КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
КИЇВСЬКА ТОРГОВО-ПРОМИСЛОВА ПАЛАТА
ТОВ «НОВЕЛЛ КОНСАЛТИНГ»
ТОВ «ВЕБ ПРО»
ГО «КІБЕРКОВЧЕГ»

КІБЕРГІГІЄНА. КІБЕРБЕЗПЕКА. БЕЗПЕКА ДЕРЖАВИ

МАТЕРІАЛИ НАУКОВИХ СЕМІНАРІВ

(Київ, 27 листопада 2020 року)

Київ 2020

УДК 004.056
К 38

Кібергігієна. Кібербезпека. Безпека держави : матеріали
К 38 наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – 101 с.

Збірник матеріалів учасників наукових семінарів «Кібергігієна. Кібербезпека. Безпека держави» присвячений актуальним питанням у сфері економічного, соціального, нормативно-правового, адміністративного безпечного функціонування кіберпростору, технічного забезпечення кібербезпеки, боротьби з кіберзлочинністю, захисту інформації в комп'ютерних системах і мережах.

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

УДК 004.056

Відповідальний редактор А. М. Десятко, ст. викладач кафедри інженерії програмного забезпечення та кібербезпеки.

ЗМІСТ

ЧУБАЄВСЬКИЙ В.І., ФРАНЧУК Т.М.
ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЕЛЕКТРОННО-ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ 7

ШВЕЦЬ Д.В.
ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ 9

КРИВОРУЧКО О.В., КОСТЮК І.В.
СТРАТЕГІЯ БЕЗПЕКИ ІНФОРМАЦІЇ 12

PASHORIN V., MAKOIEDOVA V.
CYBERSECURITY TECHNOLOGIES IN DECISION SUPPORT SYSTEMS 14

САМОЙЛЕНКО Ю.О., КОСТЮК Ю.В.
ТЕОРІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 16

САВЧЕНКО Т.В., САШНЬОВА М.В., СТЕПАШКІНА К.В.
ТАКСОНОМІЯ АТАК ТА МЕХАНІЗМІВ БЕЗПЕКИ В МЕРЕЖІ 18

КОТЕНКО Н.О., АЛЕКСАНДРОВ А.Ю.
МЕХАНІЗМ ЗАХИСТУ PYTHON ФРЕЙМВОРКУ DJANGO ВІД МІЖСАЙТОВОЇ ПІДРОБКИ ЗАПИТУ (CSRF) 21

КРИВОРУЧКО О.В., ДЕСЯТКО А.М.
МІЖНАРОДНІ СТАНДАРТИ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА 23

ЦЮЦЮРА М.І.
ФОРМУВАННЯ КЛЮЧОВИХ ІНДИКАТОРІВ УСПІХУ З ПОЗИЦІЙ ЇХ ЗАСТОСУВАННЯ ПРИ ПІДГОТОВЦІ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ 24

HNATCHENKO T., IL'YIN V.
CYBERSECURITY OF UKRAINE IN CONDITIONS OF THE COVID-19 PANDEMIC 26

СЕМІДОЦЬКА В.А., АНДРУСЕНКО В.П.
QUANTUM COMPUTING AND CYBERSECURITY 28

ТЕРЕЙКОВСЬКИЙ І.А.
МЕТОД КОДУВАННЯ ОЧІКУВАНОГО ВИХІДНОГО СИГНАЛУ НЕЙРОННОЇ МЕРЕЖІ 30

БУРМАКА І.А.
BLOCKCHAIN ТЕХНОЛОГІЯ ЯК ОСНОВА ДЛЯ РОЗПОДІЛЕНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ 32

БЕБЕШКО Б.Т., ЛАЗОРЕНКО В.В., ХОРОЛЬСЬКА К.В.
БЕЗПЕКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ ЦИФРОВИМИ АКТИВАМИ ЗА ДОПОМОГОЮ МЕТОДУ K-MEANS ПРИ ДОСЛІДЖЕННІ ВИДОБУТКУ ДАНИХ 34

ВІКТОРОВ В.В., ЗАХАРОВ Р.Г.
КІБЕРГІГІЄНА – БЕЗПЕЧНИЙ ОСОБИСТИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР 37

ГАРИСТ А.В.
ПРОГРАМНО ОБУМОВЛЕНІ РАДІОСИСТЕМИ ТА АТАКИ НА НАВІГАЦІЙНІ СИСТЕМИ 38

ГНАТЧЕНКО Д.А., МАКАРЕНКО К.Р.
МЕХАНІЗМ ЗАХИСТУ АВТЕНТИФІКАЦІЇ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ 39

ЖЕРЕБЕЦЬ О.М.
ПРОГРАМНО ОБУМОВЛЕНІ РАДІОСИСТЕМИ ТА АТАКИ НА WIFI МЕРЕЖІ 43

ЦЕНЗУРА М.О.
ЗАХИСТ ЕЛЕКТРОННИХ НАВЧАЛЬНО-МЕТОДИЧНИХ ВИДАНЬ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ 44

ЦЮЦЮРА С.В., КИЇВСЬКА К.І., ТЕРЕНТЬЄВ О.О.
ДОСЛІДЖЕННЯ СФЕРИ КІБЕРБЕЗПЕКИ В УКРАЇНІ 46

ГНАТЧЕНКО Д.Д., ГНАТЧЕНКО Т.О., КАЛЬБЕНКО А.С.
ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ЗАХИСТУ КІБЕРПРОСТОРУ ЯК КОМПОНЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 48

РЗАЄВА С.Л., ДРАПЕЙ Л.Л.
МЕТОДИ ЗАХИСТУ CRM-СИСТЕМИ ПІДПРИЄМСТВА 51

ГНАТЧЕНКО Д.Д., ЗБОРЩИК І.О.
ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО В КІБЕРПРОСТОРІ 54

ДОРОШ М.С., ВОЙЦЕХОВСЬКА М.М.
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПРОЄКТІВ 56

РАССАМАКІН В.Я.
WHO'S WHO У СВІТІ ХАКЕРІВ ВІД THALES ТА VERINT 58

ХАРЧЕНКО О.А., ЯРЕМИЧ В.Р.
КІБЕРРИЗИКИ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ЕЛЕКТРОННОЇ ТОРГІВЛІ 60

HONCHARENKO T.A., LYASHCHENKO T.O.
CONCEPT OF DATA PROTECTION AND VERIFICATION OF BIM-MODELS
FOR LIFECYCLE BUILDING TERRITORY 62

TSIUTSIURA S.V., YERUKAIEV A.V., KOSTYSHYNA N.V.
THE SYSTEM OF FUZZY DERIVATION OF CLASSIFICATIONS OF FACTORS
OF COMFORT OF LIVING IN APARTMENT BUILDINGS 63

ПАШОРІН В.І., КУКЛІНСЬКИЙ Д.В., ШАБАЛІН Д.С.
ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ 65

ПАЛАГУТА К.О., ГАНАХ О.І.
БЕЗПЕКА СИСТЕМ SMART HOME 67

ШЕСТАК Я.І.
КІБЕРБЕЗПЕКА, ОРГАНІЗАЦІЙНІ ЗАХОДИ БЕЗПЕКИ 70

ТИЩЕНКО Д.О., БАРОЯН В.А.
СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ PGP ПРИ ВИКОРИСТАННІ
ЕЛЕКТРОННОЇ ПОШТИ 72

КОСТЮК М.А.
КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ПІД РЕГУЛЮВАННЯМ GDPR 74

САЛЕОМОН А.А., САШНЬОВА М.В.
АНАЛІЗ СИСТЕМИ ЗАХИСТУ НА ПІДПРИЄМСТВІ «САМСУНГ
ЕЛЕКТРОНІКС УКРАЇНА» 76

ТИЩЕНКО Д.О., ФРАНЧУК Т.М., КОПА В.О.
ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ
ЕЛЕКТРОННОЇ ПОШТИ 79

ПАШОРІН В.І., ШАПОЧНІКОВА А.О., БОЙКО Т.В., ОЛЕКСЮК В.А.
ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ
ЗА ДОПОМОГОЮ SWOT-АНАЛІЗУ 81

ЧУДІК М.І., ЖИРОВА Т.О.
ПЕРЕОСМИСЛЕННЯ КІБЕРБЕЗПЕКИ У ПОСТПАНДЕМІЧНОМУ СВІТІ 83

КАРПЕНКО В.О.
ФІШИНГ. БЕЗПЕКА В ІНТЕРНЕТІ 85

БАЙ А.С.
НАЙБІЛЬШ КРИТИЧНІ ВРАЗЛИВОСТІ ВЕБДОДАТКІВ 87

ВАСИЛЬЄВА В.Ю.
ЯК УБЕЗПЕЧИТИ СЕБЕ ВІД ХАКЕРСЬКИХ АТАК ТА ЗАХИСТИТИ ДАНІ 88

ЛИТВИНЕНКО В.В.
ФІШИНГ ТА ЙОГО ВПЛИВ НА ІНТЕРНЕТ-КОРИСТУВАЧІВ 90

КОЛЕСНИК Д.С.
POPULAR TYPES OF CYBERATTACKS AND METHODS TO PREVENT THEM..... 92

ПАШОРІН В.І., ЛІЩУК О.В., ВОЛЧАТОВ І.С., ФІЛАТОВ О.І.
ЗАХИСТ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ НА РІВНІ ОПЕРАЦІЙНОЇ СИСТЕМИ..... 94

МУКВІЧ А.Л., ЖИРОВА Т.О.
КІБЕРБЕЗПЕКА У СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СВІТІ – КЛЮЧОВІ ТЕНДЕНЦІЇ ТА ЗАГРОЗИ..... 96

КУПІНА В.Я.
КІБЕРБЕЗПЕКА ТА СЗД. ПІДХІД NETAPP: ПРІОРИТЕТ НА ІНФОРМАЦІЮ 98

PASHORIN V., SALEOMON A.
AN INTEGRATED APPROACH TO PROVIDE A SECURITY OF PERSONAL DATA IN THE ORGANIZATION 99

ГАЛИЧ І.В.
КІБЕРБЕЗПЕКА В РАМКАХ ЗАКОНУ ПРО НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ..... 100

УДК 004.49

ЧУБАЄВСЬКИЙ В. І.,
кандидат політичних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки, заступник начальника Департаменту інформаційно-аналітичної підтримки Національної поліції України – начальник управління розвитку інформаційних технологій, полковник поліції
Київський національний торговельно-економічний університет.
ФРАНЧУК Т. М.,
здобувач вищої освіти ОС «магістр» /PhD, заочна форма навчання,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: t.franchuk.fit.121.2m.20.m.z@knute.edu.ua

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЕЛЕКТРОННО-ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Технологічний прогрес створює все ширше коло потреб та можливостей для збору та обробки персональних даних, а самі персональні дані знаходять все ширше використання в найрізноманітніших сферах від бізнесу до політики. Їх використання стає багатоаспектнішим і, окрім допомоги в роботі та побуті, вони можуть слугувати для декого інструментом порушення прав та свобод людини, зокрема права на приватність. У зв'язку з цим, розвиток системи захисту персональних даних є одним із найбільш актуальних завдань, які стоять перед українським суспільством на сучасному етапі. Захист персональних даних та його вдосконалення є не просто обов'язком держави, але і є предметом державного регулювання. Крім того, створення дієвої системи захисту персональних даних належить до міжнародних зобов'язань України, в тому числі пов'язаних із європейською інтеграцією нашої держави. Зокрема, саме від виконання цього зобов'язання значною мірою залежать євроінтеграційні прагнення української держави.

Проблема, як виток персональних даних громадян України із автоматизованих систем державних органів та приватних компаній стає пріоритетом діяльності злочинів. Ситуація стає все більш складнішою, оскільки з'являються нові форми приховування злочинцями не лише своїх комунікацій (в т.ч. із використанням можливостей Darknet та Deepweb), але й інструментів виведення коштів (кріптовалюти).

На сьогоднішній день органи державної влади стикаються із низкою загроз та викликами в сфері кібербезпеки. В Україні існує понад 100 державних та єдиних реєстрів, які містять конфіденційну інформацію. Більшість з них використовує авторизацію за допомогою логіну та паролю, що в свою чергу має певні вразливості. Зокрема, у такий спосіб не можливо достовірно ідентифікувати особу, яка отримує інформацію з реєстру [2].

В сучасних умовах гостро стоїть проблема із захистом інформації, яка зберігається у розпорядників (держателів) реєстрів. Здебільшого мережева інфраструктура має застаріле та вразливе програмне забезпечення. Переважно користувачі, а деколи і адміністратори поряд з доступом до реєстрів мають доступ в мережу інтернет, що в рази збільшує ризики зовнішнього ураження та подальшої кібератаки на системи зберігання інформації.

За період незалежності України, переважна більшість інформації накопичена на паперових носіях. З метою її цифрової трансформації залучаються приватні компанії. Вони тимчасово отримують доступ до інформації, що містить персональні данні. Тобто в рази зростають ризики витоку конфіденційних даних. На противагу, накопичення, обробка та зберігання більшої кількості інформації потребує збільшення цифрової інфраструктури (сервери, мережі, дата центри), а їх збільшення та розростання потребує підвищеної уваги до забезпечення безпеки цих об'єктів [1].

Збирання, опрацювання та накопичення даних в реєстрах вимагає реалізації принципу прозорості. Будь-яка інформація та опрацювання персональних даних повинні бути доступними і зрозумілими. Спеціальні цілі опрацювання конфіденційної інформації на момент їх збирання мають бути прямо вираженими, означеними та законними. В той же час, персональні дані повинні бути достатніми, відповідними та обмежуватися досягненням мети, для яких їх збирають. Крім цього, період, протягом якого зберігаються персональні дані, має бути скорочений до абсолютного мінімуму, з метою реалізації принципу «дані не зберігаються довше, ніж це необхідно». Чітко визначений період зберігання та знищення, убезпечить від несанкціонованого витоку інформації [1].

Національною поліцією встановлено, що на спеціальних форумах та у закритих спільнотах циркулюють різні бази даних. Деякі дійсно актуальні та постійно оновлюються, інші мають застарілий характер, однак містять персональну інформацію. Наявність такої циркулюючої інформації, створює підґрунтя для вчинення протиправних дій у кіберпросторі метою, яких є отримання прибутку від продажу персональних даних. Злочинці створюють спеціальні сервіси для перевірки інформації чи безпосереднього продажу баз даних.

Більш широка сфера – шахраї. Вони під приводом продажу інформації, баз даних здійснюють заволодіння коштами. Великий суспільний розголос, а також інше привертання уваги до будь-яких витоків інформації активізує злодіїв. Латентність таких злочинів значна, а їх розслідування переважно не розпочинається з заяви потерпілої сторони, більшість таких фактів розкривається ґрунтуючись на оперативній інформації [2].

Наразі, Національною поліцією на постійній основі забезпечено відслідковування активності учасників російськомовного сегменту хакерської спільноти. Зокрема, на закритих онлайн майданчиках «darknet», «tor», на закритих каналах «skype», «telegram». Відслідковуються публікації приватних дослідників з інформаційної безпеки щодо витоку персональних даних громадян України із автоматизованих систем державних органів та приватних компаній. За наявною інформацією, такі витоки відбуваються щонайменше раз на 2 місяці.

Найпопулярнішими серед таких майданчиків є закриті веб-форуми «exploit.in», «phreaker.pro», «peers.fm» та «xss.io» доступ до участі в яких здійснюється на підставі численних перевірок кандидатів. Наявності в них хакерських навичок та поручителів, а також за вступними внесками, що в деяких випадках перевищують 150 доларів США.

У Національній поліції зазначений напрямок роботи забезпечується системними заходами особистого пошуку, які здійснюються найдосвідченішими працівниками, агентурною роботою з учасниками хакерської спільноти, роботою із власними оперативними обліками, які напрацьовані у ході збору вмісту закритих онлайн майданчиків «darknet», «tor», та у тому числі завдяки активній участі поліції у співпраці із правоохоронцями інших держав. Крім цього, Національною поліцією уживається комплекс заходів, спрямованих на викриття кримінальних правопорушень у сфері використання високих інформаційних технологій.

Таким чином, підсумовуючи вищезазначене, можна дійти висновку, що сьогодні загострюється проблема неправомірних дій різних суб’єктів, які використовують засоби електронно-інформаційного середовища. Активність у формуванні баз даних, обробка та поширення відомостей про осіб без їх відома призвели до виникнення глобальної за своїми масштабами у часі та просторі проблеми інформаційної безпеки людини, суспільства і держави щодо захисту персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. Київ: К.І.С, 2015. 220 с.

2. Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / упор. А. В. Пазюк; рец. О. О. Гріненко, О. В. Олійник. Київ: ФОП Клименко, 2014. 221 с.

УДК 004.056

ШВЕЦЬ Д. В.,
керівник відділу аудиту ІТ та ІБ ТОВ «Новелл Консалтинг»
e-mail: dsh@ncu.com.ua

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ

Поринаючи у процес діджиталізації українських інституцій та переведення важливих систем забезпечення життєдіяльності держави у площини віддаленого управління ми стикаємося з новими викликами безпеки інформаційних технологій та низку питань щодо їх захисту на всіх етапах життєвого циклу.

Слід зазначити, що на сьогодні інформаційні технології є невід'ємною частиною майже всіх сфер сучасного суспільства.

За всіма оцінками експертів, до теперішнього часу склалася ситуація, коли можливості і стійкість інформаційних систем, в значній мірі визначаються показниками якості, надійності і безпеки програмних засобів (в більшій мірі в порівнянні з апаратними засобами).

Програмне забезпечення стає одним з найбільш вразливих компонент сучасних інформаційних технологій, а використання програмних засобів у складі систем забезпечення діяльності об'єктів критичної інфраструктури, а також інших критичних систем породжує нову проблему – не можливості достатнього забезпечення інформаційної безпеки програмних засобів.

З огляду на це, справедливо визначити основні загрози сучасного світу щодо забезпечення інформаційної та кібербезпеки на об'єктах критичної інфраструктури:

1. Відсутність достатньої кількості фахівців з інформаційної безпеки та кібербезпеки на ОКІ;
2. Наявність вразливостей в програмному забезпеченні, що використовується на ОКІ;
3. Збільшення висококваліфікованих кібератак на ОКІ;
4. Застарілі підходи щодо забезпечення захисту інформації/інформаційної безпеки в державних установах та ОКІ;
5. Відсутність єдиних протоколів протидії кібератакам на ОКІ.

В історії нашої держави визначено ряд гучних кібератак [10, 11] наведених у табл. 1.

Таблиця 1

Перелік реалізованих кібератак на ОКІ у період з 2015–2017 років

№	Найменування атаки	Вражені ОКІ	Дата реалізації
1	Кібератака «BlackEnergy 3»	«Прикарпаттяобленерго»	23 грудня 2015 року
		«Київобленерго»	23 грудня 2015 року
		«Чернівціобленерго»	23 грудня 2015 року
3	Кібератака з використання вірусу Petya	Аеропорт «Бориспіль», «Харків», «Київ»	27 червня 2017 року
		Укренерго, Київенерго, ДТЕК	27 червня 2017 року
		Чорнобильська АЕС	27 червня 2017 року
		Київський метрополітен	27 червня 2017 року
		ЗМІ	27 червня 2017 року
		Укрзалізниця	27 червня 2017 року
		Київводоконал	27 червня 2017 року
		ДП «Антонов»	27 червня 2017 року
		Оператори мобільного зв'язку	27 червня 2017 року

Пропонуємо розглянути поетапну реалізацію Кібератаки «BlackEnergy 3» на системи електропостачання «Прикарпаттяобленерго».

Рис. 1. Етапи реалізації кібератаки «BlackEnergy 3» в «Прикарпаттяобленерго» '2015

На рисунку 1 відображено етапність реалізації кібератаки [9], а саме:

1) Було проведено фішшінг-атаку шляхом направлення електронного листа зі шкідливими кодом оператору «Прикарпаттяобленерго» для отримання доступу до мережі Обленерго. Шкідливий код був внесений у вигляді макросу до файлу Microsoft Office;
2) Ідентифікація та встановлення у фоновому режимі шкідливого програмного забезпечення «BlackEnergy 3» на робочій станції оператора;
3) Викрадення критичних даних для адміністрування з мережі «Прикарпаттяобленерго»;
4) Використання віртуальних приватних мереж (VPN) для входу до ICS мереж «Прикарпаттяобленерго»;
5) Використання існуючих інструментів для віддаленого доступу та управління в мережі «Прикарпаттяобленерго»;
6) Використання модифікованого KillDisk для видалення основних записів завантаження уражених елементів системи, а також цільове видалення деяких журналів подій;
7) Управління системи енергопостачання для впливу на підключене навантаження із запланованим відключенням обслуговування;
8) Телефона атака на відмову в обслуговуванні call-центру.

Результатами цієї атаки було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин.

Протидія або профілактика запобіганню таким або подібним кібератакам, які були наведені в таблиці 1 – є проведення на ОКІ аудитів інформаційної безпеки з тестуванням на проникнення.

Тестування на проникнення [1, 2] (Pentest) – це процедура (спроба) оцінки реальної захищеності інформаційної системи з використанням контрольованих і максимально безпечних для інфраструктури та бізнес-процесів атак, а також виявлення та спроби експлуатації вразливостей.

Проведення пентесту дозволяє надати детальну інформацію про існуючі прогалини в безпеці інформаційних систем та запланувати найбільш важливі напрямки щодо поліпшення стану їх захищеності.

