційних технологій
Київський національний університет будівництва і архітектури
Пономаренко Ярослав Юрійович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ПРОБЛЕМИ ФІКТИВНИХ ІНТЕРНЕТ-МАГАЗИНІВ. БЕЗПЕКА ІНТЕРНЕТ-МАГАЗИНУ.

Інтернет заполонила реклама онлайн-магазинів, що пропонують придбати популярні товари за вкрай привабливими цінами. Розрахунок іде, як зазвичай, на людську жадібність, і в більшості випадків шахраї залишають покупців ні з чим.

Своїх клієнтів шахраї шукають, як правило, за допомогою найпримітивніших способів реклами: це спам по електронній пошті, в меседжерах і соціальних мережах, а також, іноді, на сайтах безкоштовних оголошень.

Найпоширеніший вид обману: шахраї створюють онлайн-магазини та копії вже існуючих, де реалізують неіснуючий товар за передоплатою.

Ще може бути варіант «відкладеної покупки». Тобто, попередня оплата без підтвердження наявності та продажу товару.

Створюючи фіктивне підприємство на реальні персональні дані – збирають кошти на свої банківські рахунки протягом певного часу та зникають.

Але спеціалісти з інтернет-безпеки звертають увагу, що вберегтися від несправжніх онлайн-магазинів можна.

Ось що про них варто знати:

Перше, на що треба звернути увагу, – рядок адреси сайту. Справжні продавці вже зайняли адреси з назвою власне бренду, тому шахраї додають до адреси різні символи. Наприклад, замість brand.com пишуть brand.hit.com. Також на сайті серйозного продавця має бути зелений замочок на початку адреси сайту, що означатиме, що сайт підтримує захищений протокол https, а отже особиста інформація з даними платіжної картки покупця не потрапить до нечесних рук. Але варто знати, що при переході на сайт, який використовує HTTPS (безпечне з'єднання), сервер веб-сайту надсилає веб-переглядачу сертифікат, щоб підтвердити ідентифікаційні дані веб-сайту. Будь-хто може створити сертифікат, щоб видати себе за будь-який сайт. Тому

для власної безпеки в інтернеті потрібно перевіряти, щоб веб-сайти використовували сертифікати від надійних організацій [1].

Здебільшого шахраї не заморочуються на дорогий, гарно прописаний і промальований сайт, а використовують недорогі чи навіть безкоштовні шаблони для простих сайтів на одну сторінку. Крім того, не заморочуються злочинці і на наповнення сайту – полистайте його, почитайте, наприклад, відгуки. Задайте якусь фразу з них в Google – може виявитись, що цей самий відгук вже є на іншому сайті, чи навіть декількох. Отже – він не справжній. Крім того, серйозний сайт-магазин повинен містити прописані правила доставки, умови оплати, можливості повернення товару, а також – інформацію про партнерів-постачальників. Шахраї цього не мають, зазвичай.

Шахраї не використовують еквайринг – оплату платіжними картками. Бо електронний платіж легко відстежити, а нечесним продавцям таке нецікаво. Тому, якщо вас просять оплатити замовлення готівкою, переказати кошти на якусь картку – варто насторожитись.

Ще один виверт – змушувати покупця купити прямо зараз, бо «акція скоро закінчиться» чи навіть бо «магазин влаштовує повний розпродаж». Як правило, такі «акції» і «розпродажі» у шахраїв не закінчуються ніколи, а зникають разом із сайтом [2].

Найбільш ефективно шукати відгуки про компанію в соціальних мережах. Багато негативу – очевидне рішення. Також чимало справжніх магазинів реєструються в каталогах prom.ua, там є система рейтингів і своя система перевірки контрагентів.

Основні рекомендацій, які можуть допомогти захистити свій бізнес в інтернеті:

– відстежуйте наявність оновлень і регулярно оновлюйте свій улюблений CMS

– використовувати складні паролі і регулярно їх міняйте

– відмовтеся від небезпечних протоколів (типу FTP, telnet) на користь SSH

– обов’язково встановіть і правильно налаштуйте SSL-сертифікат

– використовуйте скрізь, де можливо, двофакторну аутентифікацію (в цьому випадку, навіть «викрадення» пароля адміністратора не призведе до масштабних руйнівних наслідків.

Список використаних джерел:

1. 33 поради з кібербезпеки, що захистять ваші пристрої, інформацію, гроші і нерви [Електронний ресурс]. - Режим доступу: https://24tv.ua/special/kiberbezpeka/

2. Безпека інтернет-магазину: що і чому потрібно захищати [Електронний ресурс]. - Режим доступу: https://rau.ua/novyni/bezopasnost-internet-magazina-chto-i-pochemu-nuzhno-zashhishhat/

УДК 37.09-047.58

Костюк Михайло Анатолійович
аспірант кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет

ОРГАНІЗАЦІЯ БЕЗПЕКИ ФУНКЦІОНАЛЬНИХ АЛГОРИТМІВ ПРИ СТВОРЕННІ МОБІЛЬНИХ ДОДАТКІВ

Поява сучасних мобільних операційних система, таких як Android, IOS, Windows phone, відіграла істотну роль в комунікації між людьми. Встановлення цих систем на телефони дала можливість з легкістю розробляти нові моделі мобільних пристроїв, розширюючи функціонал як телефонів, так і самих операційних систем. Проте операційна система в першу чергу призначена для надання можливості роботи спеціальних мобільних додатків, які забезпечують основну взаємодію користувача та мобільного пристрою.

При розробці мобільного додатку слід враховувати, що дані, якими оперує цей додаток, можуть представляти певний інтерес для третіх осіб. Ступінь цінності цих даних варіюється в широких межах, проте, навіть найбільш проста приватна інформація, наприклад, пароль входу в додаток, вимагає опрацювання її захисту. Особливо це важливо в світлі поширення мобільних додатків на всі сфери електронних послуг, включаючи фінансові, банківські операції, зберігання і передачу особистих даних та інші.

Можна виділити основні види атак на мобільні додатки:

- Декомпіляція файлів програми на файли з вихідним кодом і розбір локально збережених даних, визначення структури даних, та дешифровка за допомогою алгоритмів отриманих з вихідного коду додатку.
- Перехоплення даних, переданих по мережі (MITM-атаки). Більшість мобільних додатків є клієнт-серверними, отже, постійно передають і приймають інформацію.
- Зміна прав доступу до пристрою (отримання прав доступу рута) та атака на додаток і його функціональні файли за допомогою налаштувань через зовнішні налагоджувальні інструменти.

Однією з досить важливих проблем є забезпечення безпеки функціональних алгоритмів, які використовуються для роботи мобільного додатку.

Якщо при розробці програми всередині компанії використовуються якісь власні алгоритми, які можуть представляти високу цінність для потенційних конкурентів або зломщиків, то ці алгоритми повинні бути захищені від стороннього доступу.

Для вирішення цієї проблеми використовують автоматичну або ручну обфускацію коду. Обфускація або заплутування коду – приведення

початкового коду або виконуваного програмного коду до вигляду, який зберігає його функціональність, але ускладнює аналіз, розуміння алгоритму роботи і модифікації при декомпіляції. Хоча обфускація допомагає зробити розподілену систему безпечнішою, не варто обмежуватися тільки нею. Обфускація – це безпека через приховування.

Основною метою обфускації є:

- Ускладнення декомпіляції/зневадження та вивчення програм з метою виявлення функціональності.
- Ускладнення декомпіляції пропрієтарних програм з метою запобігання зворотної розробки або обходу DRM і систем перевірки ліцензій.
- Порушення авторських прав програмістів і приховування авторства.
- Оптимізація програми з метою зменшення розміру працюючого коду і (якщо використовується мова, яка не компілюється) прискорення роботи.
- Демонстрація неочевидних можливостей мови і кваліфікації програміста.

Для того, щоб компанія змогла забезпечити цілісність власних алгоритмів, при створенні мобільних додатків, використовують підхід тонкого клієнта. А саме всі алгоритми обчислення, створення, збереження та обробки даних виносяться на сторону сервера. В такому випадку, мобільний додаток лише збирає дані та відправляє їх на сервер для подальшої обробки. Такий підхід в першу чергу забезпечую високий рівень захищеності обчислювальних алгоритмів та забезпечує легкість мобільного додатку (мобільний додаток утримує в собі лише логіку побудови інтерфейсу та комунікацію з сервером).

Отже, для забезпечення безпеки мобільних додатків необхідно розподіляти логіку між сервером, що забезпечує основну функціональну потужність, та легким мобільним клієнтом, який по факту являється віддаленим інтерфейсом сервера. В такому випадку, доступ до всіх алгоритмів буде повністю закритий, дані системи будуть зберігатися на сервері, і доступ до них буде отримати вже набагато складніше.

Список використаних джерел:

1. Garg V., Srivastava A., Mishra A. Obscuring Mobile Agents by Source Code Obfuscation / V. Garg, A. Srivastava, A. Mishra. International Journal of Computer Applications, 2013. – 61(9). – P. 46-50.
2. Моісейкін О.С. Технологія розробки веб-додатків реального часу. // МОДС 2016. – Жукин, 2016. – С. 473-475.
3. Andrew Lombardi. WebSocket. Lightweight Client-Server Communications // O`Reilly Media – Sebastopol, USA, 2015. – P. 144.
4. Chris Anderson. CouchDB: The Definitive Guide // O`Reilly Media – Sebastopol, USA , 2014. – P. 272.

УДК 004.056.5:343.9

Добровольська Наталія Вікторівна
кандидат педагогічних наук, доцент,
доцент кафедри економічної кібернетики та інформаційних систем
Вінницький торговельно-економічний інститут КНТЕУ

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Широке використання сучасних інформаційних технологій у суспільстві висуває вирішення проблем інформаційної безпеки в число основних. Міжнародні організації визнають небезпеку кіберзлочинності та її трансграничний характер. Одним із шляхів вирішення цієї проблеми розглядають впровадження необхідних технічних заходів. Слід зазначити, що кількість виявлених кіберзлочинів в Україні щорічно збільшується в середньому на 2500.

На нашу думку, основним засобом протидії кіберзлочинності є організація безпечного кіберпростору. Під безпечним кіберпростором будемо розуміти інтерактивне інформаційне середовище, яке функціонує за допомогою комп'ютерних систем, причому властивості комп’ютерної техніки, комунікаційного обладнання та програмного забезпечення, характеризуються високим степенем захищеності від зовнішнього несанкціонованого втручання.

Важливим фактом з точки зору інформаційної безпеки є властивості операційних систем та мережевого комунікаційного обладнання. Слід зауважити, що з самого початку виникнення комп’ютерної техніки і комп’ютерних мереж превалюючим напрямом всіх технологічних новацій у цій сфері було досягнення все більшої швидкості обробки і передачі інформації на різних ієрархічних рівнях з метою спрощення процедур обміну і підвищення їх ергономічної привабливості. Тому спочатку головним принципом при розробці операційних систем був принцип відкритості. На поточний момент головним напрямом розвитку операційних систем є модифікація раніше створених з метою їх адаптації до сучасних технологічних новацій і вимог (зокрема, вимог до інформаційної безпеки). Це стосується, в першу чергу, таких груп ОС як Windows та Unix. Найчастіше для проникнення в роботу цих систем хакери використовують приховані помилки в ядрі і драйверах ОС. [1]. Виходячи з цих обставин інша група експертів, зокрема, фахівці компанії «Лабораторія Касперського» пропонують іншій напрям розвитку захищених операційних систем – створення принципово нових ОС, які задовольняють вимогам надійності і захищеності функціонування. З їх точки зору така операційна система повинна відповідати наступним вимогам [3]:

• ОС не може бути заснована на якомусь вже існуючому програмному коді, тому повинна бути написана з нуля;

• з метою гарантії безпеки вона не повинна містити помилок і вразливостей в ядрі, контролюючому інші модулі системи. Як наслідок, ядро має бути верифіковано засобами, що не допускають існування вразливостей і коду подвійного призначення;

• з тієї ж причини ядро має містити критичний мінімум коду, а значить, максимальне можлива кількість коду, включаючи драйвери, має контролюватися ядром і виконуватися з низьким рівнем привілеїв;

• в такому середовищі повинна бути потужна і надійна система захисту, що підтримує різні моделі безпеки. Додамо, що така операційна система повинна бути максимально сумісною з певною групою операційних систем, наприклад, з ОС групи Windows, для забезпечення мобільності або, в крайньому випадку, мінімальних витрат на конвертацію застосувань, що вже функціонують. В іншому випадку такий проект буде приречений на комерційний провал.

На даний час існують наступні проблеми щодо використання інформаційних технології у сфері протидії економічній злочинності: складність отримання інформації про рух коштів по банківських рахункам; застаріла матеріально-технічна база та програмне забезпечення, несвоєчасне оновлення електронних баз і банків даних; відсутність чіткого плану розвитку та удосконалення інфюрмаційних систем для забезпечення оперативно-розшукової та кримінально процесуальної діяльності; неналежний рівень фінансування на модернізацію та розвиток існуючих і створення нових інформаційних систем у сфері протидії економічній злочинності; відсутність курсу підвищення кваліфікації для працівників практичних підрозділів з питань впровадження та користування новими інформаційними технологіями в інтересах інформаційно-аналітичного забезпечення оперативнорозшукової діяльності у процесі розслідування злочинів у сфері економіки [2].

Проблема боротьби з кіберзлочинністю – це актуальна проблема для нашої країни, для ефективного вирішення якої, на нашу думку, слід впроваджувати діючу стратегію кібербезпеки держави, в основі якої необхідно: створити безпечний кіберпростір, вдосконалити українське законодавство у сфері боротьби з кіберзлочинністю; створити механізм партнерства в інформаційному суспільстві для взаємодії та координації заходів щодо забезпечення кібербезпеки; забезпечити підготовку висококваліфікованих ІТ-фахівців для запобігання будь-яким злочинам в інформаційному та комп’ютерному просторі.

Список використаних джерел:

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП Україна», 2015. – 449 с

2. Мовчан А. В. Використання сучасних інформаційних технологій у боротьбі зі злочинами, пов'язаних з торгівлею людьми / А. В. Мовчан / / Вісн. Запоріз. юрі-щ. ін-ту. - 2010. - № 3. - С. 170-176.

УДК 004.4

Пашорін Валерій Іванович
кандидат технічних наук,
професор кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Сперисенко Олександр Валерійович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ЗАХИСТ ДОДАТКІВ ВІД ВЗЛОМУ

У сучасному світі інтелектуальна власність стає одним з найбільш цінних активів, і тому, як і будь-який інший вид власності, часто є об'єктом протиправних дій, зловживань з боку третіх осіб. Тому власнику потрібно подбати про забезпечення захисту своєї інтелектуальної праці.

Це явище особливо гостро стає в кіберпросторі, де більшість програм використовуються неправомірно. Таке програмне забезпечення має потенційну загрозу. Наприклад, програмне забезпечення може бути скопійоване, а потім «модернізоване» зловмисником для отримання персональних даних або отримання прибутку(додаткова реклама, підключення комп’ютера до ботнету, зараження вірусом).

Метою роботи є аналіз існуючих засобів захисту. Проте спочатку для кращого розуміння розглянемо основні утиліти для злому, їх можна класифікувати так:

- Відладчики. Дозволяють переривати виконання програми при досягненні заздалегідь заданих умов, виробляти покрокове виконання програми, змінювати вміст пам'яті і регістрів і т.п.
- Дизасемблери. Проводять дизасемблювання програми для подальшого вивчення отриманого коду.
- Засоби моніторингу. Це набір утиліт, які відстежують операції з файлами, реєстром, портами і мережею.
- Засоби пасивного аналізу програми. Показують різну інформацію про програму - витягують ресурси, показують зв'язку, що використовуються бібліотеки.
- Інші утиліти. Це різноманітні редактори, аналізатори і т.п.

Повністю надійних систем від злому немає. Інше питання, що можливо має сенс зробити так, щоб програмну системи було безглуздо зламувати. Розглянемо основні опції захисту: оффлайн, онлайн та апаратний.

- Програмний захист оффлайн.

Як правило, це недорогий варіант. Зазвичай таке рішення реалізується після компіляції програми. Найчастіше для захисту програми

використовується програмна обгортка з певними настройками. Коли програма запущена у користувачів, вона не підключається до жодних зовнішніх систем. Так як всі параметри ліцензування знаходяться на комп'ютері, на якому запускається ПО, такий захист досить просто обійти. Рівень захисту при використанні даного рішення знаходиться між низьким і середнім. Наприклад: програми-пакувальники(пакують виконуваний файл); програми-протектори(часто пакують виконуваний код програми та всіляко переробляють його: змінюють таблиці імпорту і розташування модулів виконуваного файлу, додають виклики зайвого коду, зашифровують код тощо); програми-обфускатори(додають зайвих код, перейменовують змінні і функції)

- Програмний захист онлайн

Обов'язкове підключення до сервера ліцензування зазвичай призводить до зростання витрат для запуску і додає періодичні витрати. Тут теж використовується програмна оболонка для захисту, однак через те, що параметри ліцензування винесені в онлайн, з'являється більше можливостей. Додаткові опції дозволяють відстежити, де використовується ПО, як використовується, з ліцензією або без.

Захист в даному випадку - між середнім і високим рівнем, так як параметри ліцензування залишаються на захищених серверах ліцензування. Наприклад: активація по ключу програми, який перевіряється на сервері; деякі функції програми можуть знаходитися на сервері, а сама програма слугує лише «оболонкою».

- Апаратний захист

Захист дуже сильний, так як за ліцензування відповідає електронний USB-ключ, якому не потрібно підключатися до інтернету. Вартість кожного ключа на кожну ліцензію низька; крім того, відсутні періодичні витрати. Цей варіант - один з найбільш простих, надійних і універсальних. Найважливішою складовою частиною системи захисту з використанням електронних ключів є її програмна компонента. Як правило, вона включає в себе захисний "конверт" (Envelope) і бібліотечні функції звернення до ключу (API - Application Program Interface). Обидва ці способи забезпечення захисту мають своє призначення і, по можливості, повинні застосовуватися спільно, що забезпечить найбільш стійкий захист.

Будь-який захист не зможе гарантувати стовідсоткової гарантії, проте навіть елементарний протектор зможе зупинити деяких зловмисників.

Список використаних джерел:

1. Как защитить ПО от копирования и взлома [Електронний ресурс]. - Режим доступу: https://tproger.ru/translations/how-to-secure-your-software/
2. Пишем защиту от взлома [Електронний ресурс]. - Режим доступу: http://about.thedeemon.com/texts/protection.html

УДК 374.73

Десятко Альона Миколаївна
старший викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Коломієць Іван Олегович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ПРОБЛЕМИ ПІРАТСТВА В ІНДУСТРІЇ ІГРОВИХ РОЗРОБОК. ЗАХИСТ ІГОР У STEAM

У 2008 році виступаючи на саміті, присвяченому ігор для PC, керуючий директор Valve Гейб Ньюелл заявив, що його не хвилюють дії піратів, що крадуть гри компанії. За його словами, система цифрової дистрибуції Steam надійно захищає видані в ній проекти від нелегального копіювання. Ньюелл вважає, що гравці високо цінують сервіс, який надає Steam. Згодом вони стають все менш зацікавленими в піратстві, адже, вкравши одну з ігор Valve, гравець ризикує втратити і всі законно придбані копії.

За замовчуванням, ігри в Steam ніяк не захищені і являють собою звичайні файли, які можуть бути скопійовані або запущені без будь-яких обмежень. Якщо потрібно захистити файл (тут під словом "файл" мається на увазі виконуваний файл програми) від копіювання на інший комп'ютер або від запуску на акаунті, Steam пропонує декілька способів.

Сервіс надає розробникам особливе API "Steamworks", за допомогою якого можна, крім іншого, отримати інформацію про призначеному для користувача акаунті і придбаних на нього іграх. Таким чином, найпростіший спосіб дізнатися, що даний акаунт має право на запуск програми – перевірити за допомогою API з самого додатка, що воно дійсно було куплено поточним користувачем. Це робиться буквально парою рядків коду. Оскільки в один момент часу акаунт може бути авторизований тільки на одному комп'ютері, цей спосіб також вирішує проблему з запуском програми на безлічі різних комп'ютерів під одним аккаунтом. У разі якщо інтернет-з'єднання немає, даний спосіб не зможе підтвердити право на запуск програми. Щоб цього уникнути, програмний клієнт Steam необхідно попередньо перевести в т.зв. Offline-режим, при якому поточний стан акаунта зберігається локально. Втім, якщо офлайн-запуск програми з яких-небудь причин небажаний, через Steamworks API завжди можна з'ясувати поточний режим і перервати запуск програми, якщо це необхідно.

На даний момент часу для злому такого типу захисту зазвичай відбувається підміна інтерфейсної бібліотеки Steamworks API (steam_api.dll) на власну, яка емулює необхідну поведінку захисту. В середині січня 2016

року з'явилася новина про те, що пірати незабаром не зможуть зламувати ігри через те, що системи захисту стануть занадто досконалими. Зокрема мова йшла про Denuvo, австрійському розробника, спадкоємця SecuROM. Дана заява більше схоже на PR хід, однак не можна не визнати, що технології захисту постійно удосконалюються, в тому числі в області обфускації коду. Останнім часом в Steam з'явилося досить багато ігор, захищених Denuvo. Що це за система і наскільки справедливо називати її DRM?

Основним завданням Denuvo є захист коду гри, тому застосовується віртуальна машина, велика кількість обфускації, і різні методи шифрування файлів. Якщо говорити саме про функціонал DRM, то Denuvo може виконувати перевірку авторизації копії гри на акаунті гравця. Захист коду виконуваного файлу накладає велику відповідальність на розробника гри, так як потрібно знайти баланс між продуктивністю і ступенем захищеності. Також при використанні цієї захисту у гравців виникає питання про швидкий вихід з ладу дисків SSD. І хоча представники Denuvo стверджують, що їх система захисту не впливає на диски, але факт залишається фактом - відбувається певне зростання операцій читання фрагментів програми з диска, отже, навантаження на диск збільшується.

Традиційно компанія StarForce пропонує свої рішення для захисту ігор на платформі Steam. Широка лінійка продуктів дозволяє вибрати оптимальний варіант захисту: тільки код, код + DRM, тільки DRM. Основним завданням StarForce в даний момент є надання захисту, яка не доставляє турбот чесному гравцеві, а для пірата стає непереборною перешкодою. Основною перевагою в порівнянні з Denuvo можна назвати економічний аспект - при високому рівні взломостойкости рішення StarForce дешевше.

Також на Steam можна зустріти ігри, захищені системами ActControl, Reality Pump, TAGES. Вони не так широко відомі, як дві попередні, що скоріше є їх перевагою. В основному ці рішення виступають як альтернативні DRM-захисту, але можуть надавати і захист коду.

В умовах посилення кризи, коли грошей у населення стає менше, а вільного часу більше, є великі сумніви щодо повного зникнення піратських копій ігор. З іншого боку лояльність гравців, особливо в такий час, є найголовнішим активом розробників і видавців, тому основним завданням при виборі системи захисту є пошук золотої середини між позитивним враженням від гри і припиненням спроб піратського поширення свого продукту.

Список використаних джерел:

1. Защита игр в Steam: собственные механизмы и сторонние DRM [Електронний ресурс]. - Режим доступу: https://bitly.su/f01E

2. Gladius Partners with Remme to Tackle Enterprise Cybersecurity. [Електронний ресурс]. URL: https://medium.com/gladius-blog/gladius-partners-with-remme-to-tackle-enterprise-cybersecurity-b1d12c288fa6

UDC 004.891.3

Bebeshko Bogdan
Server-side Developer
Softorino Inc.
Khorolska Karyna
Master of Economics
Kyiv National University of Trade and Economics

CYBERATTACKS PREDICTION WITH INCOMPLETE DATA

In case cyber-attacks are predicted a vast amount of time before they occur, defensive actions to prevent their negative impacts could be planned. Unfortunately, most of the time one do not have enough data or incomplete existing data of the harmful activities before they are already under way.

This thesis stresses the urgent problem concerning prediction of the cyberattacks. Some of the hosts are meant to detect earlier steps in an attack cycle that do not involve engaging the actual network infrastructure. Furthermore, the determination of the significant threads could be automated for relevant hosts, in order to enable the forecast system to be adaptive to the varying characteristics of the unconventional threads.

There are several prior works which forecast future cyber incidents against target organizations before they happen and achieve quite high accuracies. But it is necessary to point out that, unlike the previous cyberattack forecast works this thesis emphasize the importance of incomplete data use which is underestimated during evaluation of actual cyberattacks within organization.

The missing host values in the data set may affect the quality of the learning process and degrade the performance of the detection algorithms. There are various approaches aimed to combat the incomplete data situation. One simplest solution is to ignore the missing host values; however, in such case, the number of training instances of the prediction system could decrease, that will result in poor performance marks. An alternative way is to replace missing values with the mean of the existing non-missing values. Another way that can be considered is more complex approach that represents or replace the missing value using prediction strategy. Saar-Tsechansky together with Provost [1] mentioned that different types of replace methods might be preferable over another, based on circumstances. Rahman and Davis [2] used mean rule induction algorithm, decision trees called J48, KNN (K-Nearest Neighbor), and also SVM (Support Vector Machines) methods to replace missing values in the dataset and concluded that machine learning methods perform better compared to other replace techniques. Luengo [3] used fourteen replace methods for the missing values and found that replacing methods results in greater performance than the approaches that ignore missing values. Supporting the previous findings in the literature, they also concluded that there was no universal replace method that performed the best for all. Farhangfar [4] made a comprehensive review of the existing replace methods and developed a unified framework aimed to incapsulate a set of techniques. They divide missing value handling techniques into three categories where missing entries in the data

were lost or absent, most preferable algorithms were used, and missing values were predicted using either mean replace or machine learning methods. However, to the best of our knowledge, it was not treated much in the cyber security domain. This thesis overview a set of incomplete host replace methods to replace the missing values and shows the increase in the predictive power for forecasting cyberattack incidents.

As it was mentioned above - missing data is one of the biggest problems in machine learning and has a significant impact on learning process and prediction. Data can be missing at a random or in a systematic way where lost value can be observed whenever some condition has been met. In any of the possible cases, missing data is a “show stopper” and needs special solution to improve the performance of a prediction technique. As it was written before - simplest solution would be ignoring missing hosts. Nevertheless, depending on the amount of the missing hosts, such approach can result in ignoring the vast of the dataset and a huge loss in the predictive power. The solution is to replace the missing data with various techniques. Support Vector Machines (SVM) is one of the learning methods that can be used to replace missing data. Another method is k-nearest neighbor (KNN) which is a classification algorithm also known as IBC (Instance-Based Classifier). KNNs’ instance is marked considering the majority mark of its k neighbors where k >= 1. KNN is one of the widely-used techniques to replace missing host values. Neural networks can be used decision making processes, because they are able to model the complex non-linear relationships within a dataset. Multilayer Perceptron (MLP) is a feed-forward neural network technique that can analyze non-linear functions classification tasks. An MLP architecture is a complex of at least three layers of nodes and can evaluate data that is not linearly separable.

To enable cyber-attack forecast with incomplete data, one can use predictive signal(host) imputation technique (PSI) that is based on the SVM, MLP, and KNN algorithms to replace in the lost values in the hosts.

The predictive power of different host replace methods are compared using the ALPHA dataset for the EM (Endpoint Malware), MD (Malicious Destination), and ME (Malicious Email) attack types. 58% of the instances in the dataset include at least one lost host and the predictive replace methods like SVM, KNN, and MLP are used to replace these lost host values. Once the lost host values have been replaced, a Bayes.Net classifier is used with 10 folds cross validation to calculate the AUC (Under Receiver Curve) value for each attack type. The AUC values shown in table 1 are obtained. The values in the row “None” shows the AUC value when no replace method was used which means that the instances with lost hosts are obsolete. It can be observed that the replace methods increases the predictive power compared to the situation when the instances with lost host values are removed. Furthermore, the k-Nearest Neighbor algorithm performs significantly better than the SVM and MLP for EM, MD and ME cyber-attacks.

According to the test of each single methods, the various PSI methods are applied to the ALPHA dataset at the same time under same conditions. It was shown that when missing signals are replaced, the use of PSI increases the model performance up to 87%, 90%, and 96% AUC for predicting endpoint-malware, malicious-destination, and malicious-email attacks, respectively. Results shows the

robustness of cyberattack forecasting where the integrated results provide approximately 0.6 to 1.0 F-Measure over time. The proposed framework enables assessment of the relevance of unconventional signals for forecasting cyberattacks. A careful integrated use of PSI without overly using the replaced signals to determine the significant lags can offer even better and more robust performance.

	EM	MD	ME
SVM	0.60	0.64	0.78
KNN	0.88	0.91	0.95
MLP	0.73	0.55	0.83
None	0.51	0.46	0.74

Table 1. The AUC values for various PSI approaches

Due to the close relationship of unconventional hosts and the entity results seems to be un stationary, the cumulative approach may not always be a good idea. Moreover, significance of the incomplete data may not always be the same. To consider the significant observations more than those insignificant, a cross correlation based signal aggregation approach should be used to aggregate hosts over the past significant lags. Taking to account that with an incomplete dataset along with need to define significance, the performance of a cyberattack classifier may not be so good. That's why, as a future work the concept of dynamic definition of optimum learn shallow for the forecast should be taken. Moreover, the evaluation of the significant threads could be automated for relevant hosts, in order to grant forecast system ability to be adaptive to the varying properties of the unconventional hosts and data.

Список використаних джерел:

1. Saar-Tsechansky M., Provost F., Handling missing values when applying classification models. [Електронний ресурс]. Journal of machine learning research 8(Jul):1623--1657, 2007. – Режим доступу: http://dl.acm.org/ citation.cfm?id=1314498.1314553

2. Rahman M.M., Davis D.N. Machine Learning-Based Missing Value Imputation Method for Clinical Datasets. IAENG Transactions on Engineering Technologies Springer Netherlands. 2013 – Режим доступу: https://doi.org/10.1007/978-94-007-6190-2_19 – ISBN978-94-007-6189-6

3. Luengo J., García S., Herrera F., (2011) On the choice of the best imputation methods for missing values considering three groups of classification methods. [Електронний ресурс]. – Knowledge and Information Systems. An International Journal – Режим доступу: https://www.researchgate.net/publication/225326715_ On_the_choice_of_the_best_imputation_methods_for_missing_values_considering _three_groups_of_classification_methods – ISSN: 0219-1377 (Print) 0219-3116 (Online)

4. Farhangfar A, Kurgan LA, Pedrycz W (2007) A novel framework for imputation of missing values in databases. IEEE Trans Syst Man Cybern Part A 37(5):692–709

УДК 621.391.037.372

Бєлозьорова Яна Андріївна
асистент кафедри інженерії програмного забезпечення
Національний авіаційний університет

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ ІДЕНТИФІКАЦІЇ ДИКТОРА НА ОСНОВІ МУЛЬТИФРАКТАЛЬНОГО ПІДХОДУ

Розвиток інформаційних технологій та необхідність реалізації людино-машинної взаємодії утворює ряд важливих наукових задач, однією з яких є ідентифікація диктора. Ця задача складається з підзадач ідентифікації та верифікації диктора, в основі яких лежить ототожнення особистості по особливостям мови та голосу.

У більшості сучасних систем вирішення завдань ідентифікації диктора по характеристикам голосу, лежить спектральний аналіз аудіо інформації, заснований на математичному апараті перетворення Фур'є. Це обумовлено з одного боку, відомими нейрофізіологічними закономірностями обробки звукової інформації первинними слуховими рецепторами. З іншого боку - відсутністю більш ефективних методів аналізу і, певною мірою, історичними традиціями в цій галузі. Однак, незважаючи на створення досить ефективних систем розпізнавання характеристик голосу, достатньої ясності в принципових теоретичних і практичних питаннях мовних технологій немає до теперішнього часу.

Незважаючи на величезну кількість досліджень в цій області і застосування потужної комп'ютерної техніки, принципового прориву в області фізико-математичних концепцій ефективної обробці мовної інформації (порівнянної з ефективністю слухового апарату) немає. На думку багатьох фахівців, багато в чому це обумовлено відсутністю ефективного математичного інструменту для аналізу мовної аудіо інформації.

З часів Гельмгольца [1] неодноразово відзначалося дослідниками (зокрема, класична робота Фанта [2]), що більшість фонемічних структур мови можуть бути побудовані на основі близьких геометричних компонент ("атомарних" структур) звукової хвилі. Геометрична подібність цих структур є приблизною, але в більшості випадків візуально очевидною, а тимчасові інтервали, займані цими структурами, протилежні величині частоти основного тону і розташовані в діапазоні від 2 до 15 мс. Ці атомарні структури, що розглядаються ізольовано, не сприймаються на слух через їхню малу тривалість звучання. З огляду на роботи Мандельброта, ці структури можна трактувати як атомарні складові мультифрактала [3,4]. За умови створення математичної моделі, при забезпеченні ефективного визначення параметрів "атомарних" структур і мультифрактала в цілому, можна очікувати коректного опису і рішення всіх основних завдань ідентифікації голосу і розпізнавання мови на фонемічному рівні.

В дослідженні виконано представлення фрагментів мови в мовному сигналі, як дискретного часового ряду амплітуди звукової хвилі та поставлена задача виділення характеристик самоподібних структур в отриманому тимчасовому ряду для отриманих атомарних фрагментів мови. Для виявлення подібних структур використовуються методи вейвлет-аналізу, в якості базису обраний комплексний вейвлет Морле. Частотно-часове представлення фрагмента мови у вигляді просторової скейлограмми на основі базису Морле має низку важливих особливостей, що дозволяють істотно підвищити ефективність виявлення самоподібних структур. Зокрема, локальні максимуми вейвлет-перетворення є досить інформативними для аналізу атомарних складових мультіфракталов в аудіо інформації. Аналіз скейлограмм показав, що розташування "хребтів" скейлограмм по тимчасовому параметру строго відповідає локальним екстремумів амплітуди звукової хвилі в тимчасовій області. Причому ці локальні екстремуми відповідають сплесків амплітуди звукової хвилі, обумовленим частотою основного тону. Представлений підхід до виділення частоті основного тону показів високу точність при виділенні частоти основного тону.

На основі розглянутого підходу до визначення частоти основного тону побудована система ідентифікації диктора, яка по цифровим записам інформаційних повідомлень здійснює автоматичний розрахунок параметрів характеристик голосу і подальше ранжування цих характеристик в базі даних голосів. Ранжирування за наступними критеріями:

- обчислення близькості кривих функцій двовимірної щільності ймовірності для частоти основного тону і розташуванню в спектрі семи формант, що виділяються з промови, зафіксованої на фонограмі;
- обчислення міри близькості абсолютних максимумів спектрів формант, що виділяються з промови, зафіксованої на фонограмі.

Проведено тестування створеної програмної системи розпізнавання диктора за набором з 300 аудіозапісів 10 дикторів. Система показала достовірність розпізнавання диктора близько 92% на обраному наборі даних. В якості напрямку подальших досліджень розглядаються питання поліпшення точності розпізнавання диктора.

Список використаних джерел:

1. Helmholtz H. von, Die Lehe von Tonempfindungen. Brannschweig, Vieweg, 1863.
2. Gunnar Fant Royal Institute of technology Stockholm MOUTION & GO. ‘S-GRAVENHAGE 1960.
3. Mandelbrot B. Statistical Methodology for Non-Periodic Cycles:From the Covariance to R/S Analysis. Annals of Economic Social Measurement 1, 1972.
4. Mandelbrot B.B. Robustness of the rescaled range R/S in the measurement of non-cycling long-run statistical dependence // Water Resources Research. 1969. V. № 5. P. 967-988.

UDC 004.056

Rzaieva Svitlana
candidate of technical sciences,
associate professor of program engineering and cyber security department
Kyiv National University of Trade and Economics
Yemelianova Olena
student of the field of training area 6.050103 «Software engineering»
Kyiv National University of Trade and Economics

INFORMATION TECHNOLOGIES IN THE FIGHTING OF CIBERCULARITY

Offenses in the field of information technology include both the spread of viruses, password hacking, the theft of bankcard numbers and other details, as well as the distribution of illegal information on the Internet, as well as harmful interference in the work of various systems through computer networks.

The fight against cybercrime is not possible without a deep understanding of the legal issues of regulation of information networks. It is an analysis of the relationship between the network's technical characteristics and the legal and social constraints imposed by law enforcement authorities on these characteristics as a first step towards the establishment of mechanisms to adequately respond to the development and growth of cybercrime.

In recent years, information technology has been developing too fast to allow existing control mechanisms to respond to new challenges. Cloud computing, automation of attacks, vulnerability of personal information in social networks, distribution of so-called "information weapons", such as "Stuxnet", developed (according to experts) for attacks on Iran's nuclear industry (but Stuxnet inflicting significant damage to the infrastructure for many to other countries too) - for all these problems legal regulation can not yet find an adequate solution.

Prevention of cybercrime consists of strategies and measures aimed at reducing the risk of committing crimes and neutralizing potentially harmful consequences for society and private individuals. Almost forty percent of surveyed countries report the existence of national legislation or policies in the area of cybercrime prevention.

Another twenty percent of countries are developing initiatives. Countries note that among the best practices in the field of cybercrime prevention is the adoption of laws, effective leadership, capacity development of law enforcement agencies, information and education activities, creation of a solid knowledge base and cooperation between public authorities, the private sector and internationally.