Головна мета пентесту – знайти в інфраструктурі і додатках клієнта уразливості, які потенційно можуть бути використані зловмисниками. Крім того, тестування на проникнення допомагає зрозуміти, наскільки ефективні розроблені політики в області IT-безпеки і чи варто їх удосконалювати. Іноді пентести проводяться, щоб перевірити готовність фахівців інформаційної безпеки до відбиття кібератак на інформаційні системи організації.

Опираючись на міжнародні практики можемо розглянути етапи [3, 4] проведення тестування на проникнення:

1. Розвідка, збір інформації щодо об'єкта тестування;
2. Вибір методів та інструментів для здійснення атаки;
3. Доставка до систем об'єкта тестування вибраного інструмента атаки;
4. Експлуатація вразливостей виявлених в системі об'єкта тестування;
5. Встановлення шкідливого програмного забезпечення;
6. Отримання доступу та контролю над системою об'єкта тестування;
7. Здійснення узгоджених дій для підтвердження успішного тестування на проникнення.

Використовуючи зазначену методику тестування на проникнення фахівці максимально наближено відображають ситуації кібератаки на системи ОКІ. При цьому, працівники відповідальні за захист інформації можуть навіть і знати про тестування та відпрацьовувати заходи щодо запобігання кібератакам.

Виходячи з цього, з метою підвищення рівня кібербезпеки на державному рівні слід встановити основні питання щодо прийняття рішення щодо:

- необхідності проведення аудитів інформаційної безпеки на ОКІ з обов'язковим проведенням тестування на проникнення;
- необхідності розробки та затвердження відповідних методик з проведення тестування на проникнення;
- розширення державно-приватного партнерства в рамках впровадження системи незалежного аудиту інформаційної безпеки та проведення тестувань на проникнення;
- можливості проведення загальнодержавних навчань з запобігання кіберзагрозам на ОКІ та державних органів в рамках державно-приватного партнерства;
- використання в системах ОКІ програмних та технічних засобів, що пройшли державну експертизу у сфері захисту інформації;
- Проведення навчань співробітників ОКІ з питань інформаційної та кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пентест: что скрывается под белым капюшоном? [Електронний ресурс]. Режим доступу: https://10guards.com/ru/articles/pentest-under-the-white-hood

2. Тестирование на проникновение. Методы тестирования [Електронний ресурс]. Режим доступу: http://amt-group.by/web/ru/pentest

3. The Open Source Security Testing Methodology Manual [Електронний ресурс]. Режим доступу: https://www.isecom.org/OSSTMM.3.pdf

4. Penetration testing execution standard [Електронний ресурс]. Режим доступу: http://www.pentest-standard.org

5. Technical Guide to Information Security Testing and Assessment [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

6. OWASP Testing Guide v4 [Електронний ресурс]. Режим доступу: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP Testing Guide v4.pdf

7. Тест на проникновение – краткое руководство [Електронний ресурс]. Режим доступу: https://cutt.ly/ihmtbYJ

8. Кібератака на енергетичні компанії України [Електронний ресурс]. Режим доступу: https://cutt.ly/GhmtxVf

9. TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid [Електронний ресурс]. Режим доступу: https://ics.sans.org/media/E-ISAC SANS Ukraine DUC 5.pdf

10. Список сайтов, пострадавших от вируса Petya.A (обновляется) [Електронний ресурс]. Режим доступу: https://ukranews.com/news/505204-spysok-saytov-postradavshykh-ot-vyrusa-petyaa

11. Хакерские атаки на Украину (2017) [Електронний ресурс]. Режим доступу: https://cutt.ly/ohmtvta

УДК 621.391.

КРИВОРУЧКО О. В.,
доктор технічних наук, професор,
завідувач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
e-mail: kryvoruchko_ev@knute.edu.ua.
КОСТЮК І. В.,
кандидат технічних наук, керівник відділу АСУТП ТОВ «ТІСЕР», м. Київ
e-mail: kostyuk@tiser.kiev.ua

СТРАТЕГІЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Протягом двох останніх десятиліть стрімко розвивалися цифрові технології. Це викликало великий ажіотаж з приводу можливостей, які відкриває нова епоха цифрових гаджетів. Перехід від аналогових технологій до цифрових, тобто ера цифрової революції, передумовами якої є широке розповсюдженням інформаційно-комунікаційних технологій, вже настала і дуже активно прогресує. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом найбільш вразливим до кіберзагроз. Нині у сучасному інформаційному суспільстві комп'ютерні злочини стали характерною ознакою сьогодення. Розріняють різні категорії комп'ютерних злочинців: «хакери», «кракери», «пірати», «шкідники».

Злочини, що утворюються злочинними угрупуваннями з використанням інформаційних технологій (ІТ): кібертероризм, загроза фізичної розправи, дитяча порнографія, «відмивання» грошей, крадіжка грошей з банківських рахунків, шахрайські операції з пластиковими платіжними картками, розповсюдження інформації про наркотики через Інтернет.

З розвитком ІТ з'являються нові системи управління корпоративним підприємством, контролем над операціями в підприємстві, передачі інформації та її захист.

Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Основними випадками порушення безпеки інформації можна назвати такі: несанкціонований доступ, витік інформації, втрата інформації, підробка інформації, блокування інформації, порушення роботи інформаційних систем (ІС).

Безперечно, стратегія інформаційної безпеки повинна обов'язково включати не тільки забезпечення захисту вже напрацьованих об'єктів інтелектуальної власності, що мають комерційну цінність, а й запобігати втраті таких об'єктів у майбутньому.

Захист інформації неможливо регламентувати через різноманітність існуючих ІС та видів інформації, що обробляється. Конкретні заходи визначаються виробничими, фінансовими та іншими можливостями підприємства (організації), обсягом конфіденційної інформації та її значущістю. Систему захисту слід будувати, виходячи з того, що основну загрозу становлять співробітники підприємства (організації, установи), при цьому повинна бути достатньою, надійною, ефективною та керованою. Ефективність захисту інформації вимірюється не витратами на її організацію, а її здатністю адекватно реагувати на всі загрози. Щодо заходів із захисту інформації, то повинні мати комплексний характер, об'єднувати різні засоби.

В основі комплексу заходів щодо інформаційної безпеки повинна бути стратегія захисту інформації, у якій визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту. На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі – політика безпеки інформації (рис. 1).

Рис. 1. Ієрархічний підхід до забезпечення безпеки інформації

Як правило, за підтримку політики безпеки мережі відповідає системний адміністратор, що повинен оперативно реагувати на усі випадки злому конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні і програмні засоби захисту.

Щодо заходів, що безпосередньо забезпечують безпеку інформації розрізняють правові (наприклад, захист авторських прав), організаційно-адміністративні (наприклад, охорона комп'ютерних систем) та інженерно-технічні (програмні засоби, криптографічні засоби). Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в ІС, криптографічний захист інформації, захист від комп'ютерних вірусів тощо.

Інформація, як сукупність знань про фактичні дані і залежності між ними, стала стратегічним ресурсом, основою для прийняття будь-якого рішення. В інформаційних системах, які створюються в органах державної влади і у комерційних структурах, циркулює інформація, що містить секретні відомості про досягнутий потенціал в області економіки, оборони, науки і техніки, конфіденційні відомості про управлінську, господарську, комерційну, фінансову й іншу діяльність. Відповідно захист інформації – складна, наукомістка і багатогранна проблема в умовах упровадження сучасних інформаційних технологій, створення розподілених обчислювальних систем і мереж зв'язку, що набуває особливої гостроти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lakhno V., Kryvoruchko O., Mohylnyi H., Semenov M., Kiryeyev I., Matiievskyi V., & Donchenko V. (2019). Model of indicator of current risk of threats realization on the information communication system of transport. ISSN Print: 0976-6308 ISSN Online: 0976 – 6316 International Journal of Civil Engineering and Technolog

2. Захист систем електронних комунікацій: навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019. 164 с.

3. Olena Kryvoruchko, Viktoria Semidotska, Mykola Tsiutsiura, Alona Desyatko Problems of information security in enterprise // INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY (VII International Scientific and Technical Conference) Захист інформації і безпека інформаційних систем: матеріали VII Міжнар. наук.-техн. конф. Львів: Видавництво Львівської політехніки, 2019. 1 електрон. опт. диск (DVD). ISBN 978-966-941-337.

UDC 004.056

PASHORIN V.,
candidate of Technical Sciences, Professor of the Department of Software Engineering and Cybersecurity
Kyiv National University of Trade and Economics
e-mail: vpashorin@knute.edu.ua.
MAKOIEDOVA V.,
postgraduate student of the Department of Software Engineering and Cybersecurity
specialty 122 «Computer sciences»
Kyiv National University of Trade and Economics
e-mail: v.makoedova@knute.edu.ua

CYBERSECURITY TECHNOLOGIES IN DECISION SUPPORT SYSTEMS

The complexity of modern decision support systems (DSS) is constantly growing. The opportunities for the use of various technologies to implement decision-making tasks are expanding. However, the complexity of developing such systems is increasing. In the process of DSS development, it is important to take into account all possible risks, to model the system architecture and the relationship between system components. One of the important risk factors to be considered in the decision support system development is the problem of data integrity and information protection in the system.

In general, the cybersecurity issue in DSS is to prevent unauthorized access to information. According to annual cybercrime surveys conducted by international agencies, unauthorized access and theft of confidential data almost always cause the greatest losses to organizations. Unauthorized access to data is the intentional access of a user to data to which he is not allowed to access, for the purpose of reading, copying or destroying it. Unauthorized access can create any threat to the security of information: leakage, declassification, breach of integrity or availability. One of the main proven methods of protection against unauthorized access is to provide protection using a set of software and technological tools that implement certain protective technologies [1].

Basically, authentication and identification technologies are used to protect information from unauthorized access. Identification technologies are used to identify users and processes in the system by assigning them an individual name or personal code. Authentication technologies allow the system to verify the identity of a user, process, or system object. The purpose of authentication is to make sure that the user or process is exactly the one who was identified [2]. A password is a standard means of authentication. The main advantage of password authentication is simplicity and ordinariness. However, using a multiply-use password is risky. To increase the reliability of password protection, it is necessary to apply such measures as: password expiration control, limiting the number of failed login attempts, using software password generators etc. OTP (One Time Password) is a much more powerful and threat-resistant tool. OTP technology is based on the use of two-factor authentication schemes. The most common hardware implementations of one-time passwords for users are OTP-tokens [1].

Another technology that can be used to ensure cybersecurity in DSS is access control technology. Access control technologies allow to isolate objects within the control sphere and to guarantee differentiation of access requests and control of information flows between objects. Distinguish two types of access control: trust and administrative. Trust access control – control in which security features allow ordinary users to control the flow of information between other users and objects of their group, the appointment and transfer of authority does not require administrative intervention. Administrative access control – control in which security tools allow you to control the flow of information between users and objects only to specially authorized users [3].

Cryptographic protection technologies are used to encrypt data. Encryption of data ensures that data is stored securely and not in plain form. As soon as data is written to the system, it is encrypted via a set of secret keys which is known only to authorized administrators of the system. The access to these secret keys is limited and controlled to ensure that only privileged users can access the encrypted data and use it. This technology safeguards the data from attackers who might attempt to gain remote access to the system and protect the data from being compromised. It's an effective way of shielding your data from anyone trying to get unauthorized access [4].

Modern decision support systems typically use network connections, including the Internet. The fundamental problem is that the Internet was not designed as a secure network and was built on a vulnerable TCP / IP protocol stack. Network security technologies allow to deal with possible threats that may arise from the network environment [1]. By encrypting network traffic, you can ensure that it cannot be intercepted by an attacker who might be snooping on the network traffic. It's crucial for all networks to use encryption if they store privacy-protected data. This applies to both the connections made by authorized users from outside the data center to access the system and network links between nodes in a multi-server system. You can use a VPN layer between the users and the system or implement an SSL/TLS to encrypt network traffic. Inside the system, communications can be secured using IPsec, SSL/TLS, or some other VPN technology [4].

Since it is impossible to completely rule out the possibility of failure or incorrect operation of the system, in particular, in connection with the implementation of attacks, the solution is to identify problems at the earliest stages and obtain the most detailed information about them. In such cases, monitoring, logging and auditing technologies will be useful. They record all violations and allow timely notification of technical experts about the identified problems [1]. The application of these technologies in the decision support systems makes it possible to register and record events that occur in the system and user actions. This gives an opportunity to track user actions as well as operating system actions. Critical events are also registered, such as attempts to violate access rights to devices, disks, and files. The administrator determines the level of criticality of events, the alert mode, as well as the actions to be taken when such events occur [2].

In general, in order for cybersecurity measures to be effective, they should be applied in combination. Therefore, when developing decision support system, it is advisable to single out data protection technologies into a separate software module or information protection subsystem. The configuration of cybersecurity technologies within one subsystem will ensure comprehensive data security, and provide adaptability to changes in the operating conditions of decision support system.

REFERENCES

1. Kovtunets′ V. V., Nesterenko O. V., Savenkov O. I. *Bezpeka system pidtrymky pryynyattya rishen′* [Security of decision support systems]. Kyiv: National Academy Of Management, 2016. 189 p.

2. Zotova I., Berestov D., Kulchizkiy A., Gritsyuk V. *Pidsystema zakhystu informatsiyi vid nesanktsionovanoho dostupu v ERP-systemi* [Subsystem of prevention from an unauthorized division in ERP-system] Collection of scientific works of the Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovskij, 2015, vol. 2, pp. 38–42.

3. Kozyura V. D., Khoroshko V. O., Shelest M. YE., Tkach YU. M., Usov YA.YU. *Kompleksni systemy zakhystu informatsiyi v informatsiyno-telekomunikatsiynykh systemakh* [Complex systems of information protection in information and telecommunication systems]. Nizhyn: FOP Luk'yanenko V.V. TPK «Orkhideya», 2019. 144 p.

4. How to Protect Your Data from Unauthorized Access, Retrieved from https://cypressdatadefense.com/blog/unauthorized-data-access

УДК 351.746.1(477)

САМОЙЛЕНКО Ю. О.,
кандидат технічних наук, доцент кафедри автоматизації та комп'ютерних технологій систем управління
Національний університет харчових технологій
e-mail: juliya_liya@bigmir.net.
КОСТЮК Ю. В.,
асистент кафедри інженерії програмного забезпечення та кібербезпеки
(здобувач освітнього рівня PhD 122 «Комп'ютерні науки»)
Київський національний торговельно-економічний університет
e-mail: kostyuk_yu@knute.edu.ua

ТЕОРІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, суспільство вже не може уявити свій день без гаджетів та Інтернету. Широке поширення обчислювальної техніки, персональних комп'ютерів, всеосяжне проникнення Інтернету, масове застосування комунікаційних пристроїв спрямовані на розвиток суспільства. І чим швидше людство розвиває інформаційні технології, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем.

Нині високотехнологічна злочинність набуває високих темпів. У зв'язку з цим виникає термінова потреба у створенні не тільки єдиного інформаційного простору, але й адекватного механізму організації інформаційної безпеки. Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери і периферія), так і програмне забезпечення та бази даних, для яких комп'ютер є середовищем.

Небезпідставні побоювання викликають вразливості в програмному забезпеченні та в автоматизованих системах. Для зменшення цих ризиків необхідно вжити всіх необхідних заходів для поліпшення кібербезпеки. Аналіз інформаційних ризиків необхідний для визначення можливої шкоди (ризику) за існуючими видами цінної інформації, співвідношення ризику з витратами на забезпечення інформаційної безпеки, оцінки ефективності витрат на забезпечення інформаційної безпеки. Комплексна оцінка захищеності інформаційної системи, оцінка вартості інформації, оцінка ризику, розробка комплексної системи забезпечення інформаційної безпеки – основні завданнями аналізу. Тому метою аналізу інформаційних ризиків є розробка економічно ефективної і обґрунтованої системи забезпечення інформаційної безпеки. Критерії проведення аудиту інформаційної безпеки встановлюються на основі загальноприйнятих міжнародних стандартів (наприклад, міжнародний ISO 17799, німецький BSI і ін.), внутрішніх стандартів аудиторських компаній і вітчизняних відомчих стандартів. Важливий елемент організації інформаційної безпеки – поділ заходів захисту на групи. Основні групи заходів захисту інформації поділяють на активні засоби захисту (наприклад, розвідка, дезінформація, зашумлення), пасивні засоби захисту (наприклад, встановлення екранів несанкціонованому витоку інформації тощо) та комплексні засоби захисту (органічне поєднання названих груп). Визначення і перевірка стану безпеки є важливим шляхом реалізації заходів захисту інформації. За допомогою метрологічної діяльності з'ясовують чи задовольняє чинним нормам система захисту на певний момент часу.

Для успішної розробки хорошої моделі безпеки необхідна наявність чітко визначеної політики безпеки. Визначення умов, яким повинно підкорятися поводження системи, створення критерію безпеки і проведення формального доведення відповідності системи цьому критерію при дотриманні встановлених правил – основна мета створення політики безпеки інформаційної системи. Зв'язок наведених напрямків теорії захисту інформації можна представити у вигляді схеми (рис. 1).

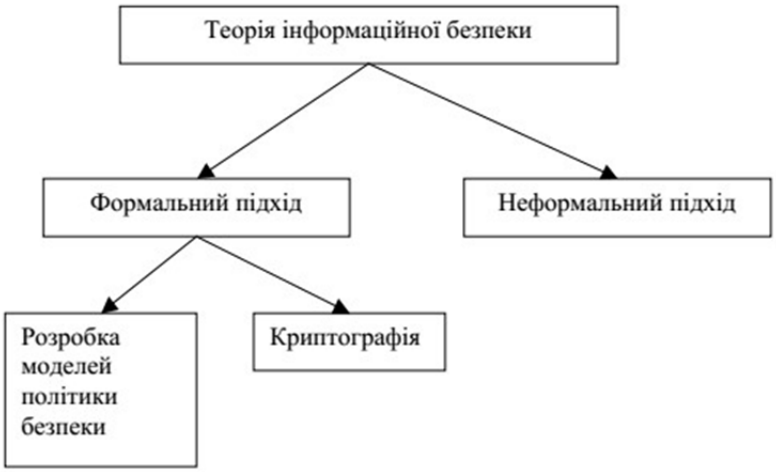


Рис. 1. Напрямки розвитку теорії захисту інформації

Незалежно від форм власності для захисту інформації створюються спеціальні служби безпеки, що підпорядковуються, як правило, керівництву установи. Керівники служб організують створення й функціонування систем захисту інформації. На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в системі: організація робіт з розробки системи захисту інформації; обмеження доступу на об'єкт і до ресурсів системи; розмежування доступу до ресурсів системи; планування заходів; розробка документації; сертифікація засобів захисту інформації; ліцензування діяльності по захисту інформації; атестація об'єктів захисту; удосконалювання системи захисту інформації; оцінка ефективності функціонування системи захисту інформації; контроль виконання встановлених правил роботи. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину комплексну систему.

Забезпечення кібербезпеки має здійснюватися єдиною інтелектуальною системою кібербезпеки, що є частиною системи інформаційної безпеки. При цьому в основу побудови перспективної системи кібербезпеки має бути покладено поняття еволюції системи, тобто здатність її адаптації через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак) і технологій, що застосовуються для протидії їм протягом свого життєвого циклу [2].

На даний час в Україні сформовано наукові школи з дослідження за різними сферами забезпечення кібербезпеки держави, насамперед, щодо планування і ведення кібероборони та кіберрозвідки, розслідування кіберзлочинів, відбиття кібератак та нейтралізації кіберзагроз; криптографічного та технічного захисту інформації; захисту в кіберпросторі державних інформаційних ресурсів; здійснення захисту та аудиту захищеності інформаційно-комунікаційних і технологічних систем об'єктів критичної інфраструктури держави на вразливість; відновлення сталості і надійності функціонування інформаційно-комунікаційних, технологічних систем після здійснення кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lakhno Valeriy, Malyukov Volodymyr, Kryvoruchko Olena, Tsiutsiura Mykola, Desyatko Alyona, Medynska Tetyana, Model of Evaluating Smart City Projects by Groups of Investors Using a Multifactorial Approach // Communications in Computer and Information Science, Book Series There are 1198 volumes in this series, Conference paper First Online: 03 March 2020, pp. 13–26 https://link.springer.com/chapter/10.1007/978-3-030-42517-3_2

2. Захист систем електронних комунікацій: навч. посіб. / В. О. Хорошко, О. В. Криворучко, М. М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019. 164 с.

УДК 004.056.5

САВЧЕНКО Т. В.,
доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київського національного торговельно-економічного університету
e-mail: savchenko_tv@knute.edu.ua.
САШНЬОВА М. В.,
доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київського національного торговельно-економічного університету
e-mail: m.sashnova@knute.edu.ua.
СТЕПАШКІНА К. В.,
асистент кафедри інженерії програмного забезпечення та кібербезпеки
Київського національного торговельно-економічного університету
e-mail: k.stepashkina@knute.edu.ua

ТАКСОНОМІЯ АТАК ТА МЕХАНІЗМІВ БЕЗПЕКИ В МЕРЕЖІ

Безпека мереж в сьогоденні стала невід'ємною частиною комп'ютерних технологій. Мережа – це та частина технологій, яка, без сумніву, буде зростати з кожним днем, але все має свої плюси і мінуси. Тому для вирішення мінусів (безпеки даних та усунення загроз) були створені різні протоколи, технології, пристрої, інструменти та методики мережевої безпеки.