At present, information technology for processing network data in information systems has been created to combat cybercrime, aimed at increasing the technical and economic efficiency of operating information systems built on the

basis of computer networks and relational databases, by reducing the impact of cyber threats on functioning mechanisms. transmission, processing and storage systems. A series of fundamental results of the branches of data flow control systems has been obtained, namely, the methods of parametric identification of mathematical models of data transfer processes based on the local model of the controlled process, interception and blocking of network packets based on WFP technology have been developed.

Also, new approaches have been proposed at parametric identification of mathematical models of network data transmission processes, overload control in network buffer buffers in DoS- and DDos-attacks, external optimization of SQL-query synthesis in the conditions of information uncertainty of database structure in problems of compensation of cyber attack effects on automated workplace management systems, identifying the content of network packets on the network layer of the OSI model in the tasks of protecting Adware from threats. The establishment of new nonconventional tasks of analyzing the influence of the parameters of the computer network and information systems and the results of the functioning of the data transfer processes, taking into account the availability of information and parametric uncertainty, has been made.

The results of work are important for the activities of organizations and enterprises that use modern computer systems and networks in the process of providing information exchange of data to solve the problem of counteracting cyber attacks and their consequences on information flows.

Due to the increasing number of computer-related crimes that contributes to the creation of global international and public electronic networks, international cooperation and coordination of activities in this area are of great importance. Education and awareness raising can reduce the number of crimes in the electronic environment.

The transnational nature of crime with the use of computer networks suggests that the development of a common policy on key issues should be part of any strategy to combat crime. Investigation of cybercrime requires staff with specific legal and technical expertise and knowledge, as well as the availability of specific procedures.

References:

1. Melnyk S. On the Problem of the Formation of the Concept-Terminology Device of Cybersecurity / S. Melnyk, O. Tikhomirov [Electronic resource]. - Access mode: http://www.nbuv.gov.ua/portal/natural/Znpviknu/2011_30/Zbirnik_30_28.pdf

2. Karchevsky M. Computer information as a subject of crime in the field of computer use, systems, computer networks and telecommunication networks / M. Karchevsky. // The fight against crime in the field of computer information: the problems and ways to solve them. - 2012. - P. 61-64.

УДК 004.056

Шакуров Євген Олексійович
вчитель вищої категорії, старший вчитель
Харківська гімназія №144

ШЛЯХИ ЗАХИСТУ ЗМІСТОВОЇ ЧАСТИНИ WEB-САЙТУ

В останні роки, з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різноманітних країн. Оскільки основний інформаційний обмін оснований на інформаційній технології, то важливою умовою безпеки стає безпека в комп'ютерних мережах. Тому захист інформації - важливе і першочергове завдання при проектуванні веб-сайтів.

На жаль, масова уразливість веб-сайтів і пов'язані з цим проблеми безпеки зачіпають не тільки інтереси власників ресурсів. Вони зачіпають всю еко-систему глобальної мережі Інтернет, тому що більше 90% всіх заражень персональних комп'ютерів відбувається саме через відвідування заражених веб-сайтів. Кіберзлочинцями давно поставлений на потік процес пошуку вразливих веб-сайтів, їх зараження і подальше інфікування пристроїв всіх відвідувачів величезних моральних і матеріальних збитків.

Щоб заразити комп'ютери користувачів, зловмисники розміщують на сторінках код, який використовує вразливості в компонентах браузера, таких як інтерпретатори JavaScript, плагіни та доповнення для відображення Flash, PDF, виконання Java тощо. Якщо вам потрібно проглянути зміст небезпечного сайту, та з якихось причин ви не бажаєте користуватися його безпечною копією - вам потрібно вимкнути ці компоненти на час відвідування небезпечних сайтів. У цьому випадку ризик зараження комп'ютера під час перегляду сторінок, що містять шкідливий код, істотно знизиться.

Таблиця 1. Класифікація загроз веб-сайтам

Назва	**Загроза**	**Розповсюдження**	**Складність захисту**	**Об'єкт атаки**
Code injection	найвища	низька	низька	скрипт (з привілеями веб-сервера)
SQL Injection	висока	середня	середня	база даних
XSS	середня	висока	висока	кінцевий користувач

Основна загроза безпеці сайту - хакерська атака. Вона може мати кінцеву мету, бути цільової атакою, або атака носить безсистемний характер.

Основні типи загроз інформаційній безпеці веб-додатки:

1. Загрози конфіденційності - несанкціонований доступ до даних.
2. Загрози цілісності - несанкціоноване спотворення або знищення даних.
3. Загрози доступності - обмеження або блокування доступу до даних.

Відсотковий розподіл загроз веб-сайтам наведений на рис 1.

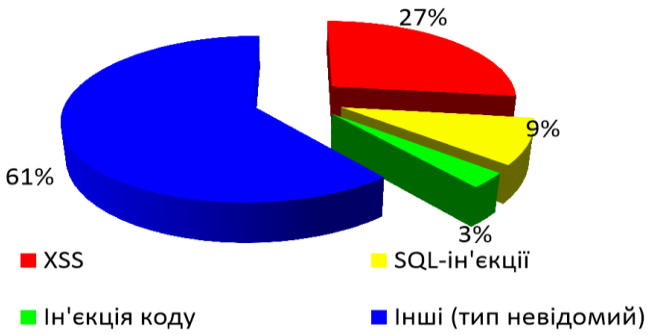

Рис. 1. Відсотковий розподіл загроз веб-сайтам

Рис. 2. Схема захисту інформації на веб-сайті

Використовуємо чотири рівня захисту інформації: 1. Використання спадаючого списку замість рядка введення даних. 2. Аудит введення даних у форми на боці клієнта за допомогою JavaScript. 3. Аудит введених даних на боці сервера. 4. Запит на сервер про правильність введення даних.

Список використаних джерел:

1. Седерхольм Д. Пуленепробиваемый Web-дизайн. Повышение гибкости сайта и защита от потенциальных неприятностей с помощью XHTML и CSS / Ден Седер- хольм, 2006. – 256 с. – (Школа Web-мастерства).

УДК 004.056

Рассамакін Володимир Якович
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Степашкін Роман Романович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Соціальна мережа (Інтернет) – інтерактивний багатокористувацький веб-сайт, контент якого наповнюється самими учасниками. Виходячи з цього визначення, зробимо висновок, що цікаві будуть персональні дані, які надаються самими користувачами. Ми найчастіше вносимо такі дані: ім'я, прізвище, по батькові, адреса, інтереси, місця відпочинку, роботи. З точки зору злочинців, соціальні мережі – вдале місце для розповсюдження шкідливих програм. Кінцева мета злочинців – отримати доступ до корпоративної мережі.

Шляхи проникнення:

- Розміщення посилань на «стіні». Під виглядом цікавих відео або милих фотографій злочинець закладає міну миттєвої дії. В кінцевому рахунку, замість фото або відео користувач відкриває дивні сайти, на яких його очікують віруси попутного завантаження;
- Використання методів соціальної інженерії. Злочинці нерідко вдаються до створення фейкових (підроблених) профілів, за допомогою яких вони зв'язуються з заздалегідь обраною жертвою і намагаються добути конфіденційну інформацію;
- Фішинг. Наприклад, користувач на робочому місці отримує повідомлення від Facebook, яке графічно дуже схоже на реальне повідомлення (а по суті, є якісно виконаної підробкою) і яке просить підтвердити особисті дані. Ні про що не підозрюючи користувач вводить логін і пароль, які вже відправляються до шахрая, а потім за старою відпрацьованою схемою – в корпоративну мережу;
- Збір особистих даних. Коли гра або будь-який інший сервіс запитує дозвіл на доступ до ваших особистих даних, то, швидше за все, це додаток займається збором інформації, щоб надалі запропонувати вам контекстну рекламу;
- Скамер-технології. Це злом і викрадення акаунту для поширення інформації серед великого кола користувачів.

Для того, щоб убезпечити себе і свої данні, необхідно дотримуватися до деяких наборів правил:

- ✓ Електронна пошта. Для реєстрації в соціальних мережах необхідно мати окрему пошту. Не можна реєструвати соціальні мережі з робочої пошти

або пошти, пов'язаної з важливими послугами (електронні гаманці, банківські послуги і т. п.).

✓ Пароль. Пароль – перша лінія захисту від зловмисників. Необхідно використовувати окремий пароль для кожного сервісу і забезпечувати його надійність.

Можливо, це незручно, але якщо паролі на всіх серверах збігаються, то зловмисник, дізнавшись пароль від одного сервісу, отримає доступ до всіх інших.

✓ Необхідно налаштувати відновлення пароля. Якщо користувач забув свій пароль або не зміг увійти до свого облікового запису, то зазвичай в таких випадках лист з відновленням пароля відправляється на додаткову адресу електронної пошти.

Крім того, ви можете додати номер телефону, на який приходить текстове повідомлення з кодом для відновлення пароля.

✓ Необхідно знайти політику приватності на веб-сайті соціальної мережі та прочитати, що відноситься до безпеки даних. Наприклад, чи може власник мережі використовувати інформацію в маркетингових дослідженнях?

✓ Необхідно з'ясувати, які програмні методи пропонує власник мережі для захисту даних. Наприклад, якщо ви заповнюєте профіль, чи можна визначити яку інформації не показувати іншим користувачам?

✓ Необхідно мінімізувати обсяг інформації, опублікованої в соціальній мережі.

Можливо, варто поділитися фотографією, але навряд чи варто розповідати світу про деталі вашого особистого життя, наприклад, про дітей або про те, як ви любите проводити вільний час.

✓ Слід проявляти обережність при натисканні на посилання, отримані в повідомленнях від інших користувачів.

✓ Не можна використовувати соціальну мережу або іншу аналогічну службу в якості основного сховища інформації.

✓ Не додавайте незнайомих людей в друзі в соціальних мережах.

✓ Не можна відвідувати соціальні мережі з робочого місця.

✓ Не можна відправляти важливі документи через соціальні мережі.

✓ Не можна публікувати фотографії документів.

Отже, проблеми захисту інформації в соціальних мережах досі остаточно не вирішені і можуть вирішитися тільки в результаті комплексного підходу, що включає в себе спільну роботу користувачів і розробників мережі, якщо ви будете використовувати всі методи в комплексі, це зменшить ризик крадіжки персональних даних до мінімуму.

Список використаних джерел:

1. Онищенко О. С. Соціальні мережі як чинник розвитку громадянського суспільства : [монографія] / [, В. М. Горовий, В. І. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2013. – 220 с.

2. Типове положення про службу захисту інформації в автоматизованій системі. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/

УДК 004.056

Козік Олександр Іванович
викладач кафедри інформаційних технологій
Київський національний університет будівництва і архітектури
Мельнічук Андрій Олександрович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

РОЛЬ ТА МІСЦЕ SSL СЕРТИФІКАТА У КІБЕРБЕЗПЕЦІ

Згідно ЗУ «Про основні засади забезпечення кібербезпеки України» Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Отже, напрямок «Кібербезпека» пов'язаний із захистом цифрової інформації, операційних систем, комп'ютерних мереж, серверів, баз даних, державних і приватних установ від несанкціонованого втручання сторонніх осіб. Як варіант, метою такого втручання може бути перехоплення конфіденційної інформації з комерційною метою.

На мою думку, визначення із законодавчого джерела не достатньо, й слід більш детально з'ясувати значення цього терміну та аспекти, які він охоплює на прикладі.

Уявіть ситуацію: ви оплачуєте замовлення в інтернеті, і вас просять ввести номер банківської картки. Із веб-переглядача вся ця інформація йде на сервер, де запускається процес валідації даних картки та надсилається квитанція-інвойс щодо банківської транзакції. Потім банк знімає з картки гроші. Крім даних картки, веб-переглядач може передавати іншу кофіденційну/особисту інформацію.

Зазвичай веб-переглядач передає всю інформацію у відкритому вигляді. Якщо в мережі знаходяться шахраї, вони зможуть перехопити інформацію й використати її в особистих цілях. Найчастіше про це дізнаються, коли з картки зникають гроші, або коли хтось змінює пароль в акаунті. Щоб уникнути таких ситуацій, потрібен SSL-сертифікат. На сайті з SSL-сертифікатом веб-переглядач використовує безпечне з'єднання.

SSL-сертифікат (англ. «Secure Sockets Layer certificate») – це засіб захисту особистої інформації користувачів в інтернеті. Якщо на сайті є SSL-сертифікат, в адресному рядку веб-переглядача з'явиться зелений замок і протокол HTTPS. Це означає, що на цьому сайті безпечно вводити пароль або номер банківської картки.

Коли користувач заповнює контактні форми на сайті із сертифікатом, веб-переглядач перетворює текст у випадковий набір символів і надсилає

повідомлення на сервер. Далі спеціальна програма на сервері перетворює зашифроване повідомлення знову у звичайний текст.

Щоб зашифрувати або розшифрувати повідомлення, потрібен ключ. Це основа будь-якого методу шифрування. Найпростіший спосіб – змінити кожну букву в слові на наступну. У цьому разі ключ – це зміщення на одну літеру вправо. Підібрати такий ключ легко. Шифрування SSL-сертифікатів значно складніше. У шахраїв підуть роки, щоб спробувати всі можливі ключі.

У роботі SSL-сертифіката бере участь два типи шифрування: симетричне й асиметричне.

Симетричне – це коли один ключ зашифровує та розшифровує повідомлення.

Асиметричне – коли є два різних ключі: публічний і приватний. Публічний лише зашифровує повідомлення, його бачить кожний веб-переглядач. Приватний лише розшифровує та конфіденційно зберігається на сервері.

Симетричне шифрування зручніше, але ключі мають знати обидві сторони. Це складно реалізувати, оскільки веб-переглядачів багато, а сервер, де встановлено SSL-сертифікат для сайту, один. Серверу довелося б щоразу надсилати ключ у відкритому вигляді, а це небезпечно. Для цього й потрібне асиметричне шифрування – щоб передати симетричний ключ.

Щоразу, коли на сайт заходить відвідувач, веб-переглядач генерує унікальний симетричний ключ, зашифровує його публічним ключем і надсилає на сервер. Сервер звіряє приватний ключ із публічним і розшифровує повідомлення. Цей процес займає кілька секунд.

Також слід зазначити, що з 2014 року з'єднання по HTTPS стало впливати на позицію сайту в Google. Це означає, що сайти з SSL-сертифікатами отримують перевагу при формуванні результатів пошуку. Співробітники Google оголосили про це в блозі компанії. Виробник сертифіката не має значення. Навіть якщо встановлено безкоштовний сертифікат від будь-якого вендора, це все буде враховано.

Нижче перелічено ключові переваги використання SSL-сертифікатів:

- ✓ Гарантує захищеність даних при їх передачі через мережу Інтернет.
- ✓ Збільшує рейтинг у пошуковій системі Google.
- ✓ Підвищує довіру клієнтів/користувачів.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 21.06.2018.
2. Офіційний сайт українського хостинг-провайдера HOSTiQ.ua – https://hostiq.ua.
3. Офіційний сайт постачальника рішень безпеки у Всеохопному Інтернеті (IoE) – GlobalSign – https://www.globalsign.com.
4. Офіційний сайт некомерційної організації The Canadian Internet Registration Authority (CIRA) – https://cira.ca

УДК 004.056

Харченко Олександр Анатолійович
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Слобожанін Ілля Іванович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ОГЛЯД НАЙБІЛЬШ КРИТИЧНИХ РИЗИКІВ, ЩО ВПЛИВАЮТЬ НА ЗАХИЩЕНІСТЬ WEB-ДОДАТКІВ

Розглянуто основні вразливості веб-додатків. Ключові слова: вразливість, OWASP, аутентифікація, конфігурація, десеріалізація.

Незахищене програмне забезпечення підриває нашу фінансову, медичну, оборонну, енергетичну та іншу критичну інфраструктуру. Наше програмне забезпечення стає все більш складним і труднощі досягнення безпеки додатків зростає експоненціально. Швидкі темпи сучасних процесів розробки програмного забезпечення дають найпоширеніші ризики, які необхідно виявити.

Щоб зламати веб-портал зловмисник збирає інформацію, необхідну і достатню для його зламу:

- перевірка використання на веб-сайтом сценаріїв, написаних власниками сайту або розроблених комерційними організаціями;
- детальний розгляд сценаріїв, які потребують введення даних користувачем;
- розгляд того, як сценарії обробляють введені дані;
- розгляд того, як фільтруються введені дані, щоб обійти ці фільтри;
- використання універсального web-фільтру, який продивляється HTTP заголовки повідомлень [5].

Існує організація OWASP (Open Web Application Security Project), що підтримується спільнотою та раз в 3-4 роки випускає список найбільш критичних вразливостей веб-додатків. При створенні даного рейтингу спільнота бере за основу різні міжнародні стандарти та інструменти найбільш відомих у сфері безпеки організацій.

Останній випуск OWASP top-10 був випущений у 2017 році, та в якості найбільш критичних ризиків визначає такі, як:

1. Ін’єкція шкідливого коду
2. Некоректна аутентифікація і управління сесією
3. Витік чутливих даних
4. Впровадження зовнішніх XML- сутностей (XXE)
5. Порушення контролю доступу
6. Небезпечна конфігурація
7. Міжсайтовий скриптинг
8. Небезпечна десеріалізація
9. Використання компонентів з відомими уразливими
10. Відсутність журналювання та моніторингу

В порівнянні з випуском 2013 року в документі є деякі зміни. XSS уразливості покинули трійку лідерів, але туди перенесли з 6 місця витік критичних (чутливих даних) – мабуть останні голосні витоки даних і зломи не пройшли даром і консорціум OWASP вирішив сфокусувати увагу на цю проблему. Додався новий тип вразливостей – eXternal Entity XML (XXE). XXE Ін'єкція – це тип атаки на додаток або препроцесор, які аналізують введення XML.

Також ми бачимо додавання пункту про небезпечну десеріалізацію – такого роду уразливості можуть призводити до віддаленого виконання коду, дозволяти підвищувати привілеї та багато іншого.

Додався пункт про відсутність моніторингу – за даними OWASP середній час виявлення інциденту становить 200 днів. Відкриті редіректи і CSRF покинули 10 найбільш значущих вразливостей. Загальна тенденція зміни списку OWASP говорить про зміщення пріоритетів вразливостей / векторів атак з client-side в server-side.

Список використаних джерел:

1. OWASP [Електронний ресурс]. - Точка доступу: URL: https://www.owasp.org/index.php/Main_Page
2. OWASP top 10 [Електронний ресурс]. - Точка доступу: URL: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
3. Основні зміни в OWASP top-10 2013 та 2017 [Електронний ресурс]. - Точка доступу: URL: https://habr.com/ru/post/342986/
4. Trevathan, Matt (1 October 2015). Seven Best Practices for Internet of Things. Database and Network Journal. Процитовано 28 November 2015 - через Шаблон:Highbeam.
5. Crosman, Penny (24 July 2015). Leaky Bank Websites Let Clickjacking, Other Threats Seep In. American Banker.

УДК 004.056

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Кінзерський Костянтин Юрійович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

БЕЗПЕКА САЙТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ КОНСУЛЬТАТИВНО-ДІАГНОСТИЧНОГО ЦЕНТРУ

З кожним днем тема захисту свого сайту стає все більш актуальною. В Інтернеті існує безліч інформації про те, як незаконно спробувати отримати доступ до сайту. Але є декілька діючих способів захисту власної інформаційної системи від несанкціонованого доступу.

Потрібно створювати якомога складніші паролі, використовуючи літери нижнього та верхнього регістру, також використовуйте цифри і символи у змішаному порядку. Довжина паролю повинна бути не менше ніж 8 символів, а далі чим більше – тим краще.

Дотримання цих нескладних правил зведе всі шанси злому програмою для підбору пароля майже до нуля. Також не потрібно користуватись однаковими паролями при реєстрації на інших Інтернет ресурсах, оскільки всі сайті схильні до злому.

Якщо зловмисники отримують доступ до бази даних web-сайту, вони можуть звідти дістати усі логіни і паролі користувачів, які потім будуть методом підбору вводити на інших сайтах, і якщо паролі однакові – злочинці знову ж таки заволодіють таким обліковим записом.

Створюючи інформаційну систему, необхідно користуватись тільки ліцензійним програмним забезпеченням, встановлювати антивіруси, і постійно оновлювати версію.

Встановлюючи піратське ПО, разом з цим на комп’ютер може бути встановлено і шпіонські програми, які можуть відслідковувати всю діяльність користувача, а також все що вводиться через клавіатуру.

На сайті інформаційної системи Консультативно-діагностичного центру не надаються права доступу до панелі адміністратора неперевіреним людям.

Для них створюються спеціальні облікові записи з обмеженими правами, оскільки несумлінні користувачі можуть додати на сайт шкідливий код.

Але не завжди злом сайту відбувається з необачності або необережності власника сайту. Іноді хакерам вдається знайти уразливість сайту саме у його вихідних кодах. Тому програміст при інформаційної системи повинен дуже уважно писати код, і не допускати помилки.

Якщо сайт побудований на готовій системі керування контентом, то розробники вже подбали про безпеку сайту. Необхідно встановлювати на web-сторінку лише перевірені плагіни, адже в них також може бути заховане шкідливе ПО.

Для додаткової безпеки сайту інформаційної безпеки Консультативно-діагностичного центру використовується протокол SSL (Secure Sockets Layer – рівень захищених сокетів) – це криптографічний протокол, який забезпечує захищену передачу інформації в мережі Інтернет.

Найчастіше SSL протокол використовують у випадках, коли необхідно забезпечити належний рівень захисту інформації, яку користувач передає на сервер. Це можуть бути дані кредитної карти, паспортні дані, ПІН-коди та інша інформація, яка може бути цікавою для зловмисників.

Безпека сайту інформаційної системи Консультативно-діагностичного центру – одна з найважливіших складових безперебійної і стабільної роботи Інтернет сторінки. Але навіть гарно захищений сайт може постраждати від хакерської атаки, тому потрібно бути завжди готовим – регулярно робити копії баз даних, щоб була можливість швидко відновити роботу web-сайту на іншому сервері, і час від часу змінювати пароль від облікових записів.

Список використаних джерел:

1. Заплотинський Б.А. Основи інформаційної безпеки.Конспект лекцій. – КІІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.

2. Башинська І.О. Основні порушники та загрози інформаційної безпеки промислових підприємств (с. 262-267) у міжнародній колективній монографії Problems of social and economic development of business: Collective monograph. – Publishing house «BREEZE», Montreal, Canada, 2014. – 408 p

4. Методи захисту від комп’ютерних вірусів [Електронний ресурс]. - Режим доступу: -https://computerbook.jimdo.com/довідник-студента/інформація-студентам/безпека-в-мережі-інтернет-та-при-роботі-з-пк/

5. Интернет-безопасность: самые распространенные ошибки и как их избежать [Електронний ресурс]. - Режим доступу: https://le-vpn.com/ru/internet-security-mistakes/

УДК 004.056

Rzayeva Svitlana Leonidivna
candidate of technical sciences,
associate professor of program engineering and cyber security department
Kyiv National University of Trade and Economics
Kucher Elvina Mikhailovna
student of the field of training area 6.050103 "Software engineering"
Kyiv National Trade and Economics University

INFORMATION TECHNOLOGY IN THE FIGHT AGAINST CYBERCRIME

Information offense - intentional acts aimed at the theft or destruction of information in informations systems, as well as in networks that derive from selfish or hooligan motives. Information crimes (cybercrime) include crimes committed under articles of the Criminal Code of Ukraine, included in Section 16 "Crimes in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks".

Although the analysis of the national legislation of Ukraine regulating public information relations allows us to state that our state is taking the necessary measures aimed at prevention and counteraction of computer crime, however, every year in Ukraine, the number of cyberattacks related to obtaining financial data and further using them for their own purposes cybercriminals.

The development of information and communication technologies has caused deep system transformations in information and cybernetic spaces. The last, by virtue of its specificity, creates new threats and challenges for information security specialists. Traditional information security specialists meet new specific tasks that require new knowledge and skills from them.

An analysis of the content of domestic textbooks on criminology, criminalistics, criminal and criminal procedural law shows that this issue was not given due attention. This, in turn, is due to the fact that in educational institutions trained by law enforcement officers and other law schools in our country, the issues of combating cybercrime have not been considered in practice.

A thorough investigation of the problems of cybercrime control was also hampered by the lack of indicators in state criminal statistics. Most of the detected crimes committed using computer technology are scattered in the reporting of various units of law enforcement agencies among economic and other types of crime. Among the state organizational, legal and information measures aimed at counteracting cybercrime, one can define the following.

The Government of Ukraine created special structures for coordinating the development of state policy in the field of ensuring the entry of our state into the world information society.

Draft Concept for the Reform of Ukrainian Legislation in the Field of Public Information Relations by Developing the Code of Information. In its content, the Concept referred to is a systematic policy in the field of information relations. The codification of information legislation will, among other things, facilitate the legal protection of the fight against cybercrime.

The Interdepartmental Committee on Protection of Rights to Intellectual Property Rights, the Interdepartmental Working Group on the Development and Coordination of the Concept of Legalization of Software Products and the Fight Against Their Illegal Use also deal with issues of improving the legal regulation, defining and organizing the implementation of state policy in the field of information relations.

1According to the Decree of the Government of Ukraine dated May 6, 2001, No. 181-r, an Interdepartmental Working Group was set up to develop a draft Information Security Concept and an Information Technology Crime Program. Unfortunately, there are no reports on the activities of this group in the media until today.

The analysis of empirical material allows us to predict that in the event of non-solving problems with the fight against organized cybercrime, especially in the sphere of international economic relations, the international community will increase information, political and economic pressure on Ukraine.

At this stage of development of the sphere of information technologies in Ukraine, systems of enterprise protection and their special data are underdeveloped and protected from cyber attacks. In order to avoid all kinds of risks, security services must protect not only the databases and work equipment of the personnel, but also computer networks, terminals of the front office employees and ATMs from cybercrime actions.

It should be emphasized that the training of specialists in information and cybersecurity and the leadership of public administration bodies on these issues for the needs of both law enforcement agencies and the production banking sector should be conducted in a unified system of education of Ukraine and be provided by the state in full.

References:

1. Karchevsky MV Computer information as a crime subject in the field of computer use, systems, computer networks and telecommunication networks / MV Karchevsky. // Combating crime in the field of computerinformation: the problems and ways to solve them. - 2012. - P. 61-64.
2. Chub O. O. Development of Internet Banking in a Global Environment / O. Chub. // Bulletin of the Ukrainian Academy of Banking. - 2009. - P. 62- 67.
3. Article on "Cybercrime as a factor in state information policy of Ukraine" - Access mode: http://goal-int.org/

УДК 004.34

Пашорін Валерій Іванович
кандидат технічних наук,
професор кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Назаренко Дмитро Миколайович
студент, 1курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ПЕРСОНАЛЬНИХ БАНКІВСЬКИХ КАРТОК

Шахрайства пов'язані із використанням пластикових карток стають все більш популярним явищем. Ця тенденція, пов'язана з поширенням безготівкового розрахунку користувачів. За даними НБУ, рівень емісії активних платіжних карток в Україні становить 30 млн шт. Враховуючи факт, що, як правило, на одну особу випущено 2 платіжні картки, то можна зробити висновок, що практично кожен другий громадянин України є власником платіжної картки.

Отримавши пластикові картки, користувачі банків, вважають що їхні кошти знаходяться в повній безпеці, оскільки без паролю, який знають лише вони, забрати ці кошти не зможе ніхто. Такою безпечністю і користуються зловмисники.

Метою дослідження є визначення видів шахрайств з платіжними картками та пошук методів та засобів їх запобігання.

Сьогодні відомо багато видів шахрайства з банківськими картками та банкоматами: скіммінг, фішинг, створення підроблених Інтернет-ресурсів, вірусні крадіжки даних про реквізити картки тощо.

Найпоширенішим із способів викрасти гроші з платіжної картки - скімінг. Зловмисники встановлюють на банкомати саморобні пристрої - скімери, які зчитують номер та штрих-код персональних пластикових карток. Також, окрім цього, на банкомат прикріплюють відеокамеру невеликого розміру, яка фіксує руку, та пароль що вона вводить і робить запис у модуль пам'яті або передає його дистанційно на комп'ютер шахрая [4, с. 146]. Далі можливі два варіанти: картку копіюють або ж банкомат не в змозі повернути її через так звану – «Леванську петлю» і картка застрягає в банкоматі. У першому випадку задоволений клієнт йде від терміналу з коштами які він отримав, навіть не підозрюючи що його дані вже знає не тільки він, у другому випадку – клієнт вирушає з коштами до банку щоб йому повернули його карту. Як тільки він відходить на певну відстань, злочинець отримує все що йому потрібно і кошти що знаходяться на рахунку до якого прив'язана дана картка, переходять до сторонньої людини.

Основними заходами з протидії даному виду шахрайства можуть бути:

- перевірка банкомату на наявність сторонніх ознак (накладна клавіатура, додатковий зчитувач) до початку користування даним банкоматом.
- вжиття додаткових заходів, що ускладнюють отримання інформації шахраями (зокрема – закривання клавіатури долонею при вводі ПІН-коду).

В Україні працює Національна система масових електронних платежів (НСМЕП) НБУ, яка застосовує чипові платіжні картки. НСМЕП використовує систему, що забезпечує неперервний захист інформації щодо здійснення операцій із застосуванням платіжних карток на всіх етапах її формування, оброблення, передавання та зберігання [2, с. 105].

Отже, проведений аналіз основних способів протидії шахрайствам із використанням банківських платіжних карток свідчить про те, що перспективним напрямом такої діяльності є використання чіп-модулів на банківських платіжних картках, оскільки окремі показники безпеки інформації можуть бути досягнуті виключно із застосуванням додаткових механізмів технічного захисту інформації. Чипові платіжні картки, що використовуються НСМЕП, цілком відповідають цим вимогам, а отже можуть розглядатися як один із перспективних платіжних механізмів в умовах активізації інформаційних шахрайств.

З метою структурувати та створити безпечні засоби протидії шахрайству в 2004 році був розроблений єдиний набір вимог до безпеки даних - Payment Card Industry Data Security Standard, що об'єднав в собі вимоги ряду програм з безпеки платіжних систем, а в 2006 році створена спеціальна Рада з безпеки - PCI Security Standards Council. Вона створила 12 обов’язкових вимог серед яких: шифрування даних тримачів карт при їх передачі через загальнодоступні мережі; не використовувати виставлених за замовчуванням виробниками системних паролів і інших параметрів безпеки; створення і супровід конфігурації міжмережевого екрану для захисту даних тримачів карт; відстеження всіх сеансів доступу до мережевих ресурсів; та інші.

Стандарт був введений для того, щоб допомогти тримачам платіжних карток, а також організаціям, що володіють інформацією про платіжні картки, вберегтися від щорічної втрати коштів через шахрайство. Він допомагає організаціям, що працюють з картками підвищити рівень безпеки, але не є єдиною причиною для реалізації відповідних рішень безпеки.

Список використаних джерел

1. Біломістна І. І. Сучасні тенденції розвитку ринку банківських платіжних карток в Україні / І. І. Біломістна // Економічні науки. - 2012. - № 9. - С. 26-36
2. Пивоваров В. В. До питання латентності корпоративної злочинності в банківській сфері І В. В. Пивоваров 11 Науковий вісник Херсонського державного університету. Серія: Юридичні науки.- 2013.- № 3. - С. 104-106.
3. Інтернет ресурс - https://news.finance.ua, 5 способів захисту від шахрайства з платіжними картками.

УДК 004.056

Крайнов Олексій Дмитрович
курсант
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

КІБЕРЗАХИСТ З ПРОВІДНИМИ ТЕХНОЛОГІЯМИ CYBER THREAT HUNTING

Кожного дня інформаційні технології все більше набувають актуальності в нашому житті. Технології переймають від реального усе підряд, включаючи кіберзлочинність. Злочини в кіберпросторі здійснюються за допомогою компютера та мережі Інтернет. Це несе загрозу для людини, суспільства та держави. Адже об'єктами кіберзлочиннів є особисті дані, паролі, банківські рахунки, нормативно-правові акти державного рівня. Найпоширенішими видами кіберзлочиннів є кардинг, фішинг, піратство, соціальна інженерія, рефайлінг.

Більшість кібератак спрямовані на такі інфраструткури як банківський сектор, траспорт тощо. Вартість захисту коштує в рази більше за саму атаку. В Україні питанням кіберзахисту займаються Державна служба спеціального зв'зку та захисту інформації, Служба безпеки України, кіберполіція Національної поліції Укаїни.

Однією із останніх та масштабних атак в Україні являється експлойт архіватора WinRAR для Windows. Успішність кібератаки заключалась в тому, що жертва повинна була розпакувати шкідливий архів. Розглянемо цю атаку на прикладі: зловмисник надсилає лист електронною поштою нібито від імені адмінстратора або служби безпеки задля уточнення свого рахунку, паролю чи ознайомлення з новим законом. В листі прикріплений архів dogovor.rar або zakon.rar, в якому міститься PDF документ. Вірус завантажує powershell скрипти, які надалі будуть використовуватися. Вразливість дає змогу розпакувати файли, що містяться в архіві, в потрібну папку для зловмисника, а не в ту, яку призначить користувач. Після цього шкідливий код поміщається в папку автозавантаження операціної системи, який буде виконуватися за замовчуванням при кожному завантаженні системи. Вразливості обходу каталогів отримали кілька ідентифікаторів: CVE-2018-20250, CVE-2018-20251, CVE-2018-20252 і CVE-2018-20253.

Для вирішення подібних питань рекомендується застосовувати технології Cyber Threat Hunting. Полювання на кіберзагрозу (Cyber Threat Hunting) - це процес активного пошуку по мережах і кінцевих точках для виявлення загроз, які ухиляються від існуючих контролів безпеки. Однією з технік Cyber Threat Hunting є Data Mining. Успішно налаштовані алгоритми здатні істотно підвищити ефективність захисту інформації.

За допомогою моніторингу та реагування на мережеві події, а також активності на окремих вузлах, полювання на загрозу (threat hunting) значно покращує видимість загроз. Це дає можливість виявлення невідомих загроз, а також виконувати аналіз, необхідний для розуміння і припинення атак.

УДК 004.056.5

Степашкіна Катерина Володимирівна
викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Яремич Валентин Романович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
Шевченко Ангеліна Анатоліївна
лаборант кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет

СТЕГАНОГРАФІЯ – МИСТЕЦТВО ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Стеганографія – це наука про передачу секретного повідомлення шляхом збереження в таємниці самого факту передачі такого повідомлення.

Слово стеганографія в буквальному перекладі з грецької означає тайнопис. На відміну від криптографії, яка приховує зміст повідомлення, стеганографія приховує саме його існування. До неї належить величезна безліч секретних засобів зв'язку: використання «невидимих» чорнил; мікрофотографія; записи на бічній стороні колоди карт, розташованих у домовленому порядку; трафарети, які будучи покладеними на текст, залишають видимими тільки значущі букви і т. д.

Стеганографія займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію. Використання стеганографічних методів приховування інформації значно знижує ймовірність виявлення самого факту надсилання секретного повідомлення. А якщо це повідомлення додатково зашифровано, то воно отримує ще один рівень захисту.

У зв'язку з активним розвитком обчислювальної техніки почали з’являтися та розвиватися нові стеганографічні методи, в основі яких лежать особливості подання інформації в комп'ютерних файлах, обчислювальних мережах і т. п. Все це призвело до становлення нового напрямку – комп'ютерної стеганографії.

В даний час ці методи розвиваються за двома основними напрямками:

- Методи, засновані на використанні спеціальних властивостей комп'ютерних форматів.
- Методи, засновані на надмірності аудіо та візуальної інформації.

Розглянемо деякі методи комп'ютерної стеганографії [1]:

1. Алгоритм LSB. Суть використання алгоритму LSB (Least Significant Bit, найменший значущий біт) та його підвидів полягає в заміні останніх значущих бітів у контейнері (зображенні, аудіо або відеозаписі) на біти приховуваного повідомлення. Його використання призводить до невеликих спотворень (зміни відтінку пікселя в зображені або частоти звуку), які людина зазвичай не сприймає. При використанні унікального контейнера (власної фотографії, аудіо або відеозапису) інформація буде додатково

захищена від можливості порівняння модифікованого та оригінального файлів, який може бути знайдений в мережі Інтернет. Цей алгоритм використовується у багатьох стеганографічних утилітах.

2. Приховування інформації в малюнках і фотографіях. Інформація може бути прихована у багатошаровому зображені: в одному із шарів розміщується прихована інформація, наприклад, у вигляді різнокольорової мозаїки. При цьому цей шар робиться прозорим. У результаті людина, яка відкриє цей файл засобами перегляду, то побачить лише початкове зображення.

Приховати архів в зображенні можна створивши так званий RARJPEG файл, для цього необхідно виконати просте злиття двох файлів форматів RAR та JPEG. Звичайно, це не акуратне «розчинення» за алгоритмом LSB, однак у цього методу є і свої переваги. По-перше, створений файл можна переглянути як картинку або ж відкрити будь-яким архіватором, який підтримує формат ZIP. По-друге, він дозволяє легко передати будь-який файл, завантаживши його як графічний, наприклад, на хостинг картинок або, частіше, іміджборд.

3. Приховування інформації в текстових документах. Методи приховування в текстових документах можна розділити на декілька видів [2]:

- Кодування інформації кількістю пробілів (наприклад, в кінці рядка).
- Виділення слів повідомлення пробілами (одним або двома).
- Синтаксичний метод (використання певної пунктуації).
- Орфографічний метод (заплановані орфографічні помилки).
- Семантичний метод (базується на кодуванні словником синонімів).
- Зміна формату тексту (кернінгу, відступів, кольору, розмірів тощо).