Технологія комп'ютерних мереж швидко розвивається і безпека мережі є нагальним питанням розв'язку, оскільки багато видів атак зростають з кожним днем. До важливих чинників розвитку безпеки мереж відносять прагнення випереджати хакерів в чорних капелюхах на крок вперед, тим самим запобігаючи виникненню потенційних атак та мінімізації наслідків атак в реальному часі. Ще одним важливим чинником розвитку мережевої безпеки – забезпечення безперервності бізнесу. Оскільки кібератаки стають дедалі складнішими, отримуючи доступ до конфіденційних даних. Ці атаки завдають серйозних збитків різним організаціям, таких як фінансові втрати, перебої в роботі сервісу тощо [1].

Зростаючий обсяг шкідливих кібератак вимагає спільних зусиль між професіоналами безпеки та дослідниками для розробки та розробки ефективних систем кіберзахисту. Тому, завдання фахівця мережевої безпеки полягає в нейтралізації мережевих атак та ослаблення їх наслідків. Вразливості в системі мережевої безпеки можуть стати причиною, наприклад, переривання електронної торгівлі та привести до витоку бізнес-даних, порушення конфіденційності та компрометації достовірності інформації. Ці проблеми можуть спричинити за собою втрату прибутку для корпорацій, крадіжку інтелектуальної власності, судові проблеми і загрозу громадській безпеці. Кібератаки продовжують зростати у всьому світі таким чином, що щорічно коштує компаніям мільйони доларів і призводить до втрати або зловживання інформаційними активами [2]. Забезпечення надійної безпеки мережі гарантує захист користувачів мережі і комерційних інтересів. Збереження безпеки мережі вимагає пильності з боку фахівців з мережевої безпеки організації. Вони повинні бути постійно в курсі нових мережевих загроз та атак, а також вразливостей пристроїв і додатків.

Метою мережевої безпеки є забезпечення активних методів захисту та механізмів захисту мережі від внутрішніх та зовнішніх загроз. Вся діяльність у сфері мережевої безпеки регулюється політикою мережевої безпеки. Мережева безпека ділиться на області, а мережеві атаки класифікуються так, щоб їх легше було вивчити і прийняти відповідних заходів (рис. 1). Віруси, хробаки та троянці – все це окремі типи мережевих атак. У більш загальному плані мережеві атаки класифікуються як розвідувальні атаки, атаки доступу або атаки типу «відмова в обслуговуванні» (DoS). Більшість векторів атак йдуть ззовні корпоративної мережі. Наприклад, зловмисники можуть через Інтернет націлитися на мережу, щоб

перервати її нормальну роботу, і для цього створюють атаку типу «відмова в обслуговуванні» (DoS). При DoS-атаці мережа стає непрацездатною і не може реагувати на запити легітимних користувачів. Вектори атаки можуть також виходити і зсередини мережі.

Внутрішній користувач, наприклад співробітник, може випадково або навмисно [3]:

- ✓ вкрасти і скопіювати конфіденційні дані;
- ✓ скомпрометувати внутрішні сервери або пристрої мережевої інфраструктури;
- ✓ відключити важливі мережеві підключення, що призведе до виходу мережі з ладу;
- ✓ підключити інфікований USB-диск до корпоративної обчислювальної системи.

Внутрішні загрози можуть заподіяти навіть більшої шкоди, ніж зовнішні, тому що внутрішні користувачі мають прямий доступ до будівлі і до інфраструктурних об'єктів. Співробітники також володіють інформацією про свою корпоративну мережу, її ресурси та конфіденційні дані. Тому, фахівці з мережевої безпеки повинні впроваджувати інструменти і техніки для нейтралізації зовнішніх і внутрішніх загроз.

Дані організації є найбільш цінним активом і можуть включати в себе дані досліджень і розробок, дані продажів, фінансові дані, юридичні та кадрові дані, дані про співробітників, підрядників і замовників.

Під втратою або витоком даних розуміється навмисна або ненавмисно втрата, крадіжка чи витік даних у зовнішній світ. Втрата даних може призвести до таких наслідків [3]:

- ✓ збитки для бренду та репутації;
- ✓ втрата конкурентної переваги;
- ✓ втрата замовників;
- ✓ втрата прибутку;
- ✓ розгляду в суді та юридичні наслідки, які можуть привести до штрафів і адміністративних санкцій;
- ✓ значні витрати і зусилля щодо повідомлення потерпілих сторін і відновлення після витоку.

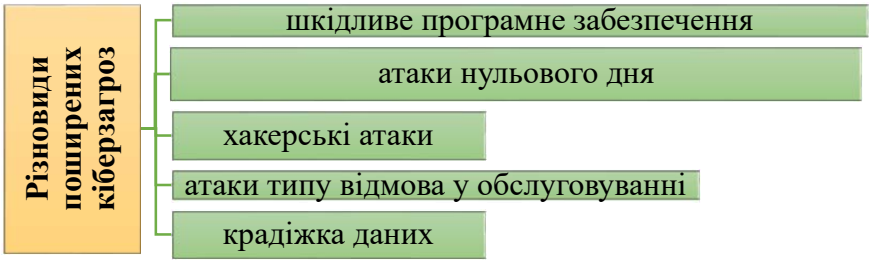


Рис. 1. Різновиди кіберзагроз

Задачею фахівців з мережевої безпеки – захист даних організації. Для цього необхідно впроваджувати різні техніки запобігання втрати даних (Data Loss Prevention, DLP), які б включали в себе стратегічні, операційні та тактичні завдання. Крім того, метою захисту є впровадження різної техніки безпеки мережі для захисту активів організації від зовнішніх і внутрішніх загроз. Підключення до недовірених мереж повинне ретельно перевірятися. Для цього, перш ніж трафік потрапить на корпоративні ресурси, необхідно організувати кілька рівнів захисту.

Все більшу роль в корпоративних мережах відіграють хмарні технології. Хмарні обчислення дозволяють організаціям використовувати такі сервіси, як сховище даних або хмарні додатки, щоб розширювати свої можливості та ємність без додавання інфраструктури. За своєю природою хмара розташована за межами традиційного периметра мережі, дозволяючи організаціям розміщувати ЦОД (центри обробки даних) як всередині, так і зовні традиційного брандмауера.

Фактично хмарна мережа складається з фізичних та віртуальних серверів, які зазвичай розміщуються в центрах обробки даних. Однак центри обробки даних все більше використовують віртуальні машини (ВМ) для надання серверних послуг своїм клієнтам. Віртуалізація серверів дозволяє використовувати незадіяні ресурси і об'єднує кілька необхідних серверів. Таким чином, також забезпечується можливість існування різних операційних систем на одній апаратній платформі. Сьогодні споживчі кінцеві пристрої, такі як IPhone, смартфони, планшети та інші пристрої, ефективно замінюють або доповнюють традиційні ПК. Все більше людей використовують ці пристрої для доступу до корпоративної інформації, тим самим спостерігається збільшення програм соціальних мереж, хмарних обчислень та передачі власного пристрою. Останнє називається тенденцією «принеси на роботу свій пристрій» (Bring Your Own Device, BYOD. Все це створило нові загрози і виклики [4].

Отже, захист мережі необхідно починати із захисту її пристроїв, а саме: захисту периметра мережі, забезпечення безпеки адміністративного доступу до інфраструктурних пристроїв, підвищення безпеки віртуального входу в систему і використання захищених протоколів замість незахищених. Також важливо обмежувати адміністративний доступ. Адміністратори повинні надавати доступ до інфраструктурних пристроїв в залежності від рівнів привілеїв і впроваджувати інтерфейс CLI на основі ролей для забезпечення ієрархічного адміністративного доступу.

Підводячи підсумок, відзначимо, що адміністратори повинні ідентифікувати всі сервіси, інтерфейси і сервіси управління, які вразливі перед мережевими атаками. Для цього необхідно регулярно проводити аудити системи безпеки (рис. 2).

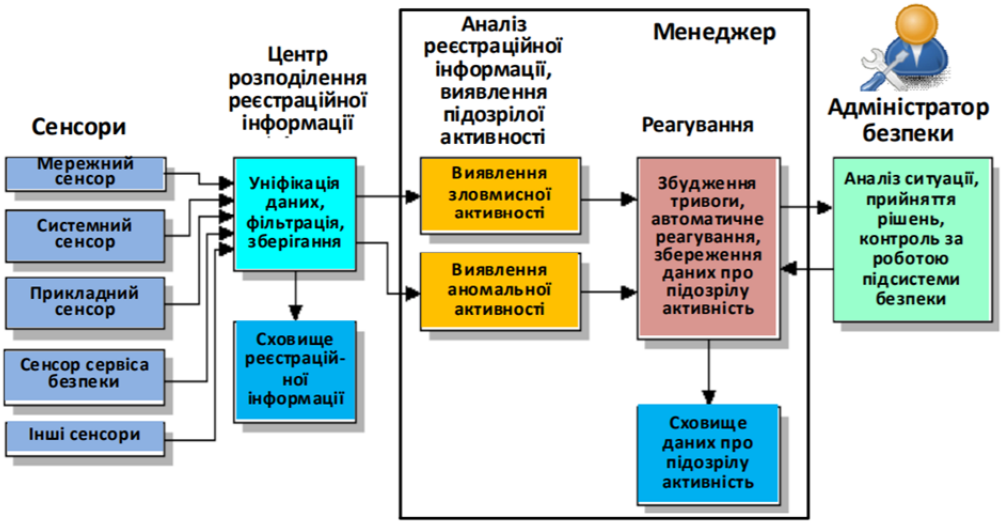


Рис. 2. Основні елементи архітектури систем активного аудита

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Maraj A., Jakupi G., Rogova E. and X. Grajqevci, «Testing of network security systems through DoS attacks,» *2017 6th Mediterranean Conference on Embedded Computing (MECO)*, Bar, 2017, pp. 1-6, doi: 10.1109/MECO.2017.7977239.

2. Alsmadi, I. *et al.* Network Security. in 121–138 (2018). doi:10.1007/978-3-319-72119-4_6

3. CCNA Security: курс з кібербезпеки. URL: https://www.netacad.com/ru/courses/cybersecurity/ccna-security

4. Asamba, M. Running head: BEST PRACTICES OF NETWORK SECURITY 1 Best Practices of Network Security Student's Name Institutional Affiliation BEST PRACTICES OF NETWORK SECURITY 2. *Technology* 23, 14–23 (2020).

УДК 654:316.774.323.28

КОТЕНКО Н. О.,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки,
кандидат педагогічних наук
Київський національний торговельно-економічний університет
e-mail: kotenkono@knute.edu.ua.
АЛЕКСАНДРОВ А. Ю.,
здобувач вищої освіти ОС «бакалавр», спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: 121-18-6-b-aleksandrov@knute.edu.ua

МЕХАНІЗМ ЗАХИСТУ PYTHON ФРЕЙМВОРКУ DJANGO ВІД МІЖСАЙТОВОЇ ПІДРОБКИ ЗАПИТУ (CSRF)

Нині питанню захисту програмного забезпечення в цілому та питанню захисту веб-сайтів зокрема приділяється надзвичайно велика увага. Від надійності як програмного забезпечення так і веб-сайтів залежить цілісність та захищеність даних користувачів даними продуктами. Тому при розробці програмного забезпечення та верстці веб-сайтів особливо пильно необхідно віднестися до моментів, що пов'язані з їх безпекою.

Створення веб-сайтів завжди передбачає впровадження додаткових механізмів задля підтримання безпеки самого сайту та даних користувачів. Python фреймфорк Django пропонує низку таких.

Django – це високоякісний веб-фреймворк Python, який стимулює швидкий розвиток та чистий, прагматичний дизайн. Він є безкоштовним та з відкритим кодом. Django серйозно ставиться до безпеки і допомагає розробникам уникнути багатьох типових помилок у безпеці, таких як SQL injection, cross-site scripting, cross-site request forgery і clickjacking. Його система автентифікації користувачів забезпечує безпечний спосіб управління обліковими записами користувачів та паролями. Серед них наявний і захист від Cross Site Request Forgery (CSRF).

CSRF – найнебезпечніша атака, яка призводить до того, що хакер може виконати на непідготовленій сторінці сайт масу різних дій від імені інших, зареєстрованих відвідувачів. Наприклад, відправка повідомлень, переказ грошей з рахунку на рахунок або зміна паролів – залежить від сайту, але в будь-якому випадку ця атака спроможна заподіяти суттєвої шкоди користувачам.

Підробка запитів між сайтами дозволяє виконувати запити від імені користувачів і без їх відома. Наприклад, існує веб-сайт «website.com», на якому потенційна жертва авторизована в момент здійснення атаки. Користувач знаходиться на іншому сайті із спеціальними зображеннями, прихованими формами або відкриває повідомлення на пошті, яке містить посилання з запитом: «website.com/send_money?amount=10000&to=John». Таким чином, запит виконується, відбувається певна дія, а користувач цього навіть не помічає [1]. Особливу небезпеку такий вид атаки становить для самого вебсайту, якщо користувач, якого атакують, має особливі права доступу, є адміністратором.

Даному виду атаки піддавалися такі потужні веб-сайти, як YouTube, де, завдяки CSRF зловмисник мав змогу проводити будь-які дії з боку користувача. Зловмисник міг використовувати вразливість, щоб впливати на популярність відео, або, помічаючи його таким, що не відповідає правилам YouTube, робити спробу видалення матеріалів з веб-сайту [2].

Вирішення проблеми, яке пропонує Django. Django має вбудований захист від різних видів атак CSRF. Суть методу полягає в створенні унікального набору символів – токену. Один з них зберігається у файлі cookie та присвоюється кожному користувачу. Інший знаходиться у додатковому полі форми, яке також містить маску для додаткового захисту,

яка змінюється при кожному запиті. При перевірці форми два цих токена (з форми та із cookie) звіряються сервером, якщо вони не збігаються, то запит відхиляється. Цей метод гарантовано захищає від CSRF атак за умови, що вебсайт також має захист від XSS-атаки, яка дозволяє отримати cookie користувача [3].

За специфікацією RFC 2616 такі методи запитів як GET, HEAD, OPTIONS, TRACE є безпечними та не потребують застосування захисту, на відміну від методів POST, PUT, DELETE, які змінюють інформацію на сервері, потенційно становлять небезпеку для важливих даних [4]. Саме до них застосовується захист від CSRF.

Метод POST надсилає на сервер дані в запиті браузера. Це дозволяє відправляти більшу кількість даних, ніж це можна зробити методом GET, оскільки у нього встановлено обмеження в 4 Кб. Великі обсяги даних використовуються у форумах, поштових службах, заповненні бази даних, при пересиланні файлів тощо.

Метод PUT використовується для підміни записів. У специфікації HTTP 1.1 зазначено, що PUT ідемпотентний. Це означає, що клієнт може виконати безліч PUT запитів по одному URI і це не призведе до створення записів дублікатів.

Метод DELETE запитує початковий сервер про видалення ресурсу, ідентифікованого URI що запрошується. Цей метод може бути скасований людським втручанням або іншими засобами на первинному сервері. Клієнту не можна гарантувати, що операція була виконана, навіть якщо код стану, повернутий початковим сервером вказує на те, що дія була завершено успішно. Однак, серверу не слід відповідати про успішне виконання, якщо під час відповіді він передбачає видалити ресурс або перемістити його в недоступний стан. Якщо запит передається через кеш і запитуваний URI ідентифікує один або кілька кешованих в даний час об’єктів, то входження їх повинні оброблятися як прострочені. Відповіді на цей метод не кешуються.

Важливою особливістю, яку варто враховувати є те, що CSRF-токен не рекомендується використовувати при здійсненні запитів на інші ресурси, адже це може призвести до його витоку і відповідно до уразливості.

Висновок. Захист від CSRF існує для того, щоб бути впевненим, що запити відправляються від фактичних користувачів веб-сайту, що убезпечує їхні дані. Такий вид атаки є досить простим для вирішення, хоча й водночас може призвести до непередбачуваних наслідків. Захист у Django побудовано на рівні фреймворку, що значно полегшує роботу розробників і для застосування вимагає лише декілька простих кроків, які гарантують безпеку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Auger R. The cross-site request forgery (CSRF/XSRF) FAQ. 2010. Режим доступу: https://www.cgisecurity.com/csrf-faq.html
2. Zeller W., Felten E. W. Cross-Site Request Forgeries: Exploitation and Prevention. Режим доступу: https://people.eecs.berkeley.edu/~daw/teaching/cs261-f11/reading/csrf.pdf
3. Cross Site Request Forgery protection // Django Software Foundation. 2020. Режим доступу: https://docs.djangoproject.com/en/3.1/ref/csrf
4. Hypertext Transfer Protocol – HTTP/1.1. 1999. Режим доступу: https://tools.ietf.org/html/rfc2616#page-51
5. Дослідження основних тенденцій сучасної розробки вебсайтів / А. М. Десятко, Н. О. Котенко, Т. О. Жирова та ін. // Кібербезпека: освіта, наука, техніка = Cybersecurity: Education, Science, Technique. Київський університет ім. Бориса Грінченка. 2019. С. 6–15.
6. Сучасні технології тестування та захисту веб-сторінок / М. І. Цюцюра, О. В. Криворучко, Т. О. Жирова та ін. // Управління розвитком складних систем. Випуск № 39, 2019. С. 100–105.

УДК 004.415.53

КРИВОРУЧКО О. В.,
доктор технічних наук, професор,
завідувач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
kryvoruchko_ev@knute.edu.ua.
ДЕСЯТКО А. М.,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
desyatko@knute.edu.ua

МІЖНАРОДНІ СТАНДАРТИ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Впровадження ISO/IEC 27001:2013 надає низку слушних векторів розвитку для управління інформаційною безпекою підприємства будь-якої форми власності, а саме:

- виявлення ризиків та застосування засобів контролю для управління або уникнення інформаційних загроз;
- можливість гнучкості в адаптації управління підприємством;
- отримання зацікавленості та довіри клієнтів в тому, що їх дані захищені;
- відповідність вимогам часу.

Система управління інформаційною безпекою ISO/IEC 27001:2013 дає можливість впровадити найкращу практику для удосконалення захисту даних та усунення загрози порушення безпеки інформаційних систем. А ефективне управління безпекою інформаційних систем підтримується при регулярному моніторингу або аудиті системи [1].

Вплив ISO / IEC 27001:2013 на роботу компанії/організації можна спостерігти в різних сферах прояву бізнесу:

- репутація – встановлення процедури швидкого виявлення порушень інформаційної безпеки;
- зацікавлені сторони – визначення всіх внутрішніх та зовнішніх зацікавлених сторін, яких стосуються система управління інформаційною безпекою;
- відповідності – надає основу, яка допомагає керувати своїми юридичними та нормативними вимогами, змушує переглядати та повідомляти свої регулярні вимоги іншим зацікавленим сторонам;
- ризик управління – оцінювання ризики інформаційної безпеки, щоб була можливість виявити потенційні недоліки та реагувати [2].

Розуміння сфери застосування стандарту ISO/IEC 27001 впливає на процес управління підприємством та даними про клієнтів. Також дуже важливим питанням сьогодення є створення культури поінформованості про безпеку на підприємстві, яка є відповідною ISO/IEC 27001, зміцнюючи при цьому довіру клієнтів до здатності захищати їхні дані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity», 50 p.

2. Аналіз стану захищеності інформаційно-телекомунікаційних систем / О. В. Криворучко, О. М. Сунічук, Д. В. Швець та ін. // Управління розвитком складних систем. 2020. № 42. С. 56–62; dx.doi.org\10.32347/2412-9933.2020.42.56-62.

УДК 004.22: 004.8: 681.3

ЦЮЦЮРА М. І.,
професор кафедри інформаційних технологій, доцент, доктор технічних наук
Київський національний університет будівництва і архітектури
e-mail: mitsiutsiura@gmail.com

ФОРМУВАННЯ КЛЮЧОВИХ ІНДИКАТОРІВ УСПІХУ З ПОЗИЦІЙ ЇХ ЗАСТОСУВАННЯ ПРИ ПІДГОТОВЦІ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Постановка проблеми. Формування системи ключових індикаторів успіху KPI (Key Performance Indicators) не є новою і складається із груп ключових показників діяльності за окремо взятими функціональними напрямками діяльності (стратегія і тактика організації, бізнес-процеси, економічна діяльність, кадрова політика, тощо). Сьогодні система KPI найбільш поширена не тільки як інструмент контролю та оцінки ефективності дій, які виконуються, але і як інструмент, на базі якого будуються ефективні системи оплати праці. У зв'язку з таким широким застосуванням KPI виникають проблеми щодо оцінки їх достатності та ефективності використання.

Аналіз досліджень і публікацій Ключові індикатори успіху – система оцінки, яка допомагає організації визначити досягнення стратегічної і тактичної (операційної) цілей. Їх використання дає організації можливість оцінити свій стан і допомагає в реалізації стратегії. KPI дозволяє проводити контроль ділової активності співпрацівників і організації в цілому в реальному часі для виконання поставлених задач в рамках визначеної цілі. Тому KPI можна розглядати як інструмент управління за цілями, під яким розуміється метод управлінської діяльності, який передбачає раціональний результат із можливих результатів діяльності і планування шляхів їх досягнення. KPI і мотивація персоналу стали нерозривними поняттями, оскільки за допомогою даних показників можна створити найбільш досконалу й ефективну систему мотивації і стимулювання працівників організації.