Розглянемо метод приховування інформації шляхом зміни кількості пробілів у тексті. Інформація для приховування надається у бінарному вигляді. Бінарна шифрограма додається у текст за допомогою символів пробілу. За допомогою одинарного пробілу кодується «1», а за допомогою подвійного – «0» [1].

4. Приховування інформації у DOCX файлі. Цей формат документа Microsoft Word надає можливість відкриття файлу архіватором, що дає змогу кодування інформації пробілами та табуляцією у вікні коментарів до архіву.

Висновок. Використання стеганографії та шифрування разом багаторазово підвищує складність виявлення і розкриття конфіденційної інформації.

Список використаних джерел:

1. Алексеев А. П. Стеганографические и криптографические методы защиты информации : учебное пособие. / А. П. Алексеев, В. В. Орлов. – Самара : ПГУТИ, 2010. – 332 с.

2. Тарасов Д. О. Класифікація та аналіз безкоштовних програмних засобів стеганографії / Д. О. Тарасов, А. С. Мельник, М. М. Голобородько // Інформаційні системи та мережі : [збірник наукових праць]. – Львів : Видавництво Національного університету «Львівська політехніка», 2010. – С. 365-373.

UDC 004.056

Holych Hanna
cadet
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

INFORMATION SECURITY SOLUTIONS IN CYBER THREAT INTELLIGENCE CYCLE

The problem of finding information security solutions for productive incident detection and response is actual and urgent nowadays as present security systems` weaknesses are vulnerable to known active and passive types of security attacks, so they need complex modernization or alternative replacement.

According to the fact, that intelligence-collection disciplines include:

- HUMINT (Human Intelligence);
- SOCMINT (Social media Intelligence);
- OSINT (Open-source Intelligence);
- ELINT (Electronic Intelligence);
- FININT (Financial Intelligence);
- TECHINT (Tech Intelligence);
- MARKINT (Market Intelligence) [1]

The definition of Cyber Threat Intelligence consolidates data from all these sources in order to provide effective cyberthreat intelligence campaign against cybercrime.

Conference paper by Khaled Elleithy and Marwah Almasri “Data Fusion Models in WSNs: Comparison and Analysis” determines 4 stages of Threat Intelligence Cycle model, which define technology requirements, needed for correlation of Threat Intelligence sharing platforms` activities:

- collection (gathering data from different sources);
- collation (interpretering and normalization of collected information);
- evaluation (data analysis and processing);
- dissemination (distribution, transmitting of evaluated information). [2]

Fundamental knowledge and understanding of Threat Intelligence Cycle stages is critically important for determining basic technology list on each stage, required for building cybersecurity centers and serving them by CIRT/CERT/CTI team/SOC team/ISAC and etc.

Providing basic data-security measures (strong passwords, firewall, antivirus protection, regular backup) are must-have, but insufficient safety protection methods.

Common usage of Cyber Threat Intelligence Platforms and hardware forms a modern approach in managing incident response activity and are indispensable in data aggregation, analysis and process automation for small/medium/large infrastructures.

Most comprehensive products among Cyber Threat Intelligence Platforms in the last 12 months, which should form a list of top complex information security software in Cyber Threat Intelligence Cycle are Comprehensive Cyber Risk Scorecard (by NormShield), Threat Connect (by Threat Connect), BrightCloud Threat Intelligence Services (Webroot), BlueCat DNS Edge (Blue Cat) and Adversary Intelligence (Intel 471). [3]

Cyber Threat Intelligence hardware stands for either proper organization network schemes planning or rational approach in hardware deployment. Network diagrams should foresee rising cost of security protecting devices, correspondence between hardware and installed software, horizontal and vertical integration.

Modern hardware solutions for organisations should count Next-Generation Firewalls, Secure SD-WANs, Secure Web Gateways, Sandboxes, Web Application Firewalls from leading Threat Intellegence vendors.

IT Central Station ranking through February, 2019 marks LogRhythm NextGen SIEM, Alien Vault, FireEye iSIGHT Threat Intelligence, ThreatConnect, ThreatStream to form the list of Top 5 Threat Intelligence Platform Vendors. [4]

Список використаних джерел:

1. Koen Van Impe. What Are the Different Types of Cyberthreat Intelligence? [Електронний ресурс] / Koen Van Impe // SecurityIntelligence. – 2018. – Режим доступу до ресурсу: https://securityintelligence.com/what-are-the-different-types-of-cyberthreat-intelligence/

2. Marwah M Almasri. Data Fusion Models in WSNs: Comparison and Analysis / Marwah M Almasri, Khaled M Elleithy. // Conference of the American Society for Engineering Education (ASEE Zone 1). – 2014.

3. Reviews for Security Threat Intelligence Products and Services [Електронний ресурс] // Gartner Peer Insights. – 2018. – Режим доступу до ресурсу: https://www.gartner.com/reviews/market/security-threat-intelligence-services/

4. Comparing the Best Threat Intelligence Platform Vendors for 2018 [Електронний ресурс] // IT Central Station. – 2018. – Режим доступу до ресурсу: https://www.itcentralstation.com/categories/threat-intelligence-platforms.

НАУКОВИЙ НАПРЯМ 3
КІБЕРЗАХИСТ НА ПІДПРИЄМСТВІ:
РЕАЛІЗАЦІЯ ПРИНЦИПІВ

SCIENTIFIC AREA 3
ENTERPRISE CYBERSECURITY:
PRINCIPLES IMPLEMENTATION

УДК 004.056.5

Чубаєвський Віталій Іванович
кандидат політичних наук,
доцент кафедри програмної інженерії та кібербезпеки КНТЕУ,
полковник поліції,
заступник начальника Департаменту кіберполіції Національної поліції України
Дроботенко Віктор Володимирович
заступник начальника управління - начальник відділу кібербезпеки Управління з протидії злочинам у сфері інформаційної безпеки департаменту кіберполіції Національної поліції України

ЕФЕКТИВНА ВЗАЄМОДІЯ ПРИВАТНОГО СЕКТОРУ ІЗ ПРАВООХОРОННИМИ ОРГАНАМИ ЯК НЕОБХІДНА ПЕРЕДУМОВА ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ

Аналіз зареєстрованих в Україні кіберзлочинів показує постійне зростання рівня кіберзлочинності та суми збитків, які завдаються кіберзлочинцями державі та бізнесу.

Відповідно до цього необхідно усвідомлювати, що рівень латентності у сфері розслідування кіберзлочинів є надзвичайно високим: в першу чергу, через те, що злочини, які мають на меті втручання у роботу комп'ютеризованих систем без їх очевидного пошкодження, або викрадення коштів у більшості випадків лишається непоміченим, або не повідомляється до органів правопорядку. Тому зазвичай, офіційна статистика за даними кримінальних справ становить менше половини від кількості кіберзлочинів.

Для попередження необ'єктивності, у своєму аналізі динаміки розвитку ситуації із кібербезпекою в Україні ми також спираємося на дані Державного центру кіберзахисту, що діє на базі Державної служби спецзв'язку та захисту інформації, а також на дослідження приватних компаній, які спеціалізуються у сфері надання послуг із забезпечення кібербезпеки та моніторингу кіберзагроз.

Так, за даними Державного центру кіберзахисту, кількість кіберінцидентів у попередні роки постійно зростає, при цьому спеціалісти центру зареєстрували сильний сплеск кібератак у 2013-2014 році, що супроводжувалися численними масованими DDoS атаками (949 DDoS атак у 2014 році). Після цього DDoS атаки начебто «вимкнули» і наступні роки характеризуються постійним зростанням зареєстрованих випадків неавторизованих утручань, шкідливого програмного забезпечення та фішингових атак, як правило пов'язаних із встановленням на комп'ютери громадян шкідливого програмного забезпечення (ШПЗ) та використанням засобів несанкціонованого віддаленого доступу до інформації на їх комп'ютерах.

Інше альтернативне джерело для аналізу – щорічне дослідження фінансових злочинів та шахрайства компанії PricewaterhouseCoopers (PwC)

свідчить про те, що 31% українських підприємств попали під приціл кіберзлочинів у 2018 році, порівняно із 24% у 2016 році [2].

Дослідження PwC також демонструє аномальну структуру кіберзлочинності в Україні та значно більшу кількість нападів з метою порушення бізнес процесів, та політично мотивованих атак, порівняно із загальносвітовим трендом. Так, політично-мотивовані атаки, тобто атаки без наміру отримати матеріальну вигоду за даними PwC в Україні стаються в 4 рази частіше ніж в інших країнах.

Така динаміка та співвідношення між різними типами атак істотно відрізняється від загальносвітових трендів та на нашу думку хоча і опосередковано проте переконливо свідчить про те, що більшість атак починаючи із 2013-2014 року здійснюються, або координуються з єдиного центру та спрямовані ексклюзивно проти України [2].

На жаль достовірних досліджень із визначенням розмірів збитків від кібератак в Україні не проводилось, проте мова йде про сотні мільйонів гривень прямих збитків та операційних втрат і колосальна репутаційна шкода, як для українського бізнесу, так і для держави вцілому.

Найбільш характерним прикладом кібератаки, яка була спрямована проти українського бізнесу та держави вцілому – атака шкідливого ПЗ NotPETYA, яка станом на сьогодні вважається найбільш руйнівною кібератакою в світовій історії.

Причина цього у тому, що обраний злочинцями первинний вектор атаки забезпечив безпрецедентну масовість та швидкість зараження комп'ютерів в Україні. Усі мережі і автоматизовані системи, уражені вірусом NotPETYA внаслідок первинного проникнення через оновлення ПЗ MeDoc, були фактично знищені на протязі 2-3 годин. За 3 години після початку атаки – злочинці згорнули свою контрольну інфраструктуру, та знищили її для приховання слідів злочину. Усі інші жертви цього нападу, тобто усі жертви за межами України, це лише «випадкова супутня шкода» зумовлена тим, що застосоване шкідливе ПЗ фактично є зброєю масового ураження невибіркової дії.

NotPETYA знищив інформацію на сотнях тисяч комп'ютерів в усьому світі та завдав близько 10 млрд. доларів США збитків десяткам організацій, включаючи об'єкти критичної транспортної інфраструктури та лікарні.

Для нас цілком очевидно, що основною метою нападників було завдання шкоди українському бізнесу та Україні як державі, проте нападники не врахували відсутність кордонів у кіберпросторі і розгалуженість ділових зв'язків, які українські підприємства та організації мали в усьому світі.

Для нас ця атака також стала очевидним доказом того, що жодна країна у світі не може ефективно протистояти таким нападам без зовнішньої допомоги, і жодна країна не застрахована від шкоди, якої завдають такі невибіркові засоби, навіть якщо основний об'єкт нападу знаходиться у іншій півкулі далеко за межами її регіональних та геополітичних інтересів.

Іншим висновком стало розуміння того, що кіберзахист неможливий без ефективної взаємодії між державними органами, які забезпечують кібербезпеку держави та приватними підприємствами, особливо тими, які в

силу популярності та розповсюдженості їх продуктів фактично набувають статус критично важливих об'єктів інформаційної інфраструктури.

За результатами нашого аналізу, що збігається із думкою більшості міжнародних експертів, важливими факультативними причинами катастрофічних наслідків цієї атаки стали:

- Відсутність належної системи забезпечення кібербезпеки на підприємстві MeDoc. Зловмисники на протязі кількох місяців мали неавторизований контроль серверів оновлень компанії та кілька разів використовували їх для розповсюдження шкідливого програмного забезпечення, очевидно тестуючи цей вектор зараження та відпрацьовуючи елементи кібератаки.
- Небажання менеджменту підприємства визнавати проблему на ранніх етапах зараження та низький рівень співробітництва із державними органами, які забезпечують кіберзахист держави, що дало зловмисникам достатньо часу для завершення атаки та знищення доказів, які могли б допомогти їх ідентифікувати.

Того ж року Верховною радою був ухвалений Закон України «Про основні засади забезпечення кібербезпеки України», який заклав правове підґрунтя для віднесення приватних підприємств до критично важливих об'єктів інформаційної інфраструктури із спеціальним статусом та запровадив поняття і основні характеристики державно-приватної взаємодії у сфері кібербезпеки.

Відповідно до положень ст. 1 та ст. 6 зазначеного Закону до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які [1]:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об'єктами потенційно небезпечних технологій і виробництв.

Стаття 10 Закону, у свою чергу, визначає шляхи здійснення державно-приватної взаємодії у сфері кібербезпеки [1]:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських

проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

Також Законом України «Про основні засади забезпечення кібербезпеки України» встановлюється обов'язок державних органів та органів місцевого самоврядування, їх посадових осіб, підприємств, установ та організацій незалежно від форми власності, осіб, громадян та об'єднання громадян сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків [1].

Запровадження такого обов'язку є необхідною передумовою створення належного рівня кіберзахисту, і за умови запровадження на кілька років раніше, можливо дозволило б попередити важкі наслідки як атаки NotPETYA так і багатьох інших руйнівних вірусів.

На жаль, національна система кібербезпеки України, так само як і законодавство у цій сфері, ще далеке від досконалості, або навіть від завершеності.

До сьогодні все ще не завершена розробка необхідних підзаконних нормативних актів, які б визначили порядок та способи реалізації положень закону. Не склалася правозастосовна практика та корпоративні традиції у цій

сфері. Все ще невирішеним залишається більшість питань щодо визначення конкретних суб'єктів, які забезпечуватимуть реалізацію положень цього закону та підготовки належної кількості спеціалістів у цій сфері.

З огляду на викладене, найбільш пріоритетними завданнями на даному етапі вважаються:

- завершення формування нормативно-правової бази у сфері кібербезпеки шляхом прийняття необхідних підзаконних актів в частині регулювання порядку віднесення підприємств до об'єктів критичної інфраструктури та проведення їх незалежного аудиту;
- підготовка та популяризація рекомендаційних вимог щодо кібербезпеки та стандартів реагування на кіберінциденти, з метою запровадження належного рівня кіберзахисту інформаційних систем держави та створення достатніх передумов для швидкого та ефективного реагування на кіберінциденти та розслідування кіберзлочинів.

Представники індустрії інформаційних технологій та власники підприємств віднесених до об'єктів критичної інфраструктури повинні більш відповідально відноситись до своїх обов'язків щодо забезпечення кібербезпеки держави та, відповідно до світової практики розпочати роботу над національними стандартами корпоративної етики та принципів взаємодії і обміну інформацією із державою та міжнародними акторами у цій сфері.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України». Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата відклику 17.03.19)
2. Pricewaterhouse Coopers Електронний ресурс. URL: https://www.pwc.com/ua/uk.html (дата відклику 17.03.19)
3. Mobile App Security. [Електронний ресурс]. URL: https://www.arxan.com/resources/technology/mobile-app-security
4. Платформа Ponemon Institute. [Електронний ресурс]. URL: https://www.ponemon.org/blog/tag/mobile%20security
5. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture, National Institute of Standards and Technology, U.S. Department of Commerce , 2015 –28c.
6. Gladius Partners with Remme to Tackle Enterprise Cybersecurity. [Електронний ресурс]. URL: https://medium.com/gladius-blog/gladius-partners-with-remme-to-tackle-enterprise-cybersecurity-b1d12c288fa6
7. P. Mell and T. Grance, The NIST definition of cloud computing, National Institute of Standards and Technology, U.S. Department of Commerce, 2014 – 100 c.
8. L. Badger, D. Berstein, R. Bohn, F. de Valux, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, US government cloud computing technology roadmap volume 1: High-priority requirements to further USG agency cloud computing adoption, National Institute of Standards and Technology, U.S. Department of Commerce, 2016 – 150 c.

УДК 004.738.5

Цюцюра Микола Ігорович
кандидат технічних наук,
доцент кафедри інформаційних технологій
Київський національний університет будівництва і архітектури

СУЧАСНІ ЗАСОБИ ЗАХИСТУ ПРИВАТНОЇ ІНФОРМАЦІЇ

Веб-ресурси на сьогодні є досить значущими на них, поряд зі звичайною інформацією розташовуються персональні дані користувачів (особисті повідомлення, адреси, телефони) або фінансова інформація (банківські сайти). Не санкціоноване використання інформації з таких ресурсів може призвести до значних збитків (як фінансових так матеріальних), та підступно-навмисне поширенням конфіденційної інформації. У зв’язку з цим необхідно дотримуватися особливих заходів веб-безпеки, застосовуючи криптографічні протоколи [1] як запобіжний захід втрати персональних даних, а саме:

1. SSL/TLS є криптографічними протоколами, призначеними для забезпечення безпеки зв'язку через комп'ютерну мережу. SSL (і його наступник, TLS) є протоколом, який працює безпосередньо над TCP. Таким чином, протоколи на більш високих рівнях (наприклад, HTTP) можуть залишатися незмінними, забезпечуючи при цьому безпечне з'єднання;
2. CORS (спільне використання ресурсів з різних джерел) – це функція HTML5, яка дозволяє одному сайту отримувати доступ до ресурсів іншого сайту, незважаючи на наявність різних доменних імен. Браузер вважатиме, що два ресурси мають однакове походження, тільки якщо вони використовують один і той же протокол (http / https);
3. Міжсайтова підробка запиту (XSS) відноситься до атаки ін'єкції коду на стороні клієнта, при якій зловмисник може виконувати шкідливий код у законний веб-сайт або веб-додаток. XSS є однією з найбільш поширених вразливостей веб-додатків і виникає, коли веб-додаток використовує непроголошений або незакодований користувальницький вхід у вихідних даних, які він створює.

Для забезпечення захисту приватної інформації слід також застосовувати і кібер-фізичні системи, тобто системи, які перебувають в інтенсивному зв'язку з навколишнім фізичним світом і його поточними процесами, забезпечуючи і використовуючи в той же час послуги доступу до даних і обробки даних, доступні в Інтернеті. Потенціал CPS – величезний і в змозі змінити будь який аспект життя. Такі концепції, як автономні автомобілі, робототехнічна хірургія, інтелектуальні будівлі, розумні електромережі, розумне виробництво і це не повний перелік прикладів, які вже існують. Працюючи в Інтернеті, реальний і віртуальний світи стають майже єдиним цілим, для формування Інтернету Речей.

Паралельний розвиток комп'ютерних систем та інформаційно-комунікаційних технологій, з одного боку, і виробництва, з іншого, вказують

на зближення двох світів – віртуального і фізичного. Кібер-фізичні виробничі системи дозволять і підтримують зв'язок між людьми, машинами та продуктами. Елементи CPPS здатні отримувати і обробляти дані, а також самоконтролювати певні завдання і взаємодіяти з людьми через інтерфейси.

Потенційні сфери застосування систем кібербезпеки стосовно захисту приватної інформації як фізичних так і юридичних осіб майже нескінченні:

- повітряний і наземний транспорт;
- дискретні та безперервні системи виробництва продукції;
- логістика, перевезення, ланцюги постачань;
- виробництво енергії; сонячні батареї, вітроенергетика, атомна енергія;
- все що оточує нас; інфраструктура, розваги тощо.

Через підходи кібербезпеки вони можуть призвести до розумних міст, виробничих, комунікаційних, логістичних і енергетичних систем; крім того, вони можуть сприяти створенню нової якості життя.

Проте, протягом останніх двох років провідні технологічні країни, такі як США, Китай та деякі країни ЄС, почали заохочувати і винагороджувати поступову реструктуризацію старих, більш вимогливих галузей до стабільних технологій, що, у свою чергу, дає можливість автоматизації та самостійності CPS Проекти, які безпосередньо вводяться в чергову хвилю повсякденних продуктів.

Розробка систем автоматичного налаштування для налаштування рівнів споживання енергії CPS та оптимізація її на основі навколишнього середовища була і залишається однією з ключових дослідницьких тем у хмарооснoвній галузі основної технології. Доступ до динамічної інформації з декількох джерел, практично резервного копіювання і часткової заміни необхідності спиратися на специфічні для датчиків і інформації, може запобігти неефективному пристосуванню КПС або, у випадку AI, що розвиваються, розвивати несправні адаптивні моделі поведінки.

На сьогодні, в той час коли соціальні та геополітичні ініціативи надають відповіді на майже всі загальні питання щодо забезпечення конфіденційності персональної інформації та висловлюють занепокоєння щодо інтеграції CPS до масштабних проектів в яких йде розробка самодостатності, рівномірної адаптивності до кожної частини інвазійних структур.

Висновок, як остаточна проблема, яку необхідно подолати, щоб забезпечити повне використання взаємодіючих та повністю автоматичних електронних взаємодій, є етика повністю цифрової динамічності розв'язання задач.

Список використаних джерел:

1. С.М. Білан, І.М. Шварц. Вдосконалення алгоритму Blowfish з метою підвищення крипостійкості та швидкодії під час передачі інформації по каналам зв’язку // Реєстрація, зберігання та обробка даних. – 2005. - №1, т.7. С.97-102.

УДК 342.9

Приходько Оксана Дмитрівна
директор мНУО Європейська Медіа Платформа
Букач Антоніна Василівна
Google for Education Certified Trainer, методист з інформаційних технологій
Науково-методичний центр управління освіти й науки Білоцерківської МР

КІБЕРБЕЗПЕКА З ТОЧКИ ЗОРУ УКРАЇНСЬКОЇ МОЛОДІ

Дослідження проведене міжнародною громадською організацією "Європейська Медіа Платформа" за підтримки Counterpart International та Google for Education Certified Trainer з метою визначення найпоширеніших кіберзагроз, з якими зустрічаються українські підлітки, та наявності в них інструментів протидії цим загрозам. Дослідження складалось з трьох етапів:

1. опитування в трьох фокус-групах в 2017-2018 роках;
2. опитування школярів-учасників он-лайн курсу з кібербезпеки (січень 2019 року);
3. опитування вчителів - учасників вебінару, присвяченого Дню Безпечнішого Інтернету 5 лютого 2019 року.

Загальна кількість респондентів - 1364 учні та 516 вчителів.

Результати:

- Більшість респондентів (68% учнів та 83% вчителів) зустрічались з кіберзагрозами. Більший відсоток вчителів пояснюється не тільки їхнім більшим досвідом користування Інтернетом, але й тим, що учні дуже часто навіть не усвідомлюють, що наразились на кібербезпеку.
- Найбільш поширеними кіберзагрозами є віруси, спам, шахрайство, піратство, крадіжка паролів. Менш поширеними – злом акаунтів, DDoS атаки, фінансові крадіжки, жорстоке поводження з дитиною, фішинг, булінг, грумінг.
- В окремих випадках респонденти скаржились на використання їхніх комп'ютерів для майнінгу біткоінів, в якості частини ботнетів, на кібертероризм та порнографію.
- Переважна більшість молоді, яка наразилась на кібербезпеку, не зверталась по допомогу (62%). Серед вчителів звертались по допомогу 54%. Найчастіше підлітки звертаються по допомогу до друзів (25%), на другому місці – батьки (23%). Невелика частка – менше 10% - звертались по допомогу до вчителів.
- Більше половини респондентів хотіли б отримати більше інформації та інструментів власної кібербезпеки, але 60 відсотків з них не знають, де і як їх шукати.
- Першоджерелом інформації з питань кібербезпеки є соціальні мережі. Близько 50 відсотків учнів продовжують користуватись російськими соціальними мережами.

Висновки та рекомендації:

1. На сьогодні у держави не існує власної «гарячої лінії» з питань кібербезпеки, зокрема окремої «дитячої» лінії. Така служба – Національна

дитяча «гаряча» лінія - є лише в ГО «Ла Страда – Україна».

Що робити? Поінформувати підлітків про існування Національної дитячої «гарячої лінії» - 0 800 500 335 або 116 123 (короткий номер з мобільного) - спільними зусиллями МОН, правоохоронних органів, навчальних закладів, операторів та провайдерів, IT бізнесу, медіа, громадських організацій.

2. І молоді, і фахівцям бракує інформації про види кіберзагроз.

Що робити? Розробити модель ризиків та алгоритм протидії кіберзагрозам для молоді – спільними зусиллями експертів правоохоронних органів, бізнесу, громадськості, молоді. Проводити регулярні опитування молоді з питань кібербезпеки з врахуванням віку, освіти, засобів доступу до Інтернету, використовуючи ресурси фахівців МОН, соціологів, кіберполіції, бізнесу, громадськості, молоді. Широко презентувати та аналізувати результати досліджень. Привести українську термінологію з кібербезпеки у відповідність до європейської

3. Молодь не усвідомлює ризики від користування російськими соціальними мережами і російським та/або піратським програмним забезпеченням (зокрема, антивірусами).

Що робити? Розробити інформаційну кампанію про ризики користування російськими соціальними мережами і піратським та/або російським програмним забезпеченням – за участі соціологів, експертів з кібербезпеки, освітян, медійників, фахівців з PR і SMM та молоді. Запровадити обов’язкову стандартизацію програмного забезпечення в навчальних закладах з метою неприпустимості використання піратського та/або російського програмного забезпечення, пропагувати відкрите програмне забезпечення – зусиллями МОН та правоохоронних органів, за участі приватних та громадських експертів

4. Молодь не знає, де шукати інформацію про кіберзагрози та як убезпечитися від них.

Що робити? Розробити державну просвітницьку програму з кібербезпеки, орієнтовану на молодь (як в якості частини шкільного курсу з інформатики, так і в якості окремих курсів) – за участі міжнародних експертів, спільними зусиллями фахівців з державного, приватного та громадського секторів, обов'язково за участі молоді. Розробити державну програму профілактичних заходів з кібербезки для навчальних закладів – за участі міжнародних експертів, спільними зусиллями фахівців з державного, приватного та громадського секторів. Регулярно інформувати молодь про нові кіберзагрози та про те, як можна убезпечитись від них – зусиллями CERT-UA та кіберполіції за допомогою приватних та громадських фахівців, медіа, активістів соціальних мереж. Просувати існуючі та створити нові он-лайн ресурси, що сприяють підвищенню поінформованості молоді з питань кібербезпеки.

Список використаних джерел:

1. Kostiainen, M. (2016). Internet safety for children: Finnish practices and stakeholders. Retrieved from: http://tampub.uta.fi/handle/10024/99386

УДК 004.056.5

Чубаєвська Вікторія Андріївна
заступник начальника відділу режиму та технічного захисту інформації, підполковник поліції
Головне управління національної поліції в Рівненській області
Гнатченко Тетяна Олександрівна
аспірант кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет

КІБЕРЗАГРОЗИ БЕЗПЕЦІ КОРПОРАТИВНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ

Розвиток інформаційних технологій все більше розширює можливості доступу до інформаційних ресурсів та передачі великих обсягів даних на необмежені відстані. У той же час, доступ широкого кола користувачів до ресурсів у межах глобальної інформаційної мережі, збільшує загрозу корпоративним інформаційним ресурсам та підприємства в цілому. Великого значення набуває забезпечення інформаційної безпеки корпоративного підприємства, у зв'язку із зростаючими обсягами інформації, наявністю значної частини інформації в електронній формі, необхідністю використання локальних і глобальних мереж у процесі ведення підприємницької діяльності.

До основних джерел загроз інформаційній безпеці корпоративного підприємства можна віднести наступні: протизаконна діяльність деяких структур у сфері формування, поширення і використання інформації; порушення встановлених регламентів збору, обробки та передачі інформації; навмисні дії та ненавмисні помилки користувачів інформаційних систем; помилки в проектуванні інформаційних систем; відмова технічних засобів і збої програмного забезпечення тощо [1].

На сьогодні питання інформаційної безпеки входить до числа головних пріоритетів менеджменту національних і світових корпорацій, оскільки все більше число керівників бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією. Так, сучасна корпоративна система інформаційної безпеки має бути побудована на принципах конфіденційності (захист інформації від несанкціонованого доступу), цілісності (запобігати зловмисним або випадковим змінам) і доступності (надавати необхідний рівень доступу).

Нехтування вищенаведеними ключовими принципами може призвести до негативних наслідків у діяльності підприємства, таких як: збої у функціонуванні систем управління технологічними та управлінськими процесами; розголошення відомостей, що становлять комерційну та інші види таємниць; порушення достовірності фінансової звітності; несанкціонованого доступу до бази даних підприємства; викривлення публічної інформації тощо; у певних ситуаціях - до повної втрати бізнесу [2].

Враховуючи розгалуженість ІТ-інфраструктури корпоративного підприємства, особливого захисту потребують сервери і мережеві пристрої. Перші – як концентратори великих обсягів інформації, другі – як елементи, в яких здійснюється перетворення даних при узгодженні протоколів обміну в різних ділянках корпоративної мережі. Також увагу слід приділити захисту каналів і засобів зв'язку. У зв'язку із великою протяжністю ліній зв'язку практично завжди існує можливість підключення до них, або втручання в процес передачі даних [3].

Розглядаючи сучасні превентивні засоби захисту інформації, розташованої у корпоративній мережі, варто виділити так званий pentest (penetration test – тест на проникність), що довів свою ефективність завдяки виявленню численних слабких місць у корпоративних мережах. До можливостей тесту на проникність можна віднести наступні: дізнатися можливості здійснення загроз безпеці інформації; оцінити наслідки спрямованої хакерської атаки; визначити уразливості в захисті інформаційної системи; оцінити ефективність засобів захисту інформації; оцінити ефективність менеджменту інформаційної безпеки; оцінити ймовірний рівень кваліфікації порушника для успішної реалізації атаки; отримати аргументи для обґрунтування подальшого вкладення ресурсів в ІБ; виробити список контрзаходів, щоб знизити можливість реалізації атак [4].

Отже, з метою забезпечення кібербезпеки корпоративної інформаційної системи, керівники підприємств мають приділити особливу увагу політиці інформаційної безпеки, а саме: розробити та впровадити систему превентивних заходів щодо потенційних загроз; поглиблено використовувати функціональні можливості програм-антивірусів та брандмауерів; вести моніторинг дій суб’єктів інформаційної системи з можливістю пост-контролю.

Список використаних джерел:

1. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства / С. В. Легомінова // Економіка. Менеджмент. Бізнес. - 2015. - № 3. - С. 87-92.
2. Нехай В. А. Інформаційна безпека як складова економічної безпеки підприємств / В. А. Нехай, В. В. Нехай // Науковий вісник Міжнародного гуманітарного університету. Серія : Економіка і менеджмент. - 2017. - № 24(2). - С. 137-140.
3. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури / Юрій Васильєв // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2015. – № 1(29). – С. 56-61.
4. Киричок Р. В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення / Р. В. Киричок, П. М. Складанний, В. Л. Бурячок, Г. М. Гулак, В. А. Козачок // Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. - № 3. - С. 48-61.

УДК 374.73

Рибак Анатолій Іванович
доктор технічних наук, професор, академік Академії зв'язку України,
професор кафедри «Технічна кібернетика ім. проф. Р.В. Меркта»
Одеський Національний морський університет
Азарова Ірина Борисівна
кандидат технічних наук, доцент кафедри проектного менеджменту
Одеський регіональний інститут державного управління НАДУ при Президентові України
Новіков Даніїл Денисович
студент напряму підготовки 122 «Комп'ютерні науки та інформаційні технології»
Одеський Національний політехнічний університет

ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ З ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ

Не зважаючи на те, що високий рівень кваліфікації українських фахівців з інформаційних технологій добре відомий в усьому світі, проблема підготовки якісних спеціалістів в цій сфері залишається актуальною. Справа у тому, що більшість з ІТ-фахівців, що зараз працюють як в Україні, так і за кордоном – самоучки. Серед них також забагато "джуніорів" (початківців) і мало справжніх "про-спеціалістів" (професіоналів), у той час, як ринок потребує кадрів, що здатні створити якісний кінцевий інноваційний продукт – проджект-менеджерів, бізнес-аналітиків та продакт-менеджерів.

Недостатній рівень підготовки ІТ-кадрів у навчальних закладах викликаний як застарілими теоретичними програми навчання у профільних вишах, що не встигають адаптуватися до стрімкого розвитку ІТ, так і низьким рівнем мотивації викладачів, умови праці яких є нецікавими для досвідчених практиків. Крім того, фахівці підкреслюють, що для підготовки конкурентних кадрів у вишах потрібно паралельно з суто технічними дисциплінами вводити курси з основ менеджменту, ведення комерційних проектів, роботи з клієнтами, маркетингу проектів, промислового програмування, які зараз або відсутні, або викладаються теоретично. Але для роботодавця важливі практичні навички кандидата, які він може привнести в компанію та удосконалити в процесі роботи. [1] Тому зараз компанії змушені витрачати час найбільш кваліфікованих кадрів на стажування випускників, а молодь змушена шукати альтернативні шляхи підвищення власної конкурентоспроможності на ринку ІТ праці. Проблема додатково ускладняється ще й тим, що вже через кілька років роботи отримана кваліфікація дозволяє новоспеченому спеціалісту знайти роботу у більш благополучній країні, що сприяє відтоку кращих кадрів і знов викликає їх нестачу в Україні.

Все це означає, що вдосконалення методів підготовки кадрів в сфері ІТ та кібербезпеки - є актуальною задачею як для навчальних закладів, так і для

майбутніх спеціалістів та компаній, що працюють у галузі. Нажаль, проведене дослідження свідчить про відсутність взаємодії ІТ-освіти і ринку праці, що також є причиною усіх згаданих проблем. Тому пошук можливості поєднання теоретичної підготовки у навчальному закладі з практикою на реальних проектах та підприємствах - є дуже важливим для всіх згаданих зацікавлених сторін.

В Одесі першими цю необхідність усвідомили саме ІТ-підприємства. Однією з таких компаній було ініційовано проект для підготовки кадрів в рамках створеного інноваційного простору «Atom Space» для підлітків, що навчає навичкам 4К (комунікація, креатив, командна робота, критичне мислення) та базовим принципам технологічної грамотності. Аналогів такого ІТ-простору в Одесі поки не існує, хоча є цілий ряд комерційних курсів з цього напрямку. На думку засновника компанії [2], проект повинен допомогти молоді визначитися з майбутньою спеціальністю і розкрити для них світ ІТ-технологій. Унікальністю цього освітнього проекту є те, що ментори (наставники) та викладачі навчають молодь (резидентів) і координують їх проекти повністю на громадських засадах. Для резидентів також відсутня плата за навчання за будь-яким обраним напрямом. Таким чином, бенефіціари проекту отримують: можливість поєднання самоосвіти і роботи з практикуючими фахівцями, як метод ефективного отримання технічних знань для резидентів; практичний досвід спільної роботи над професійними завданнями в команді із менторами і такими ж резидентами як спосіб отримання навичок командного досягнення цілей; можливість роботи без обмежень над своїми проектами та ідеями в максимально доброзичливому співтоваристві, як спосіб розвитку креативності [3].

Ініціатор проекту також отримує свої вигоди - у середньостроковій перспективі він створює для свого бізнесу кваліфікований кадровий потенціал, повністю лояльний та адаптований до роботи в компанії. Додатковим бонусом для нього є також розвиток креативності менторів, отримуваний від спілкування з творчою молоддю.

Отже, висновком цього дослідження є те, що успішне вирішення проблем підготовки кадрів у сфері інформаційних технологій в майбутньому можливе лише на засадах організації взаємодії між усіма зацікавленими сторонами в галузі – закладами ІТ освіти, бізнес-одиницями та майбутніми фахівцями. А поки що прикладами успішних локальних рішень можуть слугувати стратегічні ініціативи окремих підприємств з фахової підготовки кадрів на власній виробничій базі, що і було висвітлено у цьому дослідженні.

Список використаних джерел:

1. Поперешняк С.В. Проблеми підготовки ІТ-спецілістів // Системи обробки інформації, 2010, № 7 (88). - С. 127-129.
2. Новое место: в Одессе появился коворкинг для подростков Atom Space [Електронний ресурс]. – Режим доступу: http://forshmag.me/2017/08/07/novoe-mesto-v-odesse-poyavilsya-kovorking-dlya-podrostkov-atom-space/
3. Освітній ІТ-простір для підлітків [Електронний ресурс]. - Режим доступу: https://www.atomspace.od.ua/

УДК 004.056.5

Мельниченко Світлана Володимирівна
доктор економічних наук, професор, проректор з наукової роботи
Київський національний торговельно-економічний університет
Криворучко Олена Володимирівна
доктор технічних наук, професор,
завідувач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Івлєв Ігор Олександрович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ПРОБЛЕМИ УПРАВЛІННЯ КЛЮЧАМИ КРИПТОГРАФІЇ В ХМАРНИХ ТЕХНОЛОГІЯХ

Криптографічні операції складають одну з основних завдань управління безпекою.У той час як хмарні послуги надають повсюдні обчислення, еластичні можливості та налаштовуванні ресурси за менших витрат, вони також тягнуть за собою виконання декількох криптографічних операцій (з точки зору споживача хмари) для:

- безпечної взаємодії споживача хмари з різними послугами;
- безпечного зберігання даних, створених або оброблених цими службами.

Система керування ключами (СКК), необхідна для підтримки криптографічних операцій для вищезгаданих функцій, може бути складною через відмінності у власності та контролі основних інфраструктур, на яких розташовані СКК та захищені ресурси. Хоча право власності на дані у хмарних службах лежить на хмарі споживача, дані фізично перебувають на ресурсах зберігання, керованих провайдером хмари, а в багатьох випадках СКК необхідний для керування криптографічними ключами, необхідними для захисту даних для запуску на обчислювальних ресурсах, що надаються постачальником хмарних послуг. Це створює проблеми для споживачів у хмарі, які прагнуть отримати необхідну гарантію безпеки від цих криптографічних операцій.

Драйвер для набору криптографічних операцій, що виконуються в основних моделях хмарних сервісів (IaaS, PaaS і SaaS), залежить від особливостей, які складають ці послуги. Хоча існують невеликі відмінності в наборі функцій серед різних постачальників хмари, можна визначити основний набір функцій.