В залежності від стратегії організації розрізняють різні KPI. В основному їх застосовують для визначення результативності роботи адміністративно-управлінського персоналу. KPI – це ключові індикатори успіху.

Ключові показники можна, зокрема, розділити на випереджаючі та на ті, що запізнюються. Показники, ті що запізнюються, відображають результати діяльності після закінчення відповідного етапу (певного періоду) діяльності. Випереджаючі показники дають можливість управляти ситуацією в межах звітного періоду з метою досягнення заданих результатів на момент його закінченні.

KPI часто використовуються як вимірювач досягнення цілей цих бізнес-процесів. Таке широке застосування та неоднозначне сприйняття KPI робить доцільним вивчити питання вимог до розроблення системи KPI. На сьогодні такі вимоги знаходяться в різних джерелах і потребують системного узагальнення та уточнення. Але в проєктній діяльності система KPI ще не знайшла такого широкого застосування, як в сфері оцінки роботи всієї компанії, окремих її підрозділів та конкретних робітників. Однією з причин можна вважати відсутність узагальнених вимог до системи KPI, з позиції якої можна було б оцінити можливість та доцільність застосування KPI в проєктній діяльності.

Мета роботи полягає у формуванні вимог до розроблення системи KPI на основі розрізненої інформації, яка міститься в різних джерелах, та оцінити можливість і напрямки застосування KPI в проєктній діяльності організацій з підготовки фахівців з кібербезпеки для виконання завдань боротьби із кіберзлочинами.

Викладення основних результатів. Аналіз контенту сайтів [1] України, які займаються розробленням системи ключових показників ефективності (KPI) показав, що усі вони містять інформацію не про вимоги до системи KPI, а проблеми, з якими може стикнутись будь-яка

організація без наявності такої системи. Структурний аналіз інформації [2], яка міститься в публікаціях з розроблення та застосування KPI, дозволив виділити дев'ять наступних базових вимог, які найбільш часто можна зустріти в публікаціях (але не усі разом та не завжди представлених експліцитно).

Вимога 1. Показники повинні відображати досягнення цілі організації як цілісної системи, так і цілі діяльності.

Вимога 2. Кількість показників не повинна бути дуже великою задля того, щоб не виникали проблеми в процесі прийняття на їх основі рішень.

Вимога 3. Усі показники повинні бути пов'язані причинно-наслідковими зв'язками між собою (прямий або непрямий зв'язок). Наявність системи непов'язаних показників дуже часто носить руйнівний характер для організації в цілому.

Вимога 4. Система показників повинна відображати не тільки фінансові та матеріальні аспекти діяльності, але і нематеріальні активи (розглядаються як показники, які виступають індикаторами правильності прийнятих управлінських рішень в напрямку досягнення цілей, тобто: показники мотивації, задоволеності клієнтів, організаційної культури тощо).

Вимога 5. Система показників повинна включати не тільки фінальні, а і випереджаючі показники, які можуть попереджувати про виникнення проблем.

Вимога 6. Всі показники повинні бути вимірювальними і мати чіткі інструменти вимірювання.

Вимога 7. Кожен показник системи KPI повинен бути закріпленим за відповідними співробітниками.

Вимога 8. Система показників повинна відображати різні рівні значень показників (припустимий, неприпустимий, критичний тощо).

Вимога 9. Система показників повинна базуватись не на суб'єктивній точці зору, а на прозорості системи, яка зрозуміла усім співробітникам організації.

Як бачимо, за своєю сутністю вимоги до системи ключових показників KPI є факторною моделлю, яка показує вплив окремих факторів на систему інтегральних ключових показників, які описують узагальнений результат.

Система KPI формалізує стратегію діяльності, яка розробляється не від досягнутих показників та існуючих можливостей, а з позицій планування майбутнього. Якщо склалась організаційна структура, розподілені відповідальність та повноваження між керівниками різних рівнів управління. Якщо виникає потреба постійно адаптувати розроблену систему KPI, то вона перестає бути логічно правильно побудованою і стає не тільки неефективною, а й небезпечною.

Висновки. Систему KPI в проєктній діяльності організацій з підготовки фахівців з кібербезпеки для виконання завдань боротьби із кіберзлочинами можна застосовувати тільки для оцінки якості управління такими проєктами за умови, що воно розглядається як стабільний процес в організації.

Наявність таких показників знімає частину ризиків на шляху ефективного досягнення організацією стратегічних цілей. Тобто, система KPI в проєктній діяльності з «кібербезпеки – безпеки держави» повинна бути спрямована не на оцінку ефективності їх реалізованих, а на оцінку ефективності управління такими проєктами в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дослідження основних тенденцій сучасної розробки вебсайтів / А. М. Десятко, Н. О. Котенко, Т. О. Жирова та ін. // Кібербезпека: освіта, наука, техніка = Cybersecurity: Education, Science, Technique. Київський університет ім. Бориса Грінченка. 2019. С. 6–15.

2. Kryvoruchko Olena. Rationale of Project-Oriented Management of Higher Educational Institution Project / Olena Kryvoruchko, Mykola Tsiutsiura, Viktor Kotetunov // Development International Journal of Science and Research (IJSR); (Issue 12), 2016. P. 1098–1100. (Index Copernicus).

UDC 004.056.5

HNATCHENKO T.,
Postgraduate of the Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics
e-mail: dmitriy.gnatchenko@knute.edu.ua
IL'YIN V.,
Student of FIT 4 course 7 group Bachelor Degree,
Program Subject Area 121 «Software engineering»
Kyiv National University of Trade and Economics
e-mail: hellworkermail@gmail.com

CYBERSECURITY OF UKRAINE IN CONDITIONS OF THE COVID-19 PANDEMIC

The stage of modern development of the Ukrainian state is characterized by the fact that all spheres of life are fully computerized. At the same time, the transfer of many processes, including those related to critical infrastructure, to cyberspace, with positive aspects, also has negative consequences: the vulnerability of these processes to numerous cyber threats. The COVID-19 pandemic, among other things, has exacerbated cybersecurity concerns as crises have traditionally contributed to the escalation of various hacker groups. The main factors that can contribute to the strengthening of destructive (illegal) cyberactivity are described below.

The practice of introducing a quarantine regime encourages employers to change the nature of industrial relations with workers to the format of remote work. In most cases, these interactions take place over the Internet. As a result, there is an increase in the number of potentially vulnerable links that can compromise information or the organization itself, its employees, and so on. Restrictions on travel, maximum restrictions on cash payments, as well as an increase in time spent by citizens at home, lead not only to an increase in the time of Internet use in general, but also to an increase in electronic payments in particular. As a result, the number of phishing attacks is traditionally growing – the number of fake emails (with embedded malware) and fake sites (to collect personal and banking information from citizens) is increasing.

The number of people who start working remotely for the first time and do not always know how to do so is growing rapidly, so some organizations are temporarily simplifying access to information by providing it to employees in a remote format. At the same time, these employees often use a much less secure telecommunications environment than in their office workplace. All this increases the risk of leakage of confidential information.

Experts also note that the source of an attack on employees' home systems may be the services of video tutors, which can be used by their children, who are also in quarantine (these services are traditionally much less protected than others).

There is currently no conclusive evidence of an increase in pandemic fraud related to cyber fraud, but an increasing number of experts are advising citizens and employers to take prompt action to minimize potential adverse effects.

These include:

- ensuring the proper level of digital hygiene for users and improving their digital skills;
- use of VPN (especially in public places);
- minimization of the use of open (public) WiFi;
- increased attention to any unfamiliar letters or those that contain «emotional» headlines with links;
- use only official information and data;
- immediate notification to the employer in case of loss / theft of a personal mobile device from which the employee could gain access to work equipment;
- constant contact between employers and employees regarding cyber incidents.

In addition, the COVID-19 pandemic has exacerbated several other issues that may have a long-term dimension.

First, cyber surveillance and human rights. Governments are looking to increase the accuracy of tracking both infected people and those with whom they have been in contact, including using modern technology. However, the greatest opportunities for such detection may be in conflict with human rights. All this raises the question of the limits of state intervention in the lives of citizens in a real threat to national security.

Second, the health care system (including its supply elements) is gaining new importance as a critical infrastructure. Although elements of the health care system used to be critical infrastructure, the focus is now shifting from understanding criticality as a place of circulation of sensitive personal data of patients to objects on which the lives of large masses of people depend. However, the level of cybersecurity of such objects is often unsatisfactory.

Organizations are encouraged to fund and implement breakthrough automated defense technologies that will support automated management capabilities and improved behavioral analytics. Examples of such technologies include artificial intelligence tools for analyzing biometric data, sophisticated machine learning algorithms that can profile typical user behavior, identify unusual patterns of activity, and identify potential threats in real time before attackers can implement them. Thanks to the automatic identification of suspicious data, the whole protection process will be more effective, and the mechanism itself will eliminate the need for manual control of the data log.

The following actions will also be appropriate in this situation:

1. To the National Coordination Center for Cyber Security of the National Security and Defense Council of Ukraine (NCCC) to recommend the Security Service of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Cyberpolice Department of the National Police of Ukraine, the National Bank of Ukraine – to inform the public about possible cyber threats when using digital devices during remote work and the danger of phishing attacks.

2. NCCC (taking into account the real epidemiological situation) – to initiate the preparation of recommendations for strengthening cyber protection of medical facilities.

3. The Ministry of Digital Transformation of Ukraine should consider the possibility of conducting additional explanatory measures on cyber literacy (cyber hygiene) and personal cyber security for citizens who, as a result of quarantine measures, may switch to remote operation using digital means. Also to inform all age groups about the basic rules of security for the use of electronic means of payment on the Internet.

Conclusions. The monitoring of Ukraine' security level in the field of cyberspace protection showed that the problem of effective cybersecurity needs to be comprehensively addressed and requires coordinated action at the national, regional and international levels to prevent, prepare, respond to and repair incidents by government, private sector and civil society response to new trends in the global movement towards the digital economy and the information society.

REFERENCES

1. EU-NATO-Ukraine Cooperation on Countering Hybrid Threats in Cyberspace (2019). Retrieved from: https://geostrategy.org.ua/ua/analitika/item/1565-cooperation-ukraine-nato

2. Trofymenko, O.H., Dubovoy, Ya.V. (2018) Concerning the legal capacity of cyberspace safe operation. Cybersecurity in Ukraine: legal and organizational issues: materials of the III All-Ukrainian scientific-practical conference (November 30, 2018). Odessa. pp. 5–7.

3. European Cybersecurity Implementation: Overview – ISACA (2014). Retrieved from: https://informationsecurity.report/Resources/Whitepapers/3251dc92-c468-4f99-bd2b-c4203ce81af3_European-Cybersecurity-Implementation-Overview_res_Eng_0814.pdf

УДК 621.389

СЕМІДОЦЬКА В. А.,
викладач кафедри сучасних європейський мов
Київський національний торговельно-економічний університет
e-mail: v.semidotska@knute.edu.ua.
АНДРУСЕНКО В. П.,
студент, ОС «Бакалавр» 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: v_andrusenko_foais_19_6_b_d@knute.edu.ua

QUANTUM COMPUTING AND CYBERSECURITY

When we analyze the impact of quantum computing on future network security, two possible scenarios will appear. One is chaotic and dangerous. Quantum computers, due to their supercomputing power, may destroy many cryptographic systems currently in use, thereby posing a potential threat. Cryptography is an important part of the infrastructure in many industries and the Internet. In another case, quantum computers use their processing power to solve problems that have not been solved so far out of ethics and responsibility when dealing with different fields such as pharmacy, chemistry, finance, or machine learning. The quantum communication network will be faster and freer from cyber-attacks in the future, which can ensure the integrity and confidentiality of the data stored and transmitted.

After all, technologies are neither bad nor good, and it is up to people to decide how to use them.

Unfortunately, most IT experts, scientists, and researchers believe that the first scenario is most likely to occur. Many companies and governments are preparing for the quantum age. The reason is not only to improve the processing capacity but also to solve the problems that traditional computers cannot solve. In the past 20 years, the complexity and number of transistors in a single CPU has grown exponentially. The extreme miniaturization of electronic gates is causing the effects of phenomena such as electromigration and subthreshold, and this phenomenon is becoming more obvious. These obstacles are other factors that motivate researchers to study new computing methods, such as quantum computers.

In the most basic sense, encryption refers to obtaining original information (such as a message) and converting it into seemingly chaotic behavior following a series of steps. Today's digital passwords use complex mathematical formulas to convert clear data into content in secure encrypted messages to be stored or transmitted. The calculation result varies according to the number of keys.

There are two main types of encryption: symmetric, where the same key is used to encrypt and decrypt data; asymmetric key or non-public key, which involves a pair of mathematically linked keys, and one key is publicly shared. The message is encrypted for the owner of the key pair, and the other key is stored privately by the owner to decrypt the message. Symmetric cryptography is much faster than public-key cryptography. Therefore, it is used to encrypt all communication and stored data.

Public-key cryptography is used to securely exchange symmetric keys, and to digitally authenticate or sign messages, documents, and certificates that pair the public key with its owner. The mathematical methods of these two types of cryptography are completely different, which affects their security. Because almost all Internet applications use symmetric encryption and public-key encryption at the same time, both forms need to be protected.

Many products, services, and businesses rely on encryption protocols. Without the expected security level, they will not operate. They do not comply with legal requirements regarding data privacy and security. The integrity, confidentiality, and availability of the stored data cannot be guaranteed.

A quantum computer using the Shor algorithm can break RSA 2048-bit encryption within 10 seconds after performing one million operations per second. A classic computer that runs one trillion operations per second takes about 300 trillion years. A quantum computer needs a throughput of 4000 qubits to crack the strongest encryption key available today. It is thought that we will see this capability by 2023.

Cybercriminals cannot have the resources to build quantum processors. Nevertheless, some countries are still developing quantum computers, which may be used to crack encryption algorithms as part of cyber espionage. This situation will not only affect businesses but also governments, the military, financial transactions, medical records, and personal data-the entire world.

Research by the National Academy of Sciences of the United States pointed out that the processing power of quantum computers currently running is too weak and error-prone to crack today's powerful codes. Tomorrow's cryptographic quantum computers will require 100,000 times higher processing power and 100 times the error rate than today's best quantum computers. This study does not predict how long these advances may take, but it does not expect them to occur within ten years. However, the potential harm is huge. If these encryption methods are broken, then even if the data is encrypted, people will not be able to trust the data they transmit or receive over the Internet. The adversary will be able to create false certificates, thereby questioning the validity of any online digital identity.

Government organizations such as the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) also participated in its development. NIST has been designing a system to evaluate the effectiveness of these new algorithms, and the results should be available by 2022. IBM has created Spectrum Protect, which will protect physical file servers, applications, and virtual environments in Quantum Files.

On October 23, 2019, Google's statement claimed to have achieved quantum supremacy (the point that quantum computers can perform mathematical calculations is not even the most powerful supercomputers). Its Quantum processor can complete calculations in 3 minutes and 20 seconds, which will take about 10,000 years to use today's most advanced classic computer (called Summit). The computer created by Google has 53 qubits.

Quantum computers use qubits, which are subatomic particles such as electrons or photons. To generate and control qubits, it is necessary to isolate them in a controlled quantum state. Advanced technology has been developed to achieve a controlled quantum state: the use of superconducting circuits to lower the temperature to a temperature lower than that of deep space, and the trapping of atoms in the electromagnetic field on the silicon wafer in an ultra-high vacuum chamber.

By linking qubits together, the number of states they can represent increases exponentially, which makes it possible to quickly calculate millions of solutions.

However, quantum computers have great obstacles, and due to their decoherence, they are more error-prone than traditional computers. When the interaction between the qubit and its environment causes its quantum behavior to decay and eventually disappear, decoherence occurs.

Imperceptible vibrations or slight temperature changes can interfere with quantum superposition and cause decoherence.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. AmericanScientist [Електронний ресурс]. Режим доступу: https://www.americanscientist.org
2. Deloitte [Електронний ресурс]. Режим доступу: https://www2.deloitte.com
3. Medium [Електронний ресурс]. Режим доступу: https://www.medium.com
4. QuantumXC [Електронний ресурс]. Режим доступу: https://quantumxc.com
5. Security Boulevard [Електронний ресурс]. Режим доступу: https://securityboulevard.com

УДК 004.056

ТЕРЕЙКОВСЬКИЙ І. А.,
професор, доктор техн. наук
КПІ ім. Ігоря Сікорського
e-mail: terejkowski@ukr.net

МЕТОД КОДУВАННЯ ОЧІКУВАНОГО ВИХІДНОГО СИГНАЛУ НЕЙРОННОЇ МЕРЕЖІ

В сучасних умовах нейронні мережі є одним із найбільш апробованих засобів обробки інформації, що набули застосування при вирішенні достатньо широкого класу задач [1]. Одним із найбільш апробованих типів нейронних мереж є мережі з прямим розповсюдженням сигналу. Слід зазначити, що до вказаного типу нейронних мереж відносяться двошаровий персептрон, глибокі та згорткові нейронні мережі. При цьому результати [2] вказують на те, що при заданій навчальній вибірці зменшити термін та похибку навчання можливо за рахунок відображення в очікуваному вихідному сигналі навчальних прикладів нейронних мереж близькості еталонів класів, що мають бути розпізнані. Тому метою даної наукової роботи є розробка методу визначення очікуваного вихідного сигналу навчальних прикладів, який забезпечує відображення близькості еталонів, що мають бути розпізнані.

Запропоновано метод кодування очікуваного вихідного сигналу, що базується на попередній обробці навчальних прикладів за допомогою малоресурсної нейронної мережі типу PNN, структура якої показана на рис. 1.

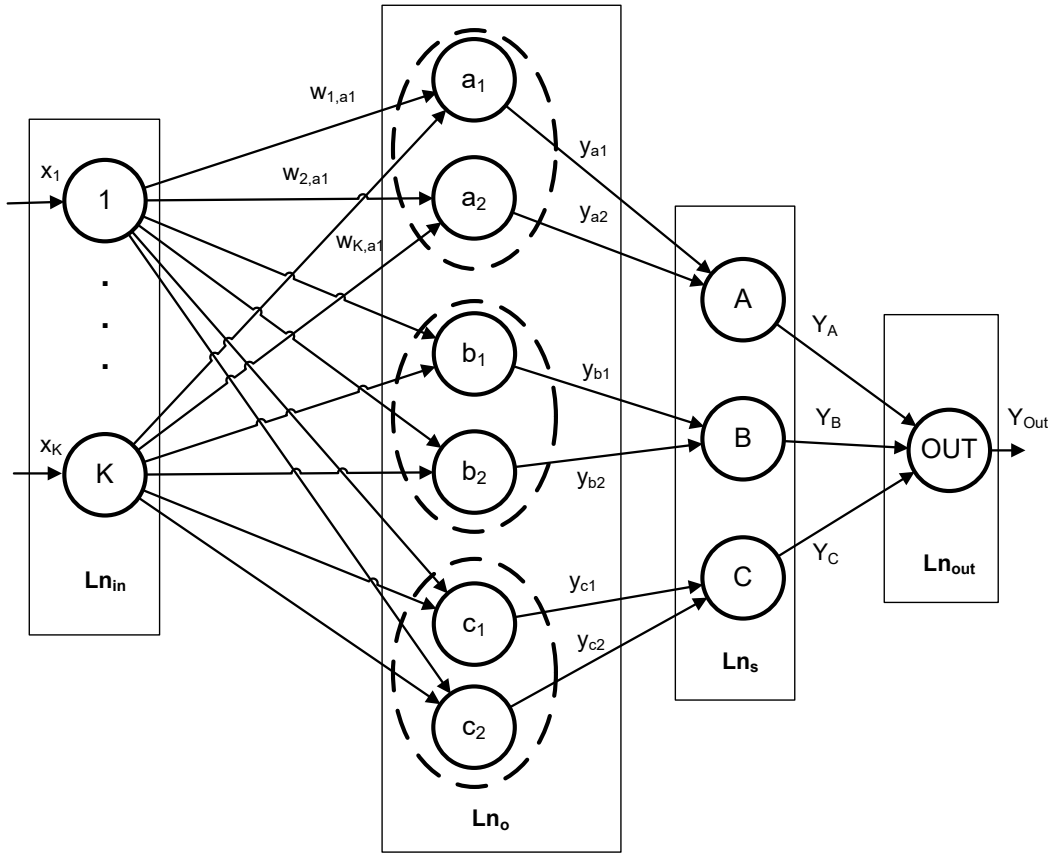


Рис. 1. Приклад структури PNN

Така PNN призначена для розподілу вхідних образів на три класи: A, B та C. Кількість вхідних параметрів дорівнює K. PNN складається із чотирьох нейронних шарів:

– вхідного – Ln_{in},

– образів – Ln_o,

– додавання – Ln_s

– вихідного – Ln_{out}.

Основною особливістю PNN є те, що очікуваний вихідний сигнал такої нейронної мережі визначається у символьному вигляді. Тобто, на відміну від більшості відомих нейронних мереж, в навчальних прикладах PNN вихідний сигнал являється не числом, а назвою еталонного класу до якого він відноситься.