Необхідно відзначити, що в усіх архітектурних рішеннях, де криптографічні ключі зберігаються в хмарі, існує межа ступеня гарантії безпеки, яку може очікувати споживач хмари, у зв'язку з тим, що логічна і фізична організація ресурси зберігання повністю під контролем постачальника хмари.

У хмарі IaaS споживач розгортає свої власні обчислювальні ресурси у вигляді віртуальних машин або орендує їх від постачальника хмари. Опція оренди включає в себе перевірку готових образів, пропонованих хмарним провайдером IaaS. Витягнуті образи віртуальних машин повинні бути автентифіковані, щоб гарантувати, що вони отримані з офіційних джерел і не були підроблені. Після налаштувань віртуальної машини її необхідно запустити в інфраструктурі хмарного провайдера, щоб вона стала працюючим екземпляром віртуальної машини. Операція запуску віртуальної машини та подальших операцій життєвого циклу на віртуальній машині (такі як Stop, Pause, Restart, Killetc) виконується споживачем хмари IaaS через доступ до інтерфейсу керування Hypervisor. Крім того, під час операцій або використання хмарних сервісів споживач хмари IaaS повинен безпечно взаємодіяти з запущеними примірниками віртуальних машин.

Метою PaaS є забезпечення обчислювальної платформи та необхідного набору засобів розробки додатків для розробки або розгортання додатків. Хоча основна платформа ОС, на якій розміщені інструменти розробки, відома споживачеві, споживач не має контролю над своїми функціями конфігурації і, отже, в результаті операційним середовищем. Споживачі взаємодіють з цими інструментами (та відповідними даними, такими як бібліотеки розробки) для розробки спеціальних програм. Споживачам також може знадобитися інфраструктура зберігання для зберігання як підтримуючих даних, так і даних додатків для тестування функціональних можливостей програми.

SaaSзабезпечує доступ до додатків, розміщених на постачальниках послуг у хмарі. Споживач хмари SaaSможе безпечно взаємодіяти з прикладними програмами (шляхом налаштування захищених сеансів і сильної автентифікації) і використовувати різні функції програми, залежно від набору призначених дозволів або прийняття їх призначених ролей (які надають дозволи). Крім того, деякі споживачі SaaS також можуть зберігати дані, що генеруються, обробляються цими додатками, в зашифрованому вигляді з причин: запобігти розкриттю своїх корпоративних даних через втрату мультимедійних даних, що використовуються постачальниками хмари, а також приховане переглядання даних спільнім орендарем SaaS або адміністратором провайдера хмари.

Список використаних джерел

1. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture, National Institute of Standards and Technology, U.S. Department of Commerce , 2015 –28c.
2. P. Mell and T. Grance, The NIST definition of cloud computing, National Institute of Standards and Technology, U.S. Department of Commerce, 2014 – 100 c.
3. L. Badger, D. Berstein, R. Bohn, F. de Valux, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, US government cloud computing technology roadmap volume 1: High-priority requirements to further USG agency cloud computing adoption, National Institute of Standards and Technology, U.S. Department of Commerce, 2016 – 150 c.

УДК 004.77

Лотюк Юрій Георгійович
кандидат педагогічних наук, доцент
Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука
Соловей Людмила Ярославівна
старший викладач
Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука
Юскович-Жуковська Валентина Іванівна
кандидат технічних наук, доцент,
декан факультету кібернетики
Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука

КІБЕРЗАХИСТ ЛОКАЛЬНОЇ МЕРЕЖІ УНІВЕРСИТЕТУ

Мережеві технології є одними з найбільш популярних і зручних засобів для організації обміну інформацією, доступу до віддалених ресурсів, баз даних, баз знань тощо. Але водночас ці технології можуть нести в собі загрози інформаційній безпеці навчального закладу. Пакети даних, які транспортуються через мережу, можуть бути випадково чи спеціально перехоплені та модифіковані. Не виключається можливість несанкціонованого доступу до внутрішніх ресурсів мережі університету.

Тому актуальним є питання організації захисту локальної мережі університету від загроз із глобальної мережі Інтернет. Можливі загрози та захист від них розглянемо на прикладі внутрішньої мережі Приватного вищого навчального закладу «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука» (ПВНЗ МЕГУ).

Локальна мережа університету містить різноманітні ресурси. Є освітні ресурси, що призначені лише для використання у внутрішній мережі, це: автоматизована інформаційно-бібліотечна система "УФД/Бібліотека"; наукова бібліотека; дистанційна освіта; бази даних деканатів: студенти, спеціальності, групи, курси, розклад занять, успішності студентів, відвідування занять; технічні ресурси, доступ до яких забезпечується для користувачів як локальної, так і глобальної мереж.

Атака на локальну мережу університету може здійснюватися як з комп'ютера внутрішньої мережі МЕГУ, так і з глобальної мережі. Для виявлення та припинення атаки потрібно, по-перше, розпізнати атаку, по-друге змінити правила брандмауера. Всі нові пакети даних, що надходять у мережу, підпадають під фільтрацію брандмауера.

У мережі ПВНЗ МЕГУ використовується брандмауер на основі ОС MicroTik, основні функції якого: фільтрування за джерелом та призначенням IP-протоколу, портів призначення та відправлення, джерела та призначення для трафіку TCP та UDP, журналювання трафіку, що відповідає кожному

правилу, визначення правил маршрутизації, вибір шлюзу для балансування навантаження тощо.

Для покращення кіберзахисту локальна мережа університету розбита на віртуальні VLAN, кожна з яких підключається до відповідного порту. VLAN створені таким чином, що кожна VLAN відповідає кожній комп'ютерній аудиторії, що унеможливлює атаки на комп'ютери поза цією аудиторією. Прозорий брандмауер 2-го рівня - дозволяє об'єднувати інтерфейси та фільтрувати трафік між ними.

На базі MicroTik організовано сервер DHCP та динамічний DNS сервер. Це спрощує приєднання комп'ютерів користувачів та дозволяє без зайвих переналаштувань міняти розміщення комп'ютерів у локальній мережі [1].

Для доступу до глобальної мережі Інтернет використовується NAT - мережева трансляція адрес. Оскільки університет підключений до високошвидкісного каналу Інтернет, то можливості проксі-сервера не застосовуються.

Для кіберзахисту мережі використовується нормалізація пакетів шляхом відкидання пакетів з невірно сформованими полями, які можуть бути як результатами помилок ОС користувачів, так і специфічно сформованими для хакерської атаки на мережу. MicroTik є брандмауером з технологією SPI, що дозволяє додатково захиститися від атак, виконуючи перевірку трафіку на коректність.

Для реалізації захисту мережі визначається набір правил - сукупність всіх правил створених адміністратором або сформованих автоматично. У MikroTik набори правил оцінюються за принципом першого збігу. Після досягнення відповідності та виконання дії необхідного правила обробка зупиняється.

Вхідна фільтрація визначає набір правил обробки трафіку, який входить у внутрішню мережу з зовнішньої мережі Інтернет. За замовчуванням в системі MikroTik застосовується політика, яка блокує весь трафік, що приходить на WAN ззовні. Тому адміністратор має ретельно вивчити та описати правила для вхідного трафіку у внутрішню мережу ПВНЗ МЕГУ.

Вихідна фільтрація застосовується до трафіку ініційованого внутрішньою мережею. У MikroTik за замовчуванням застосовується правило, що дозволяє весь трафік з LAN транспортувати в зовнішню мережу. Слід намагатись мінімізувати трафік, тобто дозволити з локальної мережі виходити мінімуму необхідного трафіку, наскільки це можливо.

Отже, сервер з встановленою на нього RouterOS Mikrotik, здатний вирішити основні завдання з кіберзахисту, обслуговування та надання необхідних сервісів локальній мережі МЕГУ та локальній мережі будь-якого навчального закладу.

Список використаних джерел:

1. Лотюк Ю. Г. Безпека Wi-Fi мережі організації [Електронний ресурс] / Ю. Г. Лотюк, Л. Я. Соловей, В. І. Юскович-Жуковська // Психолого-педагогічні основи гуманізації навчально-виховного процесу в школі та ВНЗ. - 2018. - Вип. 2. - С. 76-83. - Режим доступу: http://nbuv.gov.ua/UJRN/Ppog_2018_2_12

УДК 004.056.53

Палагута Катерина Олексіївна
кандидат економічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Тютюнник Ілля Сергійович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет
Іванова Дарина Олексіївна
студентка 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

З давніх часів людство хвилювала проблематика питання захисту інформації способом її перетворення, для запобігання її прочитання сторонньою особою.

Можна сказати, шо історія криптографії є ровесницею нашої мови, оскільки саму по собі писемність можна назвати криптографічною системою, бо раніше, у стародавні часи, нею володіли тільки обрані. Прикладами тому слугують численні стародавні священні книги Єгипту, Індії та ін.

Криптографічні методи захисту інформації – це спеціальні методи захисту інформації, а саме: шифрування, кодування та ін., в результаті дії яких, прочитання її стає недоступним без наявності ключа криптограми і зворотного перетворення.

Найнадійніший метод захисту однозначно криптографічний метод, оскільки він охороняє саме інформацію, а не доступ до неї, тому навіть у випадку втрати або її крадіжки зашифрований файл неможливо прочитати. Зазвичай даний метод реалізується як програма або пакет програм.

На даний момент криптографія поділяється на такі розділи:

1) Криптосистеми з відкритим ключем або асиметричний шифр

Це система, у якій використовується відкритий і закритий ключі, які пов’язані математичним способом між собою. Шифрується інформація відкритим, доступним для усіх ключем, а розшифровується за допомогою закритого, який відомий лише отримувачу.

2) Симетричні криптосистеми

Відповідно до їх назви, у таких криптосистемах використовується один ключ і для алгоритму шифрування, і для дешифрування. Сам ключ повинен зберігатися у секреті, оскільки симетричні криптоалгоритми виконують перетворення невеликого блоку даних таким способом, що прочитання інформації можливе лише при наявності секретного ключа.

Ця система має чотири класи перетворень, а саме: підстановка, перестановка, аналітичне перетворення та комбіноване перетворення.

3) Електронний підпис

Системою електронного цифрового підпису називається криптографічне перетворення його електронних даних, до яких додається сам підпис або логічне їх поєднання, яке дає змогу перевірити його цілісність та ідентифікувати користувача (передплатника) та достовірність повідомлення.

4) Управління ключами

Ця система грає найважливішу роль і криптографії, вона є основою забезпечення конфіденційності, цілісності та ідентифікації інформації. Процес полягає у складанні та розподілі ключів поміж користувачами.

Цей інформаційний процес включає в себе три елементи: накопичення ключів, їх генерацію та розподіл.

Кожен з криптографічних методів, розглянутих вище, може бути реалізований як програмним, так і апаратним способами.

Сама можливість програмної реалізації методів, обумовлена тим, що усі методи криптографічного перетворення є формальними. Вони можуть бути представлені у вигляді кінцевої алгоритмічної процедури. А при апаратній реалізації усі процеси шифрування і дешифрування виконуються за допомогою спеціальних електронних схем.

1. Найбільшою перевагою програмних методів реалізації захисту є їх гнучкість, а саме можливість швидкісної зміни шифрування алгоритмів та систем. Водночас найгіршим недоліком програмної реалізації є набагато менша швидкодія, якщо порівнювати з апаратними засобами (приблизно в 10 разів).

2. На сьогоднішній день поступово стали з'являтися комбіновані засоби шифрування або програмноапаратні засоби. При таких способах у комп'ютері використовується своєрідний «криптографічний співпроцесор» - обчислювальний пристрій, який орієнтується на виконання криптографічних операцій. Міняючи програмне забезпечення для даного пристрою, можна вибирати будь-який метод шифрування. Такий метод поєднує у собі переваги що програмного, що апаратного методів.

Отже, вибір типу реалізації криптозахисту для конкретної інформаційної системи в основній мірі залежить від її особливостей і повинен враховувати усі вимоги, що пред'являються системою захисту.

Список використаних джерел:

1. Аналіз Методів Криптографічного Захисту Інформації [Електронний ресурс]. – Режим доступу до ресурсу: http://ir.nmu.org.ua/jspui/bitstream/123456789/149264/1/6-7.pdf

2. Бабак В.П. Теоретичні основи захисту інформації / В. П. Бабак: Підручник. – Книжкове видавництво НАУ, 2008. – 752 с.

3. Криптографічні засоби захисту інформації [Електронний ресурс]. – Режим доступу до ресурсу: https://studfiles.net/preview/5462915/page:18/

УДК 004.056.5

Цюцюра Микола Ігоревич
кандидат технічних наук,
доцент кафедри інформаційних технологій
Київський національний університет будівництва та архітектури
Тіхонов Антон Олегович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

СИСТЕМИ ТА МЕТОДИ ЗАПОБІГАННЯ КОМПРОМЕНТАЦІЇ ТА ЗБЕРЕЖЕННЯ ДАННИХ НА ПІДПРИЄМСТВІ

У сучасному світі всі компанії, підприємства працюють з конфіденційною інформацією. Яка інформація є конфіденційною та як запобігти викрадення або виток її, саме це буде розглянуто нижче.

Будь які персональні дані співробітників, будь які дані стосовно внутрішніх процесів виробництва або надання послуг можна вважати конфіденційною інформацією.

Норми захисту персональних даних в Україні регулюються Законом України про захист персональних даних від 2010 року. Хоча на той час і існували інтернет технології, мережа, веб простір, але він не був такий розвинений, як зараз. Саме тому у травні 2018 року Європейський Союз приймає резолюцію GDPR (General Data Protection Regulation), котра регулює правила збереження та обробки персональних даних європейців.

Компанії несуть власну відповідальність за збір, збереження та оброку інформації клієнтів, у разі порушення цих правил їх чекає покарання у вигляді штрафу, а саме 20 млн. євро або 4% від глобального оберту компанії, якщо ж випадок не тяжкий, то сума штрафу складатиме – 10 млн. євро або 2% від глобального оберту компанії.

Як захистити інформацію, які існують способи захисту інформації в корпоративній мережі та яких методів слід дотримуватись?

По перше, треба чітко розділити технічний та людські фактори. Тобто, існують технології, стандарти, процедури які націлені на захист інформації як з технічної точки зору, так і правила поведінки з даними для працівників компанії.

Спочатку розглянемо технічні застосування, технології котрі допоможуть нам зберегти інформацію. Коли ми говорим про технічну частину, перш за все це стосується – мережевої інфраструктури компанії та технічне забезпечення (персональні комп’ютери, телефони, мережеві пристрої, сервера). Існує такий вислів в сфері інформаційної безпеки – « Ваша мережа вже скомпрометована, але ви про це ще не знаєте», виходячи з

цього, потрібно розуміти, що на 100 відсотків захищених систем – не існує. Але це не означає, що про безпеку зовсім не потрібно дбати.

Почнемо з проектування мережі в компанії. Потрібно розуміти, кількість офісів, кількість робочих місць та основні задачі підприємства. Якщо це компанія з одним офісом, та всі працюють лише в межах цього офісу, то нам не потрібно налаштовувати IPSEC\VPN тунелі між різними будівлями, нам вистачить встановити фізичний фаєрвол, котрий буде контролювати вхідний та вихідний трафік в мережу інтернет. Також можна розділити офіс на підмережі, тим самим ізолюючи один підрозділ від іншого, це допоможе в разі втручання в локальну мережу та обмежить розповсюдження шкідливих програм, вірусів, скриптів.

За статистикою компаній, котрі займаються кібер безпекою, захистом конфіденційної інформації - дуже великий відсоток, близько 70-80 відсотків даних компрометують або «зливають» самі користувачі. Іноді навмисно, іноді через власну неуважність. В інтернеті можна прочитати дуже багато статей, де причиною «зливу» конфіденційних даних є людський фактор.

Саме для цього в великих компаніях існують підрозділи, котрі працюють над системами безпеки. Створюють внутрішні процедури, правила поведінки з корпоративною інформацією.

Іноді через людську неуважність компанія може понести дуже великі збитки, втратити репутацію та своїх клієнтів. Тому ця сфера є дуже важливою в будь-якій компанії, яка працює в будь-якій сфері. Не важливо компанія займається доставкою їжі, чи будівництвом, чи то онлайн платформа для спілкування чи щось інше.

Сучасні практики з захисту інформації наголошують на тому, щоб люди не користувались флеш носіями, не записували ніякої інформації на диски при роботі з будь-якою інформацією. Обмін інформацією повинен бути лише через корпоративну пошту або портали по типу SharePoint та інші. Всі ці засоби в основному працюють через захищені канали в інтернеті та скомпрометувати їх – дуже важко.

Підводячи висновки, можна сказати, що з розвитком інформаційних технологій – оберт інформації стає все більше і більше, як і можливості цю інформацію викрасти, підробити чи то видалити. Тому необхідно приділяти дуже багато уваги до внутрішньої політики праці з інформацією та заводити підрозділи або наймати окремого фахівця в цій сфері, знов ж таки залежить від обсягу компанії.

Список використаних джерел:

1. Gladius Partners with Remme to Tackle Enterprise Cybersecurity. [Електронний ресурс]. URL: https://medium.com/gladius-blog/gladius-partners-with-remme-to-tackle-enterprise-cybersecurity-b1d12c288fa6.
2. SwiftKeychainWrapper від Джейсона Ренделя (jrendel) для Swift. https://cocoapods.org/pods/SwiftKeychainWrapper. Електронний ресурс. URL: https://github.com/jrendel/SwiftKeychainWrapper.

УДК 004.056, 004.8

Демідов Павло Георгійович
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій
Київський національний торговельно-економічний університет
Краскевич Валерій Євгенович
доктор технічних наук, професор,
завідувач кафедри інформаційних технологій
Київський національний торговельно-економічний університет

НЕЙРОННІ ТА НЕЧІТКІ ПІДХОДИ ДО ВИРІШЕННЯ ЗАДАЧ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В сьогоднішніх умовах функціонування підприємств в значній мірі спирається на розвинуті інформаційні технології, що приводить до зростання залежності організацій від інформаційних систем і сервісів та, як наслідок, відбувається різке збільшення ризиків, пов'язаних з недостатнім рівнем забезпечення безпеки одержання, зберігання і переробки інформації.

Інформаційна безпека підприємства - це стан захищеності корпоративних даних, при якій забезпечується їх конфіденційність, цілісність, автентичність і доступність. Завдання систем інформаційної безпеки підприємства (СІБП) різні: забезпечення захищеного зберігання інформації на носіях; захист даних, що передаються по каналах зв'язку; створення резервних копій, після аварійне відновлення і таке інше.

Забезпечення інформаційної безпеки підприємства можливо тільки при системному і комплексному підході до захисту.

Інформаційна безпека підприємства передбачає проведення наступних видів робіт:

- виконання оцінки вразливих місць на системному рівні. Комп'ютерні системи повинні бути досліджені на відомі уразливості і найпростіші політики відповідності технічним вимогам;
- виконання оцінки на мережевому рівні. Повинна бути зроблена оцінка існуючої комп'ютерної мережі та інформаційної інфраструктури, виявлені зони ризику;
- виконання загальної оцінки ризику в рамках організації. Повинен бути зроблений аналіз всієї організації з метою виявлення загроз для її інформаційних активів;
- проведення аудиту. Повинна бути досліджена існуюча політика і відповідність організації цієї політики;
- проведено випробування на можливість проникнення. Досліджено здатність організації реагувати на змодельоване проникнення [3].

Складнощі з якими стикаються розробники під час розробки систем інформаційної безпеки підприємства характеризуються наступними рисами [1]:

1. Недостатністю або невизначеністю знань про задачі СІБП, коли отримання необхідної інформації є складної, трудомісткою, дорогої або зовсім неможливою задачею.

2. Неможливістю враховувати та адекватно обробляти невизначену інформацію традиційними методами.

3. Неможливістю проводити моделювання і ідентифікацію реальних систем, які є нелінійними в своїй основі і не можуть бути представлені моделями, які використовують традиційні методи ідентифікації.

Наслідком сказаного, є необхідність залучення до традиційного математичного апарату моделювання складних систем теорії нечітких множин та нечіткої логіки, які дозволяють розробляти моделі в умовах невизначеності знань, враховувати та адекватно обробляти невизначену інформацію, проводити «прозоре» моделювання і ідентифікацію реальних систем.

Побудова нечітких моделей для вирішення задач СІБП спирається, як правило, на апріорно визначені компоненти цих моделей (нечіткі висловлювання, функції приналежності та інше). Оскільки ці компоненти найчастіше вибираються суб'єктивно, вони можуть бути не цілком адекватні системі або процесу, які моделюються.

Вирішення цієї проблеми потребує також залучення технологій штучних нейронних мереж, які дозволяють виявити закономірності в даних, провести їх узагальнення, провести налаштування параметрів функцій приналежності нечітких моделей на основі експериментальних даних.

Індустрія інформаційної безпеки швидко змінюється. Наведене вище дозволяє зробити висновок, що без технологій штучного інтелекту в цій області не обійтися. І цьому є також підтвердження величезного росту об’ємів даних. В Cisco підрахували, що в 2021 році загальний обсяг IP-трафіку складе 278 Ебайт в місяць (ексабайт, екса - x10 ^ 18). Не захищати ці дані не можна, а ресурсів для захисту «людськими» методами не вистачає. В такий ситуації для підвищення рівня інформаційної безпеки фахівці пропонують залучити технології блокчейн та квантові генератори. Звичайно, це ще не всі технології, які варто вивчати фахівцям у сфері інформаційної безпеки. Big data, machine learning, deep learning, ботнети і IoT, хмарні технології - список можна продовжувати ще довго [4]. Але поки (в майбутньому теж) ми робимо акцент в галузі інформаційної безпеки на технології штучного інтелекту.

Список використаних джерел:

1. Борисов В. В. Нечёткие модели и сети. – 2-е изд., стереотип./ В.В.Борисов, В.В. Круглов, А.С. Федулов – М.: Горячая линия–Телеком, 2012. – 284 с.

2. Демідов П.Г. Про підходи до розробки програмного забезпечення систем кібербезпеки / П.Г. Демідов // Тези доповідей Всеукр. науково-практ. конф. «Кібербезпека в Україні: правові та організаційні питання», 30 листопада 2018 року. - Одеський державний університет внутрішніх справ, 2018. – С. 53-55.

3. Інформаційна безпека підприємства. Режим доступу: https://ru.wikipedia.org/wiki/Информационная_безопасность

4. Як зміниться індустрія кібербезпеки в найближчі 10 років. Режим доступу: https://dou.ua/lenta/articles/future-of-cybersecurity.

УДК 346.11

Нескороджена Лариса Леонідівна
кандидат юридичних наук,
доцент кафедри міжнародного приватного, комерційного та цивільного права
Київський національний торговельно-економічний університет

ПРИНЦИПИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

За статистичними даними щороку здійснення купівлі товарів через Інтернет збільшується, однак не дивлячись на всі зусилля кіберполіції, все ще є випадки шахрайства з Інтернет - магазинами, неправомірне використання отриманих персональних даних, викрадення коштів з рахунків тощо. Крім того, розвиток цифрових технологій породив безмежну та безпрецедентну ймовірність ідентифікації особи за її персональними даними, що може заподіяти шкоду життю і здоров'ю особи. Актуальність визначення принципів захисту персональних даних полягає ще й в тому, що з 25 травня 2018 року в Європейському Союзі вступив в силу новий нормативний акт - Загальний Регламент Захисту Даних, більш відомий як GDPR (General Data Protection Regulation). Зазначений нормативний акт встановлює нові правила поводження з персональними даними, а Регламент стосується будь-якої роботи з персональними даними, зокрема збору, зберігання, передачі[1]. Відповідно до Плану заходів з виконання Угоди про асоціацію між Україною та Європейським Союзом[2], Україна зобов'язана була до 25 травня 2018 року узгодити законодавство України про захист персональних даних із GDPR. Закон України «Про електронну комерцію»[2] у ст.14 визначає загальні положення щодо захисту персональних даних у сфері електронної комерції. Деталізація принципів захисту персональних даних розкрита у Директиві ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»[3] (надалі – Директива ЄС) та Законі України «Про захист персональних даних»[4] (надалі - Закон України).

Ключовими принципами захисту персональних даних в електронній комерції є:

- принцип законності обробки персональних даних. Відповідно до ст.6 Директиви ЄС та ст.6 Закону України законною є лише та обробка персональних даних, яка здійснюється чесно і законно; для встановлених, чітких і законних цілей; не є надлишковою щодо цілей, заради яких персональні дані збираються і/або надалі обробляються;

- принцип конкретизації мети та обмежень обробки даних. Закон України визначає, що обробка персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних;

- принцип конфіденційності та безпеки обробки персональних даних. Держава зобов'язана створити ефективну правову базу, яка буде гарантувати реалізацію права на захист конфіденційності і персональних даних, адже воно є фундаментальним правом людини;

- принцип правомірного використання та збирання персональних даних. Отримання персональних даних може бути лише за вільної згоди особи, яка є власником таких даних;

-принцип відповідальності за заподіяну шкоду.

Відповідно до ст. 23 Директиви ЄС передбачено, що будь-яка особа, якій завдано шкоди в результаті незаконної операції із обробки чи будь-якої іншої дії щодо персональних даних має право на одержання компенсації за завдану шкоду. Ст.28 Закону України носить відсилочний характер та зазначає, що порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом. Конкретизація санкції за порушення законодавства у сфері захисту персональних даних міститься у ст. 188-39 Кодексу України про адміністративні правопорушення[4]. Позитивним моментом, який закріплений в GDPR, є те що особа, яка збирає та обробляє персональні дані, зобов'язана вжити всіх заходів для безпеки зберігання, обробки та використання даних, адже вона несе повну відповідальність за шкоду яка може бути заподіяна. Крім того, GDPR встановлює штрафні санкції за порушення законодавства в сфері захисту персональних даних. Щодо відшкодування майнової та моральної шкоди, то з аналізу рішень Європейського суду з прав людини та Верховного суду можна зробити висновок, що в разі доведеності порушення законодавства в сфері захисту персональних даних така шкода відшкодовується автоматично.

Список використаних джерел:

1. Нужний В. Нові вимоги ЄС до захисту персональних даних з травня 2018 року // hannel4it.com/publications/Nov-vimogi-S-do-zahistu-personalnih-danih-z-travnya-2018-roku-30154.html#

2. Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: постанова КМУ від 25 жовтня 2017 р. № 1106// Офіційний вісник України. - 2018 р.- № 24.- Ст. 27.

3. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII//Відомості Верховної Ради. - 2015. - № 45.- Ст.410.

4. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива Європейського Парламенту і Ради від 24 жовтня 1995 року № 95/46/ЄС// https://zakon.rada.gov.ua/laws/show/994_242

5. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI//Відомості Верховної Ради України.-2010.- № 34.- Ст. 481

6. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 № 8073-X//Відомості Верховної Ради УРСР.- 1984.- №51.-1122.

УДК 004

Дорош Марія Сергіївна
доктор технічних наук,
доцент кафедри інформаційних технологій та програмної інженерії
Чернігівський національний технологічний університет
Войцеховська Марія Михайлівна
аспірант кафедри інформаційних технологій та програмної інженерії
Чернігівський національний технологічний університет

ВПРОВАДЖЕННЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ УПРАВЛІННІ ПРОЕКТАМИ

Сьогодні інформаційне суспільство динамічно розвивається та зумовлює зростання кількості різних видів взаємодій із застосуванням сучасних інформаційних технологій. Основною метою таких змін є підвищення продуктивності роботи учасників, що в свою чергу дасть можливість досягти масштабніших та більш достовірних результатів за більш короткий проміжок часу.

В міжнародних проектах інформаційні процеси значно ускладнюються наявністю більшої кількості рівнів різних факторів формування культури. Це і загальна культура, і культура традицій, і культура соціальної та бізнес поведінки різних країн-учасників проекту.

При цьому культура інформаційної безпеки проекту (КІБП) виступає невід'ємним елементом системи управління комунікаціями в проектах. Важлива роль КІБ підчас проектної діяльності наголошена положеннями засадничого міжнародного стандарту ISO/IEC 27001 [1]. Як і організаційна культура, КІБП є повноцінною системою, і поняття «стан» являє для неї упорядковану множину суттєвих властивостей, які має система в кожний момент часу [2]. Отже, питання формування культури інформаційної безпеки в міжнародних проектах є актуальним на фоні постійного збільшення їх кількості і потребує окремих досліджень.

Спираючись на [3], в залежності від етапу життєвого циклу проекту, можна виділити декілька етапів зрілості культури ІБ.

Перший етап – нульовий – співпадає із етапом ініціалізації проекту. На цьому етапі основна увага приділяється вирішенню питань можливості здійснення проекту, а зусилля менеджера проекту спрямовані на доведення ефективності проекту та залучення необхідних учасників для його реалізації. При цьому вирішення питань ІБ може бути ініціативою потенційних учасників та цілком залежить від їх власного ставлення до цієї проблеми. Тут можуть формуватися тільки первинні способи інформаційної взаємодії між учасниками. На цьому рівні важливо визначити ступінь важливості інформаційної безпеки для кожного учасника проекту.

Етап другий – фрагментарний захист. Має формуватися на етапі планування проекту, оскільки тут вже визначені учасники проекту, та складається план комунікацій в проекті. Важливим є вибір програмних засобів взаємодії, планування та контролю проекту в залежності від визначених вимог до безпеки. В проекті формуються окремі документи, що регламентують інформаційну безпеку проекту та його учасників.

Третій етап – системний захист – має досягатися на етапі впровадження (реалізації) проекту. Напрацювання минулих етапів дають змогу формувати загальний інформаційно-безпечний простір для учасників проекту. Сталість процесів на цьому етапі дає змогу формалізувати та задокументувати основні положення КІБП; учасники розуміють її цінності а всі процеси поєднані в загальний інформаційний потік. Завдяки цьому в проекті з'являється можливість аналізу інформації за всіма аспектами управлінської діяльності, а також отримання оперативної інформації про ступінь використання ресурсів для всіх учасників проекту. При цьому використовуються засоби захисту, які необов'язково мають бути сертифікованими. Але вся діяльність щодо захисту вже має бути зарегламентована нормативними документами.

Етап четвертий – керований захист – співпадає з етапом завершення проекту. Тут важливим є збереження напрацьованої інформації по проекту, та забезпечення технічної підтримки впровадження результатів проекту. При цьому сформована КІБ персоналу може бути основою для подальшої взаємодії із коригуванням для нових учасників.

На даному етапі засоби захисту функціонують повноцінно, а побудована комплексна система захисту інформації в проекті створює умови надійної та безпечної роботи за допомогою застосування комплексу заходів захисту, які відповідають основним вимогам:

- вдало відбивати більшу частину ймовірних атак;
- при істотних порушеннях нормального функціонування, які можуть виникати при зовнішніх впливах різного роду (в тому числі, і в результаті реалізованих атак) система повинна мати здатність або до повного самовідновлення, або до відновлення за нормативні терміни та з мінімальними втратами;
- при побудові системи необхідно дотримуватися оптимального співвідношення (ціна системи) / ймовірні втрати.

Список використаних джерел:

1. ISO/IEC 27001:2013 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».
2. Терещенко Т. Теорія організації : навчальний посібник / Тетяна Василівна Терещенко. - Хмельницький : Хмельницький університет управління та права, 2015. – 335 с.
3. Загинайлов Ю.Н. Комплексная система защиты информации на предприятии: учебно-методическое пособие / Ю.Н. Загинайлов и др., - Алт.гос.техн.ун-т им. И.И.Ползунова. - Барнаул: АлтГТУ. – 2010 - 287с.

УДК 368.1

Ротова Тетяна Анатоліївна
кандидат економічних наук, доцент
Київський національний торговельно-економічний університет
Шевченко Юлія
студентка 3 курсу 1 групи ФФБС,
спеціальність 072 «Фінанси, банківська справа та страхування»
Київський національний торговельно-економічний університет

СТРАХУВАННЯ ЯК ФІНАНСОВИЙ ІНСТРУМЕНТ ЗАХИСТУ ВІД КІБЕР-РИЗИКІВ

Поняття кіберстрахування для України є доволі новим і мало дослідженим, але сьогодні воно набуває актуальності, оскільки багато українських підприємств та організацій потребують захисту від кібератак.

Враховуючи те, що кібер-ризики, під якими мається на увазі ризик, що у результаті виходу з ладу ІТ систем й систем інформаційної безпеки призводить до фінансових та матеріальних втрат (штрафи регулюючих органів, втрати корпоративних даних та даних клієнтів, інтелектуальної власності, репутаційні втрати), необхідність розробки програм страхування не викликає сумніву.

Страхування як фінансовий інструмент набув поширення на міжнародному ринку ще у 2010 році. За оцінками Munich Re, обсяги кіберстрахування у 2020 році складуть $8-9 млрд проти $3,4-4 млрд у 2017 році. [1] Щорічне дослідження Allianz Global Corporate & Specialty AGCS) що проведено 2415 експертами з 86 країн (включаючи топ-менеджерів компаній, страхових експертів, брокерів і ризик-менеджерів), кібер-ризики (кіберзлочинність, збої у роботі ІТ-систем, вразливість даних, штрафи) посідають друге місце серед глобальних ризиків підприємств та фінансового сектора на 2019 рік. [2]

Найбільш привабливими для кіберзлочинців є фінансово-кредитні установи, особливо банки, які широко використовують сучасні ІТ. У зоні ризику також будь-яка компанія, що зберігає інформацію щодо клієнтів в електронному вигляді: аудитори, рітейлори, брокерські, туристичні, транспортні, страхові компанії, заклади сфери розваг. Страхування відповідальності перед третіми особами у сфері ІТ особливо актуальне для ІТ-провайдерів, хостинг-центрів, розробників програмного забезпечення.

Страхування кібер-ризиків дозволяє відшкодувати прямі збитки (перерва діяльності, витрати на відновлення даних, втрати доходу в результати виходу з ладу ІТ-мереж або веб-сайтів), а також збитки третім особам та додаткові витрати (позовні витрати у зв’язку з відповідальністю щодо злому бази даних, судова експертиза, експертна, юридична підтримка).

У даний час вітчизняний страховий ринок суттєво відстає від страховиків інших країн у питанні кіберстрахування. Можна лише відмітити «PZU Україна», «ВУСО», «АСКА», «Global Garant», «Українська страхова група», «ІНГО Україна», які працюють над розробкою і впровадженням таких

програм страхування, а масштабні хакерські атаки в Україні, що спостерігалися у 2014-2017 роках, підтверджують їх необхідність.

Укладення договору страхування кібер-ризиків пов'язане з комплексною оцінкою клієнта і його систем. Оцінюється економічний стан компанії, канали продажів, безпека комп'ютерних мереж, ступінь захисту персональних даних клієнтів. Чим більше у страхувальника доступу до конфіденційної інформації користувачів, тим дорожче буде ціна страхової програми. Також впливає фізична охорона серверних, доступ до них, наявність ключів доступу, регулярність резервного копіювання даних.

Факторами, що стримують розвиток страхування кібер-ризиків в Україні є наявність неякісної IT-інфраструктури, у багатьох компаній неліцензійне програмне забезпечення та потреба у доведенні підприємством саме факту кібератаки. Не всі із постраждалих від кібератак бажають повідомляти про витоки даних та проломи у системі безпеки. Перешкодою є й висока вартість страхових програм, оскільки страховики працюють із недостатньою страховою статистикою, а відтак важко правильно розрахувати страхові тарифи.

Розвиток кіберстрахування потребує об’єднання зусиль страхових компаній, Департаменту кіберполіції, Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації задля протидії кіберзагрозам. У Законі «Про основні засади забезпечення кібербезпеки України» зазначено, що «державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом: періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки». [3]

Отже, з розвитком страхування кібер-ризиків стає вагомим інструментом ризик-менеджменту для підприємств як державної, так і недержавної форми власності. Це перспективний напрямок розвитку страхового бізнесу, оскільки створення страхових програм захисту крім безпосереднього відшкодування збитків, значною мірою охороняє від таких ризиків та не дозволяє припинити або знищити бізнес.

Список використаних джерел:

1. Пігулка від хакерів: як бізнес захищає себе від кібератак. [Електронний ресурс] : [Веб-сайт]. – Режим доступу : https://mind.ua/publications/ 20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak (дата звернення 12.03.2019) – Назва з екрана.
2. Барометр рисков. Allianz назвал глобальные риски предприятий и финансового сектора на 2019 год. [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://forinsurer.com/news/19/01/16/36513?hl=%EA% E8%E1%E5%F0% F0%E8%F1%EA%E8 (дата звернення 14.03.2019) – Назва з екрана.
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. [Електронний ресурс] – Режим доступу : https://zakon.rada.gov.ua/laws/ show/2163-19. (дата звернення 14.03.2019) – Назва з екрана.

УДК 004.056

Тимчик Лариса Петрівна
викладач інформаційних систем і технологій, спеціаліст вищої категорії
Торговельно-економічний коледж КНТЕУ
Катане Тетяна Михайлівна
викладач інформаційних систем і технологій, спеціаліст
Торговельно-економічний коледж КНТЕУ

SMART-GRC РІШЕННЯ КОМПАНІЇ SAP ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ

З появою сучасних технологій та стрімкого розвитку IT-сфери навіть проста спроба кібератаки може паралізувати всю роботу підприємства, а також привести до несанкціонованого витоку даних.

Тому актуальним на сьогодні є вирішення завдання забезпечення сучасного підходу до ефективного захисту конфіденційної інформації підприємства, внутрішнього контролю та постійного моніторингу всіх робочих процесів, що супроводжуються використанням даних, реалізацію афективного захисту від кібератак (кіберпезпеку) необхідно гарантувати високий рівень кібербезпеки та впровадження в робочі процеси й бази даних підприємства інструменти, що забезпечать захист від майбутніх кібератак. Одним із таких інструментів, який гарантує безпеку є програмне рішення SAP, що дає змогу швидко пристосуватися під сучасні виклики суспільства та розвиток інформаційних технологій.

Автоматизовані та інтегровані SMART-GRC (управління, ризики, відповідність) рішення SAP організовані в чотири рівнів, кожному із яких притаманна своя модель:

- три лінії оборони;
- управління та контроль доступу;
- управління міжнародною торгівлею;
- кібербезпека та захист даних.

Саме завдяки дотриманню роботи відповідно до кожного рівня та ефективному використанні програмного забезпечення SAP на кожному із рівнів, здійснюється ефективна робота з захисту інформації.

Моніторинг системи SAP, аналіз отриманих даних та необхідні дії з захисту є важливою складовою процесу забезпечення інформаційної безпеки.

Для ефективності впровадження першої моделі «Три лінії оборони» треба мати уявлення про програмне забезпечення для першої лінії захисту, в яку входить: управління бізнес-операціями, управління ризиками та правова безпека GRC, внутрішній аудит.

Управління ризиками SAP. Вдосконалення процесів управління фінансами, IT, постачальниками та операційними ризиками (ERM), надає змогу прийняти розумні та обґрунтовані рішення. Основними перевагами

використання є: визначення та аналіз ризиків, комплексне управління ризиками (IRM), стратегія та планування; можливість розгортання на місці або в хмарі.

SAP Process Control – це програмне забезпечення, яке надає можливість постійного внутрішнього контролю та дотримання законодавства відповідно до інформаційних, галузевих, корпоративних та фінансових заходів, при цьому здійснюється постійний моніторинг, підтримка внутрішніх елементів керування та безпосередньо – управління.

Наступним етапом є – *управління аудитом SAP*. Управління аудитом представляє собою зручний, багатофункціональний процес, що дає можливість планувати, управляти, організовувати діяльність з внутрішнього аудиту, поліпшити якість аудиту за допомогою аналітичних інструментів, привести їх у відповідність з бізнесом щодо ключових ризиків та засобів контролю.

Покращення виявлення та запобігання шахрайства шляхом перевірки великих обсягів транзакцій у реальному часі здійснюється за допомогою SAP Business Integrity Screening.

Важливою частиною концепції безпеки у проектах розгортання і запуску рішень SAP *є забезпечення контролю доступу до даних і процесів*. За автоматичне виявлення, усунення та запобігання порушенням доступу у системах SAP відповідає - управління та контроль доступу. Управління доступом до ідентифікатора Cloud забезпечує постійний аналіз доступу та ідентифікації, динамічне налаштування та контроль.

Управління міжнародною торгівлею (SAP Global Trade Services) - автоматизація ручних завдань для управління та дотримання міжнародної торгівлі.

Кібербезпека та захист даних є завершальною категорією у SMART-GRC рішенні компанії SAP, що забезпечує повний і цільовий захист бізнесу. Програмне забезпечення, що буде відповідати саме за захист та кібербезпеку є визначення загроз SAP Enterprise. Цей інструмент захисту інформації та керування подіями (SIEM) використовує інтелект в реальному часі для ефективного управління вразливістю відповідних систем до зовнішніх та внутрішніх загроз та забезпечує захист даних.

Отже, SMART-GRC рішення SAP – це програмне забезпечення допоможе автоматизувати надання користувачам можливості контролювати та перевіряти доступ до додатків і даних, а також вбудовувати профілактичні перевірки у бізнес-процеси, надає доступ до самообслуговування, розгортання в хмарі та автоматизованих оглядів доступу користувачів.

Список використаних джерел:

1. SAP Cybersecurity and Governance, Risk, and Compliance [Електронний ресурс]:[Веб-сайт]. – Електронні дані. : SAP Cybersecurity and Governance, Risk, and Compliance (GRC) 2019. – Режим доступу: https://sap.com/ (дата звернення 25.02.2019) – Назва з екрана.

УДК 657:004.056

Степашкіна Катерина Володимирівна
викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Бердар Костянтин Сергійович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
Шевченко Ангеліна Анатоліївна
лаборант кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет

БЕЗПЕКА В МОБІЛЬНИХ ДОДАТКАХ НА СИСТЕМІ IOS

В даний час безпека є однією з найважливіших тем в IT-індустрії. Користувачі, компанії, все більш серйозно ставляться до питання безпеки даних і конфіденційності. Це також стосується мобільних додатків через їхню близькість до користувачів. Частота використання та зручність означають, що мобільні додатки часто зберігають важливі приватні дані.

iOS, завдяки своїй замкнутій системі і обмеженням, накладеним Apple, вважається однією з найбільш безпечних мобільних операційних систем. Однак це не означає, що ви можете нехтувати безпекою при розробці програми iOS.

Потенційні ризики безпеки в iOS:

Витік даних. За допомогою програми користувач в основному вводить свої приватні дані і зберігає ці дані в незахищеному порядку, що створює ризик просочування цих даних, якщо пристрій отримав неавторизовані руки.

Людина в середній атаці. Захопити HTTP / HTTPS запити і відповіді відносно легко зробити, коли справа доходить до iOS додатків. Використовуючи інструменти, такі як Charles Proxy, навіть аматор може дізнатися про наші запити додатків, відповідні відповіді на сервер і маніпулювати мережевим трафіком, надіславши запити на навчання. На жаль, SSL не достатньо, щоб забезпечити безпеку вашої програми.

Щоб зберегти конфіденційні дані наших програм, ми повинні використовувати служби безпеки, надані компанією Apple.

API служб Keychain допомагає вирішувати ці проблеми, надаючи вашому додатку спосіб зберігати невелику кількість даних користувача в зашифрованій базі даних, що називається брелок .

У брелку ви можете вільно зберігати паролі та інші секрети , про які користувач безпосередньо піклується, наприклад, інформацію про кредитну картку або навіть короткі чутливі нотатки.

Увімкнути безпеку транспортування програм:

З запуском iOS 9 і OS X El Capitan, Apple представила App Transport Security, яка змушує розробників використовувати захищені мережеві з'єднання. Ця зміна передбачає, що кожне з'єднання, яке робить додаток, має використовувати протокол HTTPS і TLS 1.2.

Іншими словами, програма не може спілкуватися з сервером за допомогою незахищеного з'єднання, такого як HTTP, якщо це не вказано явно. Оскільки це було переломним явищем, Apple надала легкий спосіб освоїти цю нову вимогу, додавши виключення або вимкнувши її у файлі plist.

Тим не менш, настійно рекомендується не обходити це обмеження, а замість цього використовуйте захищені з'єднання в наших програмах, щоб уникнути потенційних (і легких) атак.

Закріплення SSL:

Після того, як ATS увімкнено, другий крок для підвищення безпеки наших програм полягає в тому, щоб активувати SSL Pinning .

SSL Pinning - це техніка, яка дозволяє нам мати справу з атакою під назвою Man in the Middle . SSL базується на «ланцюжку довіри» сертифіката. Коли зв'язок починається, клієнт перевіряє, чи довіряється SSL сертифікату отриманого сервера будь-якою службою сертифікації SSL.

Ми можемо використовувати закріплення SSL для того, щоб програма спілкувалася тільки з призначеним самим сервером. Це робиться шляхом збереження SSL-сертифіката цільового сервера всередині програми.

Закріплення SSL має помітний недолік, не пов'язаний із самою безпекою: додаток має бути оновлено кожного разу, коли ключ SSL сервера змінюється через закінчення терміну дії та інші причини.

Список використаних джерел:

1. Офіційний сайт компанії Apple. Електронний ресурс. URL: https://www.apple.com/business/resources/docs/iOS_Security_Overview.pdf
2. SwiftKeychainWrapper від Джейсона Ренделя (jrendel) для Swift. https://cocoapods.org/pods/SwiftKeychainWrapper. Електронний ресурс. URL: https://github.com/jrendel/SwiftKeychainWrapper
3. Яремчук Ю. Є. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця : ВНТУ, 2017. – 120 с.
4. Комплексна_система_захисту_інформації. Електронний ресурс. URL: https://uk.wikipedia.org/wiki/
5. Gladius Partners with Remme to Tackle Enterprise Cybersecurity. [Електронний ресурс]. URL: https://medium.com/gladius-blog/gladius-partners-with-remme-to-tackle-enterprise-cybersecurity-b1d12c288fa6

УДК 004.056.4

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Драпей Леонід Леонідович
студент 4 курсу 7 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ WEB-САЙТУ ПРИВАТНОГО ПІДПРИЄМСТВА ТОВ ТВД «РІВС»

На сьогоднішній день проблеми й завдання підприємств стають на рівні із проблемами й завданнями цілих держав. Як і держави, вони співпрацюють або конкурують. Конкуренція тут саме інформаційна: той хто має інформацію той володіє фінансовими потоками.

Зараз не всі керівники усвідомлюють нагальну потребу захисту комерційної таємниці на їхньому підприємстві. Серед тих, хто таку необхідність розуміє, чимало не знають, що потрібно робити, щоб зберегти інформацію в таємниці, вигідно реалізувати її, не зазнавши збитків від витоку або втрати цієї інформації.

Деякі йдуть тільки шляхом оснащення підприємства технічними засобами захисту, повністю ігноруючи організаційно-правові методи. Мається на увазі, створення нормативно-правової бази, прийняття й суворе дотримання якої дозволять фірмі не лише зберегти, а й вигідно використати свої секрети, але у разі витоку інформації мати підстави для подання позовної заяви.

Отже, тільки «досягнення максимальної ефективності захисту інформації може гарантувати комплексну систему, тому що системність забезпечує необхідні складові захисту й установлює між ними логічний і технологічний зв'язки, а комплексність, що вимагає повноти цих складових, всеохоплення захисту, забезпечує її надійність» [1].

Основні випадки порушення безпеки інформації:

- несанкціонований доступ – здійснюється через порушення установлених в інформаційній системі правил розмежування доступу;
- витік інформації – результат дій порушника, завдяки якому інформація стає відомою та/або доступною суб'єктам, що не мають права доступу до неї;
- втрата інформації – дія, внаслідок якої інформація в інформаційній системі перестає існувати;

- блокування інформації – дії, внаслідок яких втрачається доступ до інформації;
- порушення роботи інформаційної системи – дії або обставини, які призводять до некоректного процесу обробки інформації.

Характеристика методів захисту, що реалізовано на підприємстві ТОВ ТВД «РІВС», з метою забезпечення безпеки інформації**:**

- На підприємстві використовується ідентифікація та аутентифікація користувачів для забезпечення захисту від несанкціонованого досутпу, таким чином доступ до ресурсів сайту обмежується згідно повноваженням користувачів, також ці процеси реєструються у системі.
- Для забезпечення захисту від витоку, втрати та підробки інформації використовується криптографічний захист, або шифрування. Реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Використовується Transport Layer Security останньої діючої версії оновлення (TLS v1.2). Також створена спеціальна сукупність правил для персоналу, що зменшує ризик витоку або втрати інформації з підприємства через їх можливі помилки.
- Збереження цілісності інформації у її первісному вигляді, щоб запобігти її втрати або блокуванню, реалізовується методом резервного копіювання в першій декаді кожного місяця на Hard Disk Drive (HDD або жорсткий диск).
- Для забезпечення стабільної роботи web-сайту та попередження порушень роботи інформаційної системи на сайті є можливість перезавантаження з іншої (не основної) IP-адреси. Це може знадобитися у випадку надмірного навантаження на web-сайт.

З метою запобігання інсталяції вірусного програмного забезпечення, яке може пошкодити, заблокувати або змінити інформацію на комп'ютері, з якого виконується адміністрування, встановлено такі види антивірусного захисту: Firewall, ESET NOD32 та Windows Defender. Антивірусні програми перевіряють нові файли, які завантажуються на комп'ютер (в тому числі з USB-флеш-накопичувачів) на наявність сигнатур вірусів та попереджають їх виникнення. Для забезпечення максимального захисту комп'ютеру, проводиться постійне оновлення антивірусних програм.

Список використаних джерел:

1. Система захисту інформації приватного підприємства. Організація Служби захисту інформації приватного підприємства. – Режим доступу: http://pnzzi.kpi.ua/14/14_p45.pdf

2. Про захист інформації в інформаційно-телекомунікаційних системах– Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/ed20050531.

УДК: 004.056

Пашорін Валерій Іванович
кандидат технічних наук,
професор кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Большак Максим Васильович
аспірант кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет

ЗАПРОВАДЖЕННЯ ПІДВИЩЕНОГО РІВНЯ КІБЕРБЕЗПЕКИ ВНУТРІШНЬОЇ БАГАТОРІВНЕВОЇ СИСТЕМИ ЗА ДОПОМОГОЮ БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ

Сьогодні кожне підприємство в тій чи інший мірі використовує внутрішні багаторівневі системи. Малі багаторівневі системи обмежуються зберіганням та розміщенням нескладно структурованої бази даних з легкою обробкою отримуваної інформації. Великі внутрішні багаторівневі системи включають в себе web-вузли, фільтрацію запитів, складно структуровані бази даних, їх підтримку та розміщення, складні алгоритми обробки даних, складну систему proxy-серверів та інше. Такі системи створюють своєрідну внутрішню екосистему в якій виведення зі строю хоча б одного елементу може призвести до важких наслідків та великих збитків. Досягнути високої надійності такої систем надзвичайно важко, і якщо ми можемо запобігти різним технічних проблемам збільшивши кількість техніки, яка підтримує нашу систему, великою проблемою залишається ідентифікація користувачів які мають доступ до внутрішньої системи.

Одною з найголовніших проблем кібербезпеки сучасності залишається надійність збереження прав доступу до внутрішніх систем. Як відомо сьогодні існує безліч способів перехопити дані для отримання доступу до різних систем якими користуються недобросовісні користувачі. Покращити надійність збереження прав доступу дозволяє багатофакторна ідентифікація користувача, яка запобігає можливості використання перехоплених даних для доступу до внутрішніх систем.

Багатофакторна ідентифікація основується на тому, що користувач знає пароль або PIN-код і також має ключ який генерує динамічний пароль для доступу до системи. Таким чином забезпечується набагато надійніший рівень перевірки автентифікації користувача в порівнянні з повторним використанням пароля. Дане рішення є надійним рішенням, яке автоматично змінює пароль кожні 60 секунд. Багатофакторні ідентифікація пропонує системам широкий спектр можливостей автентифікації користувачів, які допомагають впевнено визначати користувачів перш, ніж вони зможуть взаємодіяти з критично важливими даними і додатками через різні мережі і ресурси.

Згенерований пароль доступу до системи визначається як токен. Кожному токену відповідає 128-бітове випадкове число - початковий вектор

генерації. Також в кожен токен вбудовані годинник. Токен-код - результат роботи алгоритму, який в якості параметрів бере поточний час, і початковий вектор генерації. За токен-коду неможливо відновити початковий вектор генерації, так як алгоритм працює в одну сторону. Так як на сервері зберігається відповідні токену початкові вектори генерації, то він в будь-який момент часу може по тому ж самому алгоритму відновити поточний токен-код. Для випадку якщо годинник у сервера і токена розходяться, передбачена автоматична синхронізація. Тобто в разі якщо наприклад годинник у токена не сходиться з серверним, то програма заносить в базу величину зсуву відповідну конкретному токену. Це досягається завдяки тому, що сервер обчислює пароль не тільки для поточної хвилини, але так само минуле і майбутнє хвилин. Таким чином, якщо PIN, введений користувачем вірний, а токен-код відповідає значенням в сусідні хвилини, то розсинхронування враховується для подальших операцій.

Сервіси для здійснення багатофакторної ідентифікації як правило включають в себе всі чотири функції, які необхідні для забезпечення гарантії достовірності особи: управління обліковими даними на основі політики перевірки автентичності користувачів, автентифікація, авторизація та інтелектуальна обробка. Застосування довірених облікових записів підвищує рівень безпеки щодня здійснюваних операцій і надає підтримку для нових моделей бізнесу, гарантуючи безпечний доступ співробітникам компанії, її клієнтам і партнерам і зберігаючи необхідний баланс між ризиком, вартістю і зручністю. Також такі сервіси виконують наступні завдання: зберігають базу користувачів, зберігають журнал подій, зберігають список зареєстрованих токенів, обробляють інформацію що надсилається користувачами.

Одним із найкращий прикладів інформаційних систем, які забезпечують своїх клієнтів можливістю багатофакторної ідентифікації користувачів є програмне забезпечення розроблене компанією RSA The Security Division of EMC під назвою SecurID яка включає в себе три основних компоненти: RSA Authentication Manager, RSA Authentication Agents, RSA SecurID Authenticators. Дане програмне забезпечення має можливість підтримки засобів генерування токенів у вигляді смарт-карток, що робить його найбільш популярним та зручним засобом досягнення високої надійності багаторівневих внутрішніх систем.

Отже, очевидно що при побудові внутрішньої багаторівневої системи необхідно подбати про надійний захист від зловмисників, які намагаються отримати доступ до системи перехопивши дані користувачів. Одним із найкращих засобів досягнення поставленої мети – багатофакторна автентифікація користувачів.

Список використаних джерел:

1. Электронные ключи для аутентификации URL: http://www.infobezpeka.com/products/keyforauntification
2. WHAT'S REALLY AT RISK WITH REPUTATION RISK URL: https://www.rsa.com/en-us/blog/2017-04/whats-really-at-risk-with-reputation-risk

УДК 67.401.212.73

Глєбова Алла Олександрівна
кандидат економічних наук,
доцент кафедри туризму та адміністрування
Полтавський національний технічний університет імені Юрія Кондратюка

ОРГАНІЗАЦІЯ КІБЕРЗАХИСТУ НА ПІДПРИМСТВІ: ОРГАНІЗАЦІЙНО- ДОКУМЕНТАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ

В умовах інформаційної економіки важливого значення набуває інформація, яка є стратегічним ресурсом як і земля, капітал та люди. Вона стає могутнім інструментом управління одночасно, що забезпечує конкурентоспроможність та здатність до стійкого розвитку. Інформаційні технології, які стрімко розвивають і впроваджують у життєдіяльність не тільки економіки, але і життя кожного індивіду. Більшість процесів стають відкритими і доступними, як і масиви даних про особисту та конфіденційну інформацію. Встановити користувачів та їх мотиви досить складно, оскільки вони можуть знаходитися у різних країнах світу одночасно. Це призвело до появи нового виду злочинності – кіберзлочинності.

Основними об'єктами злочину стають громадяни, підприємства, уряди, стратегічно важливі підприємства тощо.

За перші 6 місяців 2018 року в Україні було порушено 4041 кримінальних порушень у сфері порушень кіберзлочинності: 1336 – у сфері платіжних систем; 810 – кібербезпеки; 1380 – у сфері електронної комерції; 515- у сфері протиправного контенту. Таким чином, у сфері платіжних систем кількість злочинів у 2018році зросла порівняно із 2017 роком у 1,4 рази. У сфері протиправного контенту кількість злочинів у 2018 році порівняно із 2017 роком також зросла [1].

У результаті виникли такі різновиди кіберзлочинності:

1) фі́шинг – вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів.

2) Грінмейл – „корпоративний шантаж, який полягає у начебто законній діяльності міноритарного акціонера (подання численних скарг, позовів проти товариства, ініціювання перевірок діяльності товариства), направленої на спонукання менеджменту або мажоритарних акціонерів товариства придбати акції у цього міноритарного акціонера за ціною, яка багаторазово перевищує їхню ринкову вартість, або отримання відступних у грошовій або іншій формі" [2]. Цей вид загрози пов'язаний на перший погляд із рейдерством, але із іншого боку саме завдяки Інтернет-мережі та розвитку сучасних інформаційних мереж стає можливим досягати поставленої мети у короткі проміжки часу.

3) кардерство – це вид шахрайства, при якому проводиться операція з використанням платіжної картки або її реквізитів, що не ініційована або не підтверджені її власником. Реквізити платіжних карт, як правило, беруть зі зламаних серверів інтернет-магазинів, платіжних та розрахункових систем, а

також з персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «троянці», «боти» з функцією формграббер). Така загроза є актуальною як для фізичних осіб, так і юридичних.

Тоді як більшість громадян та керівників підприємств приділяють значну увагу організації фізичної безпеки, а не інформаційної. Тоді як основні протиправні дії нині пов'язані саме із інформацією. Тому пропонується керівникам на рівні підприємства, акцентувати увагу на інформаційній безпеці і вживати низку наступних заходів:

1. обмеження доступу працівників на робочому місці до соціальних мереж або заборона;

2. робоче місце головного бухгалтера і керівника повинне бути обладнане таким чином, щоб на комп'ютері, де зберігається цінна інформація був встановлений пароль і не було доступу до Інтернет-мережі;

3. для працівників проведення тренінгів з метою підвищення інформаційної культури. Зокрема, для того, щоб захисти від фітингу: заведіть собі декілька поштових адрес, одну з яких використовуйте лише для особистого спілкування, іншу - для публічного доступу;візьміть собі за звичку ніколи не відповідати на спам;замисліться про наслідки перш ніж перейти за запропонованим посиланням, воно може вести на фішінгові сайти;користуйтеся спам-фільтрами;своєчасно оновлюйте свій інтернет-браузер; ніколи нікому не повідомляйте пін-код карточки.

4. для посилення відповідальності за «безвідповідальне відношення» до роботи з інформацією нині існує необхідність не тільки розробка положення про інформаційну безпеку підприємства, яке повинно бути, але і включення окремих пунктів у контракти працівників, які працюють із важливою інформацією. Оскільки нині саме працівники через соціальні мережі можуть нашкодити, не тільки підприємству, але і собі. Наприклад, після того як у Великій Британії в середині 2009 року оголосили, що сер Джон Соерс очолить управління контррозвідки – Таємну розвідувальну службу (колись відому як MI6), газета Daily Mail знайшла публічні фотографії його з дружиною, розміщені нею на Facebook. Там були знімки зі свят, зображення друзів сім'ї й подробиць про те, де він жив і чим займався. Таким чином, доцільно зробити висновок, що нині важливо на підприємстві приділяти увагу формуванню організаційно-документційного забезпечення саме інформаційної безпеки, що буде включати заходи щодо підвищення інформаційної культури працівників, так і посилення відповідальності за її розголошення.

Список використаних джерел:

1. Кіберполіція відмічає збільшення кількості правопорушень у сфері платіжних систем та кібербезпеки [Електронний ресурс] – Режим доступу: Офіційний сайт Національної поліції – https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vidmichaje-zbilshennya-kilkosti-pravoporushen-u-sferi-platizhnix-sistem-ta-kiberbezpeki.

2. Нікульников Д. Ґрінмейл і право акціонера на отримання інформації про діяльність товариства // Юридичний радник. – 2007. - №1(15).

УДК 004.056.5

Савченко Тетяна Віталіївна
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Кутковий Нікіта Георгійович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ОСНОВНІ НАПРЯМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

На сьогоднішній день важливу роль в соціальному та економічному розвитку багатьох країн світу відіграє кібернетичний та інформаційний простір, а також інформаційне суспільство, яке сформувалися внаслідок стрімкого розвитку науково-технічного прогресу та комп'ютеризації. Проте, існування глобального інформаційного простору призвело до появи інформаційних загроз. Отже, тема кібербезпеки є надзвичайно актуальною і відкритою, особливо для України, враховуючи сучасний стан держави.

Кібербезпекою є стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання та нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам.

Згідно Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпекою є захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

До складових кібернетичної безпеки належать: кібернетичні впливи; розвідка інформаційно-телекомунікаційних систем та криптосистем протиборчих сторін; захист власної інформаційної сфери.

Досягається такий стан завдяки сукупності активних захисних і розвідувальних дій, що у процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо інформаційних ресурсів, інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем.

Кібербезпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм.

Вибір конкретних засобів і шляхів забезпечення кібербезпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз життєво важливим інтересам людини і громадянина, суспільства і держави.

Основними напрямами забезпечення кібербезпеки України є:

- розвиток інформаційної інфраструктури держави, забезпечення безпечного функціонування об'єктів критичної інформаційної інфраструктури;
- розвиток міжнародного співробітництва у сфері кібербезпеки; зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з проявами кіберзлочинності та кібертероризму;
- забезпечення ефективного застосування Збройних Сил України для адекватної відповіді реальним та потенційним кіберзагрозам національному сегменту кіберпростору;
- розвиток пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій; підтримка виробників продукції та послуг у сфері кібербезпеки на засадах стимулювання вітчизняних виробників;
- адаптація законодавства України до норм ЄС, створення нормативно-правових та економічних передумов для розвитку інформаційної інфраструктури держави, підвищення її стійкості до кібератак, спроможності держави більш ефективно захищати національні інтереси у кіберпросторі;
- забезпечення неухильного дотримання власниками об'єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та технічного захисту інформації, захисту персональних даних; підвищення рівня обізнаності суспільства щодо ризиків, викликів і загроз у кіберпросторі.

Таким чином, можна стверджувати, що у час глобалізаційних процесів інформаційно-телекомунікаційні системи стають уразливими, тому кібернетична безпека України є пріоритетним напрямком, що захищає інтереси держави, підтримує обороноздатність, забезпечує повноцінну діяльність економічних та інших сфер, отже, сприяє збалансованому існуванню суспільства та нейтралізації дії внутрішніх і зовнішніх загроз та небезпек.

Список використаних джерел:

1. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія / В. Л. Бурячок.— К.: НАУ, 2013. — 432 с.
2. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. — К.: ДУТ, 2015. — 288 с.
3. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19
4. Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016/.

УДК 004.056.5

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент,
доцент, кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Архипчук Броніслав Павлович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

КІБЕРБЕЗПЕКА ПРОГРАМ ВІДДАЛЕНОГО КОРИСТУВАННЯ

Під абревіатурою RAT ховається, не дуже приємне для кожного користувача, позначення трояна, за допомогою якого зловмисник може дістати видалений доступ до комп'ютера. Багато хто помилково переводить цю абревіатуру як Remote Administration Tool – інструмент для видаленого адміністрування, але на самій же справі абревіатура RAT означає Remote Access Trojan – програма троян для видаленого доступу.

Насправді шпигунська програма RAT це одна з найбільш небезпечних шкідливих програм, яка дозволяє зловмисникові отримати не просто доступ до вашого комп'ютера але і повний контроль над ним.

Використовуючи програму RAT, зломщик може видалено встановити клавіатурний шпигун або іншу шкідливу програму. Також за допомогою даної програми хакер може заразити файли і багато чого ще наробити без відома користувача.

RAT складається з двох частин: клієнт і сервер. На комп'ютері зловмисника програма RAT-клієнт створює програму RAT-сервер, яка посилається «жертві». Після запуску жертвою RAT-сервера у вікні програми клієнта з'являється видалений комп'ютер (хост), до якого можна видалено підключитися. З цієї миті комп'ютер «жертви» під повним контролем зловмисника.

Можливості трояна RAT: стежити за діями користувача, запускати файли, відключати і зупиняти сервіси Windows, знімати і зберігати скріни робочого столу, запускати веб-камеру, сканувати мережу, викачувати і модифікувати файли, моніторити, відкривати і закривати порти тощо.

Популярні Rat-програми: Darkcomet Rat, Cybergate, PRORAT, Turkojan, Back Orifice, Cerberus Rat, Spy-net.

Кращий троян RAT на сьогодні це Darkcomet Rat (на хаЦкерському жаргоні просто Камета).

Зараження вірусом RAT відбувається майже також як іншими шкідливими програмами через:

- масове зараження торрент сайтах;

- скрипти (експлойти) на сайтах, які без відома користувача завантажують RAT на комп'ютер.

Варто відзначити що, в більшості зараження Rat-трояном походить не від масового, а від цілеспрямованого зараження комп'ютера друзями або колегами.

До речі не завжди антивірусне програмне забезпечення здатне запобігти зараженню, оскільки сьогодні вже ніхто не посилає просто трояна, сьогодні його заздалегідь криптують.

Зрозуміти що на комп'ютері встановлений RAT дуже не легко, але можна. Ось ознаки які можуть говорити про наявність троянської програми на комп'ютері: дивна сітьова активність у фаєрволі, зокрема високий витікаючий трафік, комп'ютер почав гальмувати або швидкість Інтернету значно просіла тощо.

Виявити троян RAT на комп'ютері досить складно. Можна закачати безкоштовні антивірусні програми з оновленими базами, наприклад сканер AVZ, і просканувати комп'ютер.

Насправді, якщо користувач мало знаєтеся на комп'ютерах, то легше заздалегідь зберегти важливі документи на зовнішніх носіях та відформатувати комп'ютер і встановити операційну систему Windows заново.

До речі, встановлюючи зламану операційну систему Windows користувач ризикуєте заразиться вірусом вже на етапі установки. Оскільки деякі «ліві» інсталяційні файли, які у вільному доступі в мережі Інтернет, мають вже ушиті закладки, шпигуни, віруси, приховані радміни тощо.

У висновку слід зазначити, що не потрібно відкривати не знайомі файли, які отримуються по електронній пошті, користуватися безпечними браузерами, скачувати і встановлювати програми лише з сайту розробника, не допускати фізичного контакту з комп'ютером сторонніх людей, видалити антивірус і поставити хороший фаєрвол і сніффер.

Список використаних джерел:

1. Schellong A.Breaking down the threat of cyber terrorism. – Режим доступу: http://blogs.csc.com/ 2016/02/04/breaking-down-the-threat-of-cyber-terrorism

2. ISO/IEC 27032. Information technology – Security techniques – Guidelines for cybersecurity. 2012. 50 p.

3. Корреспондент.net 5 січня 2016. Хакери атакували низку українських обленерго: – Режим доступу: http://ua.korrespondent.net/ ukraine/3611402-khakery-atakuvaly-nyzku-ukrainskykh-oblenerho-zmi

4. UA Crypto. Що таке RAT? – Режим доступу: https://uacrypto.top/blog/darknet.

УДК 004.056.1

Десятко Альона Миколаївна
старший викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Віон-Дюрі Ярослав Дмитрович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВІ

Тиждень за тижнем заголовки новин про кібербезпеку переважають над новинами. Злочинці продовжують орієнтуватися на високопоставлені організації та окремих осіб у масштабах і не виявляють ознак уповільнення.

Від крадіжки персональних даних, до витоків фінансової інформації, до матеріалу, захищеного авторським правом – ці напади відбуваються знову і знову. Злочинцям потрібно всього лише дев'ять хвилин, щоб використати дані, розміщені на темній павутині.

Незалежно від заходів, вживаних для запобігання порушенням, злочинці знаходять все більш інноваційні способи їх обійти. Чим швидше ми визнаємо, що це не зміниться, тим краще, тому ми можемо зосередитися на тому, що дійсно можна виконати: зменшення впливу кібератак.

В наш час технологій кібератаки дуже поширені. Що гірше, дані компанії стають все більш і більш цінними. На нашу думку, слід звернути свою увагу на нове рішення цієї проблеми, а саме на аутентифікацію підприємств.

Аутентифікація вирішує такі питання:

- Довіра до централізованого центру сертифікації (CA - CertificationAuthority)
- Взлом ключів CA
- Видача підробленого сертифіката
- Видача "прихованих" сертифікатів, що намагаються перехопити і перенаправити з'єднання

Це дозволяє здійснювати повний і прозорий контроль і відстеження всіх виданих сертифікатів, відсутність можливості видачі "прихованих" сертифікатів, а також усунути спроби перехопити і перенаправити з'єднання. Різні сторони намагалися вирішити ці питання. Блокчейн системи забезпечують незмінність даних, що зберігаються в них, забезпечуючи ефективне і практичне рішення.

Таку технологію можуть запропонувати компанії Gladius та Remme які саме розроблять комплексне рішення безпеки для компаній. Розробляючи надійний програмний пакет, для компаній будь-якого розміру.

Якщо торкнутися регулювання на підприємствах питань безпеки інформації та кіберзахисту підприємницької діяльності, шляхом визначення

обов’язкових вимог, щодо організації заходів інформаційної безпеки, які поетапно мають впроваджуватися на підприємстві:

По-перше: основний – впровадження базових заходів інформаційної безпеки. По-друге: впровадження додаткових заходів – для підвищення рівня зрілості інформаційної безпеки.

Зокрема вказані заходи безпеки інформації включають в себе:

- захист від зловмисного коду,
- заходи безпеки при використанні електронної пошти,
- контроль доступу до інформаційних систем підприємств,
- заходи безпеки в мережі підприємства,
- криптографічний захист інформації тощо.

Крім того, відповідно до кращих світових практик з питань інформаційної безпеки, передбачається призначення в підприємствах відповідальної особи за інформаційну безпеку (Chief Information Security Officer, CISO) та наділення її повноваженнями, достатніми для прийняття управлінських рішень. Також підприємства повинні сформувати окремі підрозділи з інформаційної безпеки виключно зі штатних працівників підприємства, які безпосередньо підпорядковуються CISO.

Кібербезпека на підприємстві повинна повністю відповідати принципам права Європейського Союзу (acquis ЄС) та зобов’язанням України у сфері європейської інтеграції, у тому числі міжнародно-правовим.

Імплементація норм дасть можливість:

- Посилити вимоги до захисту інформації в інформаційних системах підприємств України з урахуванням актуальних кіберзагроз.
- Установити принципи управління інформаційною безпекою в підприємствах.
- Визначити принципи криптографічного захисту інформаційних систем підприємств в Україні.
- Установити обов’язкові мінімальні вимоги щодо організації заходів із забезпечення безпеки інформації та порядок поетапного упровадження цих вимог на підприємствах.

Підводячи підсумок визначаємо, що хоча кібербезпека підприємства є широкою і різноманітною темою, очевидно, що Інтернет-технології є рушійною силою інновацій у цьому секторі. Дослідження цієї проблеми неймовірно складні рішення для кібербезпеки. Це змушує відчувати більш оптимістично щодо здатності організацій в майбутньому захиститись від кібератак, чи в малих організаціях, чи в великому бізнесі – утримати зловмисників і мінімізувати порушення безпеки.

Список використаних джерел:

1. Gladius Partners with Remme to Tackle Enterprise Cybersecurity. [Електронний ресурс]. URL: https://medium.com/gladius-blog/gladius-partners-with-remme-to-tackle-enterprise-cybersecurity-b1d12c288fa6.

УДК 004.5

Пашорін Валерій Іванович
кандидат технічних наук,
професор кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Гасімов Орхан Хемідага огли
студент 1 курсу магістратури ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ЗАХИСТ СЕРВЕРІВ НА РІВНІ ВЕБ-ДОДАТКІВ

Компанії застосовують для оптимізації бізнес-процесів CRM, ERP та інші системи для роботи з даними. Це має свої переваги, але і додає в інформаційну систему нові загрози, до 80% випадків компрометації систем починаються з веб-додатків.

Для побудови ефективної і достатньої системи захисту необхідно: провести повний аудит додатків; встановити цінність оброблюваної інформації; скласти матрицю доступу користувачів до даних; побудувати карти всіх модулів програми та їх взаємодії; визначити слабкі місця і найімовірніші точки витоку інформації.

Якщо в компанії використовуються додатки, що розроблені на замовлення стороннім підрядником, і вихідний код програм недоступний, співробітникам інформаційної безпеки при прийманні програмного забезпечення має сенс використовувати сканер вразливостей.

При знаходженні критичних вразливостей додаток повертається на доопрацювання розробнику. У разі, коли веб-додаток є внутрішньою розробкою компанії, рекомендується вибудовувати процес безпечної розробки програмного забезпечення з використанням аналізаторів вихідного коду, перевіряючи весь код на відсутність помилок, що призводять до вразливостей. Такий підхід дозволяє виправити помилки в додатку на ранньому етапі і уникнути зайвих витрат. Більшість аналізаторів коду дозволяє проводити як статичний аналіз коду без його виконання, так і динамічний, перевіряючи вже встановлене і запущене застосування. В останньому випадку виникне потреба у вказівках точок входу і велика кількість вхідних даних. Поєднання перерахованих методів дозволяє виявляти уразливості до впровадження програм в компанії. У той же час реалізація в компанії процесів верифікації додатків може зажадати значних матеріальних витрат. Іноді просто немає можливості вносити зміни в додаток, що працює. Має сенс розглянути можливість використання спеціалізованих засобів захисту веб-додатків, наприклад Web Application Firewall (WAF). Принцип роботи WAF: HTTP-трафік від користувачів до веб-додатків проходить спочатку через WAF або на WAF направляється копія трафіку. Далі трафік піддається перевірці на наявність атак. Якщо WAF

встановлений «в розрив» (проксі, міст), атаки можуть бути заблоковані. У пасивному режимі роботи (копія трафіку) можливі тільки моніторинг і оповіщення про атаки. Для виявлення атак можуть використовуватися такі методи, як: сигнатурний аналіз; репутаційні списки; автоматичне навчання; поведінковий аналіз; ручна настройка правил. Крім цього, WAF може мати модулі для динамічного аналізу вразливостей додатків, віртуального патчінга знайдених вразливостей, управління автентифікацією користувачів, взаємодії з іншими системами захисту.

Небезпеку для інформації в веб-додатках представляють і внутрішні порушники - співробітники, які мають доступ до даних для виконання службових обов'язків, адміністратори з прямим доступом до сервера баз даних. В цьому випадку для забезпечення безпеки веб-додатків можливо використовувати рішення, що реалізують різний підхід до моніторингу і контролю звернень до баз даних.