Враховуючи вказану особливість, метод кодування очікуваного вихідного сигналу складається із наступних етапів:

1. Визначити множину класів, що потребують розпізнавання.
2. Сформувати навчальну вибірку, що складається із еталонів класів, які мають бути розпізнані.
3. Побудувати PNN та провести її навчання. Для цього:
   3.1. Визначити множину вхідних нейронів Ln_{in}, що відповідає множині вхідних параметрів.
   3.2. Визначити множину нейронів Ln_s, що відповідає множині класів, які мають бути розпізнані.
   3.3. Визначити множину нейронів Ln_o, що відповідає множині навчальних прикладів.
   3.4. Для кожного із нейронів Ln_o визначити вагові коефіцієнти вхідних зв'язків.
   3.5. Для кожного із нейронів шару образів визначити зв'язок із відповідним нейроном Ln_s.
4. Почергово подати на вхід PNN еталони класів та для кожного із еталонів розрахувати величину вихідного сигналу кожного із нейронів Ln_s.
5. За необхідності отримані величини вихідних сигналів масштабуються [3, 4]. Масштабовані величини і будуть очікуваним вихідним сигналом для еталонів класів.

Висновки. В результаті проведених досліджень розроблено підхід до кодування очікуваного вихідного сигналу нейромережевих моделей з прямим розповсюдженням сигналу, що базується на оцінці близькості еталонів класів за допомогою мережі PNN.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tereikovskyi I. A., Chernyshev D. O., Tereikovska L. A., Mussiraliyeva S. Z. and Akhmed G. Z., 2018. The procedure for the determination of structural parameters of a convolutional neural network to fingerprint recognition. Journal of Theoretical and Applied Information Technology, vol. 97, no. 8, pp. 2381–2392.

2. Tereikovskyi I., Mussiraliyeva S., Kosyuk Y., Bolatbek M. and Tereikovska L., 2018. An experimental investigation of infrasound influence hard drives of a computer system. International Journal of Civil Engineering and Technology, vol. 9, no. 6, pp. 1558–1566.

3. Sambetbayeva A., Tereikovska L., Tereikovskyi I, Mussiraliyeva S., Akhmed and Beketova G., 2019. Recognition of emotions by facial geometry using a capsule neural network. International Journal of Civil Engineering and Technology (IJCIET), no.10, pp. 1424–1434.

4. Tereikovskiy I., Parkhomenko I., Toliupa S. and Tereikovska L., 2018. Markov model of normal conduct template of computer systems network objects. In: 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 20–24 Feb. 2018. Slavske, pp. 498–501.

УДК 004.75

БУРМАКА І. А.,
аспірант кафедри ІТ та ПІ за напрямкм 122 «Комп'ютерні науки»
Національний університет «Чернігівська політехніка»
e-mail: Ivan.Bourmaka@stu.cn.ua

BLOCKCHAIN ТЕХНОЛОГІЯ ЯК ОСНОВА ДЛЯ РОЗПОДІЛЕНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Для захисту корпоративних мереж від вторгнень частіше за все застосовуються розподілені системи виявлення вторгнень, оскільки об'єми трафіку в мережвх постійно зростають, а підходи до проведення атак стають ільше професійними. Але до суттєвих недоліків більшості систем виявлення вторгнень можна віднести не використання глобальної інформації про структуру мережі та розповсюдженння атаки, оскільки частіше за все система виявлення вторгнень захищає лише певну локальну мережу або її фрагмент. Але між іншим вчасне використання інфорації про атаку або спробу атакувати дало б можливість значно ускладнити пошук слабких місць у системі захисту, а інформація про розповсюдження атаки завчасно заблокувати вразливі місця більшої частини систем.

Для вирішення цієї проблеми потрібно змінити архітектуру системи виявлення вторгнень на більш глобальну, яка охоплюватиме значно більшу кількість локальних мереж та їх сегментів, і відповідно інформація між модулями системи виявлення вторгнень буде оперативно передаватися, що дасть можливість при перших ознаках атаки на один їз сегментів мережі підготувати інші сегменти мережі для зменшення негативних наслідків атаки.

Але використання архітектури з наявністю центрального вузла для такої системи недоцільно, оскільки наявність центрального вузла робить систему більш вразливою та менш стабільною. А отже архітектура повинна бути максимально децентралізованою. Одним із шляхів реалізувати це безпечно є технологія Blockchain.

Blockchain – це фактично структура, що являє собою ланцюжок блоків, що поєднані між собою за допомогою криптографічних хешів, при цьому ланцюжок може тільки збільшуватися за рахунок додавання нових блоків. Кожен блок містить в собі хеш попереднього блоку, що дозволяє забезпечити цілісність даних та попередити зміну інформації в попередніх блоках. Кожен блок містить в собі структуру даних у вигляді списка, що дозволяє зберігати певний набір транзакцій [1]. Зазвичай blockchain використовується для побудови криптовалют, але використання Blockchain не обмежується тільки криптовалютами.

У системах виявлення вторгнень blockchain можна використовувати для створення безпечного, децентралізованого, розподіленого сховища для зберігання сигнатурних баз, налаштувань та інформації про виявлені вторгнення та аномалії [2].

Для запобігання підробки блоків зазвичай використовуються алгоритми proof-of-work, proof-of-stake та proof-of-elapsed-time – дані алгоритми дозволяють обмежити неконтрольований випуск та підробку блоків (за умови що більш ніж половина мережі утворена доброчесними вузлами), що значно ускладнює проведення атак на сховище такого типу [3].

Слід мати на увазі що Blockchain передбачає створення сховищ лише в форматі журналу, тобто такого сховища до якого можна тільки додавати нові дані, і не можна змінювати або видаляти старі. Для системи виявлення вторгнень такий варіант сховища цілком придатний, оскільки усі дані з якими працює система в основному тільки додаються (це як сигнатурні бази та налаштування, так і журнали подій).

Отже до переваг використання Blockchain для системи виявлення вторгнень можна віднести:

– створення децентралізованого сховища, яке не залежить від жодного конкретного вузла.

– контроль цілісності даних на усіх вузлах.

– довірений обмін інформацією між вузлами без використання центрального довіреного вузла.

До недоліків Blockchain для систем виявлення вторгнень можна віднести:

– зростання об’ємів внутрішнього трафіка.

– неможливість зміни даних що були записані раніше.

– постійне зростання розміру ланцюжка блоків.

Виходячи з цього можна зробити висновок, що Blockchain можна використовувати в розподілених системах виявлення вторгнень з великою кількість клієнтів, коли коли облік і контроль клієнтів виконати достатньо складно.

Blockchain технологія в системі виявлення вторгнень фактично виконує функцію об’єднуючого компонета, що забезпечує захищений обмін інформацією та її зберігання. І при цьому збільшення кількості blockchain вузлів підвищує надійність та зламостійкість системи.

Розподілена система виявлення вторгнень має містити кілька основних компонентів, включаючи компоненти моніторингу, компоненти блокування, компоненти обробки та контролю, які поєднані між собою в цілісну систему.

Окрім цього для системи виявлення вторгнень на основі Blockchain необхідні компоненти для роботи з Blockchain – повні blockchain вузли та тонкі blockchain клієнти. Повний вузол зберігає у себе повну копію ланцюжка блоків, тоді як тонкий клієнт звертається до повних вузлів для отримання ланцюжка блоків.

При цьому блоки будуть зберігати як інформацію про сигнатури атак так і поточну інформацію про стан усіх вузлів та підозрілу активність виявлену будь-яким із них. При цьому вузли системи виявлення вторгнень фактично утворюватимуть рівноправну peer-to-peer мережу де кожен вузол може працювати самостіно, але ділиться і отримує інформацію від інших вузлів про стан захищеної мережі.

ВИСНОВКИ

Blockchain технологія дозволяє побудувати більш надійну розподілену систему виявлення вторгнень, за рахунок відмови від архітектури зав’язаної на використанні центрального вузла. Архітектура на основі blockchain дозволяє не тільки створити значно масштабніше систему виявлення вторгнень, що буде використовувати дані від багатьох вузлів, а і раціонально розподілити навантаження міжвузлами розподіленої системи виявлення вторгнень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nakamoto S., «Bitcoin: A peer-to-peer electronic cash system», 2008 [Online]. Available: https://bitcoin.org/bitcoin.pdf

2. Li W., Tug S., Meng W., Wang Y. Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems 96, 481–489 (Jul 2019). http://www.sciencedirect.com/science/article/pii/S0167739X18327237

3. Burmaka Ivan, et al. Proof of Stake for Blockchain Based Distributed Intrusion Detecting System. In: International scientific-practical conference. Springer, Cham, 2020. P. 237–247.

УДК 004.942:519.216.3

БЕБЕШКО Б. Т.,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
b.bebeshko@knute.edu.ua.
ЛАЗОРЕНКО В. В.,
старший викладач кафедри цифрової економіки та системного аналізу
Київський національний торговельно-економічний університет
v.lazorenko@knute.edu.ua.
ХОРОЛЬСЬКА К. В.,
асистент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
k.khorolska@knute.edu.ua

БЕЗПЕКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ ЦИФРОВИМИ АКТИВАМИ ЗА ДОПОМОГОЮ МЕТОДУ K-MEANS ПРИ ДОСЛІДЖЕННІ ВИДОБУТКУ ДАНИХ

Однією з тенденцій розвитку кібербезпеки України є створення концепції та впровадження технологій Smart Information Systems. Основними досягнутими результатами повинні стати здатність до спостереження, контрольованість, інтелектуальне керування системи прийняття рішень управління цифровими активами, що забезпечує високу надійність і високі економічні показники роботи. Все більше впровадження знаходять глобальні розподілені системи моніторингу, захисту та управління, в основі яких лежить технологія векторних вимірювань з високою точністю синхронізації просторово рознесених пристроїв. Найбільш повно загальну функціонально-технологічну ідеологію цієї концепції, очевидно, відображає таке визначення Smart Information Systems як концепції «повністю інтегрованої, саморегулюючої і самовідновлювальної системи прийняття рішень управління цифровими активами».

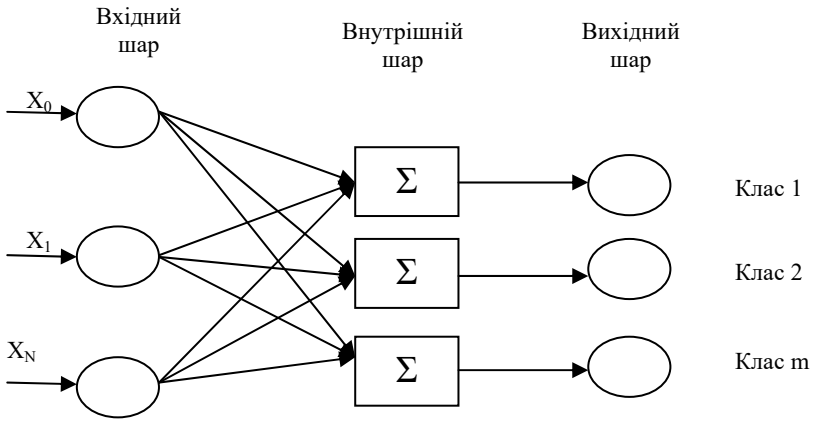
Інтелектуальна система управління цифровими активами передбачає інтеграцію баз даних цифрових активів з новими електронними комунікаціями і цілісною багатоконтурною системою прийняття рішень. Оскільки в такій системі передбачається самостійне прийняття рішень системою, то важливою складовою постає створення системи виявлення вторгнень як частини цілісної системи.

Ми пропонуємо розглянути варіант створення системи виявлення вторгнень на основі інтелектуальної технології аналізу даних (Data Mining). Саме такі математичні і програмні методи та засоби, що дозволяють виявляти невідомі раніше закономірності і тенденції в даних, які неможливо або важко виявити при традиційному аналізі через великі обсяги даних або їх складність.

Основою системи є передбачувані класи Data Mining, які дозволяють побачити нові факти вторгнення до системи. [1]

Одними із методів Data Mining які дозволяють прослідковувати певні закономірності та надавати їм оцінку є використання нейронних мереж Кохонена та карт Кохонена. [2]

Мережа Кохонена навчається методом послідовних наближень. Починаючи з випадковим чином обраного вихідного розташування центрів, алгоритм поступово покращується для кластеризації навчальних даних. Проте, алгоритм може працювати і на іншому рівні. В результаті ітеративної процедури навчання мережа організовується таким чином, що елементи, які відповідають центрам, розташованим близько один від одного в просторі входів, будуть розташовані близько один від одного і на топологічній карті.



На вході мережа отримую всю інформацію про вторгнення, яка надходить в результаті діяльності, після чого проходить процес групування однотипних надходжень за подібними критеріями. Після опрацювання інформації та побудови мережі на виході ми можемо отримати відповідь по вирішенню загрози вторгнення, які ми можемо задати попередньо в нашу систему з прийняття рішень.

Коли система отримує інформацію в результаті побудови мережі вона аналізує існуючі типи вторгнень, якщо є відповідності то виводиться інформація про можливі варіанти вирішення даної проблеми, в іншому випадку, коли система не знаходить можливості вирішення, вона має надати інформацію про новий тип загрози, який має бути опрацьований користувачем. Після вирішення проблеми, якої не було в системі вона додає його до варіантів, які користувач отримує після побудови мережі та можливих варіантів її вирішення. Таким чином система проходить самонавчання, для вирішення раніше невідомих проблем після їх вирішення користувачем.

Система побудови мережі функціонує за наступним алгоритмом:

1. Ініціалізація мережі. Ваговим коефіцієнтам мережі надаються малі випадкові значення. Початкова зона сусідства показана.

2. Пред'явлення мережі нового вхідного сигналу.

3. Обчислення відстані до всіх нейронів мережі:

Відстані d_j від вхідного сигналу до кожного нейрона j визначаються за формулою:

$$d_j = \sum_{i=1}^{N} (x_i(t) * w_{ij}(t))^2$$

де x_i – i-й елемент вхідного сигналу в момент часу t,

$w_{ij}(t)$ – вага зв'язку від і-го елемента вхідного сигналу до нейрона j у момент часу t.

4. Вибір нейрона з найменшою відстанню:

Вибирається нейрон-переможець j^*, для якого відстань d_j найменше.

5. Налаштування ваг нейрона j^* і його сусідів:

Робиться налаштування ваг для нейрона j^* і всіх нейронів з його околу NE. Нові значення ваг:

$$(t+1) = w_{ij}(t) + r(t)(x_i(t) - w_{ij}(t))$$

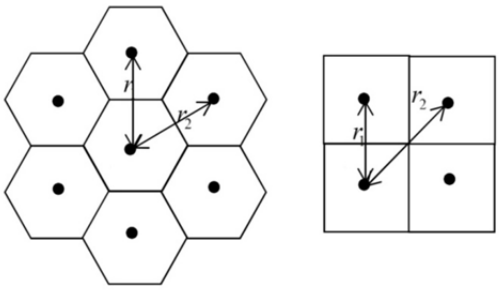
де $r(t)$ – швидкість навчання, що зменшується з часом (додатне число, менше одиниці).

6. Повернення до кроку 2.

В алгоритмі використовується коефіцієнт швидкості навчання, який поступово зменшується, для тоншої корекції на новій епосі. В результаті позиція центру встановлюється в певній позиції, яка задовільним чином кластеризує приклади, для яких даний нейрон є переможцем. [4]

Карти Кохонена (самоорганізуючі карти, або SOM) [5–7] призначені для візуального представлення багатовимірних властивостей об'єктів на площині з двома осями. Карти Кохонена проводять відображення вхідних даних високої розмірності на елементи регулярного масиву малої розмірності (зазвичай, двовимірного). Відмінність карт і мереж Кохонена полягає в тому, що в карті нейрони, які є центрами кластерів, впорядковані в деяку структуру (зазвичай двовимірну сітку). В результаті близькі за деякою метрикою вхідні вектори в мережі Кохонена відносяться до одного нейрона (центру кластера), а в карті Кохонена можуть ставитися до різних близько розташованим на сітці нейронів. Зазвичай нейрони розташовуються у вузлах двовимірної сітки з прямокутними або шестикутними осередками.

Нейрони-сусіди визначаються відстанню між нейронами на карті. [5–7] На рисунку показані шестикутні і прямокутні осередки, в центрах яких розташовуються нейрони. Шестикутні осередки більш коректно відображають декартову відстань між об'єктами на карті, так як для цих осередків відстань між центрами суміжних осередків однакові.



Отже, подібна система виявлення вторгнень у порівнянні з традиційними заходами безпеки має великі переваги. Може вирішити недоліки оригінального пасивного натхнення, може також обробити його до виникнення пошкодження.

Згідно стратегії кібербезпеки України, одним з пріоритетних напрямків її забезпечення є створення таких систем своєчасного виявлення, запобігання та нейтралізації кіберзагроз і створення умов для впровадження в Україні сучасних технологій кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ситюк В. Є. Прогнозування. Моделі. Методи. Алгоритми: навч. посіб. Київ: Маклаут, 2008. 364 с.

2. Олещук О. В., Попель О. Є., Копитчук М. Б. Моделювання повнозв'язної нейронної мережі з використанням технології CUDA // Вісник Національного університету «Львівська політехніка». 2012. № 747. С. 131–139.

3. Lakhno V., Malyukov V., Kryvoruchko O., Desiatko A. Model of evaluating smart city projects by group of investors using a multifactorial approach. Appl. Technol. First Int. Conf. 1193: 13–27 (2020). https://doi.org/10.1007/978-3-030-42517-3_2 8.

4. Димо О. Б., Морозова Г. С. Використання нейронної мережі Кохонена у проектах розпізнавання рекламних текстів // Управління проектами та розвиток виробництва. 2010. № 4. С. 50–56.

5. Lakhno V., Matus Y., Malyukov V., Desiatko A. Smart city cybersecurity projects financing model in case of description of investors' resources with fuzzy. IEEE Int. Conf. Adv. Trends Inf. Theory: 249–252 (2019). https://doi.org/10.1109/ATIT49449.2019. 9030499

6. Beale M. H., Hagan M. T., Demuth H. B. Neural Network Toolbox. User's Guide. Natick: Math Works, Inc., 2015. 406 p.

УДК 004.415

ВІКТОРОВ В. В.,
аспірант кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
121-18-M-viktorov@knute.edu.ua.
ЗАХАРОВ Р. Г.,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
r.zakharov@knute.edu.ua

КІБЕРГІГІЄНА – БЕЗПЕЧНИЙ ОСОБИСТИЙ ІНФОРМАЦІЙНИЙ ПРОСТІР

Кількість інтернет-шахрайств, фактів втручання в особистий інформаційний простір, поширення неправдивих відомостей тощо нині набуває рис епідемії. Тож таке поняття як кібергігієна є звичайною та актуальною темою сьогодення. основні Виклики сучасного технічного прогресу вимагають знання загроз в цифровому просторі, розуміння, яка інформація є головною метою хакерів та засвоєння основних рекомендації щодо захисту власних даних, а також безпечного користування гаджетами та інформаційними ресурсами.

Слід звернути увагу на збільшенням отримання фішингових листів в інформаційному просторі суспільства, що містять шкідливе програмне забезпечення урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA (спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України) пропонує основні правила кібергігієни:

1. Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів та не відкривати файли навіть з безпечними розширеннями.
2. Не переходьте за невідомими посиланнями та не завантажуйте файли, що мають потенційно небезпечне розширення (наприклад: *.exe,.bin,.ini,.dll,.com,.sys,.bat,.js* тощо) та навіть безпечне (наприклад: *.docx,.zip,.pdf*), адже можуть використовуватися вразливості, макроси та інші небезпеки.
3. Проводьте роз'яснювальну роботу з підлеглими, що мають доступ до мережі Інтернет та працюють з поштовими агентами.
4. Використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлюйте.
5. Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу.
6. Здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштуйте функцію «відновлення системи».
7. Забороніть доступ до мережі Інтернет програмам, які потенційно можуть бути використані зловмисниками, якщо це не вплине на стабільність їх роботи.

Дотримання всіх цих правил ускладнить процес використання гаджетів. Але не варто забувати, що профіт від дотримання кібергігієни з легкістю нівелює будь-який дискомфорт. Безпека перед усім.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016».

УДК 621.396.42

ГАРИСТ А. В.,
старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України
garist@ukr.net

ПРОГРАМНО ОБУМОВЛЕНІ РАДІОСИСТЕМИ ТА АТАКИ НА НАВІГАЦІЙНІ СИСТЕМИ

У галузі кібербезпеки програмно обумовлені радіо системи (далі – ПОРС) відкрили новий напрямок розвитку. З'явився новий вектор атаки, з яким не зрозуміло що робити. Зараз з допомогою ПОРС зламують автомобілі, декодують GSM, прослуховують спеціальний зв'язок. Велика кількість елементів критичної інфраструктури використовує технології радіозв'язку при проектуванні яких ніхто не задумувався про можливі атаки.

Для навігації і зв'язку використовуються наступні основні системи:

– ILS (Instrument Landing System) – курсо-глісадна система. Це система, в якій кутові координати визначаються методом порівняння коефіцієнтів амплітудної модуляції сигналу частоти-носія сигналами з частотою 90 Гц і 150 Гц.

– ADS-B (Automatic dependent surveillance-broadcast) – автоматична система спостереження і радіомовлення, ця система базується на технології Global Positioning System (далі – GPS). Вона два рази в секунду видає у відкритий ефір стислий 120-бітний сигнал, що містить код судна, його координати, швидкість та параметри бортових систем.