Для контролю локальних і прямих мережевих підключень до баз даних використовуються агенти, що встановлюються безпосередньо на сервери баз даних. При використанні таких систем для захисту даних може виникнути складність з визначенням користувача, який зробив запит до бази даних: в трафіку, що йде від сервера додатків, всі звернення виробляються від службового облікового запису. Для персоніфікації співробітника передбачена інтеграція з WAF, який аналізує трафік до сервера додатків, або передача копії цього трафіку безпосередньо на систему захисту баз даних. У випадках, коли можливість аналізу копії трафіку відсутня або необхідно застосувати маскування і блокування, чи встановити систему захисту «в розрив» неможливо, використовуються рішення, засновані на інших принципах перехвата звернень користувачів до баз даних. Так як агент знаходиться на сервері веб-додатків, він обробляє і запити клієнтів і запити додатків до баз даних, персоніфікуючи запити. Створюючи правила обробки запитів, можна маскувати «на льоту» будь-які поля в відповідях від бази даних, блокувати нелегітимні запити, повністю управляти бізнес-процесом роботи користувача з додатком.

Системи захисту інформації від витоків, засновані на використанні криптографії і дозволяють вибірково шифрувати інформацію, що зберігається в таблицях баз даних. Доступ до інформації надається тільки авторизованим користувачам, з веденням детальних протоколів їх дій.

Список використаних джерел:

1. WAF очима хакерів.URL: https://habr.com/ru/company/dsec/blog/340144/.
2. SECURITYLAB. Чим захищають сайти, або Навіщо потрібен WAF? URL: https://www.securitylab.ru/analytics/475861.php
3. BISA. Впровадження і настройка web application firewall URL: https://bis-expert.ru/blog/1984/49145
4. CYBERLENINKA. Аналіз і методи захисту web- додатки від атак типу xss URL: https://cyberleninka.ru/article/n.

УДК 004.056.53

Криворучко Олена Володимирівна
доктор технічних наук, професор,
завідувач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Вікторов Владислав Віталійович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
Таха Загер Ваелійович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

КОМПЛЕКСНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Як було сказано Крістіаном Норберг-Шульцом «Тільки при повному розумінні задач можна знайти відповідні способи їх вирішення. Для результатів важливіше поставити правильні запитання чим правильно відповісти на хибні». Тому необхідно строго визначити усі області і задачі що охоплює автоматизована система, а також визначити усі суміжні з нею інші системи та їх складові підсистеми.

Системи інформаційної безпеки в автоматизованих системах (АС), в тому числі в загальних і корпоративних мережах, призначені для забезпечення безпеки інформаційних технологій, тобто забезпечення конфіденційності, цілісності, доступності інформаційних та інших ресурсів АС.

Характерною особливістю подібних систем є насамперед наявність людини в кожній зі складових підсистем і віддаленість людини від об'єкта її діяльності. Це відбувається у зв'язку з тим, що безліч компонентів, які складають об'єкт інформатизації, інтегрально може бути подано сукупністю трьох груп систем: перша – люди (біосоціальні системи); друга – техніка (технічні системи та приміщення, в яких вони розташовані); третя – програмне забезпечення, яке є інтелектуальним посередником між людиною і технікою (інтелектуальні системи). Сукупність цих трьох груп утворює соціотехнічну систему. Таке уявлення про соціотехнічну систему є досить поширеним і може стосуватися багатьох об'єктів. Коло наших інтересів обмежується дослідженням безпеки систем, призначених для обробки вхідної на їх вхід інформації і видачі результату.

Для кожної конкретної інформаційної системи склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами її експлуатації.

Технічний захист інформації (ТЗІ) є невід'ємною складовою частиною системи забезпечення національної безпеки України в інформаційній сфері і представлений як діяльність, що спрямована на забезпечення інженерно-

технічними заходами конфіденційності, цілісності та доступносты інформації в інформаційно-телекомунікаційних, інформаційних, телекомунікаційних, автоматизованих системах і на об'єктах інформаційної діяльності.

Організаційно-правовими заходами реалізується комплекс відповідних в нормативно- правовій базі держави адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом аналізу загроз, регламентації діяльності персоналу і визначення порядку функціонування засобів забезпечення інформаційної діяльності та засобів ТЗІ, а також шляхом створення служб (або призначення адміністраторів ТЗІ), відповідальних за їх реалізацію. Для реалізації заходів цієї групи в більшості випадків немає необхідності використання засобів, що є компонентами АС.

Вирішуючи питання розподілу відповідальності за безпеку комп'ютерної системи, слід ураховувати такі правила:

- ніхто, крім керівництва, не може прийняти основоположні рішення в галузі політики комп'ютерної безпеки;
- ніхто, крім спеціалістів, не зможе забезпечити правильне функціонування системи безпеки;
- ніяка зовнішня організація чи група спеціалістів життєво не зацікавлені в економічній ефективності заходів безпеки.

Одним із напрямів захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ поділяють на два великих класи завдань:

- захист інформації від несанкціонованого доступу (НСД);
- захист інформації від витоку технічними каналами.

Комп'ютерна мережа будь-якої сучасної організації – це різнорідна багатокомпонентна система. Захист одного або декількох компонентів не може забезпечити необхідний рівень захищеності інформаційних ресурсів підприємства. Головною проблемою захисту інформації в комп’ютерних мережах є те, що питаннями безпеки починають цікавитись коли інформаційна та технічна структура мережі уже розгорнута, тобто сформований не тільки функціонал мережі, а також і технічний потенціал. Дана ситуація викликає проблему в правильному підході до будови комплексної системи захисту, адже часто спеціалістів, що розуміють усю структуру функціонування підприємства немає, не говорячи уже про висококваліфікованих спеціалістів в галузі захисту інформації. Тож найкращим захистом інформації на підприємстві може виступати комплексна система захисту інформації.

Список використаних джерел:

1. Яремчук Ю. Є. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця : ВНТУ, 2017. – 120 с.

2. Комплексна_система_захисту_інформації. Електронний ресурс. URL: https://uk.wikipedia.org/wiki/

УДК 004.056.53

Палагута Катерина Олексіївна
кандидат економічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Тютюнник Ілля Сергійович
студент 5 курсу 5м групи ФОАІС
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ЗАХИСТ ДАНИХ ПРИ РОЗРОБЦІ МОБІЛЬНИХ ДОДАТКІВ

Додатки, що створюються для операційної системи Android і продаються на Google Play, легко зламуються. Після злому програми стають доступні для безкоштовного скачування з різних ресурсів. Після появи піратських копій розробники щодня втрачають свій прибуток через те, що не захистили свої розробки від недобросовісних користувачів.

Захист Android додатків, як правило, включає в себе захист коду програми. Захист коду для Android додатків полягає в захисті функцій, а також в проведенні заходів по заплутування машинного коду.

Для захисту андроїд-додатків потрібно дотримуватися таких правил:

1. Відмовитися від моделі поширення Pro / Lite. Додаток дуже легко витягти зі смартфона, тому злодієві буде досить один раз купити додаток, і далі його можна поширювати.
2. Необхідно подбати про захист коду від реверсу.
3. Створення функції, щоб в разі успішного злому додаток просто не став працювати.
4. Використовувати захищені локальні сховища.
5. Не зберігати власних даних користувача в коді або ресурсах додатка.
6. Застосовувати тільки сучасні симетричні алгоритми з генеруванням випадкових одноразових ключів, що володіють високою стійкістю до злому.
7. Попереджати користувача, що запуск додатку проводиться на пристрої з Root-правами.
8. Не використовувати вбудований браузер і вбудований веб-движок в операціях з власними даними користувача.

Для захисту даних на мобільних пристроях використовуються також різноманітні технічні засоби. У стільникових мережах GSM / GPRS / 3G і WiFi, а також в протоколі Bluetooth використовуються наступні стандартні криптографічні алгоритми:

1. Алгоритм аутентифікації A3, алгоритми шифрування A5 / 0, A5 / 1, A5 / 2, GEA1 і GEA2, A5 / 3, GEA3 і UEA1, алгоритм розподілу ключів A8.
2. Алгоритми, використовувані для аутентифікації, шифрування і генерації ключів в протоколах стандарту Wi-Fi 802.11 b / g / n: RC4 (з

довжиною ключа 40 і 104 біт) в протоколі WEP, RC4 (з довжиною ключа 128 біт) в протоколі WPA, AES (з довжиною ключа 128 біт) в протоколі WPA2.

3. Алгоритми аутентифікації і генерації ключів, які використовуються протоколом Bluetooth: E1, E21, E22 на базі алгоритму SAFER + з довжиною ключа 128 біт.

Інші заходи забезпечення безпеки даних на мобільному пристрої реалізуються засобами ОС мобільних платформ або засобами їх управління. Серед них:

1. Аутентифікація, включаючи посилений PIN (парольний захист пристрою, додатків і даних), в т.ч. двофакторна.
2. Шифрування даних на пристрої.
3. Віддалене управління мобільним пристроєм: видалення даних на пристрої,
4. Блокування пристрою, контроль, установка і видалення додатків, контроль налаштувань мобільного пристрою.
5. Захист від шкідливого коду.
6. VPN для віддаленого доступу (на рівні пристрою і / або додатків).
7. Налагодження та установка політики безпеки відповідно до вимог
8. організації.
9. Ведення чорних/білих списків додатків і сайтів.
10. Визначення і захист від злому пристрою для Google Android).
11. Трасування з використанням GPS / ГЛОНАСС.

Список використаних джерел:

1. Корпанюк Т. М., Мулик Я. І. Застосування мобільних додатків в бізнесі та їх облік [Електронний ресурс]. – Режим доступу до ресурсу: http://www.economy.nayka.com.ua/pdf/3_2018/59.pdf/.
2. Privacy and data protection in mobile applications [Електронний ресурс]. - Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications.
3. Дослідження лабораторії G Data SecurityLabs [Електронний ресурс]. – Режим доступу до ресурсу: https://www.gdatasoftware.com/.
4. Сайт SecureList [Електронний ресурс]. – Режим доступу до ресурсу: http://www.securelist.com/.
5. A Window into Mobile Device Security: Examining the security approaches employed in Apple’s iOS and Google’s Android [Електронний ресурс]. – Режим доступу до ресурсу: http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf
6. Веб-сайт www.phonearena.com, стаття «Study finds that Android lock patterns tend to be too simple, just like passwords» [Електронний ресурс]. – Режим доступу до ресурсу: http://www.phonearena.com/news/Study-findsthat-Android-lock-patterns-tend-to-be-too-simple-just-like-passwords_id72948/
7. Проблеми в сфері кібербезпеки в Україні [Електронний ресурс]. – Режим доступу до ресурсу: https://www.pravda.com.ua/rus/columns/2017/02/15/7135442/

УДК 004.056.53

Степашкіна Катерина Володимирівна
викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Александренко Андрій Анатолійович
студент 5 курсу 5м групи ФОАІС
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

БЕЗПЕКА МІКРОСЕРВІСНИХ WEB-ДОДАТКІВ

Практично не існує ситуації в сфері програмного забезпечення, яка повністю звільняє від міркувань безпеки. Що стосується мікросервісів, деякі питання стають більш виразними і набагато складнішими. За мікросервісних технологій мережа все ще є вразливим місцем.

Такі речі, як контроль доступу, які промисловість вже повністю уподобає в рамках монолітних додатків, передбачає новий рівень складності. Це відкриває шлях до обговорень і перевірки того, чи архітектура мікросервісів фактично вирішує більше проблем, ніж вона створює.

На сьогодні визначені такі рекомендації, які є важливими та основними аргументами щодо захисту мікросервісних web-додатків:

1. Використання OAuth для ідентифікації користувача та контролю доступу.

OAuth / OAuth2 є практично промисловим стандартом, що стосується авторизації користувача. Під час створення власного протоколу авторизації явно можливим, багато хто з них не рекомендує його, якщо нема суттєвих і цілком конкретних причин для цього.

2. Застосування «захисту в глибину» для визначення пріоритетів ключових послуг.

«Захист в глибину» визначається як «концепція забезпечення інформації, в якій багатошарові засоби контролю безпеки (захисту) розміщені по всіх рівнях застосування інформаційних технологій».

3. Не слід прописувати свій власний криптографічний код.

Не потрібно намагатися копіювати власні нові рішення та алгоритми, якщо немає вагомих і конкретних причин. Суттєвим є достатньо кваліфікований персонал для розробки ефективних рішень, наявність доступних інструментів, які пройшли апробацію і були всебічно протестовані.

4. Використання автоматичного оновлення засобів безпеки.

Для того, щоб архітектура мікросервісів була одночасно безпечною і масштабованою, раціональною ідеєю буде визначення на ранній стадії

розробки засобу автоматизації або принаймні збереження всіх оновлень програмного забезпечення під контролем.

5. Застосування розподіленого брандмауера з централізованим контролем.

Здебільшого, це все ще мало застосований інструментарій, але вважається, що брандмауер дозволяє користувачам більш детально контролювати кожний мікросервіс (як це робиться за допомогою проекту Calico). Він повинен бути аналогічним створюємим брандмауером для мікросервісів.

6. Вилучення своїх контейнерів з загальнодоступної мережі.

Amazon, з його AWS API Gateway, ймовірно, зробив це поняття більш поширеним і легко прийнятим, ніж будь-хто раніше. API Gateway встановлює єдину точку входу для всіх запитів, що надходять від всіх клієнтів.

За допомогою цієї методики можна захистити всі мікросервіси за брандмауером, дозволяючи AWS API Gateway обробляти зовнішні запити, в той час, коли мікросервісу будуть комунікувати між собою за брандмауером.

7. Використання сканерів безпеки для своїх контейнерів(сервісів).

У своєму автоматизованому тестовому наборі має сенс включати періодичну перевірку вразливостей і безпеки для своїх контейнерів. Головним чинником з відкритим вихідним кодом у цьому просторі є Клер, з CoreOS. Docker Security Scanning і Twistlock є це кілька комерційних опцій.

8. Всебічне контролювання за допомогою інструментів.

Не можна працювати з розподіленою системою без суччасної та надійної моніторингової платформи.

Створена інженерами SoundCloud, Prometheus є платформою моніторингу з відкритим вихідним кодом і частиною Cloud Native Computing Foundation. Його підтримують і приймають деякі з найбільших гравців у цій галузі, такі як самі SoundCloud, CoreOS та Digital Ocean.

Хоча вищезазначене не є вичерпним списком, воно стосується проблем, з якими, швидше за все, можна зіштовхнутися при створенні програми на основі мікросервісної архітектури.

Що стосується безпеки, то вона завжди сприймає будь який винахід корисною ідеєю.

Слід завжди досліджувати найкращі практичні доробки, прийняті промисловістю та запропоновані експертами.

Список використаних джерел:

1. Соціальна мережа (Інтернет). – Режим доступу: https://dataart.ru/news/o-bezopasnosti-mikroservisny-h-prilozhenij/
2. Соціальна мережа (Інтернет). – Режим доступу: https://www.owasp.org/images/2/20/Microservice_Security.pdf
3. Соціальна мережа (Інтернет). – Режим доступу: https://techbeacon.com/app-dev-testing/8-best-practices-microservices-app-sec

УДК 004.056.5

Пашорін Валерій Іванович
кандидат технічних наук,
професор кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Савон Олексій Євгенійович
студент 1 курсу магістратури ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КЛІЄНТСЬКОЇ БАЗИ ДАНИХ

Конфіденційність економічної інформації та безпека клієнтських даних має важливе значення для успіху бізнесу сучасних компаній будь-якого розміру.

Клієнтська база - це дані про покупців, їх споживчу поведінку і минулих покупках зібрані й організовані таким чином, щоб їх можна було швидко витягти для отримання необхідної інформації. Крім даних про існуючих клієнтів, клієнтська база містить відомості про потенційних клієнтів.

Першочерговими та добре всім відомими способами захисту інформації у клієнтських базах даних є встановлення надійних паролів, резервування копій і оновлення системи. Оскільки інформація, яку містять бази даних, особливо цінна для компаній та приваблива для зловмисників, вони потребують особливої уваги та додаткового захисту.

Є різні методи крадіжки даних, якими можуть скористатися хакери:

- злочинець починає атаку на фізичні файли бази даних для перегляду або зміни інформації, він може фізично отримати доступ до системи, навіть не маючи авторизації. Це відбувається, наприклад, при використанні мобільних клієнтських систем;

- злочинець хоче стати авторизованим користувачем системи, бази даних або програми. Для цієї мети існує програмне забезпечення для генерації та автоматичного використання списків користувачів. Часто досить просто подзвонити по телефону з “служби з технічної підтримки користувачів” і запитати ім’я і пароль користувача;

- злочинець використовує існуюче підключення до бази даних через мережу, яке було встановлено вповноваженим користувачем (напад);

- злочинець перехоплює незакодовану інформацію під час її передачі по мережі.

Наступні шляхи дозволять захистити бази даних підприємств:

1. *Контроль доступу до бази даних* - обмеження дозволів та привілеїв. Крім базових системних дозволів, слід застосувати наступні дії:

- обмеження доступу до конфіденційних даних для певних користувачів;

- обмеження дій користувачів по редагуванню баз даних;

- заборона використання баз даних в неробочий час.

2. *Визначення критично важливих даних.* Не всі дані є критично важливими або потребують захисту, тому на них немає сенсу витрачати час і ресурси.

3. *Шифрування інформації.* Слід застосувати надійні алгоритми шифрування конфіденційної інформації. У разі отримання доступу до сервера або системи, зловмисники в першу чергу спробують викрасти дані з бази, які, зазвичай, містять багато цінної інформації.

4. *Анонімність баз даних* – багато підприємств інвестують час та ресурси у захист своїх баз даних, але при розробці проектів або створення тестового середовища вони просто роблять копію вихідної бази даних і починають використовувати її в середовищах з менш жорстким контролем, тим самим розкриваючи всю конфіденційну інформацію і роблять її доступнішою для зловмисників.

Маскування та анонімізація допоможуть створити аналогічну версію бази даних з тією ж структурою, що і в оригіналі, але дані повинні бути зміненими для їх захисту. Шляхом цієї технології значення змінюються за умови збереження формату. Конкретні метод, правила і формати, залежать від вибору адміністратора, але, незалежно від вибору, метод має забезпечити неможливість отримати вихідні дані стороннім особам за допомогою реверсної інженерії.

Даний метод рекомендований для баз даних, які є частиною середовища тестування і розробки. Він дозволяє зберегти логічну структуру даних, забезпечуючи відсутність доступу до конфіденційної інформації поза виробничим середовищем.

5. *Моніторинг активності бази даних (DAM)* – аудит і відстеження процесів та дій всередині бази даних передбачають знання про те, яка інформація, коли, як і ким була оброблена. Повна історія транзакцій дозволяє зрозуміти шаблони доступу до даних і модифікацій іх, таким чином, допомагає уникненню витоку інформації, контролю небезпечних змін і виявленню підозрілої активності в режимі реального часу.

Список використаних джерел:

1. Захист баз даних — запорука безпека корпоративної мережі. URL: https://eset.ua/ua/ blog/view/14/index2/

2. Формування клієнтської бази URL: https://stud.com.ua/21501/marketing/ formuvannya_kliyentskoyi_bazi

3. Як захистити свою базу даних URL: http://easy-code.com.ua/2012/06/yak-zaxistiti-svoyu-bazu-danix-rezervne-kopiyuvannya-rizne-statti/

УДК 004.056.53:004.7

Крижанівський Володимир Григорович
доктор технічних наук, професор
Донецький національний університет
Сергієнко Сергій Петрович
кандидат фізико-математичних наук, доцент,
Донецький національний університет

ПОТЕНЦІЙНА ЗАГРОЗА ЗНІМАННЯ ІНФОРМАЦІЇ В ПОЛІ ШУМОВИХ ПЕРЕШКОД

В роботі розглядається потенційна загроза знімання інформації в поле шумових перешкод, що включаються для глушіння сигналів радіозакладок. Відомі принципи роботи пасивної радіозакладки, яка отримує енергію від зовнішнього джерела при подачі зондуючого сигналу досить великий амплітуди. В цьому випадку радіозакладка перетворюючи енергію зондуючого сигналу випромінює інформаційний сигнал на гармоніці зондуючого сигналу. Генерація гармонік відбувається на нелінійному елементі, найчастіше в якості нелінійного елемента використовується p / n перехід. Вихідна потужність сигналу мала, тому для придушення несанкціонованого знімання інформації використовують генератори шуму спектр випромінювання яких перекриває можливий діапазон частот роботи радіозакладки. В роботі показано, що вплив шумового сигналу на радіозакладка призводить до генерації шуму на частотах в смузі близькою до нульової і кратних частотних смугах до смуги випромінювання генератора шуму. Математичне моделювання спектра шуму при нелінійному перетворенні здійснювалося в припущенні, що ні лінійний елемент перебував на кінці лінії підключеної до прийомної антени. Рівняння зв'язують падаючу хвилю з відбитої в припущенні неінерційної системи мають вигляд:

$$u_{\varphi} - u_{\psi} = j_0 \cdot \left(e^{u_0 + u_{\psi} + u_{\varphi}} - 1 \right) \cdot z$$

де: u_{φ} , u_{ψ} - миттєве значення напруги падаючої і відбитої хвиль відповідно; z - хвильовий опір лінії; u_0- напруга зсуву. Шумовий сигнал моделювався нормально розподіленим сигналом з кореляційної функцією відповідної вузькосмугового сигналу виду:

$$r(\tau) := \frac{2 \cdot \sin(\Delta\omega\ \tau) \cdot \cos\left(\omega_0 \cdot \tau\right)}{\pi \cdot \Delta\omega \cdot \tau}$$

де: ω_0 - центральна частота смуги шуму; $\Delta\omega$ - ширина смуги шуму. Кореляційна функція відбитого сигналу знаходилась стандартним методом використовуючи двовимірну щільність ймовірності нормально розподіленого сигналу Фур'є перетворення кореляційної функції дає спектр потужності відбитої хвилі.

$$B(\tau, \sigma, u_0, z) := \left[\int_{-3\cdot\sigma}^{3\cdot\sigma} \int_{-3\cdot\sigma}^{3\cdot\sigma} \frac{1}{z} \cdot u_{\psi}\left(u_{\varphi 1}, u_0, z\right) \cdot u_{\psi}\left(u_{\varphi 2}, u_0, z\right) \cdot \frac{1}{2 \cdot \pi \cdot \sigma^2 \cdot \sqrt{1 - r(\tau)^2}} \cdot e^{\frac{-\left(u_{\varphi 1}{}^2 - 2 \cdot u_{\varphi 1} \cdot u_{\varphi 2} \cdot r(\tau) + u_{\varphi 1}{}^2\right)}{2 \cdot \sigma^2 \cdot \left(1 - r(\tau)^2\right)}} du_{\varphi 1}\, du_{\varphi 2} \right]$$

Моделювання процесу нелінійного перетворення шумового сигналу на p / n переході показало, що спектральна щільність шуму на смузі на частотах рівних подвоєною смузі частот роботи генератора шуму залежить від співвідношення диференціального опір переходу і лінії передачі, що з'єднує перехід з випромінюючої антеною, напруги зсуву переходу. Спектр сигналу генератора шуму і спектр перетвореного сигналу, що відбивається від нелінійного елемента представлені на рис.1. Величина спектральної щільності потужності шуму відбитої хвилі на подвоєною частоті визначається смугою генератора шуму і напругою зсуву див. Графік Ротр. рис.2. Залежність спектральної щільності потужності на подвоєною частоті від напруги зсуву при відносно опору лінії і диференціального опору переходу рівне 9 рис. 3 і для величини відносини рівне 0,1 представлена на рис. 4. Як випливає з залежності, представленої на графіку рис. 3, 4., використання прямо зміщеного переходу рис.4 дозволяє найбільш ефективно перетворювати енергію генератора шуму в випромінювання в смузі частот кратна відрізняються від діапазону частот генератора шуму. При подачі на перехід змінної напруги, що несе інформацію на прямо зміщений перехід, буде спостерігатися амплітудна модуляція шумового сигналу на частотах поза діапазоном випромінювання генератора шуму. В роботі аналізуються методи, що дозволяють реєструвати інформаційний сигнал використовуючи кореляційний вимір. Пропонуються методи боротьби з несанкціонованим зніманням інформації.

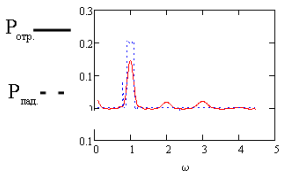

Рис.1 Спектр потужності шуму падаючої та відбитої хвиль

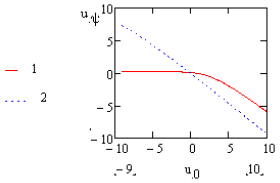

Рис.2 залежність амплитуди відбитої хвилі від напруги зсуву

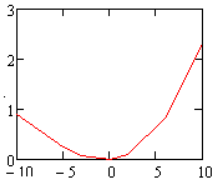

Рис.3 Залежність спектральної потужності $\omega := 2$ від напруги зсуву для відношення імпедансів переходу та лінії 9

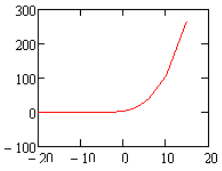

Рис.4 Залежність спектральної потужності $\omega := 2$ від напруги зсуву для відношення імпедансів переходу та лінії 0,1

Список використаних джерел:

1. Колодій З. О. Флікер-шумова діагностика внутрішньої структури елементів електроніки / Колодій З. О. // Радиоэлектроника и информатика. - 2005. № 3. - С. 40-42.

UDC 004.056:334.7=111

Semidotska V.
Lecturer,
Kyiv National University of Trade and Economics
Polyuhovych A.
Student,
Kyiv National University of Trade and Economics

CYBER SECURITY IN ENTERPRISES

The threat of cybercrime to business is rising very quickly. And how to create a cyber protected business is what companies really need to understand.

There are several agents which cause possibility of cyber attacks in enterprises.

The most important element in cyber security net is the human factor because the human understanding of cyber security is absent in most cases. Looking at even last year 93% of the cyber attacks in the United States happened because of human error. That's why it is important to educate and train employees to spot the breach and mitigate the risks. Organization should create training to help employees to understand how their digital attainments affect the surroundings they work in. Workman have to understand where the risks are and the way of consideration that give offense them to online attacks.

What about hardware protection mechanism? While hardware may be a source of insecurity hardware-based computer security also offers an alternative to software-only computer security.

- USB dongles are typically used in software licensing schemes to unlock software capabilities. They can also be a way to prevent unauthorized access to a computer.
- Trusted platform modules (TPM) secure devices by integrating cryptographic abilities onto access devices. TPMs used in connection with server-side software offer a way to detect and certify hardware devices, interfering unauthorized network and data access.
- Computer case intrusion detection refers to a device, characteristically a push-button switch, which detects when a computer case is opened.

There are widespread types of cyberattacks.

1. Malware (malicious software): spyware, viruses, worms and ransomware. Malware can:

- Get information underground by transmitting data from the hard drive (spyware).
- Block access to key elements of the network (ransomware).
- Installs extra adverse software.

2. Man-in-the-middle attack (MitM) attacks: hackers insert themselves into a two-party transaction. There are two ways of entry for Man-in-the-middle attacks:

- Via unsecure public Wi-Fi: hackers can enclose themselves between a visitor's device and the network. Remaining above suspicions hackers interfere into the process of transmitting data by visitors.
- If malware has broken a device, hacker can install software to process all of victim's information.

3. Phishing is a type of attack often used to carry out user data, including login credentials and credit card numbers or install malware on the victim's devices. Phishing is usually carried through email.

4. Denial-of-service attack: A DOS attack block up systems, servers, or networks with traffic to drain resources. Attackers can also use multiple compromised devices to set off this attack (distributed-denial-of-service (DDoS) attack).

Who is responsible for cyber security in the enterprise? The responsibility for cyber security depends of the company. Enterprise security budget depends on the size of the organization and type of industry they are a part of. On the whole, cost devoted to security move between 3% and 15% of an IT budget. The value of recovering from a serious cyber crime can run into millions of dollars and no-one is protected fully. Security investment will vary depending on the type of business and how and where it operates.

Here are several hints for cyber security of your enterprises:

✓ Use a firewall (The Federal Communications Commission (FCC) recommends that all business set up a firewall to provide a barrier between your data and cybercriminals).

✓ Document your cybersecurity policies (cyber security is area where it is significant to document your protocols).

✓ Educate all employees. Employees must be educated on network security best practices. They should be a human firewall.

✓ Enforce safe password practices (it's essential that all employees' devices accessing the company network be password protected).

✓ Regularly back up all data (backing up word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files, be sure to also back up all data stored on the cloud).

✓ Install anti-malware software (it's substantiality to have anti-malware software installed on all devices and the network).

✓ Use multifactor identification (using the multifactor identification settings on most major network and email products is simple to do and provides an extra layer of protection).

The Cabinet of Ministers of Ukraine has approved an action plan on the implementation of Ukraine's cyber security strategy. The action plan includes tasks

in the following areas: regulatory support for activities in the field of cyber security, development of the technological component of the national cyber security system; establishment of cooperation with international partners of Ukraine, and establishment of the process of training personnel in the field of cyber security.

References:

1. Big Data Made Simple//Why enterprises should be investing in cyber security. [Electronic resource] - Electronic text data. – Mode of access: https://bigdata-madesimple.com/why-enterprises-should-be-investing-in-cybersecurity/
2. Information age//Who is responsible for cyber security in the enterprise. [Electronic resource] - Electronic text data. – Mode of access: https://www.information-age.com/responsible-cyber-security-enterprise-123474640/
3. International college of Yayasan Melaka // Computer Protection. [Electronic resource] - Electronic text data. – Mode of access: http://www.icym.edu.my/v13/about-us/our-news/general/473-computer-protection-countermeasures.html
4. Everipedia International // Computer security. [Electronic resource] - Electronic text data. – Mode of access: https://everipedia.org/wiki/lang_en/Computer_security/
5. Cisco // What Are the Most Common Cyberattacks? [Electronic resource] - Electronic text data. – Mode of access: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
6. CoxBlue // 8 Cyber Security Best Practices For Your Small To Medium-Size Business (SMB) [Electronic resource] - Electronic text data. – Mode of access: https://www.coxblue.com/8-cyber-security-best-practices-for-your-small-to-medium-size-business-smb/
7. Federal Communications Commission // Cybersecurity for Small Business. [Electronic resource] - Electronic text data. – Mode of access: https://www.fcc.gov/general/cybersecurity-small-business
8. SymQuest // Cyber Security for Businesses. [Electronic resource] - Electronic text data. – Mode of access: https://www.symquest.com/cyber-security-for-business/
9. NATO // Enhancing cybersecurity in Ukraine. [Electronic resource] - Electronic text data. – Mode of access: https://www.nato.int/cps/en/natohq/news_159840.htm
10. Ukrinform // Information and cyber security in the modern world: experience of the SSU. [Electronic resource] - Electronic text data. – Mode of access: https://www.ukrinform.net/rubric-society/2510267-information-and-cyber-security-in-the-modern-world-experience-of-the-ssu.html
11. Thegfce // Cybersecurity in Ukraine: National Strategy and international cooperation. [Electronic resource] - Electronic text data. – Mode of access: https://www.thegfce.com/news/news/2017/05/31/cybersecurity-in-ukraine

УДК [330.526.33:004.056.53](477)

Маковоз Оксана Сергіївна
доктор економічних наук, доцент,
завідувач кафедри економіки та фінансів
Харківський національний університет внутрішніх справ
Передерій Тетяна Сергіївна
слухач магістратури
Харківський національний університет внутрішніх справ

ПРОДУКТИ ТА СЕРВІСИ КІБЕРЗАХИСТУ ПІДПРИЄМСТВА ЕЛЕКТРОННОЇ КОМЕРЦІЇ

У сучасних умовах одним із найціннішим активів будь-якого підприємства є інформація, і в основі всіх бізнес-процесів лежать інформаційно-комунікаційні технології. Сьогодні інформація має великий вплив на процеси, що відбуваються в суспільстві і саме тому грамотно вибудуваний захист даних компанії – це одна з ключових умов забезпечення її конкурентоспроможності та розвитку.

Забезпечення інформаційної безпеки є одним з ключових моментів забезпечення безпеки підприємства. Як вважають західні фахівці, витік 20% комерційної інформації в шістдесяти випадках зі ста призводить до банкрутства підприємства, тому фізична, економічна та інформаційна безпека дуже тісно взаємопов'язані[1].

Інформаційна безпека є одним з найважливіших компонентів інтегральної безпеки електронної комерції. Кількість атак на інформаційні системи у всьому світові щороку подвоюється. В таких умовах система інформаційної безпеки електронної комерції повинна вміти протистояти численним і різноманітним як внутрішнім так і зовнішнім загрозам. Основні загрози інформаційній безпеці електронної комерції пов'язані: з навмисними посяганнями на інтереси суб'єктів електронної комерції (комп'ютерні злочини і комп'ютерні віруси); ненавмисними діями обслуговуючого персоналу (помилки і т. д.); вплив технічних чинників, здатних призвести до спотворення і руйнування інформації (збої електропостачання, програмні збої); вплив техногенних факторів (стихійні лиха, пожежі, великомасштабні аварії і т. д.). Загрози безпеці можуть бути пов'язані з діями факторів, значення і вплив яких практично завжди невідомо, тому неможливо створити абсолютно безпечну систему. При створенні системи безпеки електронної комерції необхідно мінімізувати ступінь ризику виникнення збитків, виходячи з особливостей загроз безпеки і конкретних умов підприємства, що займається електронною комерцією.

Ринок електронної комерції у світі зростає зі швидкістю 23-25%, що значно швидше за класичні роздрібні магазини. Український ринок e-commerce зростає зі швидкістю понад 30%, посідаючи друге місце за темпами в Європі. При цьому подібні темпи можуть зберігатися тривалий час, оскільки частка онлайн-продажів у роздрібній торгівлі загалом в Україні складає 3,2%, тоді як в середньому в Європі 8,8%, а у Британії – 17,8% [2].

PT ISIM freeView Sensor надається у вигляді віртуальної машини, яка підключається до порту Віддзеркалення (Mirror, SPAN) комутатора мережі

АСУ ТП. Система обробляє копію трафіку мережі АСУ ТП (в тому числі таких протоколів, як CIP, IEC-104, MMS, Modbus TCP, OPC DA, Profinet DCP, S7, Spabus, ARP, DHCP, DNS, FTP, HTTP, ICMP, SNMP, SSH, Telnet, TFTP), не впливаючи на її компоненти. Ключові завдання, які вирішує щоденне використання PT ISIM freeView Sensor – інвентаризація мережевих активів АСУ ТП, контроль інформаційної взаємодії в АСУ ТП, виявлення мережевих і промислових атак, а також випадків несанкціонованого управління [3].

InfoWatch Traffic Monitor – програмний комплекс для захисту даних, запобігання витоків і контролю переміщення конфіденційної інформації за межі організації, а також захисту підприємства від внутрішніх загроз. DLP-система здійснює: контроль інформації, що передається через корпоративну поштову систему, інтернет-ресурси, засоби загального доступу до файлів (SMTP, HTTP, HTTPS, FTP); контроль систем обміну повідомленнями (ICQ, Skype і інші); контроль голосового трафіку (Skype); контроль використання пристроїв і портів на робочих станціях; керування з'єднаннями з мережею на робочих станціях; тіньове копіювання роздрукованих і тих,що копіюються на зйомні носії; запобігання витоку конфіденційних даних шляхом блокування процесу передачі даних в разі порушення політики безпеки [4].

Створюючи єдину концепцію кібербезпеки слід відштовхуватися від наявної системи загальної безпеки і грамотно транслювати її в сфері інформаційних технологій. Концепція повинна містити моделі інформаційних ризиків і негативних наслідків, а також план заходів щодо їх мінімізації та усуненню. Модель інформаційних ризиків визначає захищені об'єкти і дані, потенційні фактори загроз, можливий збиток і способи захисту. До заходів щодо забезпечення кібербезпеки відносяться впровадження адміністративних та технологічних регламентів, спеціалізованих програмних і апаратних комплексів, створення ешелонованих комплексів технічних засобів захисту. Єдина концепція кібербезпеки розглядає всю діяльність на підприємстві, інформаційні системи в цілому і включає кількісний і якісний аналіз загроз, заходи по їх запобіганню. До основних завдань концепції інформаційної безпеки, що реалізується можна віднести забезпечення конфіденційності наявних даних, їх доступності, цілісності та автентичності. Таким чином, захист може включати засоби контролю поширення електронних документів, запобігання несанкціонованих поштових розсилок, забезпечення автентичності документів, редагованих віддаленими користувачами й чимало інших аспектів[5].

Список використаних джерел:

1. Безопасность электронной комерции. [Электронный ресурс] – Режим доступа: http://csaa.ru/bezopasnost-jelektronnoj-kommercii/
2. Зелена книга ринок електронної комерції. Офіс ефективного регулювання. Грудень 2018р. [Електронний ресурс] – Режим доступу: https://cdn.regulation.gov.ua/e5/ea/4c/d5/regulation.gov.ua
3. Positive Technologies приучает предприятия к мониторингу АСУ ТП. [Электронный ресурс] – Режим доступа: https://www.comnews.ru/content/114869/2018-09-12/positive-technologies-priuchaet-predpriyatiya-k-monitoringu-asu-tp.

УДК 004.056

Пострелко Юрій Михайлович
директор Департаменту Інформаційної Безпеки
ТОВ «M.E.Doc»

КІБЕРЗАХИСТ ЗА M.E.DOC – РЕЗУЛЬТАТ ВЗАЄМОДІЇ З БІЗНЕСОМ, ДЕРЖАВОЮ І МІЖНАРОДНИМИ ЕКСПЕРТАМИ

ТЕЗИ ДОПОВІДІ:

- Попит і вимоги до фахівців у сфері кібербезпеки. Вчора і сьогодні.
- Історія найбільшої кібератаки на Україну. Правда з перших уст.
- Як це було. Forensic від міжнародних і вітчизняних експертів.
- Практичний кейс з побудови захисту від сучасних кіберзагроз. Аналіз і підбір продуктів по ІБ.
- Державна підтримка бізнесу в організації кіберзахисту.

НАУКОВИЙ НАПРЯМ 4
КРИПТОГРАФІЧНІ МЕТОДИ
ЗАХИСТУ ІНФОРМАЦІЇ

SCIENTIFIC AREA 4
CRYPTOGRAPHIC TECHNIQUES
IN INFORMATION SECURITY

УДК 004.056.55

Фесенко Андрій Олексійович
кандидат технічних наук,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Гнатюк Сергій Олександрович
доктор технічних наук, доцент,
професор кафедри безпеки інформаційних технологій
Національний авіаційний університет
Кінзерявий Василь Миколайович
кандидат технічних наук,
доцент кафедри безпеки інформаційних технологій
Національний авіаційний університет

ШВИДКІСНИЙ СИМЕТРИЧНИЙ БЛОКОВИЙ АЛГОРИТМ ШИФРУВАННЯ

Одним із найважливіших напрямів діяльності щодо забезпечення конфіденційності даних був і залишається захист інформації криптографічними методами , беззаперечною перевагою яких є забезпечення захисту безпосередньо самих даних, а не доступу до них. Основним критерієм при виборі криптосистем є стійкість, проте для деяких завдань ключову роль відіграє швидкість криптографічної обробки даних [1]. Незважаючи на різноманітність сучасних криптографічних методів та систем, далеко не всі володіють необхідним рівнем ефективності (швидкодії та стійкості) для забезпечення захисту даних, а розвиток і здешевлення інформаційно-комунікаційних технологій позитивно впливає на ефективність криптоаналізу, одними з найефективніших методів якого є лінійний та диференціальний криптоаналіз [2-4].

Нехай $t', p', r', q'-$ натуральні числа, $t = 2t'$, $p = 2p'$, $r = 2r' + 1$, $n = tp, q = pq'$, $w = p$, $k = 2n$, $b = 2^{q'}$ (параметр b визначає кількість різних таблиць замін (підстановок), що можуть використовуватись у методі). Тоді r-раундовий метод криптографічного захисту $\Im$ із множиною відкритих (шифрованих) повідомлень $V = \{0,1\}^n$, множиною секретних ключів V_k, множиною раундових ключів V_{n+q+w} можна описати такою послідовністю етапів:

Етап 1 − Вироблення раундових ключів. На цьому етапі із секретного ключа $K, K \in V_k$, виробляється r раундових ключів $K_i, K_i \in V_{n+q+w}, i = \overline{1,r}.$

Етап 2 − Процедура шифрування. На цьому етапі відбувається шифрування секретного повідомлення $\grave{A} = (A_1, A_2, A_3, ..., A_u)$, $\grave{A} \in V_{n \cdot u}$, $\grave{A}_j \in V_n$, $j = \overline{1,u}$, u −натуральне число.

На основі запропоновано методу розроблено БШ Luna-2k17. Для даного шифру обрано такі параметри: $t' = 8, t = 2t' = 16$ (розрядність таблиць замін), $p' = 4$, $p = 2p' = 8$, $r' = 4$, $r = 2r' + 1 = 9$ (кількість раундів), $n = tp = 128$ (розмір блоку даних, біт), $q' = 3$, $q = pq' = 24$, $b = 2^{q'} = 8$ (використовується 8

таблиць замін на множині V_{16}), $w=8$, $k=2n=256$ (розмір секретного ключа, біт).

Запропонований шифр працює із 128-бітними блоками даних з підтримкою секретного ключа довжиною 256 біт. При розширенні секретного ключа виробляється необхідна кількість 160-бітних раундових ключів ($n+q+w=128+24+8=160$). Блоки даних та розширені ключі представляються у вигляді 8×2 байтної матриці.

Для експериментального дослідження блоковий шифр Luna-2k17 був програмно реалізований у вигляді консольного застосунку «Luna-2k17».

Статистичні властивості послідовностей, утворених за допомогою цього застосунку (у режимі лічильника) досліджено у середовищах статистичних тестів NIST STS. Шифр Luna-2k17 пройшов комплексний контроль за методиками NIST STS та показав не гірші результати ніж ДСТУ (ГОСТ) 28147-89, Калина, AES.

Також досліджені швидкісні характеристики шифрів. Експериментальні дослідження показали, що шифр Luna-2k17 швидший за шифр ДСТУ (ГОСТ) 28147-89 приблизно у 3,11 рази, а за шифри Калина та AES у 1,271 рази. Дослідження проводилися в однакових умовах на Intel (R) Core (TM) i7-2600K CPU 3.4 GHz.

Таким чином, розроблено криптографічний метод захисту, який за рахунок нової послідовності операцій в процедурах вироблення раундових ключів та шифрування (використовуються таблиці замін із збільшеною розрядністю та рандомізуються лінійні і не лінійні операції) дозволяє підвищити ефективність криптографічного захисту. На основі даного методу побудовано блоковий си-метричний шифр Luna-2k17. Розраховано значення верхніх оцінок параметрів, що характеризують його практичну стійкість до кібератак лінійного та диференціального криптоаналізу. За однакових умов, проведені експериментальні дослідження з оцінки швидкісних характеристик шифрів, які показали, що шифр Luna-2k17 швидший за шифр ДСТУ(ГОСТ) 28147-89 приблизно у 3,11 рази, а за шифри Калина та AES у 1,271 рази. Також, досліджено статистичні властивості послідовностей сформованих блоковим шифром Luna-2k17, результати порівнянь показали, що шифр Luna-2k17 пройшов комплексний контроль за методиками NIST STS та показав гарні результати в порівнянні з інші шифрами.

Список використаних джерел:

1. Основні критерії та вимоги до побудови сучасних криптосистем / О.Г. Корченко, С.О. Гнатюк, Ю.Є. Хохлачова, А.О. Охріменко // Вісник Інженерної академії України. – 2011. – №3-4. – С. 77-83.
2. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.
3. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17 – 38.
4. Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93, Proceedings.– Springer Verlag, 1994. – P. 386 – 397.

УДК 004.056.5

Харченко Олександр Анатолійович
кандидат технічних наук, доцент,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Прокоп'єв Андрій Костянтинович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ЕВОЛЮЦІЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ

Сучасна криптографія з'явилась в результаті розвитку алгоритмів шифрування інформації, який почався в середині 70-х років. Серед найпоширеніших напрямків криптографії можна виділити: симетричне та асиметричне шифрування, з закритим та відкритим ключами відповідно.

Симетричне шифрування заключається в тому, що для шифрування і дешифрування використовується один ключ. Криптографічний ключ – це параметр, використовуваний в алгоритмі достовірності, автентифікації шифрування або дешифровки повідомлення. Ключ алгоритму обирається перед початком обміну, повідомляється обом сторонам і є секретним, він передається іншим каналом обміну. Саме симетричне шифрування лягло в основу першого алгоритму шифрування, тому що він відносно технічно простий в реалізації. Найпростішим прикладом симетричного шифрування може бути заміна символів за певним законом.

На відміну від симетричного шифрування асиметричне має два типи ключів: відкритий, який передається незахищеним каналом, і секретний ключ, що використовується при автентифікації і декодуванні інформації. Під час інтенсивного розвитку мережі Internet, набули великої популярності системи шифрування з відкритим ключем. Основний принцип таких алгоритмів заключається у використанні односторонньої функції. Прикладом асиметричного шифрування може бути використання певної книги в ролі таємного ключа. В цьому випадку відкритий ключ передається незахищеним каналом і являється послідовністю даних, в якій містяться номера сторінок, рядків і слів закодованого повідомлення. Знаючи всю послідовність даних відкритого ключа декодувати повідомлення не вдається не знаючи послідовність в таємній книзі.

В сучасних алгоритмах шифрування передбачено, що в каналі передачі даних міститься інформація про сам алгоритм і частини відкритого коду, але секретний ключ передається окремим каналом, тому розшифрувати дані неможливо. Щоб дізнатися секретний ключа можливо лише послідовно перебрати всі можливі варіанти шифрування. При цьому, довжина секретного коду, що використовується при шифруванні даних, не дозволяє розкодувати інформацію за прийнятний час. Також однією з важливих характеристик при шифруванні даних є стійкість криптографічному аналізу.

В 70-х роках XX століття в США почали проводити конкурс на такий криптографічний алгоритм, який зміг би відповідати всім вимогам високої надійності. Спочатку учасникам не вдавалось створити надійний алгоритм, але результатом третього конкурсу було представлено криптографічний алгоритм шифрування DES, що став першим міжнародним криптографічним алгоритмом шифрування.

Не зважаючи на те, що є теоретичні алгоритми злому 3-DES-шифрування, досі невідомо випадків про успішне розшифрування алгоритму. Але 3-DES-шифрування, окрім зламостійкості, має і велику кількість недоліків, серед яких: низька швидкість шифрування і розшифрування, складність для програмної реалізації. Всі недоліки алгоритму 3-DES зумовлюють неконкурентно-спроможність перед алгоритмом шифрування AES.

В порівнянні з іншими алгоритмами, AES має достатньо простий математичний опис. При цьому алгоритм ґрунтується на стверджуванні про важкість розв'язку певних видів математичних рівнянь, на яких базується код, тому немає впевненості втому, що він є абсолютно безпечним. Деякі вчені навіть описували в своїх роботах теоретичну процедуру розшифрування AES алгоритму. У 2001 році Нільс Фергюсон опублікував статтю під назвою XSL-атака, в якій алгоритм шифрування AES записали в вигляді алгебраїчної формули і припустили, що шифр можна зламати, якщо не враховувати аргументи в -1 степені. Але під час практичних досліджень так і не вдалося зламати алгоритм. Через декілька років довели, що XSL-атака на алгоритм AES не може розшифрувати дані чи зламати його.

В свою чергу Даніель Бернштейн у 2005 році провів дослідження процедури зламу алгоритму шифрування, які базувались на тестуванні недоліків в математичній моделі алгоритму. Під час практичного дослідження на алгоритм здійснювались атаки сторонніми каналами. Для здійснення однієї вдалої атаки знадобилось більше двохсот мільйонів зашифрованих алгоритмом AES текстів.

Незважаючи на те, що алгоритм AES вдалось зламати, сьогодні він є найрозповсюдженішим алгоритмом симетричного шифрування. Компанія Intel в процесорах сімейства Sandy Bridge використовує на апаратному рівні саме алгоритм шифрування AES. Також цей алгоритм набув високого розповсюдження в мережевих протоколах HTTPS і більшості платних сервісах.

Список використаних джерел:

1. Зегжда Д. П. Основи безпеки інформаційних систем. / Д. П. Загжда - Основи безпеки інформаційних систем.
2. Діффі У. Захищеність і імітостійкість. Введення до криптографії. / У. Діффі, М.Е. Хеллмен - Захищеність і імітостійкість. Введення до криптографії.
3. Романець Ю. В. Захист інформації в комп'ютерних системах і мережах / Ю.В. Романець, П. А. Тімофеєв, В. Ф. Шаньгин - Захист інформації в комп'ютерних системах і мережах.

УДК 004.056

Цюцюра Світлана Володимирівна
доктор технічних наук, професор
завідувач кафедри інформаційних технологій
Київський національний університет архітектури та будівництва
Мокляк Аліна Олександрівна
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ЗАГРОЗИ КЛЮЧАМ У СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

Великий інтерес до впровадження хмарних сервісів та їх широке застосування спричинило появу новітніх методів забезпечення безпеки в хмарному середовищі з урахуванням особливостей його функціонування. Однією з таких задач є забезпечення конфіденційності, цілісності, спостережливості та доступності ключів та ключових даних в хмарі.

Крім того до традиційних ризиків безпеки, що існують в обчислювальних системах, підключених до Інтернету, хмарні системи мають своєрідні проблеми безпеки та конфіденційності через віртуалізацію хмар та характер своєї багаторівневої природи.

Метою дослідження є обґрунтування та розробка моделі загроз компрометації ключів при управлінні ключовою інформацією в хмарі, а також пропозиції щодо захисту від них.

Відносно ключових даних у середовищі хмари порушник може реалізовувати такі загрози [1]:

- злом ключів та ключової інформації;
- незаконне знищення ключів та ключової інформації;
- перейняття та створення копій ключів та ключової інформації;
- створення невірних ключів та ключової інформації;
- створення слабких ключів або напів-слабких ключів;
- спотворення ключів або ключової інформації;
- отримання незаконного доступу до ключів чи ключової інформації;
- отримання можливості несанкціонованого використання ключів тощо.

Проаналізувавши вищезгадане, було встановлено, що відносно ключових даних в середовищі хмари є та можуть бути реалізовані такі загрози як перехоплення та запам’ятовування, компрометація, незаконне знищення, створення слабких та несанкціоноване використання ключів. Але найнебезпечнішими для ключових даних користувача є привілейовані користувачі - адміністратори хмарних сервісів, які володіють доступом до середовища, в якому існують хмарні додатки користувача.

Беручи до уваги рекомендації, нормативні документи та стандарти було створено профіль правопорушника, до якого відносять категорію осіб,

характер дій, рівень доступу та можливостей, рівень ознайомленості, методи та засоби, що використовуються та мету дій порушника [2]. Його використання має на меті формалізувати процес побудови моделі загроз хмари та розглянути можливості порушника, щодо ключової інформації в хмарі.

Також на основі детального аналізу стану та вимог відносно безпечності управління ключами зі сторони нормативно-правових документі та стандартів, включаючи проекти, обґрунтовані механізми захисту конфіденційних, особистих та відкритих ключів користувача від виявленої множини загроз. Вони зводяться до використання для забезпечення високого рівня безпеки, тобто високого рівня ймовірностей реалізації загроз у середовищі хмарних обчислень, комплексу технічних, організаційних та організаційно-технічних заходів та засобів, у тому числі до використання, а саме [3]:

– на рівні користувача захищених з необхідним рівнем безпеки ключових носіїв;

– на рівні каналів зв’язку між користувачем та хмарою захищених каналів зв’язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються;

– на рівні сервісів ідентифікації, автентифікації, авторизації та керування правами доступом надійних протоколів автентифікації з стійкими криптографічними алгоритмами, а також методів багатофакторної автентифікації;

– для здійснення криптографічних операцій на рівні сервісів додатків та інфраструктури захищених відповідним чином модулів криптографічного захисту – HSM.

Список використаних джерел:

1. Зикратов, И. А. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода [Текст] / И. А. Зикратов, С. В. Одегов // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 121–126.

2. Jansen, W. Cloud Hooks: Security and Privacy Issues in Cloud Computing [Text] / W. Jansen // 44th Hawaii International Conference on System Sciences (HICSS) – 2011. – P. 1–10. doi: 10.1109/hicss.2011.103

3. Безпека даних в хмарних середовищах: матеріали V міжнар. наук.-практ. конф. з інформаційних систем та технологій, 1-2 грудня 2017 р., Київ / відп. ред. А. В. Писаренко. – К.: Вид-во ТОВ «Інжиніринг», 2017. – 28 с.

4. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture, National Institute of Standards and Technology, U.S. Department of Commerce , 2015 –28c.

5. P. Mell and T. Grance, The NIST definition of cloud computing, National Institute of Standards and Technology, U.S. Department of Commerce, 2014 – 100 c.

УДК 004.6

Тесленко Олександр Кирилович
кандидат технічних наук, старший науковий співробітник, доцент
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Бондарчук Максим Юрійович
аспірант
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

ОЦІНКА КІЛЬКОСТІ МОЖЛИВИХ ПІДСТАНОВОК НА КІНЦЕВИХ АВТОМАТАХ

Методи реалізації та використання підстановок довільної розрядності на комбінаційних структурах лінійної складності розглядались в ряді робіт. Зокрема в [1] наведена класифікація таких структур – одновимірних каскадів конструктивних модулів (ОККМ), визначені поняття найпростіших, простих, складних, одно направлених, двонаправлених та регулярних каскадів.

В [2] показано, що на найпростіших однонаправлених регулярних ОККМ можна реалізувати 48 різних підстановок довільної розрядності, більшої за 2. В даній роботі розглядається реалізація підстановок довільної розрядності на одно направлених складних регулярних ОККМ.

Конструктивний модуль (КМ) такого каскаду складається з двох комбінаційних схем – перша з них реалізує значення сигналів на первинних виходах , друга реалізує значення сигналів на бокових виходах. На входи обох комбінаційних схем поступають сигнали з первинних та бокових входів КМ. Очевидно, що такий ОККМ реалізує відображення вхідних даних, яке співпадає з відображенням вхідних послідовностей відповідного цифрового автомату Мілі. Це дозволяє використовувати теорію цифрових автоматів [3] для аналізу властивостей ОККМ будь якої складності.

Нехай маємо скінченний вхідний алфавіт X розмірністю n: $\{x_1, x_2, \ldots, x_n\}$, скінченний вихідний алфавіт Y розмірністю n: $\{y_1, y_2, \ldots, y_n\}$. Досліджувана функція підстановки $f:X \to Y$ перетворює множину X в множину Y за допомогою автомата Мілі зі скінченною множиною станів Q розмірністю m, функцією переходів $\delta:Q \times X \to Q$, функцією виходів $\theta:Q \times X \to Y$ і початковим станом $q_0 \in Q$ і який в якості алфавіту входів використовує множину X, а в якості алфавіту виходів – множину Y. Тоді для умови унікальних вихідних послідовностей (повідомлень) необхідно визначити наступні питання: яку кількість унікальних автоматів Мілі можна побудувати та скільки унікальних послідовностей можна згенерувати.

Позначимо $\dot{X}_r$ множину всіх послідовностей довжиною r із елементів вхідного алфавіту, а $\dot{Y}_r$ – вихідного. Тоді можна сказати, що функція f виконує відображення множини $\dot{X}_r$ в множину $\dot{Y}_r$ ($\dot{X}_r \to \dot{Y}_r$).

Реалізація даної функції підстановки базується на наступних твердженнях.

Твердження 1. Якщо функція виходів θ задана двома параметрами q та x, то для того, щоб функція f реалізовувала бієктивне відображення $\dot{X}_r \rightarrow \dot{Y}_r$, достатньо, щоб для будь-яких $x_1,x_2 \in X$, де $x_1 \neq x_2$ та бідь-якому $q \in Q$ виконувалась умова $\theta(x_1,q) \neq \theta(x_2,q)$, тобто кожний рядок таблиці виходів є перестановкою елементів множини Y.

Твердження 2. Для не еквівалентності відображень автомата, згідно Твердження 1, при різних початкових станах достатньо, щоб для будь яких станів $q_1,q_2 \in Q$, де $q_1 \neq q_2$, та будь якого $x \in X$ виконувалась умова $\theta(x,q_1) \neq \theta(x,q_2)$.

Позначимо як G множину автоматів, які задовольняють твердженням 1 та 2 і відрізняються початковими станами, при цьому $|G|=|Q|$. Автомати цієї множини формують різні бієктивні відображення $\dot{X}_r \rightarrow \dot{Y}_r$. Це твердження випливає із алгоритму визначення еквівалентних станів автомата.

Нехай $p(q)$ – деяка перестановка елементів множини Q, а $p^{-1}(q)$ – обернена перестановка, тобто $p(p^{-1}(q))= p^{-1}(p(q))= q$. Для будь якого автомата $A \in G$ створимо автомат $\tilde{A}$ з тими самими алфавітами X,Y, Q і з наступними функціями $\dot{f}_o(x,q) = f_o(x, p(q))$, $\dot{f}_o(x,q)= p^{-1}(f_s(x, p(q))$, та початковим станом $q_{0A}=p^{-1}(q_0)$. Легко бачити, що автомат A та $\tilde{A}$ еквівалентні, але не ізоморфні, згідно з визначенням в [3].

Ґрунтуючись на викладеному, визначимо оцінку $O(n,m)$ різних бієктивних відображень, які можуть бути створені при $|X|=|Y|=n$, $|Q|=m$:

$$O(n,m) \approx \frac{m^{m \times n} \cdot (n!)! \cdot m}{((n!-m)!) \cdot 2 \cdot m!}$$

На етапі структурного синтезу автоматів (ОККМ) значення m та n є степенями двійки. Це не впливає на наведені результати. Шляхом вибору кодувань елементів множин X, Y та Q, створюються ізоморфні автомати, які можуть бути не еквівалентними . Тому наведена оцінка є нижньою для кількості різних підстановок довільної розрядності, які можуть бути реалізовані на регулярних односторонніх ОККМ будь якої складності.

Список використаних джерел:

1. Тарасенко В. П. Проблеми апаратної реалізації підстановок / В.П Тарасенко, О. К. Тесленко, О. Ю. Яновська //Наукові записки УНДІЗ, №2, 2007, с. 52-58.

2. Тарасенко В. П. Властивості повних підстановок, які реалізуються найпростішим однонаправленим регулярним ОККМ/ В. П Тарасенко, О.К.

3. Тесленко, О. Ю. Яновська // Радіоелектронні і комп’ютерні системи. №6, 2010, с.123-128.

4. Глушков В. М. Синтез цифрових автоматов.

УДК 004.056.4

Криворучко Олена Володимирівна
доктор технічних наук, професор,
завідувач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Проява Владислав Вікторович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

ЗАХИСТ ДАНИХ У ДОДАТКАХ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Мобільні пристрої дозволяють робити майже все онлайн – з будь-якого місця, у будь-який час. Ми маємо можливість керувати банківськими операціями, відстежувати наш прогрес у фітнесі і навіть працювати віддалено. Підвищення продуктивності мобільних пристроїв – це безліч мобільних додатків: програмне забезпечення, яке підключається до програмного інтерфейсу додатку (API) та серверів по всьому світу для надання даних і послуг.

Але все це має відбутися під наглядом добре сконструйованого захисту, так як компанії ризикують поставити під загрозу свої дані, власну систему, інформацію про своїх клієнтів та їхню репутацію.

Адже, де інформаційні технології впровадженні у всі сфери діяльності людини і мають значне фінансування процвітає кіберзлочинність.

Багато компаній в світі проводять дослідження в сфері захисту як персональних даних, так і даних, які мають значення державного рівня.

Нижче представлені останні дослідження компанії Arxan, які вказують на те, що серед кращих платних і безкоштовних мобільних додатків [1]:

- до 100% з 100 найкращих платних додатків на платформі GoogleAndroid отримали доступ злочинці
- до 56% з 100 найкращих платних додатків для AppleiOS отримали доступ злочинці
- до 73% популярних безкоштовних програм на Android отримали доступ злочинці
- до 53% популярних безкоштовних додатків на AppleiOS отримали доступ злочинці

Ці цифри викликають тривогу, особливо беручи до уваги те, що багато компаній все частіше приймають політику «принеси свій власний пристрій» (bring-your-own-device – BYOD), щоб дозволити співробітникам об'єднати їх особисте і професійне життя в один мобільний пристрій.

За даними Інститута Понемон, 84% споживачів використовують один і той же смартфон для роботи та особистого користування, до якого прив’язані

сервіси (е-пошти, банкінг, соціальні мережі, геолокаційні дані та ін.), що полегшує доступ кіберзлочинцям до будь-якої інформації за допомогою одного девайсу.

Нижче наведено поради для забезпечення захищеності даних [2]:

1. Захист коду

Мобільні шкідливі програми часто використовують дефекти та недоліки в дизайні або коді програмного забезпечення. Якщо вони не захищенні добре, хакери можуть легко отримати копію програмного забезпечення, та переробити їх для використання в злочинних цілях. Після цього, програмне забезпечення може містити шкідливий код та бути розміщеним для завантаження користувачами, які нічого не підозрюють.

2. Шифрування даних

Під час створення програмного продукту, розробник повинен розуміти, що збираючись зберігати інформацію користувача, він також буде зберігати і конфіденційну інформацію, таку як стан здоров'я, місцезнаходження, особисті данні та інше. Тому вся інформація має бути зашифрована, охоплюючи всі дані, такі як адреса електронної пошти, імена або буть яку іншу інформацію, пов'язану з ними. Якщо безпека бази даних буде скомпрометована, то зловмисники можуть мати легкий доступ до конфіденційних даних користувачів.

3. Двоступенева аутентифікація

Розробник може ввести добровільну двоступеневу аутентифікацію для тих користувачів, які вважають що вона їм потрібна.

Також, можна надати додатковий рівень захисту користувачам, надсилаючи їм одноразовий пароль для входу. Це може бути потрібно користувачам, які не хочуть ділитися своїм номером телефону, та потребують додаткового рівня захисту.

4. Сповіщення користувача

Надійною практикою є сповіщення користувача на його е-пошту чи телефон про те, що до його профілю намагалися ввійти з іншого пристрою чи місця. Таке трапляється, коли зловмисник дізнався приватну е-пошту користувача, і намагається підібрати пароль. Прикладами такої функції є сервіси Google та Dropbox.

Список використаних джерел:

1. Mobile App Security. [Електронний ресурс]. URL: https://www.arxan.com/resources/technology/mobile-app-security

2. Платформа Ponemon Institute. [Електронний ресурс]. URL: https://www.ponemon.org/blog/tag/mobile%20security

3. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture, National Institute of Standards and Technology, U.S. Department of Commerce, 2015 –28c.

УДК 681.3.053

Цензура Микола Олександрович
кандидат технічних наук, доцент
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет

МОЖЛИВОСТІ API ФУНКЦІЙ WINDOWS ДЛЯ СТВОРЕННЯ ЗАХИЩЕНИХ ДОДАТКІВ

Розвиток систем дистанційної освіти, тиражування електронних курсів на CD зажадало звернути особливу увагу на проблему захисту даних і додатків від несанкціонованого використання.

Одним із підходів, щодо створення захищених додатків може бути засновано на стандартному набору компонентів, призначених для реалізації технологій шифрування, які входять до складу ядра операційної системи Windows.

Доступ до цих засобів виконується через виклик функцій спеціального інтерфейсу прикладного програмування CryptoAPI. Звернення до криптографічних функцій здійснюється за принципом пакету, в якому звернення до функцій API є рівнем зв'язку із додатками, а за ним розташовується інший рівень, відчинений для оновлення і приєднання нових функцій у вигляді вбудованих компонентів, у тому числі і таких, які розробляються незалежними розробниками. Ця структура, що ілюструється схемою, забезпечує передачу повідомлень між додатком і провайдерами служби шифрування.

Вбудовуванні компоненти такого типу, які реалізують той або інший алгоритм шифрування, створення ключів і підписів в термінології Microsoft називаються провайдерами служби шифрування [1] – Cryptographic Service Provider (CSP). У складі операційної системи Windows реалізуються наступні типи провайдерів:

- загального призначення, який підтримує і шифрування, і формування цифрового підпису;
- підмножина загального призначення, яка використову-ється тільки для хешування і цифрового підпису;
- такий, що реалізовує алгоритм цифрового підпису Digital Signature Algorithm (DSA);
- тип, що реалізовує один з алгоритмів, який створено в Національному інституті стандартів і технології (National Institute of Standards and Technology – NIST);
- для застосування з поштовою службою Microsoft Exchange;
- загального призначення, які підтримують як протокол RSA, так і протокол Schannel.

Щоб отримати інформацію про доступні CSP шляхом послідовної перенумерации потрібно скористатися функцією *CryptEnumProviders,* визначення якої має наступний вигляд [1]:

Public Declare Function CryptEnumProvidere Lib “advapi32.dll” _
Alias “CryptEnumProvidersA” (ByVal dwindex As Long _
ByVal pdwReserved As Long, ByVal dwFlags As Long _
pdwProvType As Long, byVal pszProvName As String. _
pcbProvName As Long) As Long

Перший параметр виклику функції (dwindex) є числовим індексом конкретного CSP, значення якого може змінюватися від 0 до 13.

Другий і третій параметри (pdwReserved і dwFlags) зарезервовані і їм привласнюється значення 0.

Через четвертий параметр (pdwProvType) передається змінна, в якій буде тип провайдера, якому адресується виклик.

П'ятий параметр (pszProvName) є рядковою змінною, в яку буде підставлено ім'я провайдера. Як значення цього параметра можна передати і пустий рядок використовуючи константу (vbNullString). Тоді можна буде визначити довжину імені провайдера і відповідно довжину необхідного для його зберігання буфера. Ця довжина буде повернена в змінною, заданою шостим параметром (pcbProvName).

Засоби CryptoAPI підтримують два методи шифрування:

- метод симетричного шифрування із формування ключа;
- метод обміну повідомленнями з використанням пари ключів відкритий / власний.

Метод симетричного шифрування складається з наступних етапів:

- хешировання рядків та повідомлень;
- знищення хеш об’єктів;
- хешировання ключів поточного сеансу роботи;
- формування ключів на основі хеша;
- шифрування та розшифрування даних.

Microsoft Windows підтримує наступні алгоритми шифрування:

- блочний шифр RC2 (довжина блока до 64 бита) із змінною довжиною ключа. Цей алгоритм шифруючи повідомлення, розбиває його на блоки фіксованої довжини. Як правило, довжина блока визначається вибраним алгоритмом. Якщо довжина повідомлення менше блоку, повідомлення доповнюється до потрібного розміру випадковими даними.
- потоковий алгоритм шифрування RC4 – має широке застосування в різних системах захисту інформації у комп’ютерних мережах. Потоковий алгоритм виконує шифрування повідомлення послідовно байт за байтом та працює швидче ніж блоковий. Потоковий алгоритм більш стійкий до перешкод, що вносяться при передачі повідомлення по каналам зв’язку.

Вибір типу алгоритму залежить від конкретної ситуації. Якщо швидкість обробки повідомлення є пріоритетною, ніж імовірність злому, використовується потоковий алгоритм.

Список використаних джерел:

1. Chapman D. Developing Secure Applications with Visual Basic . / D. Chapman – M. Sams Publishing, 2007. – 608 с.

UDC 004.056

Rzaieva Svitlana
candidate of technical sciences,
associate professor of program engineering and cyber security department
Kyiv National University of Trade and Economics
Geletukha Alexander
student of the 1 course of 5m group of FOAIS,
speciality 121 "Software Engineering"
Kyiv National University of Trade and Economics

USING KALI LINUX IN THE EDUCATIONAL PROCESS

The Kali Linux distribution has gained enormous popularity recently. Hacking and testing safety is becoming part of our culture and more and more people are interested in it.

Kali Linux is one of the Linux distributions developed for hackers and information security professionals. So it is not surprising that Kali is so popular and many newbies and people who do not have any knowledge of information security are trying to use this distribution as the main system. But Kali Linux is not intended for this.

Kali Linux was developed by Security Offensive Security. It is based on Debian and includes the development of a distribution for digital forensics and security testing of BackTrack.

The first version of BackTrack was released in 2006, it combines several projects whose main purpose was to test penetration. The distribution was intended for use as LiveCD.

In 2012, such a distribution as BackTrack has ceased to exist, and instead of it appeared Kali Linux, which took all the advantages of the previous version and all software.

It was the result of the merger of two projects: WHAX and Auditor Security Collection.

Now the distribution is developing steadily and the developers' efforts are aimed at correcting errors and expanding the set of tools.

The Linux distribution is nothing more than a kernel and a set of basic utilities, programs and settings by default. Kali Linux does not provide anything unique in this regard. Most programs can simply be installed in any other distribution, or even in Windows.

The difference between Kali Linux is that it is packed with tools and settings that are required for security testing, not to ensure the normal operation of the normal user.

If you want to use Kali instead of the main distribution - you make a mistake. This is a specialized distribution for solving a certain set of tasks, which means that solving tasks for which it has not been designed will be more difficult, for example, the same program search. Kali Linux's capabilities are focused on security testing.

Kali Linux strives to be as quiet as possible. This is necessary to hide your presence in the attacked network and protect yourself from potential attacks.

To achieve this, Kali disables many services that are included by default in Debian. Of course, you can install the required service from the Debian repositories.

Kali Linux is a specialized distribution, at least because it is designed to work in an aggressive environment. And if you've installed a web server and some more applications have added them to the startup, perhaps you've already cracked Kali and reduced its security.

If you only need a few tools, it's best to choose some more simple distributions, such as Ubuntu or Debian.

You can install all the necessary tools in it. The same option is best suited for new users.

But if you are already well versed in Linux and are ready to spend a lot of time looking into information security, perhaps this system is for you.

References:

1. Our most advanced penetration testing distribution, ever. - Access mode: https://www.kali.org/

2. Official Kali Linux Releases - Access mode: https://www.kali.org/kali-linux-releases/

3. Hacking with Kali: Practical Penetration Testing Techniques - Access mode: https://books.google.com.ua/books?isbn=0124078834

4. Operating System for Penetration Testing in a Nutshell; Kali Linux vs Parrot Security OS - Access mode: https://hackernoon.com/operating-system-for-penetration-testing-in-a-nutshell-kali-linux-vs-parrot-security-os-384809e7b7ae

5. Karchevsky M. Computer information as a subject of crime in the field of computer use, systems, computer networks and telecommunication networks / M. Karchevsky. // The fight against crime in the field of computer information: the problems and ways to solve them. - 2012. - P. 61-64.

УДК 004.056

Савченко Тетяна Віталіївна
кандидат технічних наук,
доцент кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Чевтаєв Микита Валерійович
студент 1 курсу 5м групи ФОАІС,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет

МЕТОДИ КРИПТОГРАФІЧНОГО ЗАХИСТУ

Криптографічний захист інформації - це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Є дві групи методів криптографії – підставлення (заміни) і переставлення. В підставному методі, кожна літера, цифра повідомлення змінюється за певною умовою на інший символ. В переставному алгоритмі змінюються порядок розміщення символів в повідомленні. У загальному випадку у криптографії ключ – це послідовність бітів, що використовуються для шифрування та розшифрування даних.

Залежно від доступності ключів розрізняють:

- симетричне шифрування – для шифрування і розшифрування використовується один ключ. Ця модель зручна для шифрування приватної інформації, але під час передавання повідомлення по каналах зв’язку слід забезпечити таємне передавання ключа, щоб одержувач міг здійснити розшифрування;
- асиметричне шифрування – для шифрування використовується відкритий (публічний) ключ, а для дешифрування інший, закритий (приватний). Це робить непотрібним таємне передавання ключів між кореспондентами. Даремно дешифрувати відкритий ключ, і його знання не дає можливості визначити секретний ключ. Єдиним недоліком такої моделі є необхідність адміністративної роботи – ключі (і відкриті, і закриті) треба десь зберігати та час від часу оновлювати.

Нині існує достатня кількість криптографічних алгоритмів. Найбільш поширеними з них є алгоритми шифрування даних DES та RSA, розроблені у 1970-х роках. Ці алгоритми є державним стандартом США. DES є симетричним алгоритмом, а RSA асиметричним.

Якість захисту під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.

Криптографічні алгоритми використовуються як для шифрування повідомлень, так і для створення цифрових підписів, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, що його підписала.

Цифровий підпис передбачає впровадження в повідомлення сторонньої зашифрованої інформації. При цьому, якщо не застосовується додаткове шифрування, сама інформація, що передається, ніяк не захищається. Сторонньою інформацією може бути контрольне значення, яке автоматичне обчислюється за певним алгоритмом і широко використовується для перевірки цілісності інформації. Вимогою до відповідного алгоритму є неможливість створення відмінних текстів з однаковою сумою.

Найбільш розповсюджений метод створення цифрового підпису є асиметричне шифрування. Накладання підпису реалізується за допомогою закритого ключа, а його перевірка за допомогою відкритого. Публічний ключ та додаткові відомості (ім'я відправника, серійний номер цифрового підпису, назва уповноваженої фірми) передається разом з підписом. Таким чином, послати зашифроване повідомлення і перевірити підпис може будь-хто, а розшифрувати або підписати повідомлення тільки власник відповідного секретного ключа.

Криптографічний захист може бути організований як програмно, так і з використанням апаратних засобів. Сьогодні фактичним стандартом для електронного листування завдяки своїй популярності й безплатному поширенню стала програма Філіпа Циммермана «Pretty Good Privacy» (PGP). У PGP застосовується модель рівної довіри – відправник знає одержувача і довіряє йому ключ шифру. Перевагами системи Циммермана є дуже висока надійність, досить велика швидкодія та потужний механізм обробки ключів. Загалом, для забезпечення належного рівня захищеності інформації потрібна криптографічна система – сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної документації. Вразливість криптографічних систем пов'язана з задачами на яких вони базуються, ці задачі можна сказати умовно нерозв'язувані, для жодної з них не знайдено ефективного розв'язання, але й не можна сказати, що його не існує. Від добору ключа методом перебирання криптосистеми поки що захищені недостатнім рівнем швидкодії комп'ютерів. Різноманітність видів можливих атак на криптографічні системи («на спосіб реалізації», «на паролі», «на користувача», «на моделі довіри» та ін.) підтверджує той факт, що захист є надійним і безпечним доти, доки не розпочинаються спроби його зламування

Отже, розвиток криптосистем і підвищення надійності цифрових підписів створює передумови для заміни паперового документообігу на електронний і переходу до здійснення електронних операцій.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]. – Режим доступу: https://zakon5.rada.gov.ua/laws/show/2163-19?lang=en

2. Засоби захисту інформації [Електронний ресурс]. – Режим доступу: https://allref.com.ua/uk/skachaty/Zasobi_zahistu_informaciyi?page=7

УДК 004.056.5

Костюк Євгенія Миколаївна
заступник директора з навчально-методичної роботи
Торговельно-економічний коледж КНТЕУ
Дудка Наталія Миколаївна
голова циклової комісії економіки та фінансів
Торговельно-економічний коледж КНТЕУ
Мединська Тетяна Миколаївна
голова циклової комісії інформаційних систем і технологій
Торговельно-економічний коледж КНТЕУ

ТЕНДЕНЦІЇ І ПЕРСПЕКТИВИ РОЗВИТКУ КРИПТОГРАФІЇ

Темпи розвитку криптографії за останні два десятиліття були особливо швидкими. Багато фундаментальних аспектів сучасного світу - фінансів, комунікацій, електронної комерції, національної безпеки - будуються на основі криптографії.