– висотомір (альтіметр). Це ключовий компонент, який призначений для вимірювання висоти. За принципом побудови висотоміри діляться на барометричні, радіотехнічні, інерційні, іонізаційні та інші. На бортах літаків використовуються барометричні висотоміри, які вимірюють атмосферний тиск повітря за бортом.

Для виводу з ладу систем навігації літака навіть не потрібно імітувати сигнали курсового і глісадного радіомаяків, досить просто поставити перешкоду, і в умовах поганого бачення це точно створить дискомфорт для пілота. Звичайно джерело перешкоди досить швидко вирахують за допомоги систем моніторингу радіоспектра, але це все займе певний час. За допомогою покупних ПОРС можна генерувати сигнали ADS-B та передавати дані на диспетчерську вежу про неіснуючий літак або поставити коротку імпульсну перешкоду та «псувати» оригінальний сигнал і передавати слідом хибні повідомлення. Враховуючи дуже високу густина трафіку над великими містами, це потенційно несе загрозу. Для отримання координат борту ADS-B система використовує сигнал GPS. Супутники GPS знаходяться на орбіті приблизно 20 000 км та мають передавачі потужністю 20 Вт. Сигнал приходить на землю з дуже низькою потужністю – 150 дБм, тому його доводиться відокремлювати від шумів за допомогою кореляційної обробки. Тому, щоб заглушити такий сигнал, потрібна дуже незначна потужність. ПОРС з вихідною пікової потужністю 1 Вт може «закривати» кілометри на відкритій місцевості.

На GPS є два види атак:

– джамінг – постановка перешкоди, при якій супутники «зникають»;

– спуфінг – генерація хибних сигналів, приймач показує невірні координати та час.

Джамінг не такий небезпечний, так як визначається одразу. Зі спуфінгом усе набагато складніше, адже можна імітувати точні координати і відводити ціль не поспішаючи, додаючи зміщення, наприклад, по висоті. Кожна атака сама по собі навряд чи представляє серйозну загрозу, але в поєднанні з умовами поганого бачення і одночасною атакою на ILS і GPS системи, може створити серйозну загрозу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мелкумян В. Г., Семенов А. А., Соломцев О. В. Радіолокаційне та радіонавігаційне обладнання аеропортів. Київ: НАУ, 2006. 218 с.

УДК 004.056.5

ГНАТЧЕНКО Д. А.,
провідний науковий співробітник
Український науково-дослідний інститут
спеціальної техніки та судових експертиз Служби безпеки України
e-mail: hnatchenko.d@gmail.com
МАКАРЕНКО К. Р.,
здобувач вищої освіти ОС «магістр»,
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: MakarenkoKatyaphoto@gmail.com

МЕХАНІЗМ ЗАХИСТУ АВТЕНТИФІКАЦІЇ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Аутентифікація – це процедура встановлення належності користувачеві інформації в системі його ідентифікатора. Терміни аутентифікації та авторизації часто використовуються як взаємозамінні. Хоча вони часто можуть бути реалізовані разом, ці дві функції відрізняються. Аутентифікація є процесом перевірки ідентичності зареєстрованого користувача перед тим, як дозволити доступ до захищеного ресурсу, в той час як авторизація є процесом перевірки того, що авторизований користувач отримав дозвіл на доступ до запитаних ресурсів. Процес, за допомогою якого доступ до цих ресурсів обмежується певною кількістю користувачів, називається контролем доступу. Процес аутентифікації завжди проходить до процесу авторизації.

Мета дослідження – розглянути існуючі напрацювання з проблематики захисту інформації та контролю доступу.

Аутентифікація користувача відбувається в межах більшості взаємодій від людини до комп'ютера. Аутентифікація користувачів дозволяє автономно взаємодіяти з машиною в операційних системах і додатках, а також як дротових, так і бездротових мережах для забезпечення доступу до мережних і підключених до Інтернету систем, програм і ресурсів. Багато компаній використовують аутентифікацію для перевірки користувачів, які входять до їхніх веб-сайтів. Без відповідних заходів безпеки дані про користувачів, такі як номери кредитних і дебетових карт, а також номери соціального страхування, можуть потрапити в руки кіберзлочинців. Організації також використовують аутентифікацію, щоб контролювати, які користувачі мають доступ до корпоративних мереж і ресурсів, а також визначати та контролювати, які машини та сервери мають доступ. Компанії також використовують аутентифікацію, щоб дозволити віддаленим працівникам безпечно отримувати доступ до своїх програм і мереж. Для підприємств та інших великих організацій аутентифікацію можна здійснити за допомогою системи єдиного входу (SSO), яка надає доступ до декількох систем з єдиним набором облікових даних для входу.

Традиційно аутентифікація виконувалася за допомогою систем або ресурсів, до яких здійснювався доступ; наприклад, сервер автентифікує користувачів, використовуючи власну систему паролів, реалізовану локально, використовуючи ідентифікатори для входу (імена користувачів) і паролі. Знання облікових даних для входу в систему вважається гарантією, що користувач є автентичним. Кожен користувач спочатку реєструється (або реєструється іншим, наприклад, системним адміністратором), використовуючи призначений або самостійно створений пароль. При кожному наступному використанні користувач повинен знати і використовувати попередньо оголошений пароль.

Проте протоколи додатків мережі, HTTP і HTTPS, не мають статусу, а це означає, що сувора аутентифікація потребує повторної аутентифікації кінцевих користувачів кожного

разу, коли вони отримують доступ до ресурсу за допомогою HTTPS. Замість того, щоб навантажувати кінцевих користувачів цим процесом для кожної взаємодії через Інтернет, захищені системи часто покладаються на аутентифікацію на основі маркерів, в якій аутентифікація виконується один раз на початку сеансу. Система аутентифікації видає підписаний маркер аутентифікації програмі кінцевого користувача, і цей маркер додається до кожного запиту від клієнта.

Аутентифікацію об'єктів для систем і процесів можна здійснювати за допомогою облікових даних машини, які працюють як ідентифікатор користувача та пароль, за винятком того, що дані облікового запису автоматично подаються відповідним пристроєм. Вони також можуть використовувати цифрові сертифікати, які були видані та перевірені центром сертифікації як частину інфраструктури відкритого ключа для аутентифікації особи при обміні інформацією через Інтернет.

Аутентифікація користувача з ідентифікатором користувача і паролем зазвичай вважається основним типом аутентифікації, і це залежить від того, що користувач знає дві частини інформації: ідентифікатор користувача або ім'я користувача і пароль. Оскільки цей тип аутентифікації спирається тільки на один фактор аутентифікації, це тип однофакторної аутентифікації. Сильна аутентифікація – це термін, який формально не був визначений, але зазвичай використовується, щоб означати тип аутентифікації, який є більш надійним і стійким до атаки, що досягається завдяки використанню принаймні двох різних типів факторів аутентифікації. Фактор аутентифікації являє собою деякий фрагмент даних або атрибут, який може використовуватися для аутентифікації користувача, який запитує доступ до системи. Наразі використовуються такі фактори аутентифікації:

- Фактор знань: «Те, що ви знаєте».
- Фактор володіння: «Те, що у вас є».
- Фактор невідповідності: «Те, ким ти є».
- Фактор розташування: «Де ви знаходитесь».
- Фактор часу: «Під час аутентифікації».

Спосіб аутентифікації заснований на принципі: «те, що ти знаєш» – це найпопулярніший і часто використовуваний механізм аутентифікації на сьогоднішній день. Він являє собою введення пароля або іншої інформації, яку знаєш тільки ти. У теорії цей механізм вважається одним з найпростіших і надійних, через криптостійкість. Але на практиці не завжди це твердження вірно. Це пояснюється тим, що для надійності пароля для підтвердження автентичності особистості в ідеалі повинні використовуватися складні і довгі паролі, довжиною не менше 8 символів, змінюватися з періодичністю хоча б раз на півроку. Проте, більшість людей не дотримуються рекомендацій при створенні пароля і подальшій зміні його для безпеки системи. Так само варто зауважити і те, що людям легше запам'ятати паролі, які складаються з слів, що мають деяку асоціацію в їх пам'яті. Це так само не додає надійності паролям. Адже в наш час величезна кількість зловмисників можуть підібрати пароль простим перебором по словнику.

Інший вид механізму аутентифікації, який найчастіше використовують, якщо був забутий пароль, є секретне питання. Ще при реєстрації людина вибирає питання, на яке, в разі втрати пароля, можна дати відповідь, відповідь вказується при реєстрації. І в разі коректної відповіді на секретне питання, система дає можливість відновити пароль, найчастіше створивши новий. Але є недолік в механізмі з секретним питанням і відповіддю на нього, у такого механізму криптостійкость ще менше ніж у звичайного пароля. Адже більшість секретних питань, це те на що може відповісти не тільки власник пароля, а й люди, що добре знають власника ідентифікаційних даних.

Аутентифікація за паролем. Аутентифікація за паролем – метод аутентифікації, що базується на логіні та паролі, що відноситься до класифікації «те, що ти знаєш», наведенної вище. Якщо розглядати цей метод аутентифікації у Web-застосунках, то існує декілька стандартних протоколів аутентифікації за паролем:

- HTTP аутентифікація;
- Forms аутентифікація.

Аутентифікація за сертифікатами. «Сертифікат являє собою набір атрибутів, що ідентифікують власника, підписаний certificate authority (CA). CA виступає в ролі посередника, який гарантує справжність сертифікатів. Також сертифікат криптографічно пов'язаний з закритим ключем, який зберігається у власника сертифіката і дозволяє однозначно підтвердити факт володіння сертифікатом...» [1].

Сертифікат може зберігатися в операціонній системі, в браузері або на окремому фізичному пристрої, такому як смарт картка або токен USB. А закритий ключ захищається, зазвичай, ще паролем.

Цей спосіб є більш надійним ніж аутентифікації за паролем, але в зв'язку з важкістю розповсюдження сертифікатів, цей метод аутентифікації є менш популярним.

Аутентифікація за одноразовими паролями. Цей метод аутентифікації використовується як другий рівень аутентифікації для двофакторної аутентифікації. Цей метод базується на принципі, що користувач для аутентифікації спочатку використовує аутентифікацію за паролем, а потім аутентифікацію за тим, що він має, наприклад фізичний пристрій для генерації одноразового ключа.

Зазвичай такий метод аутентифікації використовують, як доповнення до аутентифікації forms. Після створення токену сесії, користувач не буде мати доступ до Web-застосунку поки не виконає аутентифікацію за одноразовим паролем [2].

Але цей метод аутентифікації є досить ненадійним через можливість сніффінгу, тобто перехоплення мережевих пакетів з одноразовим паролем, або, якщо це апаратне рішення, то поблизу може не бути зчитувача.

Аутентифікація за ключами доступу. Цей метод аутентифікації використовується для застосунків та сервісів при їх звернені до Web-сервісів. Для аутентифікаціїї в даному методі використовються ключі доступу, наприклад access key, API key. Ключі доступу – це довгі унікальні строки, що являють собою рандомний набір символів.

Зазвичай користувачі, які хочуть отримати доступ до Web-сервісу роблять запит на створення ключа доступу і в подальшому зберігають його у клієнтському застосунку. Цей ключ може давати не повний доступ до ресурсу після аутентифікації, це може бути задано при створенні ключа доступу.

Так як ключ доступу є випадково підібраними символами, його складніше буде підібрати, на відміну від звичайного пароля. І у випадку компрометації ключа, його можна анулювати і створити новий.

Аутентифікація за токенами. Даний метод аутентифікації використовується зазвичай для розподілених систем Single Sign-On (SSO), де аутентифікація відбувається за рахунок іншого сервісу, наприклад здійснення аутентифікації через обліковий запис соціальних мереж. Соціальні мережі виступають в ролі сервіса аутентифікації.

Токен – це структура даних, що складається з інформації: строк дії токена, відправник, можливий отримувач токену та деяка інформація про користувача, що здійснив запит на створення токену. Токен для збереження цілісності даних і захисту від несанкціонованого змінення даних додатково підписується.

Одними з найрозповсюджених форматів токенів є: Simple Web Token (SWT), JSON Web Token (JWT), Security Assertion Markup Language (SAML).

Для даного методу аутентифікації використовуються стандарти, що описують протокол взаємодії між клієнтами та IP і SP застосунками, також, як і формат токенів, що надсилаються. До таких стандартів належать: стандарт SAML, стандарт WS-Trust, стандарт WS-Federation, стандарт OAuth,стандарт OpenID Connect.

Стандарт SAML складається з assertions, protocols, bindings, profiles, де assertions формат токенів стандарту SAML у форматі XML, protocols виступає набором повідомлень, наприклад запит на створення нового токену, отримання існуючих токенів, вихід з системи, управління ідентифікаторами користувачів тощо, bindings – це механізми передачі повідомлень через транспортні протоколи, profiles – типові сценарії стандарту, що визначають набір перших трьох пунктів assertions, protocols та bindings.

Стандарт WS-Trust описує інтерфейс сервісу авторизації Secure Token Service (STS). Стандарт працює по протоколу SOAP і підтримує створення та анулювання токенів і використовує зазвичай SAML-токени.

Стандарт WS-Federation відноситься до механізму обміну токенами. При цьому WS-Federation розширює функції сервісу STS. Він вирішує ті ж самі задачі, що й SAML, але має інші підходи і реалізацію.

Стандарт OAuth (Open Authorization) на відміну від інших стандартів не описує протокол аутентифікації користувача. Він визначає механізм отримання доступу одного застосунку до іншого від імені користувача. Роботу стандарту можна описати так:

1. Користувач дає згоду застосунку на доступ до певного ресурсу у виді гранту.
2. Застосунок отримує токен доступу до ресурсу від сервера авторизації в обмін на свій грант.
3. Застосунок використовує токен для отримання даних від сервера ресурсів.

Гранти бувають чотирьох видів:

- Authorization Code – цей грант надається після аутентифікації і підтвердження про надання доступу до ресурсу.
- Implicit – використовується при неможливості безпечно отримати токен від серверу авторизації, при такому розкладі грант є токеном, отриманим від серверу авторизації без другого кроку, описаного вище.
- Resource Owner Password Credentials – грант виступає логіном і паролем користувача, шо використовується, якщо застосунок є інтерфейсом для сервера ресурсів.
- Client Credentials – грант використовується при відсутності користувача і застосунок отримує доступ завдяки ключам доступу і тоді перший крок виключається з процесу, описаного вище.

Стандарт OpenID Connect розробленний як доповнення до облікових даних OAuth. Сервер авторизації надає додатковий токен формату JWT ідентифікації на другому кроці.

Двофакторна аутентифікація – це механізм аутентифікації, заснований на двох різних методах аутентифікації для більш ефективного захисту системи від несанкціонованого входу. У двофакторній аутентифікації перший рівень аутентифікації – це метод аутентифікації з паролем та логіном, а для другого рівня аутентифікації частина інформації надається з центрального сховища. Хоча двофакторна аутентифікація підвищує рівень безпеки з другим рівнем аутентифікації, він все ще стикається з недоліком, що централізована база даних зберігає список секретної інформації про користувача. Центральна база даних може бути підроблена або пошкоджена атаками зловмисника, і це може призвести до масових порушень даних.

Отже, аутентифікація є важливою, оскільки вона дозволяє організаціям підтримувати безпеку своїх мереж, дозволяючи лише авторизованим користувачам отримувати доступ до захищених ресурсів, які можуть включати комп'ютерні системи, мережі, бази даних, вебсайти та інші мережеві програми або служби. Системи і процеси можуть також потребувати авторизації своїх автоматизованих дій в мережі. Кожен метод аутентифікації має свої переваги і недоліки. На сьогоднішній день для більш ефективного захисту систем використовують комбінацію механізмів захисту, що знижує ризик з можливих недоліків і підвищує рівень безпеки системи, так звану двофакторну аутентификацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Виростков Д. Огляд способів і протоколів аутентифікації в веб- додатках [Електронний ресурс] / Д. Виростков. 2015. Режим доступу: https://habr.com/ru/company/dataart/blog/262817

2. Malan. Класифікація механізмів аутентифікації користувачів і їх огляд [Електронний ресурс] / Malan. 2013. Режим доступу: https://habr.com/ru/post/177551

УДК 621.396.42

ЖЕРЕБЕЦЬ О. М.,
начальник відділу
Український науково-дослідний інститут спеціальної техніки
та судових експертиз СБ України
amixal@ukr.net

ПРОГРАМНО ОБУМОВЛЕНІ РАДІОСИСТЕМИ ТА АТАКИ НА WIFI МЕРЕЖІ

Програмно обумовлені радіо системи (далі – ПОРС) відкрили новий вектор атак у галузі кібербезпеки. Розглянемо можливість зламати мережу WiFi з шифруванням WPA/WPA2 шляхом перехоплення handshake.

В протоколі захищеного доступу WPA (Wi-Fi Protected Access) зазвичай використовується протокол цілісності тимчасового ключа TKIP (*Temporal Key Integrity Protocol*). TKIP є частиною стандарту IEEE 802.11. TKIP був розроблений для підвищення шифрування WEP (*Wired Equivalent Privacy*), який не потребує зміни обладнання для роботи. WPA2 в обов'язковому порядку використовує алгоритм шифрування AES-CCMP.

WPA і WPA2 дозволяють використовувати або EAS-bases аутентифікацію (RADIUS Server «Enterprise») або Pre-Shared Key (PSK) «Personal»-based аутентифікацію. Шифрування WPA / WPA2 PSK уразливі до атак за словником. Для здійснення цієї атаки, необхідно отримати 4-way WPA handshake між wifi-клієнтом і точкою доступу (AP), а також словник що містить парольний фразу.

WPA / WPA2 PSK працює наступним чином: він випливає з ключа попередньої сесії, яка називається Pairwise Transient Key (PTK). PTK, в свою чергу використовує Pre-Shared Key і п'ять інших параметрів – SSID, Authenticator Nounce (ANounce), Supplicant Nounce (SNounce), Authenticator MAC-address (MAC-адресу точки доступу) і Suppliant MAC-address (MAC-адреса WiFi-клієнта). Цей ключ надалі використовує шифрування між точкою доступу (AP) і wifi-клієнтом.

За допомогою ПОРС, при прослуховуванні ефіру, можливо перехопити всі п'ять параметрів. Pre-Shared key залишається єдиним параметром який не можливо отримати при прослуховуванні ефіру. Pre-Shared key створюється завдяки використанню парольної фрази WPA-PSK, яку відправляє користувач, разом з SSID. Комбінація цих двох параметрів пересилається через Password Based Key Derivation Function (PBKDF2), яка виводить 256-bit'овий загальний ключ.

У атаці по словнику буде виводитись 256-bit'овий Pre-Shared Key для кожної парольної фрази та буде використовуватись з іншими параметрами, які були визначені за допомогою ПОРС. PTK буде використовуватися для перевірки Message Integrity Check (MIC) в одному з пакетів handshake.

У атаці KRACK (Key Reinstallation Attack) використовується вразливість в протоколі handshake яка дозволяє примусити клієнта повторно використати вже наявний ключ шифрування. Повторне використання (reinstall) відбувається в такий спосіб, що клієнт вимушений скинути лічильник пакетів криптографічного нонса та інші параметри до їх початкових значень. Атака спроможна знайти шлях для обходу шифрування завдяки повторному використанню нонса.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wi-Fi Alliance® introduces security enhancements. // Wi-Fi Alliance. 2018. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements

2. DAN GOODIN. Serious flaw in WPA2 protocol lets attackers intercept passwords and much more. // Ars Technica. https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/

УДК 004.38:37.013.42

ЦЕНЗУРА М. О.,
доцент, канд. техн. наук
Київський національний торговельно-економічний університет
email: zna-foaek@knute.edu.ua

ЗАХИСТ ЕЛЕКТРОННИХ НАВЧАЛЬНО-МЕТОДИЧНИХ ВИДАНЬ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Заходи, щодо захисту повинні бути адекватні потенційному збитку, який може бути нанесений в тому випадку, якщо загроза здійсниться. Сучасний підхід до вирішення цієї проблеми полягає в застосуванні принципів ситуаційного управління. При такому підходу необхідний рівень безпеки встановлюється відповідно до ситуації, яка визначається співвідношенням між цінністю методичного видання та витратами, які необхідні для досягнення цього рівня.

Вибираючи захисні заходи, необхідно враховувати не тільки прямі витрати на закупівлю програм, але і витрати на навчання і перепідготовку персоналу. Зарубіжний досвід в області захисту інтелектуальної власності та вітчизняний досвід показують, що ефективною може бути тільки комплексний захист, що поєднує в собі такі напрямки захисту, як правове і організаційне.

Правовий напрямок передбачає формування сукупності законодавчих актів, нормативно-правових документів, вимоги яких є обов'язковими в системі захисту інформації. Організаційний напрям – це регламентація виробничої діяльності на нормативно-правовій основі таким чином, що розголошення, витік і несанкціонований доступ до інформації стають неможливими або істотно неможливими.

До організаційних заходів належать:

– підтримка надійного пропускного режиму, охорони приміщень;

– зберігання і використання документів та носіїв інформації;

– підбор персоналу.

Одним з компонентів організаційного забезпечення інформаційної безпеки ЗВО є інформаційно-обчислювальний центр-головний центр інформаційних технологій (ІОЦГЦІТ). Саме від професійної підготовленості співробітників служби ІОЦГЦІТ багато в чому залежить ефективність заходів щодо захисту інформації.