Але що буде відбуватися в наступні 10 років і як ваша організація повинна готуватися до змін?

Криптографічні алгоритми є основою протоколів і додатків безпеки, але вони не є постійними - вони повинні розвиватися, щоб протистояти кіберзагрозам.

Алгоритми, які ми колись вважали сильними, тепер відомі як слабкі, наприклад MD5 (Message Digest 5), SHA-1 і DES (Data Encryption Standard). Інші, такі як RSA (Rivest, Shamir та Adleman) та 3DES, вважаються безпечними лише за допомогою відповідних великих ключів та/або частого оновлення ключів.

На даний момент існує цілий ряд криптографічних алгоритмів, яким ми довіряємо, такі як AES (Advanced Encryption Standard), ECDSA (Elliptic Curve Digital Signature Algorithm) і SHA-2 (Secure Hash Algorithm Version 2), ми знаємо принцип їх роботи і застосування, щоб забезпечити належний рівень безпеки. А як же завтра?

Алгоритми гешування: SHA-2 був створений на заміну старих алгоритмів, таких як MD5 і SHA-1, зараз вже є SHA-3 (хоча він ще не використовується широко). Незважаючи на подібність звучання, SHA-3 дуже відрізняється від SHA-2 і був створений як альтернатива, якщо SHA-2 стане вразливим. У будь-якому випадку обидва алгоритми повинні існувати протягом наступного десятиліття.

Асиметричні алгоритми: ECDSA був створений як альтернатива RSA і менш популярному DSA (Digital Signature Algorithm). Використовуючи технологію еліптичної кривої, ECDSA є набагато ефективнішим, ніж RSA, хоча очікується, що ECDSA (і навіть RSA, враховуючи досить довгий ключ) залишатимуться стійкими протягом наступного десятиліття.

Симетричні алгоритми: AES (Advanced Encryption Standard) був створений як заміна 3DES, яку NIST планує припинити для нових додатків у найближчому майбутньому і повністю припинити до кінця 2023 року. Очікується, що AES залишатиметься безпечним протягом наступного десятиліття, навіть з можливою появою квантових обчислень (за умови використання 256-бітових ключів) [1].

Цифрові підписи - це ще одна область, де ми можемо очікувати значного зростання протягом наступного десятиліття. Незважаючи на те, що технології цифрових підписів з нами тривалий час, нещодавнє впровадження законодавства eIDAS в Європейському Союзі означає, що «Кваліфіковані електронні підписи», нарешті, мають таке ж юридичне значення, що і традиційні підписи. Це означає, що мільйони транзакцій, контрактів та інших документів тепер можуть бути підписані та оброблені набагато швидше і ефективніше ніж раніше [2-3].

Квантова технологія також обіцяє багато досягнень у галузі криптографії: по-перше - це генерація квантових випадкових чисел (QRNG). Саме тут використовуються квантові явища для створення джерела шуму з більш високим рівнем ентропії (тобто випадковості); по-друге - це квантові обчислення. Квантовий комп'ютер достатнього розміру зможе порушити багато сучасних алгоритмів - зокрема, він би зробив сьогоднішні асиметричні алгоритми, такі як RSA і ECDSA, абсолютно марними, і зменшив би вдвічі ефективну довжину ключа симетричних алгоритмів. Ця технологія вже була доведена в малих масштабах, і тепер уряди, наукові кола та промисловість поспішають розробити великі комп'ютери.

Вже існують алгоритми, засновані на нових підходах, таких як криптографія на основі решітки, багатоваріантна криптографія, на основі гешу, еліптичних кривих та інші. Однак процес оцінки, порівняння, стандартизації та впровадження нових алгоритмів, які повинні бути достатньо малими і швидкими, як сьогоднішні алгоритми і стійкими до атак як класичними, так і квантовими методами, займе більше 10 років [4].

Загалом, квантова технологія - це область значних і швидких інвестицій, але непередбачуваних досягнень.

Список використаних джерел:

1. Rob Stubbs. Trends in Cryptography. URL: https://www.cryptomathic.com/news-events/blog/cryptography-the-next-10-years-part-2.
2. The Future of Cryptography. URL: http://qeprize.org/createthefuture/the-future-of-cryptography/.
3. Nicholas G. McDonald. Past, present, and future methods of cryptography and data encryption. URL: https://pubweb.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf.
4. Dr. Andrew Shields. Quantum Cryptography: The next-generation of secure data transmission. URL: https://www.information-age.com/quantum-cryptography-123477496/.

УДК 004.056

Котенко Наталія Олексіївна
кандидат педагогічних наук,
старший викладач кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет
Карташ Дмитро Олегович
студент 4 курсу 10 групи ФОАІС,
напрям підготовки 6.050103 «Програмна інженерія»
Київський національний торговельно-економічний університет

ЗАХИСТ ІНФОРМАЦІЇ ПІД ЧАС ОБМІНУ ДАНИМИ У WEB-ПРОСТОРІ

У зв’язку зі стрімким зростанням інформаційних технологій, сьогодні більше ніж 1,5 мільярда людей користуються Інтернетом та електронною поштою. Люди мають доступ до інформації на будь-яку тему. Пошукові системи, такі як Google, дозволяют швидко отримувати потрібну інформацію. Ще однією перевагою використання Інтернету є спілкування з людьми без кордонів. У свою чергу Інтернет відчиняє двері для різноманітних ризиків та загроз.

Конфіденційність інформації – це термін, пов'язаний з особистими даними в інформаційних системах. Вимога конфіденційності інформації застосовується до різних особистих даних, наприклад інформація про web-сайт, фінансові документи або медичні відомості. Конфіденційність інформації в Інтернеті є основною потребую користувачів Інтернету, які використовують соціальні мережі, грають в онлайн-ігри, купують продукти через Інтернет або ведуть іншу онлайн-діяльність. Якщо інформація про користувача буде викрадена, вона може бути використана проти нього.

В загальному концепція конфіденційності відрізняється від концепції конфіденційності інформації в Інтернеті. Конфіденційність стосується інформації або даних про фізичних осіб, і полягає в тому, щоб утримувати інших від розголошення особистої інформації або даних стороннім особам. Конфіденційність стосується фізичних осіб. Вона передбачає індивідуальний контроль над обміном інформацією з іншими. Конфіденційність та приватність також пов’язані між собою. Коли особиста інформація та дані збираються, зберігаються або спільно використовуються, люди повинні узгодити питання про конфіденційність та приватність. У контексті Інтернету, конфіденційність передбачає індивідуальне право вирішувати, яка інформація може бути зібрана і як така інформація може бути використана.

Конфіденційність у контексті Інтернету полягає у впровадженні заходів безпеки для захисту особистої інформації та забезпечення безпеки комп'ютерних систем та обладнання. Коли web-сайти не беруть на себе етичні обов'язки щодо конфіденційності, особиста інформація та дані

розкриваються. Тому конфіденційність інформації в Інтернеті може бути легко порушена.

Існує думка, що технологічні рішення або методи можуть допомогти досягти або підвищити конфіденційність. Інтернет-провайдери можуть використовувати брандмауери, щоб розпізнавати, звідки надходять запити або повідомлення, і дозволяють лише ті IP-адреси, які вважають надійними.

Вразливості web-додатків можна класифікувати наступним чином: XSS атаки; SQL-інєкції; Інклуди; DDoS-атаки [1].

Файли cookie - це технологія, яка може бути використана для збору особистої інформації, наприклад, переваг пошуку, купівлі або налаштувань використання Інтернету. Як правило, для запису файлів cookie використовується JavaScript [2]. Хоча користувачі Інтернету і використовують різні браузери, вони можуть видаляти файли cookie для захисту особистої інформації або даних [3].

Вважається, що для захисту даних під час обміну інформацією можна застосувати популярну техніку шифрування. Цей метод називається шифруванням повідомлень. Якщо два користувачі хочуть обмінюватися інформацією та даними, вони можуть використовувати алгоритми у вигляді прохідної фрази. Інформація, якою обмінюються два користувачі, буде зашифрована, і обидва користувачі повинні використовувати публічні та приватні ключі для розшифровки та шифрування інформації.

Проте, забезпечення конфіденційності інформації в Інтернеті стосується, скоріше, етичного обов'язку конфіденційності, а не лише застосування на практиці високих технологічних рішень. Інтернет-провайдери, інтернет-компанії, web-сайти та багато інших, які займаються особистою інформацією, мають етичний обов'язок зберігати конфіденційність інформації користувачів або клієнтів. Багато підприємств стверджують, що вони можуть збирати особисті дані або інформацію для покращення своїх послуг або цільової реклами. Тим не менш, встановлено, що багато хто з цих підприємств отримують величезний прибуток, продаючи особисту інформацію. Наприклад, електронні адреси користувачів можуть бути продані. Гірший сценарій полягає в тому, що особиста фінансова або медична інформація розкривається і продається. Інтернет-компанії, які мають доступ до персональних даних або інформації, повинні переконатися, що вони не порушують кодекс етики, розкриваючи особисту інформацію. Вони повинні обґрунтовувати цілі використання особистої інформації або даних.

Список використаних джерел:

1. Жирова Т.О., Котенко Н.О., Безпека Web-додатків // Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. – Одеса : ОДУВС, 2018. – Стор. 91-93.

2. Duckett J. JavaScript and JQuery: Interactive Front-End Web Development 1st Edition / J. Duckett. - Wiley, 2017. – 643p.

3. Онлайн-підручник з Javascript – Режим доступу: http://www. w3schools.com/js/. - (дата звернення: 21.03.2018)

УДК 004.056

Чернігівський Іван Андрійович
студент, напрям підготовки 051 «Економіка»
Київський національний торговельно-економічний університет

ПРОБЛЕМИ СТВОРЕННЯ І ВДОСКОНАЛЕННЯ ШИФРІВ ВІД КРИПТОАНАЛІТИЧНИХ АТАК

Проблема захисту інформаційних ресурсів набуває все більш важливого значення, що пояснюється виникненням нових технічних та електронних засобів, які становлять небезпеку витоку інформації. Для вирішення цієї проблеми необхідна система заходів, головною метою якої є захист від несанкціонованого доступу, наслідком якого може бути втрата, модифікація і витік інформації. Серед багатьох програмних і системних засобів, криптографія є одним з основних інструментів, що забезпечують секретність і цілісність інформації, авторизацію, електронні платежі, оперативний контроль за процесами управління й обробки даних, тобто всіх автоматизованих процесів створення, збереження і передачі інформації. Автоматизація призводить до зростання загроз несанкціонованого доступу до інформації і, як наслідок, до необхідності постійної підтримки і розвитку системи захисту [5].

Захист інформації є безперервним процесом, який реалізовується на всіх етапах життєвого циклу автоматизованої системи обробки інформації. Підвищення продуктивності обчислювальної техніки і поява нових видів атак на шифри веде до зниження стійкості відомих криптографічних алгоритмів. Отже, використовувані криптографічні засоби повинні постійно оновлюватися. Підтримка і забезпечення надійного функціонування механізмів системи захисту інформації може здійснюватися лише висококваліфікованими фахівцями, які можуть гарантувати надійність використовуваних алгоритмів і програмних засобів, що реалізують функцію захисту інформації. Криптографія здійснює пошук, дослідження і розробку математичних методів перетворення інформації, основою яких є шифрування, а криптоаналіз досліджує можливості розшифровки інформації, що власне і є криптоаналітичною атакою [1].

Сучасна криптографія вивчає і розвиває такі напрямки: симетричні криптосистеми (із секретним ключем); асиметричні криптосистеми (з відкритим ключем); системи електронного підпису; системи керування ключами; системи хешування. Такі криптографічні системи забезпечують високу стійкість зашифрованих даних за рахунок підтримки режиму таємності криптографічного ключа. Однак, на практиці будь-який шифр, який використовується в тій чи іншій криптосистемі, піддається розкриттю з визначеною трудомісткістю (наприклад, повний перебір ключового простору в 256 біт буде триваліший ніж квадриліони років). У зв’язку з цим виникає необхідність оцінки криптостійкості шифрів, які застосовуються в криптографічних каналах. Зберегти зміст повідомлення в таємниці можна

використовуючи криптографічні протоколи (набір правил, що регламентують використання криптографічних перетворень та алгоритмів в інформаційних процесах) для забезпечення аутентифікації, цілісності, незаперечності переданої інформації [2].

До поширених алгоритмів шифрування належать: TEA\XXTEA\Raiden, 3DES, IDEA, Магма, які поступово виводять з обігу на користь більш стійких: блокові шифри Camelia, Twofish, Serpent, Blowfish, CAST, Mars, MISTY1, Калина; поточні шифри Salsa20, ChaCha20, SOSEMANUK, Trivium та асиметричні шифри RSA, ECDSA, Rabin, Elgamal. Частіше використовуваним є AES (Advanced Encryption Standard) за його швидкість [3].

На блокові шифри можливе здійснення таких атак: на основі лише шифротексту, на основі відкритих текстів і відповідних шифротекстів, на основі підібраного відкритого тексту, на основі адаптивно підібраного відкритого тексту, на основі підібраного шифротексту, на основі підібраного ключа, атака зі зв'язаним ключем, частотний аналіз, диференціальний криптоаналіз, лінійний криптоаналіз, алгебраїчний XLS криптоаналіз, інтегральний криптоаналіз, інтерполяційна атака, усічений диференційний криптоаналіз, сдвигова атака, атака бумерангом, неможливий диференційний криптоаналіз. Хеш-функції вразливі до кореляційних атак, пошуку першого та другого прообразів, знаходження колізії, атак «днів народження». Для асиметричних шифрів небезпечними є: частотний аналіз та MItM-атака. Атаки для всіх типів шифрів: за часом, по стороннім каналам, енергоспоживання, «холодного перезапуску», компроміс «час-пам'ять», атака при збоях ПЗ і ТЗ, атака на ГПСЧ, атака внесенням змін, «бандитський» криптоаналіз, перебір за словником та повний перебір [4].

Кожний з шифрів реалізує власний спосіб криптографічного захисту інформації і має певні переваги і недоліки, проте найважливішою їх характеристикою є стійкість до криптоаналітичних атак. Всі сучасні криптосистеми спроектовані таким чином, щоб не було іншого шляху їх розкриття, ніж повний перебір по всіх можливих значеннях ключа, тобто стійкість таких шифрів визначається розміром використовуваного в них ключа. Отже, використання комбінованих методів шифрування є найбільш надійним способом криптографічного захисту.

Список використаних джерел:

1. Криптографічні засоби захисту інформації [Електронний ресурс] – Режим доступу : https://studfiles.net/preview/5462915/
2. Криптографічні методи захисту інформації [Електронний ресурс] – Режим доступу : https://www.bestreferat.ru/referat-381220.html
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер – М. : Триумф, 2002. – 816 с.
4. Фергюсон Н. Практическая криптография / Нильс Фергюсон, Брюс Шнайер : пер. с англ. – М. : Издательский дом «Вильямс», 2005. – 424 с.
5. Аналіз методів криптографічного захисту інформації [Електронний ресурс] – Режим доступу: http://ir.nmu.org.ua/jspui/bitstream/123456789/149264/1/6-7.pdf

УДК 004.056.55

Чаплінський Роман Ігорович
аспірант
Тернопільський національний технічний університет імені Івана Пулюя

МІС СПОСОБИ ЗАХИСТУ ПЕРСОНАЛЬНОЇ МЕДИЧНОЇ ІНФОРМАЦІЇ ПАЦІЄНТА

Безпека є однією з найбільш важливих критеріїв будь-якої програмної архітектури. Захист бізнес даних та даних клієнтів має критично важливе значення для будь-якого підприємства чи організації.

Різке цифрування даних в медичному секторі покращило надання медичних послуг та надало можливість всім учасникам медичної системи (від пацієнтів до фармацевтичних компаній) обмінюватися даними в електронному вигляді, наприклад електронні медичні картки (electronic medical records – EMR) значно спростили лікарям і пацієнтам доступ до історії хвороби, стану аналізів та багато іншого. Подібні рішення успішно використовуються в Естонії, Тайвані, США [1], EMR відкривають нові перспективи в медицині. Але цей розвиток має небезпечний побічний ефект – ризик інформаційної безпеки. В 2016 році порушення інформаційної безпеки в медичному секторі зачепили більш ніж 27 мільйонів записів пацієнтів. Інформація про здоров'я людей є дуже привабливою для кіберзлочинців. Відповідно до дослідження Ponemon Institute за 2016 рік 89% із опитаних керівників медичних установ визнали, що стикалися, як мінімум з однією втратою даних за останній рік [2]. Державні організації, на кшталт МОЗ і соціальних служб США (HHS) і закони, такі як Акт про мобільність і підзвітність медичного страхування від 1996 року (HIPAA), дають рекомендації, як захистити медичні дані [3], но втрати все рівно трапляються.

Хакери завжди зайняті вдосконаленням своїх методів та підходів. Вони використовують різні способи виявлення і використання навіть незначних недоліків в наших системах і мережах. Крадучи особисті дані пацієнтів, хакери можуть використовувати їх в шахрайстві, продавати іншим злочинцям та використовувати в незаконних фінансових транзакціях.

На сьогоднішній день, нажаль, немає універсального способу або методу який забезпечить захист медичної інформаційної системи та повністю зробить її безпечною. Але комплекс методів, що досліджені у цій темі дозволить забезпечити безпеку інформаційним системам, що використовуються медичними закладами.

Допомогти з вирішенням проблеми безпеки персональних даних в МІС здатний блокчейн. (англ. **Blockchain –** розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає. База захищена від підробки та переробки. Кожен блок містить часову мітку та посилання на попередній блок хеш дерева [4] Така розподілена база даних закладена в основу криптовалюти Bitcoin [5]). Розподілені реєстри можуть формалізувати

процес обміну медичними даними, а також надати пацієнтові більше контролю над своїми показниками здоров'я. Як може здійснюватися реалізація:

- в блокчейні зберігаються невеликі файли з медичними даними, файли великого розміру зберігаються в хмарному сховищі. В блокчейн записується інформація про файли завантажені в хмару, а також права на їх читання та запис;
- для обміну даними використовуються спеціальні токени, (їх кількість залежить від важливості медичної інформації в блокчейні) індивідуальний запис пацієнта розглядається як система із трьох елементів (дріада) – тип, час, якість;

Тип даних може бути динамічним (наприклад , аналіз крові) або статичним (відбитки пальців). Час – це період коли дані були отримані, а якість – це актуальність поданих даних.

Після завантаження даних в хмарне сховище, інформація шифрується методом симетричного шифрування, за допомогою алгоритму Шамира, ключі відправляються в вузли блокчейна, по аутентифікованих каналах зв'язку та при підтвердженні електронним підписом інформація може бути записана в блокчейн. Якщо дані будуть потрібні певному лікарю для проведення досліджень або поставлення діагнозу, він формує запит і відправляє його на валідацію. Запит, який пройшов перевірку у вузлах блокчейна повідомляє, що необхідно відправити лікарю криптографічні ключі для розшифрування даних з хмарного сховища. Аналогічний процес буде для фармацевтичних компаній, державних медичних закладів, а також дослідницьких інститутів.

В майбутньому блокчейн може стати єдиною (децентралізованою) базою даних медичної інформації. В перспективі цю базу даних можна буде заповнювати, не лише зусиллями лікарів, які вносять дані електронних карт, але й за допомогою медичних IoT-пристроїв. Також в блокчейн можна записувати результати групових обстежень із діагностичних центрів та відомості про клінічні випробування препаратів.

Список використаних джерел:

1. Чурпій І.К. Сучасний стан інформатизації в медицині / І.К. Чурпій, Н.В. Чурпій, В.Д. Скрипко; Буковинський медичний вісник, 2011 – с. 171-173.
2. United States Department of Health and Human Services (HHS) [Electronic resource] – Regime of access: https://www.hhs.gov/
3. Blockchain: Blueprint for a New Economy. / M. Swan, 2015. –152 p. – ISBN 978-1-4919-2047-3.
4. Understanding Bitcoin: Cryptography, Engineering and Economics / P.Franco, J.Wiley & Sons, 2014. – 288 p. – ISBN 978-1-119-01916-9.
5. The Blockchain Mastering Bitcoin. / A. Antonopoulos, 2014. – ISBN 978-1-4493-7404-4.

УДК 004.56

Фурса Світлана Євгенівна
кандидат технічних наук, доцент
Донецький національний університет імені Василя Стуса
Соловей Олена Василівна
Донецький національний університет імені Василя Стуса
Савін Кирило Костянтинович
Донецький національний університет імені Василя Стуса

ПРОГРАМНИЙ ПРОДУКТ НАВЧАННЯ АЛГОРИТМАМ ШИФРУВАННЯ

Стрімкий розвиток інформаційних технологій дозволив людству автоматизувати та комп'ютеризувати майже усі сфери людської діяльності. З одного боку, це дозволило відкрити широкі перспективи розвитку усіх галузей, а з іншого – гостро постала проблема забезпечення безпеки усіх суб'єктів інформаційних відносин та захисту їх конфіденційної та персональної інформації від розголосу, фальсифікування та несанкціонованого використання. Тому, проблема забезпечення інформаційної безпеки є як ніколи актуальною.

Одним з провідних підходів до захисту інформації є криптографічний. Криптографічні методи захисту інформації – це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті дії яких її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді різного роду програм [1].

Тому метою даної роботи є розробка програмного продукту, що дозволяє як виконувати навчання алгоритмам програмування різного ступенію складності, так і безпосередньо шифрувати та дешифрувати інформаційні повідомлення.

Алгоритми шифрування, що використовувалися при створенні програмного комплексу: вертикальна перестановка; шифр заміни; DES; RSA; PGP.У порядку від найпростіших до більш складних відповідно [2].

Принцип роботи комплексу розглянемо на прикладі алгоритму DES.

Будь-який з алгоритмів обов'язково влачає в себе файли, що містять реалізацію графічного інтерфейсу, список змінних (у даному випадку таблиці, перестановок ключа та фрагментів тексту розміром 64 біти кожен), виклики методів при натисканні на кнопки, а також основний файл, що виконує покрокове виконання шифрування\дешифрування відповідно до обраного алгоритму. Крім цього для кожного алгоритму додатково включається реалізація та перевірка на правильність введених даних (рис. 1).

```
<script src="./js/constants.js"></script>
<script src="./js/button_actions.js"></script>
<script src="./js/interface.js"></script>
<script>
    var methods = document.createElement('SCRIPT');
    var valid = document.createElement('SCRIPT');
    var cname = localStorage.getItem("cypher_id");
    methods.src = `./js/algorithms/${cname}_methods.js`; //Реалізація
    алгоритму
    valid.src = `./js/validation/${cname}_valid.js` //Перевірка полів
    document.getElementsByTagName("body")[0].appendChild(methods);
    document.getElementsByTagName("body")[0].appendChild(valid);
    //Посилання на сторінку з теорією
    document.getElementById("cypher_theory").setAttribute("href", `./theory/
        ${cname}.html`);
</script>
<script src="./js/main.js"></script>
```

Рис. 1. Ілюстрація файлів коду алгоритму шифрування

У користувача є можливість обрати формат введення у вигляді звичайного тексту або у 16-річному представленні (у такому разі розмір ключа є фіксованим і складає 16 символів). У випадку звичайного тексту при запуску алгоритму виконується перевірка, що відповідності довжини ключа 64 бітам. Текст для шифрування може бути довільної довжини, з додатково доданими нулями для виконання умови кратності 64 бітам (рис. 2) [3].

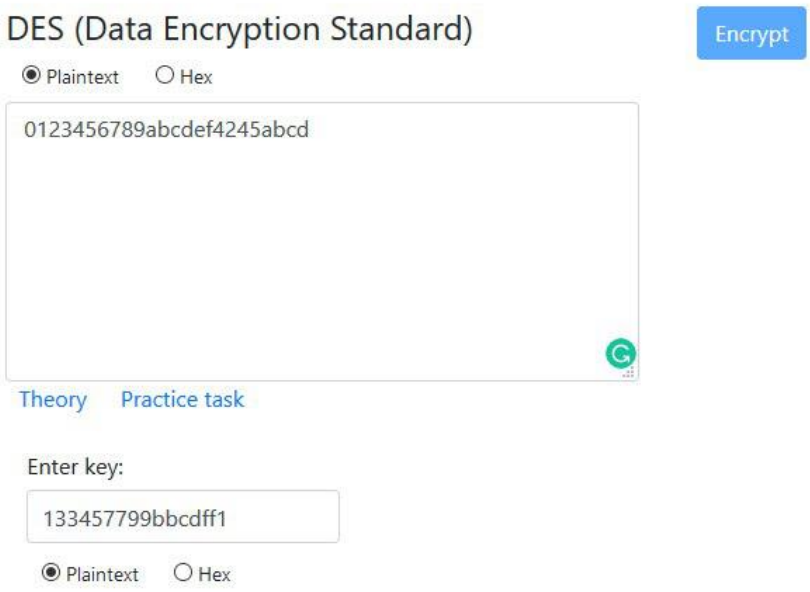

Рис. 2. Введення даних

Детальний покроковий опис шифрування відбувається спочатку для першої ітерації. Для наступних блоків тексту результат роботи записується у кінцеву таблицю виводу. По кожному кроку у користувача є можливість скористатися частиною довідкової інформації або переглянути її у повному обсязі за посиланням розміщеним на початку сторінки (рис. 3) [4].

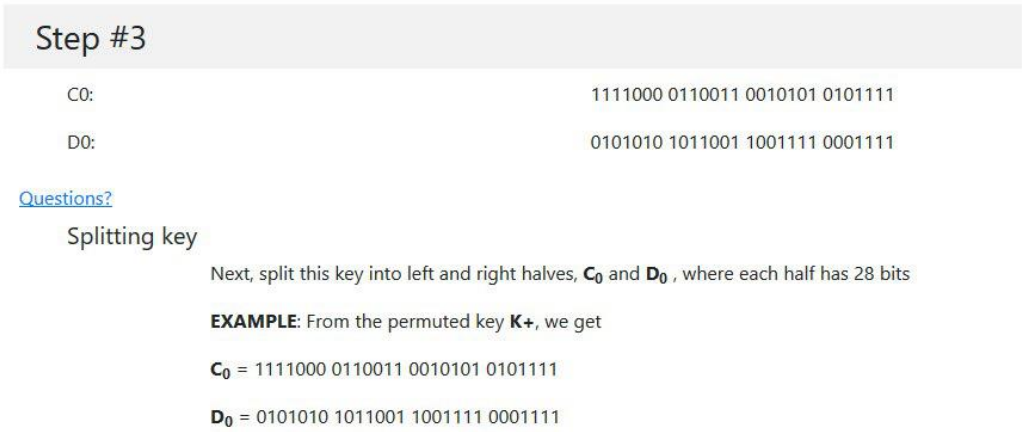

Рис. 3. Крок алгоритму, довідкова інформація

У даному прикладі шифрування виконується за 2 ітерації із вихідним розміром 32 символи у 16-річній системі числення (рис. 4).

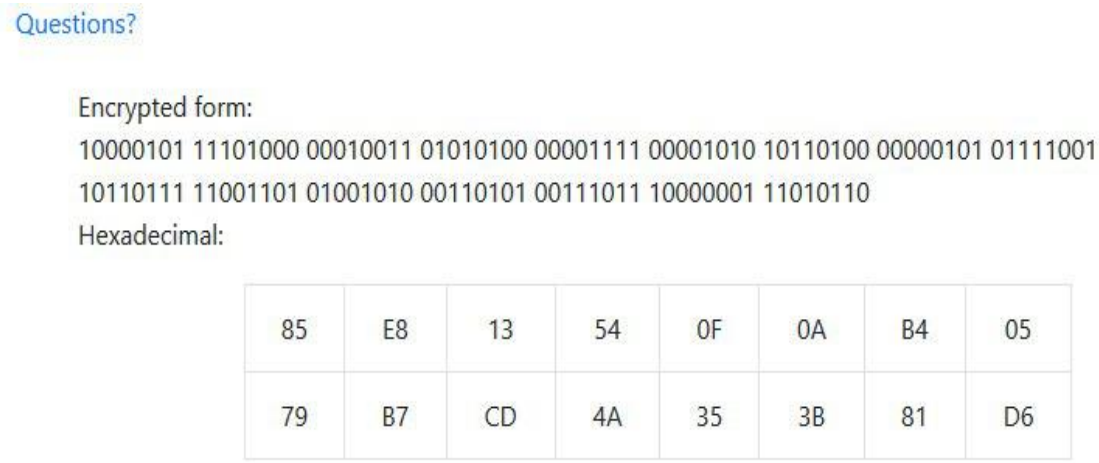

Рис. 4. Результати роботи

Особливостями запропонованого продукту є: детальний покроковий опис результатів виконання алгоритму; теоретичний супровід усіх етапів шифрування у зручному вигляді; можливість перевірити засвоєння матеріалу на практичних завданнях. Також перевагою програмного комплексу є невибагливість до ресурсів.

Список використаних джерел:

1. Ховард М. Защищенный код / М. Ховард, Д. Лебланк; пер. с англ. – Издательство «Русская Редакция», 2005. – 704 с.
2. Каторин Ю.Ф. Защита информации техническими средствами: учебное пособие / Каторин Ю.Ф, Разумовский А.В, Спивак А.И. – СПб: НИУ ИТМО, 2012. – 416 с.
3. Панасенко С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 576 с.
4. Designing and Executing Information Security Strategies [Електронний ресурс]. – Режим доступу: https://www.coursera.org/course/infosec.

УДК 004.056:001

Шестак Ярослав Іванович
старший викладач кафедри програмної інженерії та кібербезпеки,
директор Інформаційно-обчислювального центру Головного центру інформаційних технологій
Київський національний торговельно-економічний університет

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РЕПОЗИТАРІЮ КНТЕУ

Репозитарій наукових праць – є інформаційною базою даних, структурованих, організованих та розміщених на інформаційних ресурсах у WEB просторі.

База даних (БД) – це комплекс програмно-апаратних рішень для збору, розміщення, реєстрації і надання доступу засобами інтернет. Тому, що наукова інформація є надбанням університету і повинна буде захищена.

В рамках інформаційної політики, інформаційної безпеки даних КНТЕУ – повинні бути відпрацьовані заходи по організації безпеки БД репозитарію.

Методи забезпечення інформаційної безпеки полягає у різних підходах до комплексної організації та реалізації захисту інформації.

1. Метод – організаційний захист, він полягає у жорсткій структурі проходження інформації з фіксацією та ознайомленням працівників із забороною розповсюдження, доведення міри відповідальності на різних рівнях допусків. Таким чином інформація проходить найкоротший шлях від отримання з кафедр, підрозділів до відповідальних фахівців для розміщення та надання певного доступу.

2. Використання захищених операційних систем, які є відкритими, безкоштовними та мають більшу ступінь захисту.

3. Виконання завдань відповідно інструкцій – робота полягає у чіткому дотримуванні всіх залучених до роботи технічних працівників, керівників та системних адміністраторів.

4. Обране програмне забезпечення, яке використовується для конфігурування та розміщення БД репозитарію, забезпечення безпечного доступу та захисту.

5. Визначення стандартів розміщення інформаційних ресурсів (наукової роботи, дипломної роботи, тези, статті та ін.) – формат, тип, розміри, роздільна здатність(dpi) та назва документів.

6. Перевірка файла документа на наявність вірусів, шкідливих утиліт чи інших можливих загроз.

7. Стандарти і структура розмежування інформації на WEB ресурсі у локальній мережі та інтернет просторі.

8. Жорстка стандартизація та обмеження доступу до ресурсів БД репозитарію, саме чітко визначені права та правила доступу до ресурсів,

розмежування та обмеження прав доступу по INTRANET та INTERNET мережі.

9. Регламентування роботи технічного персоналу, що розміщує інформацію.

Розглянемо методи більш детально.

Організаційний метод – є найбільш поширеним і дієвим. Якщо правильно інформувати про небезпеку чи можливу атаку, то не витрачаючи великих ресурсів можна досягти значних успіхів, але цей метод ризикований.

Використання захищених операційних систем – це використання операційних систем типу MAC OS, Linux, Android, FreeBSD, Solyaris, та інші. Всі ці системи об'єднує відмінність від Windows систем – мала доля вірусів і складність порушити протоколи, але на відміну від Windows – вони є більш складними, менше розповсюдженими і суттєво складніші у використанні. Користувачі таких систем є більше продвинутими і працюють думаючи. Є також складність у супроводі, налаштування адміністраторами та є певна не сумісність з Windowsпрограмами, але у WEB просторі, тобто у хмарах – вони працюють однаково. Виконання завдань відповідно інструкцій _ це організована робота всіх технічних працівників за інструкціями, за регламентом у певних рамках, досягається найвищий ефект якості виконання.

Обране програмне забезпечення – це засоби керування інтерфейсом системи та його контентом. В залежності від апробації та вибору Операційної системи, версії сумісної програми – залежить якість роботи сервера, де розміщується вся інформація, організовується резервування, доступ до інформації програмними засобами, та ведеться протокольне адміністрування, обмежується доступ до регламентного внесення інформації. Обмеження прав по знищенню інформації, таке право мають працівники тільки найвищого рівню доступа.

Визначення стандартів розміщення інформаційних ресурсів – це особливо важливий етап у вирішенні питань рівню захисту наукової інформації. При передачі файлів між відповідальними працівниками повинні використовуватися захищені канали передачі інформації чи передаватися закриті електронним ключем електронною поштою, або іншим меседжером. Також можна використовувати групову роботу у хмарі Майкрософт, викладати матеріали та ділитися ними для спільної роботи з відповідальними підрозділів. Також можна використовувати Обмін файлами портала КНТЕУ у персональних кабінетах.

Перевірка файла документа на наявність вірусів – всі файли перед обробкою та розміщенням у системі репозитарію повинні проходити детальну перевірку на наявність шкідливих кодів, програмного забезпечення чи просто утиліт для убезпечення від можливих атак.

Стандарти і структура розмежування інформації на WEB ресурсі – для уніфікації документів, їх автентифікації та позиціювання необхідно прийняти рішення по структурі документа, яка інформація може там міститись, який фон необхідно встановити і які повинні бути параметри документа. Саме тому всі документи приймаються у форматі Word(*.DOC) фоном логотипом

КНТЕУ, та параметрами, що відповідають вимогам до статей, тез чи дипломних робі та ін.

Жорстка стандартизація та обмеження доступу до ресурсів БД репозитарію, а саме права, що надають відповідно регламенту виконувати певні функції, а саме розміщення інформації, резервування, надання певного статусу документа, забезпечення розмежування та обмеження прав доступу по INTRANET та INTERNET мережі. Визначення документів з різним статусом і доступом до них, ви визначення прав користувачів системи, як технічного персоналу так і користувачів-читачів.

Регламентування роботи технічного персоналу – треба чітко визначити всьому технічному персоналу межі доступу, передбачення збереження інформації при зміні адміністраторів, чи операторів, регламент передачі прав на доступ до певних структур даних. Також необхідно проінструктувати всіх адміністраторів системи про сурову відповідальність за коректне використання ввірених йому даних, про їх заборону розповсюдження та заборону надання доступу до ресурсів систем чи користувачів, які не мають регламенту доступу.

Коли всі дії виконані – починаємо будувати логічну структуру потоків даних, яка повинна містити всі ланки, для усунення можливих слабких чи вразливих місць.

Наступним етапом буде побудова захисту БД репозитарію у INTRANET та INTERNET мережі. Прийняття рішення побудови захисту за певними фізичними, програмними та віртуальними принципами здійснюється відповідно до визначених критеріїв та ступеню захисту, та в подальшому кількості можливих фізично наданих доступів на реалізацію. Саме побудова ланок захисту за допомогою сервера, на якому реалізовано БД репозитарію. Окремо за допомогою мережевого програмного забезпечення будуємо окремий або загальний простір захищеного доступу до сервера БД репозитарію. Найкраще використовувати повний захист із INTRANET та INTERNET мережі, тобто будуємо зовнішній FireWall та внутрішній, перший для захисту від зовнішніх загроз, а внутрішній – з середини власної мережі. Це дуже актуально коли у мережі багато користувачів, та в них суттєво різні рівні доступу та різні форми роботи, тому можлива загроза зсередини.

Список використаних джерел:

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. / [Електронний ресурс]. - Режим доступу: http://www.nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf (дата звернення 10.03.2019).
2. Гриджук Г.С. Систематизація методів інформаційної безпеки підпримства. / [Електронний ресурс]. - Режим доступу: http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/64.pdf.
3. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи. / [Електронний ресурс]. - Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.

Наукове видання

БЕЗПЕКА СОЦІАЛЬНО-ЕКОНОМІЧНИХ ПРОЦЕСІВ В КІБЕРПРОСТОРІ

МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

(Київ, 27 березня 2019 року)

Формат 60х84/8. Ум. друк. арк. 14,18. Тираж 135. Зам. 175.

Видавець і виготовлювач
Київський національний торговельно-економічний університет
вул. Кіото, 19, Київ-156, Україна, 02156

Свідоцтво суб'єкта видавничої справи серія ДК № 4620 від 03.10.2013 р.