Для забезпечення успішної роботи ІОЦГЦІТ необхідно визначити її права і обов'язки, а також правила взаємодії з іншими підрозділами з питань захисту інформації.

Під програмним забезпеченням безпеки інформації розуміється сукупність спеціальних програм, що реалізують функції захисту інформації та режиму функціонування.

Сформована сукупність правових, організаційних та інженерно-технічних заходів перетворюється у відповідну політику безпеки.

Політика безпеки визначає структуру системи захисту інформації у вигляді сукупності організаційних заходів, правових норм, комплексу програмно-технічних засобів і процедурних рішень, спрямованих на протидію загрозам для мінімізації можливих наслідків прояву інформаційних впливів. Після прийняття того чи іншого варіанту політики безпеки необхідно оцінити рівень безпеки інформаційної системи. Оцінка захищеності проводиться за сукупністю показників, основними з яких є вартість, ефективність, реалізація.

Коли намічені заходи прийняті, необхідно перевірити їх дієвість, тобто переконатися, що залишкові ризики стали прийнятними.

Один з можливих способів атестації безпеки системи – запрошення хакерів для злому без попереднього повідомлення персоналу. Для цього виділяється група з двох-трьох чоловік, що мають високу професійну підготовку.

Поряд з таким способом використовуються програмні засоби тестування.

Якщо ЗВО здійснює обмін електронними методичними матеріалами з партнерами, то необхідно в план захисту включити договір про порядок організації обміну електронними матеріалами, в якому відображаються наступні питання:

– розмежування відповідальності суб'єктів, що беруть участь в процесах обміну електронними документами;

– визначення порядку підготовки, оформлення, передачі, прийому, перевірки автентичності та цілісності електронних матеріалів;

– порядок вирішення спорів у разі виникнення конфліктів.

План захисту інформації – це пакет текстово-графічних документів, тому поряд з наведеними компонентами цього пакета в нього можуть входити:

– положення про комерційну таємницю, що визначає перелік відомостей, які становлять комерційну таємницю, і порядок його визначення, а також обов'язки посадових осіб щодо захисту комерційної таємниці;

– положення про захист інформації, яка регламентує всі напрямки діяльності по реалізації політики безпеки, а також ряд додаткових інструкцій, правил, положень, що відповідають специфіці інформації.

Реалізація плану захисту (управління системою захисту) передбачає розробку необхідних документів, укладання договорів з постачальниками, монтаж і налаштування обладнання та ін. Після формування системи захисту інформації вирішується завдання її ефективного використання, тобто управління безпекою. Управління – процес цілеспрямованого впливу на об'єкт, який здійснюється для організації його функціонування за заданою програмою.

Аналіз вітчизняного та зарубіжного досвіду переконливо доводить необхідність створення цілісної системи інформаційної безпеки, яка погоджує правові, оперативно-технічні та організаційні заходи захисту. Причому система безпеки повинна бути оптимальною з точки зору співвідношення витрат і цінності ресурсів. Необхідна гнучкість і адаптація системи до швидко мінливих чинників навколишнього середовища, організаційної та соціальної обстановці в установі. Досягти такого рівня безпеки неможливо без проведення аналізу існуючих загроз і можливих каналів витоку інформації, а також без вироблення політики інформаційної безпеки. У підсумку повинен бути створений план захисту, який реалізує принципи, закладені в політиці безпеки.

Таким чином, практична діяльність в області підвищення економічної та інформаційної безпеки наочно демонструє, що створення реально діючої системи захисту інформації знаходиться в сильній залежності від своєчасного вирішення перерахованих проблем. Однак всі розглянуті питання успішно вирішуються за умови щільної спільної роботи представників замовника і виконавця. Головне – усвідомити важливість проведення таких робіт, своєчасно виявити існуючі загрози і застосувати адекватні заходи протидії, які, як правило, специфічні для кожного конкретного ЗВО. Наявність бажання і можливостей є достатньою умовою для плідної роботи, метою якої стало б створення комплексної системи забезпечення безпеки навчального закладу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (Відомості Верховної Ради України, 2005 р., № 26, ст. 347; 2014 р., № 22, ст. 816).

2. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки // Стратегічні приоритети. 2012. No 3(24). С. 15.

3. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly. 2000. № 55/28. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/07/PDF/N0056107.pdf?OpenElement

4. The Department of Defense Cyber Strategy. URL: https://strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

УДК 004.056.5

ЦЮЦЮРА С. В.,
професор кафедри інформаційних технологій, доктор технічних наук, професор,
спеціальність 122 «Комп'ютерні науки»
Київський національний університет будівництва і архітектури
e-mail: svtsutsura@gmail.com.
КИЇВСЬКА К. І.,
доцент кафедри інформаційних технологій, кандидат технічних наук, доцент,
спеціальність 122 «Комп'ютерні науки»
Київський національний університет будівництва і архітектури
e-mail: kievkatya77@gmail.com.
ТЕРЕНТЬЄВ О. О.,
професор кафедри інформаційних технологій, проектування та прикладної математики,
доктор технічних наук, професор, спеціальність 126 «Інформаційні системи і технології»
e-mail: terentyev79@ukr.net

ДОСЛІДЖЕННЯ СФЕРИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Останнім часом суспільство дедалі частіше стикається з різноманітними видами кібератак: збої при наданні електронних послуг призводять до блокування роботи забезпечення державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційно-психологічний комплексний тиск на населення, кібертероризм, кібершпигунство, інформаційна комплексна експансія в національному інформаційному просторі послуг країни, блокування роботи або руйнування стратегічного комплексну важливих для приватної економіки та безпеки держави підприємств, тощо.

Шлях України до створення власної кібербезпеки держави потребує радикальних і тому негайних змін. Необхідність змін підкріплюється завдання атаками на критичну інфраструктуру, наприклад NotPetya та багато інших інцидентів, які зробили Україні сумнівну репутацію. Для знаходження шляхів вирішення проблеми кібербезпеки в державі необхідно визначити перелік проблем, які існують в цій галузі.

Однією з найважливіших проблем є неефективна нормативна база та саме система управління кібербезпекою. Аналіз першопричин призводить до низки системних проблем у галузі, які стає важче ігнорувати з кожним наступним інцидентом. Однією з найважливіших проблем є неефективна нормативна база та система управління. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [1] та низка нормативних документів щодо технічного захисту інформації (НД ТЗІ) безнадійно застаріли [2]. Більше того, вони зобов'язують органи державної влади, об'єкти критичної інфраструктури та приватні компанії, які хочуть надавати послуги державним органам (наприклад, Інтернет-провайдери), впроваджувати так звану Комплексну систему захисту інформації (КСЗІ). Вона, окрім того, що морально застаріла, впродовж багатьох років довела свою неефективність.

Наступною проблемою є низька готовність реагувати на кібератаки. Ще одна і не менш важлива проблема – небажання реагувати на кіберінциденти [3]. Більшість компаній ще організаційно не готові до нових хвиль кібератак і не мають належно підготовлених фахівців у своїй державі. На національному рівні також немає централізованого управління силами реагування на кіберінциденти. Рівень обізнаності з кібербезпеки саме серед українців залишає бажати кращого [4]. На жаль, в Україні не існує державної програми для усунення цього недоліку.

Ще однією проблемою є низький рівень залучення професійної спільноти, відсутність трансформаційного підходу. В цілому управління кібербезпекою в Україні на державному рівні важко назвати ефективним. Національна система кібербезпеки обмежується переважно участю в ній силових органів (Нацполіція, Служба Безпеки України, Держспецзв'язок тощо).

Приватний бізнес та кіберспільнота навряд чи будуть притягнуті до вирішення важливих питань. Не існує трансформаційного підходу до управління національною кібербезпекою, який передбачає наявність організації, що управляє виконанням програми з кібербезпеки, та виконує регулярний моніторинг процесу впровадження [5, 7]. В силу специфіки багатьох галузей промисловості (охорона здоров'я, енергетика, телекомунікації програми, тощо) виникає нагальна потреба в окремих галузевих стандартах по кіберзахисту.

Крім того, покращення потребує кіберрозвідка. Інша основна проблема полягає в тому, що в Україні все ще недостатньо ефективно працює система кіберрозвідки (Threat Intelligence) [6]. Є приклади, коли приватні організації та волонтерські угрупування попереджають державу про стан запланованих атак. Але ж в умовах існуючих можна загроз цього видається недостатньо [8].

Проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора та громадянського суспільства. З огляду на сучасні суспільно-політичні та інформаційні виклики визначення політичних, науково-технічних, організаційних та просвітницьких напрямів конструювання ефективної системи кіберзахисту в рамках комплексної протидії кіберзагрозам сприятиме формуванню ефективного механізму протидії загрозам у кібернетичній сфері, випереджальному реагування на динамічні зміни, що відбуваються у кіберпросторі, розробленню та впровадженню ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі. Також потрібен китай перехід на міжнародні одним стандарти кібербезпеки, в одним тому числі визнано галузеві. Найважливішим комплексну кроком є заміна науково-дослідних інститутів на більш штати ефективний та вимогами сучасний базовий залучення стандарт та безпеки впровадження конкретних безпеки галузевих стандартів кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.
2. Про основні засади забезпечення кібербезпеки України: Закон України [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19 (23.11.2020)
3. Tsiutsiura S. V., Kyivska K. I., Tsiutsiura M. I., Kryvoruchko O. V., and Dmytrychenko A. M. (2019) «Formation of a generalized information model of a construction object», International Journal of Mechanical Engineering and Technology, Volume 10, Issue 2, p. 69–79.
4. Дешко Л. М., Бондарєва К. Д. Кібербезпека в Україні: національна стратегія та міжнародне співробітництво // Електронне наукове фахове видання «Порівняльно-аналітичне право». 2018. № 2. С. 379–382.
5. Рудик В. А., Ярош Д. Р., Київська К. І. «Модель організації функцій керування та обчислення мобільного робота», in Seventh international scientific-practical conference «Management of the development of technologies», Kyiv, KNUCA, 2020, pp. 81–83.
6. Цюцюра М. І., Єрукаєв А. В., Гоц В. В., Костишина Н. В. «Реалізація генетичного алгоритму шляхом застосування продукційних правил», Управління розвитком складних систем, Volume 39, p. 64–68, 2019.
7. Mykola Tsiutsiura, Volodymyr Baka and Bohdan Rosinskyi (2019) «Cyber–physical systems, their applications and related challenges», in Sixth international scientific-practical conference «Management of the development of technologies», Kyiv, KNUCA, pp. 92–94.
8. Svitlana Tsiutsiura and Julia Vigor (2018) «Information subsystem for ensuring the increase of the productivity of agricultural crops in the south of ukraine in the northern steppe region», in Fifth international scientific-practical conference «Management of the development of technologies», Kyiv, KNUCA, pp. 52–53.

УДК 35: 004.056.5

ГНАТЧЕНКО Д. Д.,
асистент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
e-mail: hnatchenko@knute.edu.ua.
ГНАТЧЕНКО Т. О.,
аспірант кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
e-mail: t.hnatchenko@knute.edu.ua.
КАЛЬБЕНКО А. С.,
здобувач вищої освіти ОС «бакалавр»
спеціальності 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: kalbenko1808@gmail.com

ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ЗАХИСТУ КІБЕРПРОСТОРУ ЯК КОМПОНЕНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Метою є висвітлення державного регулювання у галузі захисту кіберпростору як складової інформаційної безпеки України на сучасному етапі державного будівництва. Методологічною основою розробки став діалектичний підхід, який передбачає розгляд передумов формування державного регулювання забезпечення кібербезпеки як об'єктивну реальність, яка постійно розвивається під впливом технічних, політичних, правових, безпекових та інших факторів.

Проведені дослідження дозволяють вказати на існуючі правові основи впровадження державної політики у забезпеченні захисту кіберпростору та кібербезпеки. Зокрема, це полягає в повільності реформування нормативної бази щодо кібербезпеки, відсутності регулювання аспектів адміністративної взаємодії суб'єктів національної системи кібербезпеки, відсутності чіткого правового регулювання основних ризиків та загроз національному кіберпростору. Пропозиції щодо оптимізації регуляторного забезпечення цих аспектів повинні стати основою для подальших наукових досліджень.

Одним з найвизначніших досягнень наукового та технічного прогресу для людства було створення і розширення функціонального потенціалу інформації та комунікаційні технології. Сьогодні, з розвитком Інтернету, цілі сфери комерційної та некомерційної діяльності, зв'язки з громадськістю в більшості країн світу розвиваються в кіберпросторі.

За оцінками експертів, десятки тисяч злочинів із використанням інформаційних технологій, програмного забезпечення, апаратне та спеціального технологічного обладнання здійснюється в Україні щорічно [1]. В даний час ці проблеми ускладнюються тим фактом, що відсутня всеосяжна система управління загальнодержавної кібербезпеки в Україні.

Науковий аналіз державного регулювання захисту кіберпростору став можливим завдяки застосуванню конкретної системи методів наукового пізнання.

Термін «кіберпростір» широко використовується в багатьох галузях техніки та гуманітарних наук. Вперше було визначено його формування та впровадження в науковий дискурс правознавства. Як зазначає Д.В. Дубов [2], переосмислюючи пріоритети національних інтересів та саморозуміння, захист інтересів держави та нації в інформаційному суспільстві якісно відрізняється від традиційного розуміння безпеки як «стану безпеки». Таке переосмислення бере свій початок з другої половини 20 століття, коли інформація стала не лише товаром, який має ринок збуту як на глобальному, так і на національному рівнях, але також отримала статус ресурсу для розвитку держави.

Як складне явище, кіберпростір включає як матеріальну складову (засоби обчислювальної техніки, обладнання зв'язку, матеріальні компоненти телекомунікаційних мереж, алгоритми написання та коди тощо), так і нематеріальні – інформація, процеси зчитування коду, процеси передачі інформації.

У правовому полі України універсальне визначення категорії «кіберпростір» з'явилося лише в 2017 р., коли був прийнятий Закон України «Про основоположні принципи кібербезпеки України» (від жовтня 5, 2017 № 2163-VIII). В статті 1 Закону [3], кіберпростір визначається як середовище, що забезпечує формування комунікацій та зв'язків з громадськістю в результаті функціонування сумісних (підключених) систем зв'язку та забезпечення електронної комунікації за допомогою Інтернету та інших глобальних мереж передачі даних.

Експерти вказують головною причиною, яка підштовхнула до визначення поняття «кіберпростір» на законодавчому рівні, повне небажання України відбивати кібератаки та відсутність правового регулювання державного адміністрування кібербезпеки [4]. Наприклад, у 2016 році вірус Petya завдав безпрецедентної шкоди в Україні: більше половини українських компаній були уражені вірусом, втративши значну кількість даних та фінансової звітності протягом декількох звітних періодів, і їм довелося довго відновлювати інформацію.

Правове регулювання категорії віртуального простору стало важливим кроком до структурування систематичної державної політики, спрямованої на забезпечення кібернетичної та інформаційної безпеки України. З точки зору захисту кіберпростору від незаконного посягання, також важливою є криміналізація злочинів у кіберпросторі. Закон передбачає поняття «кіберзлочинність», якою називається соціально небезпечне діяння, за яке передбачена кримінальна відповідальність.

Слід підкреслити дві важливі особливості щодо питання державного регулювання у сфері захисту кіберпростору.

Перша особливість полягає в тому, що відповідно до змісту статті 7 вищезазначеного Закону України «Про основні принципи кібербезпеки України», ключовий принцип забезпечення кібербезпеки в Україні – це здійснення заходів, спрямованих на безпечний захист кіберпростору за умови забезпечення його відкритості, доступності та стабільності. Відповідно, державна адміністрація безпеки кіберпростору повинна відповідати вимогам демократичного державного устрою та верховенства права при зведеному до мінімуму потенційному обмеженні права людини на інформацію. О.І. Яременко пояснює це тим, що кіберпростір є своєрідним «провідником» інформації для процесів і є домінуючою частиною інформаційної сфери сучасного суспільства.

Друга особливість полягає в тому, що на рівні адміністративно-правового регулювання процесів кібербезпеки, заходи державного регулювання у галузі захисту кіберпростору не визначаються систематично, і вони не мають чіткого переліку.

Слід зазначити, що головною передумовою державної регуляторної політики у сфері захисту кіберпростору є створення нормативної та термінологічної бази в галузі кібербезпеки, а також розробка відповідної нормативної підтримки із зазначеного питання. Національна практика нормо-творення з цього питання лише формується і проходить етап свого становлення. Імператив формування має бути ефективним правовим полем для реалізації державного регулювання у сфері захисту кіберпростору політичних, правових, технічних, енергетичних, інтелектуальних, фінансових аспектів розвитку та впровадження правових структур для забезпечення безпеки кіберпростору[5].

Питання стратегії ефективного функціонування системи державного регулювання у сфері захисту кіберпростору на сучасному етапі державотворення включає перелік факторів, які є основними проблемами для національної влади. Зокрема, це недостатність інфраструктури електронних комунікацій держави та рівня її розвитку та безпеки згідно із сучасними вимогами.

Крім того, ми також вважаємо за доцільне зосередити увагу на повільності внесення змін до основних документів, які складають правове поле кібербезпеки. Наприклад, з 2016 року в стратегію кібербезпеки [6] не були внесені зміни, незважаючи на збільшення кількості та рівня небезпеки кіберпросторових загроз в Україні. Це було лише наприкінці 2019 року, коли

про необхідність внесення змін до стратегії кібербезпеки було офіційно оголошено належним чином до необхідності протидії сучасній кіберзброї та розвитку Національної кібербезпеки. Ситуація схожа із Законом України «Про основоположні принципи кібербезпеки України», в який протягом кількох років було внесено зміни лише один раз. Ця ситуація потребує перегляду та мобілізації зусилья законодавчої влади за участі міжнародних партнерів та за умови позитивного досвіду країн світу у реалізації політики захисту кіберпростору.

Пріоритетними є напрямки реформування державного регулювання у сфері захисту кіберпростору відповідно з Угодою про асоціацію. У 2014 році між Україною та Європейським Союзом було підписано історичний документ – Асоціація.

У документі визначено стратегічні основи реформування всіх сфер суспільного життя в Україні в відповідно до стандартів та правил Європейського Союзу. Відповідно, на національному рівні, Україні потрібно розробити та впровадити заходи, спрямовані на реалізацію угоди про асоціацію, щодо розвитку та захисту кіберпростору. Такий багатоетапний і систематичний проект передбачає залучення широкого кола фахівців для реалізації сформульованого завдання з акцентом на забезпечення інформаційної безпеки України.

Отже, державне регулювання процесів захисту кіберпростору в Україні є невід'ємною частиною забезпечення інформаційної безпеки держави. На початку 2020 року основна законодавча база для реалізації державної політики щодо забезпечення захисту кіберпростору та кібербезпеки була сформована на рівні правової системи України. Однак адміністративно-правове регулювання державного захисту кібербезпеки характеризується певними пробілами. Зокрема, це повільність реформування нормативних баз для кібербезпеки, відсутність регулювання аспектів адміністративної взаємодії між суб'єктами національної системи кібербезпеки, відсутність чіткого регулювання основних ризиків та загроз національному кіберпростору України.

Ці концепції повинні лягти в основу перспективних наукових досліджень з визначених питань, з метою внесення обґрунтованих пропозицій щодо вдосконалення національного законодавства про кібербезпеку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Нікулеско Д. С. Кібербезпека: вразливі моменти [Електронний ресурс] // Юридична газета. 2019. Режим доступу: https://yur-gazeta.com /publications/practice/inshe/kiberbezpekavrazlivi-momenti.html

2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с. Режим доступу: http://old2.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

4. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. 2012. № 2. С. 162–169. Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2012_2_24

5. Безпека в мережі: як Україна регулюватиме кіберпростір. Та як новий закон «Про основні засади забезпечення кібербезпеки України» вплине на бізнес / А. Красний, А. Зимарин, І. Мягка, М. Полєтаєва [Електронний ресурс] // mind.ua. 2018. Режим доступу: https://mind.ua/openmind/20184620-bezpeka-v-merezhi-yak-ukrayina-regulyuvatime-kiberprostir

6. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96. Режим доступу: http://www.president.gov.ua/documents/962016-19836

УДК 004.056.5

РЗАЄВА С. Л.,
доцент кафедри інженерії програмного забезпечення та кібербезпеки,
доцент, канд. техн. наук
Київський національний торговельно-економічний університет
e-mail: rzaevasl@knute.edu.ua.
ДРАПЕЙ Л. Л.,
здобувач вищої освіти ОС «магістр»
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: l.drapey@knute.edu.ua

МЕТОДИ ЗАХИСТУ CRM-СИСТЕМИ ПІДПРИЄМСТВА

CRM система – це програмне забезпечення для організації та автоматизації роботи з замовниками. CRM повинна сприйматися бізнесом не як інструмент продажів, а як інструмент безпеки, оскільки саме в ній зберігаються записи про всіх клієнтів (клієнтська база) та інформація про більшість транзакцій. Важлива можливість призначення прав доступу для кожного співробітника. Керівнику підприємства не потрібно влаштовувати пошук зловмисника на власному підприємстві та перевіряти кожного співробітника – досить налаштувати заходи безпеки для однієї CRM-системи і керівник бізнесу буде спати спокійніше.

Питання захисту даних, конфіденційності та безпеки повинні бути головними питаннями корпоративної порядку денного. Важливо забезпечити безпеку інфраструктури, в якій зберігаються дані CRM, створивши кілька рівнів безпеки, які ускладнять проникнення зловмисників. Починаючи з використання брандмауера або мережного екрану, який дозволить контролювати дозволи і доступ до даних.

CRM-система підприємства ТОВ «Торгово-виробничий дім» знаходиться в інтернет-хостингу і працює у веб-інтерфейсі. Хостинг передбачає собою додатковий рівень безпеки інформації надаючи захист від DDOS-атак, а також має свій антивірус, який не дасть завантажити файли зі шкідливим програмним забезпеченням до кореневої директорії. Для безпечного з'єднання використовується HTTPS протокол, що означає підтримку шифрування з використанням протоколу SSL. У разі, якщо дані будуть пошкоджені, на хостингу присутнє резервне копіювання даних.

Паролі зберігаються в базі даних хостингу і для захисту цих даних використовується хешування. Хешування паролів є одним із самих основних міркувань безпеки, які необхідно зробити при розробці програми, що приймає паролі від користувачів. Без хешування, паролі, що зберігаються в базі даних, можуть бути вкрадені, наприклад, якщо база даних була скомпрометована, а потім негайно можуть бути застосовані для компрометації не тільки розробленої програми, але і акаунти користувачів на інших сервісах, якщо вони не використовують унікальних паролів.

В CRM-системі підприємства наразі реалізований такий функціонал: перегляд усіх замовлень від клієнтів сайту rivs.com.ua на якому наявний SSL-сертифікат, в замовленнях є можливість переглянути всю історію взаємодій з клієнтом від оформлення замовлення до моменту, коли клієнт забере своє замовлення. Статус замовлення змінюється оператором почергово, спочатку приймається та опрацьовується в телефонному режимі або за допомогою електронної пошти, а далі все залежить від клієнта, після здійснення оплати статус змінюється на наступний. Відміна замовлення теж реалізована, виконати її можливо лише з активними замовленнями.

Застосовуючи хешуючий алгоритм Argon2, сучасний простий алгоритм, спрямований на високу швидкість заповнення пам'яті та ефективне використання декількох обчислю-

вальних блоків до призначених для користувача паролів перед збереженням їх у своїй базі даних, розгадування оригінального пароля робиться неможливим для атакуючого базу даних, в той же час зберігаючи можливість порівняння отриманого хешу з оригінальним паролем.

Важливо пояснити, що у алгоритму Argon2 є три варіанти, які працюють трохи порізному: Argon2d, Argon2i та Argon2id. Загалом, для хешування паролів слід використовувати варіант Argon2id. По суті, це гібрид алгоритмів Argon2d й Argon2i, в якому використовується комбінація доступу до пам'яті, що не залежить від даних (для захисту від тимчасових атак по побічним каналам), і доступу до пам'яті, що залежить від даних (для захисту від атак злому GPU).

Алгоритм Argon2 приймає ряд параметрів, що налаштовуються:

- Пам'ять – обсяг пам'яті, який використовується алгоритмом (в кібібайтах).
- Ітерації – кількість ітерацій (або проходів) по пам'яті.
- Паралелізм – кількість потоків (або доріжок), використовуваних алгоритмом.
- Довжина солі – довжина випадкової солі. Для хеширования пароля рекомендується 16 байт.
- Довжина ключа – довжина згенерованого ключа (або хешу пароля). Рекомендується 16 байтів або більше.

Параметри пам'яті й ітерацій керують обчислювальної вартістю хешування паролю. Чим вище ці цифри, тим більше вартість генерації хеша. Звідси також випливає, що витрати зловмисника, який намагається вгадати пароль, вийдуть дорожчими.

Важливо зауважити, однак, що хешування паролів захищає їх тільки від компрометації в сховищі, але не від втручання шкідливого коду в додатку і саме тому в необхідно використовувати ліцензійне антивірусне програмне забезпечення.

Співробітники мають використовувати свої особисті облікові записи для входу в систему, а не користуватись одним акаунтом. Крім того, коли працівник звільняється з компанії його доступ до інформації має бути анульованим.

Після хешування дані для доступу в акаунт, після здійснення хешування, шифруються за допомогою алгоритму Galois/Counter Mode (рис. 1). GCM – лічильник з автентифікацією Галуа) – режим роботи, що широко застосовується в симетричних блокових шифрах, має високу ефективність і продуктивність. Є режимом автентифікованого шифрування (AEAD), надаючи як конфіденційність, так і автентифікацію переданих даних (гарантуючи їх цілісність).

UserID	UserLogin	HashedPassword	Language	Nonce	Tag
55	[redacted]	yBdhgCo7doBfna4GFuO8fUQZhQ[redacted]	ua	0d5lvv[redacted]	1Uo1g8RAm[redacted]
56	[redacted]	CYAtHhHZ0iSck7DgYs3sIngT7YsE[redacted]	ua	mgWc[redacted]	9PD2seHjqji[redacted]
57	[redacted]	RBwk1fCamkbWXe8P0t9UYDYr/B[redacted]	ua	6AczT[redacted]	63xu+zM6Sn[redacted]

Рис. 1. Зашифрований хеш паролів користувачів

У звичайному режимі шифрування CTR вхідні блоки нумеруються послідовно, номер блоку шифрується блоковим алгоритмом E (зазвичай AES). Вивід функції шифрування використовується в операції XOR (виключне або) з відкритим текстом для отримання шифротексту. Як і для інших режимів на базі CTR, схема являє собою потоковий шифр, тому обов'язковим є використання унікального вектора ініціалізації для кожного шифрованого потоку даних.

Блоки зашифрованого тексту вважаються коефіцієнтами полінома, який потім обчислюється в залежній від ключа точці H з використанням арифметики кінцевих полів. Потім результат шифрується, створюючи тег автентифікації, який можна використовувати для перевірки цілісності даних. Потім зашифрований текст містить IV, зашифрований текст і тег автентифікації.

GCM вимагає однієї операції блочного шифрування і одного 128-бітного множення в полі Галуа на кожен блок (128 біт) зашифрованих і автентифікованих даних. Операції блочного шифру легко конвеєризуються або розпараллелюються; операції множення легко конвеєризуються і можуть бути розпараллелені з деякими скромними зусиллями (або шляхом розпаралелювання фактичної операції, або шляхом адаптації методу Хорнера відповідно до вихідним поданням NIST, або і тим і іншим).

Часто упускається поширений з виду ризик безпеки CRM – це можливість завантаження інформації. Хоча багатьом співробітникам для виконання своєї роботи необхідний доступ до звітів, широкий доступ може становити небезпеку для цінних даних, що зберігаються у CRM. Обмеживши кількість осіб, які можуть завантажувати дані, треба ще переконатись, що всі знають політику компанії про те, як правильно поводитися з інформацією.

Управління внутрішніми адміністраторами може бути однією з найбільших проблем при реалізації безпеки CRM. Співробітники хочуть відчувати, що їм можна довіряти, але потрібно керувати доступом і рівнями доступу до своєї CRM – навіть якщо це означає обмеження доступу адміністратора.

Загальний висновок. На сьогоднішній день в мережі Інтернет та книжковому ринку майже відсутня інформація про захист CRM-систем, переважно це має підґрунтя через низьке їх впровадження компаніями в своїй діяльності. Важливість клієнтів та захисту їх персональних даних є одним з основних критеріїв в розробці CRM-системи. Порушення безпеки може зіпсувати раніше зароблену репутацію компанії і полегшити конкурентам можливість крадіжки клієнтів. Методи захисту інформації розглянуті в цій статті допоможуть проаналізувати безпеку CRM і забезпечать надійний захист даних. Поєднання багаторівневої системи безпеки і добре навчених співробітників дозволить зосередитися на розвитку бізнесу, не турбуючись про те, що він може стати наступною ціллю для зловмисників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Payne Adrian. Handbook of CRM: Achieving Excellence in Customer Management. 2005. 438 p.

2. How to Secure Your CRM (Customer Relationship Management) Data From Hackers [Електронний ресурс]. Режим доступу: https://www.cloudbric.com/blog/2018/01/secure-crm-data-hackers

3. PHP: Password Hashing – Manual [Електронний ресурс]. Режим доступу: https://www.php.net/manual/en/faq.passwords.php

4. How to Hash and Verify Passwords with Argon2 in Go – Alex Edwards [Електронний ресурс]. Режим доступу: https://www.alexedwards.net/blog/how-to-hash-and-verify-passwords-with-argon2-in-go

5. Ways to Protect Your Company From a CRM Data Breach [Електронний ресурс]. Режим доступу: https://www.nimble.com/blog/crm-data-breach-protection

6. How to Secure Your CRM (Customer Relationship Management) Data From Hackers [Електронний ресурс]. Режим доступу: https://www.cloudbric.com/blog/2018/01/secure-crm-data-hackers

УДК 351: 004.056.5

ГНАТЧЕНКО Д. Д.,
асистент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
e-mail: hnatchenko@knute.edu.ua.
ЗБОРЩИК І. О.,
здобувач вищої освіти ОС «бакалавр»
спеціальності 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: izborsik1@gmail.com

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО В КІБЕРПРОСТОРІ

Проблеми кібербезпеки зачіпають як державний, так і приватний сектори. Державно-приватне партнерство (далі – ДПП) – це місце, де обидва сектора можуть співпрацювати і спільно використовувати методи протидії кіберзагрозам. Атаки на інфраструктуру країни можуть завдати величезної шкоди життю людей, послугам та операціям. Кілька моделей успішного ДПП в цій сфері є зразковими у всьому світі. Розвиток технологій і Інтернету відповідає зростанню загроз в кіберпросторі, постійно ставить під загрозу дані навіть у найбільш безпечних середовищах. Помітні або приховані загрози невигідні для інформаційних систем, активів і даних організації. Критично важливими інфраструктурами країн є телекомунікації, електроенергетика, енергетика, транспорт, фінанси, операції, водопостачання, аварійні служби, продукти харчування, здоров'я, хімічні речовини та засекречені матеріали. Велика частина критично важливих інфраструктур країни працює через онлайн-технології, що ведуть до позитивного економічного розвитку і поступового зростання. Отже, організації та країни повинні колективно створювати системи для відслідковування і контролювати критично важливу інфраструктуру від загарбників.

Сучасна модель. Основна аксіома підходу кібербезпеки до захисту критично важливої інфраструктури – це аксіома суспільно-корисного державно-приватного партнерства, коли обидва сектора працюють в гармонії для досягнення спільної мети. Цей підхід багато в чому виходить з того факту, що державний контроль над телекомунікаційною інфраструктурою обмежений, оскільки мережі і підприємства в основному знаходяться в приватній власності. Спроби поліпшити діалог між державним і приватним секторами часто були незадовільними через такі проблеми, як відсутність довіри, невиправдані очікування, конфлікти інтересів, а також урядові закони, що вимагають певного рівня секретності або відкритості, які можуть працювати проти інтересів держави (розглядається приватна особа). Концепцію державно-приватного партнерства можна розглядати як спектр (як показано на рисунку 1), який з одного боку – це довіра до ринкових сил, що забезпечує необхідний результат, а з іншого – державна власність.

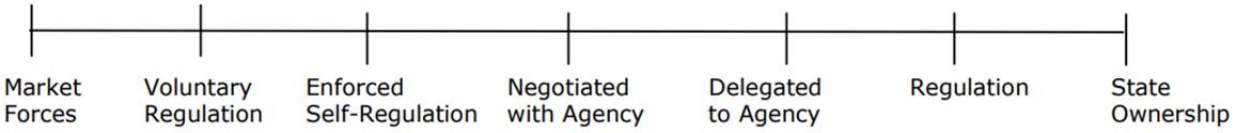


Рис. 1. Приклад моделі державно-приватного партнерства

Модель метауправління. Метауправління можна визначити як «непряму форму управління зверху вниз, яка здійснюється шляхом впливу на процеси самоврядування за допомогою різних способів координації, таких як формування рамок, сприяння і переговори.

Ця концепція забезпечує гнучкий і послідовний спосіб налагодження співпраці між державними та приватними суб'єктами. Ця модель вимагає мінімального ступеню регулювання з боку держави, але забезпечує достатню жорсткість для уряду, щоб гарантувати саморегулювання галузі. Існує три підходи до співпраці державних та приватних суб'єктів:

1. Метауправління ідентичностями: вимагає визначення завдань і обов'язків, щоб дати чітке уявлення про те, чому потрібна допомога з боку приватного сектора, які завдання необхідно виконати і яка організація відповідає за досягнення результату. Цілі та очікування власників приватного сектора повинні бути визначені, і уряд повинен заручитися підтримкою приватного сектора за допомогою розвитку чіткого зв'язку між благополуччям суспільства і успіхом приватного сектора. Цей зв'язок буде сприяти більш тісному співробітництву між урядом і промисловістю в сфері критично важливої інфраструктури.

2. Метауправління без допомоги рук: описують незалежне метауправління, яке дозволяє уряду побічно впливати на партнерство, змінюючи навколишнє середовище. Існує три способи досягнення незалежного метауправління: координація, сприяння і стимулювання. Координація може здійснюватися шляхом створення міжгалузевих консультативних рад для партнерств із захисту критичної інфраструктури, які слугують платформами для координації між різними партнерствами. Сприяння використовується для підтримки існуючих партнерських відносин і дозволяє їм працювати ефективно, створюючи сприятливе середовище для партнерства. Уряд може просувати їх, давати їм поради (наприклад, шляхом створення спільних рамок для взаємодії або розробки типових угод), а іноді й послаблення дії законів, що перешкоджають співпраці. Нарешті, стимулювання – це спосіб, у який уряд надає плани економічного або соціального стимулювання для збільшення участі приватного сектора.

3. Практичне метауправління: це найбільш ефективний спосіб для уряду гарантувати, що приватний сектор діє в громадських інтересах. Цей підхід схожий на традиційну концепцію прямого ДПП і фокусується на участі державного сектора у вузькоспеціалізованих партнерствах шляхом полегшення і управління спільною роботою. В результаті уряд може контролювати діяльність приватного сектора і впливати на нього, знижує вартість участі, нейтралізує конфлікт між приватними партнерами та стабілізує загальну схему. Такий підхід прямого впливу не існує в традиційному ДПП, показаному на рисунку 1. Він має недоліки, один з них – це роль уряду як учасника, так і регулюючого органу, що може призвести до недовіри.

Отже, одним із рішень проблем кібербезпеки стає використання моделей державно-приватного партнерства. Філософія такого підходу визначається забезпеченням окремих функцій держави на основі ринкових механізмів, які може реалізовувати приватний партнер, що має фінансові, технічні та інтелектуальні можливості. Завдання, які повинні вирішити ДПП у сфері кібербезпеки: забезпечити надійний доступ до Інтернет мережі; регулювати технічну безпеку та обробку даних; проводити обмін інформацією щодо загроз і вразливостей; сприяти вирішенню ситуацій, пов'язаних із загрозами або незаконним контентом в мережі Інтернет. Формування можливостей співпраці держави та приватних суб'єктів у сфері кібербезпеки у формі ДПП в значній мірі буде залежати від розробки законодавчих актів, які визначають принципи безпеки щодо критичних інфраструктур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Круглов В. В. Державно-приватне партнерство у сфері кібербезпеки [Електронний ресурс]. Режим доступу: http://www.pubadm.vernadskyjournals.in.ua/journals/2018/ 3_2018/13.pdf

2. Spencer, Fm. (2017). Public-Private Partnerships (PPP)s for Cybersecurity Infrastructures. DOI: 10.13140/RG.2.2.22703.59044. https://www.researchgate.net/publication/ 332182533_Public-Private_Partnerships_PPPs_for_ Cybersecurity_Infrastructures

3. Shore, Malcolm & Du, Yi & Zeadally, Sherali. (2011). A Public-Private Partnership Model for National Cybersecurity. Policy & Internet. Volume 3. DOI: 10.2202/1944-2866.1114. https://www.researchgate.net/publication/261543516_A_Public-Private_Partnership_Model_for_ National_Cybersecurity

УДК 004.056:005.8

ДОРОШ М. С.,
професор кафедри інформаційних технологій та програмної інженерії
Національний університет «Чернігівська політехніка»,
д-р техн. наук, доцент
e-mail: mariyaya5536@gmail.com.
ВОЙЦЕХОВСЬКА М. М.,
викладач кафедри інформаційних технологій та програмної інженерії
Національний університет «Чернігівська політехніка»
e-mail: m.voitsekhovska@gmail.com

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПРОЄКТІВ

Сьогодні, з оглядом на глобальний перехід на дистанційні форми діяльності, інформаційне суспільство отримало додаткове прискорення розвитку. Це стимулювало зростання кількості різних видів взаємодій із застосуванням сучасних інформаційних технологій. Міждисциплінарна практика управління проектами, синтезуючи перспективні інформаційно-комунікативні технології та використовуючи бурхливий розвиток обчислювальної техніки, дає можливість значно скоротити строки та вартість реалізації проекту, зменшує ризики управління вимогами та забезпечувати високу якість самого проекту, що є ключовими факторами його успіху.

З іншого боку, інформаційний простір проектів є частиною штучно створеного середовища в результаті інформаційно-виробничої діяльності учасників проекту та інформаційного простору самого проекту. І кожен учасник цього процесу впливає на стан захищеності бізнес-процесів, що нерозривно пов'язані з інформаційними активами проекту.

Постійне збільшення видів кібератак та масштабів їх реалізації потребує відповідної обізнаності та наявності певних компетенцій в галузі безпеки всіх учасників інформаційних процесів в проектах. Звичайно, менеджер проекту не повинен бути експертом у галузі інформаційної безпеки, але без розуміння важливості організації її забезпечення на всіх етапах життєвого циклу проекту значно збільшуються ризики довіри між учасниками та зменшується відчуття приватності та безпеки кожного окремого учасника.

Сьогодні, в залежності від об'єкту дослідження, є три основні підходи до управління інформаційною безпекою в проектній діяльності.

Перший визначає особливості управління проектами створення систем інформаційної безпеки в організаціях, де об'єктом є система безпеки організації.

Другий визначає систему безпеки для розроблювальних інформаційних систем, де об'єктом є продукт IT проекту.

Третій підхід досліджує саме процеси інтеграції систем управління безпекою до системи управління проектами.

Саме третій підхід лежить в рамках досліджень авторів.

Вперше питання інформаційної безпеки в проекті було стандартизоване у міжнародному стандарті ISO/IEC 27001 «Information technology – Security techniques – Information security management systems – Requirements» у 2013 році [1]. З того часу увага до цього питання в управлінні проектами постійно збільшується, що виявляється в кількості публікацій досліджень у цьому напрямку.

Перевагами впровадження системи управління інформаційною безпекою у проектах є можливості:

- управління доступом до інформації по проекту та до внутрішньої (персональної) інформації учасників проекту, включаючи захищені документи компанії, цифрові бази даних, дані та інформацію з девайсів та хмарних сервісів;

– управління стійкістю до різних інформаційних загроз, включаючи вилучення даних та кібератаки;
– створення єдиної безпекової платформи для всіх стейкхолдерів проекту.

Впровадження стандарту ISO 27001 в проектах також може бути корисним під час визначення та планування системи управління ризиками, яка безпосередньо впливає на вартість проекту.

Інформацію в проектах можна розділити на такі групи:
– конфіденційна інформація,
– інноваційна,
– персональна,
– бізнес-інформація.

При розробці технічного завдання включення такого елементу, як система захисту інформації, може суттєво підвищити рівень довіри її учасників. Приділення уваги до такої актуальної проблеми створить безпечні умови для співпраці географічно розподілених команд, а також підвищить інвестиційну привабливість. Розмежування ж доступу до робочої інформації забезпечить належний рівень безпеки інформаційних активів проекту (інноваційні розробки, інтелектуальна власність, конфіденційність внутрішньої інформації тощо).

Впровадження системи управління інформаційною безпекою в проекті в основному може здійснюватися в рамках процесів управління інформаційним зв'язком у проекті, які містять за PMBoK чотири основні групи процесів [2]:
– планування інформаційного зв'язку;
– поширення інформації;
– звітування про виконання проекту;
– адміністративне закриття проекту.

Під час створення планів з управління різними предметними галузями проекту, аспекти, пов'язані з ІБ, повинні бути включені та достатньо деталізовані. Так, наприклад, на етапі визначення конвергенції місії, стратегії та цінностей стейкхолдерів міжнародного проекту мають бути висвітлені та зафіксовані ставлення до інформації обмеженого доступу, загальні для всіх учасників проекту. Розроблені, задокументовані та стандартизовані процеси моніторингу та менеджменту ІБ в рамках проекту.

При цьому культура інформаційної безпеки проекту (КІБП) виступає невід'ємним елементом системи управління комунікаціями в проектах. Як і організаційна культура, КІБП є повноцінною системою, і поняття «стан» являє для неї упорядковану множину суттєвих властивостей, якими наділена система у кожний момент часу. Отже, питання формування культури інформаційної безпеки в проектах є актуальним і потребує окремих досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements

2. Shkarlet S., Dorosh M., Druzhynin O., Voitsekhovska M., Bohdan I. (2021) Modeling of Information Security Management System in the Project. In: Shkarlet S., Morozov A., Palagin A. (eds) Mathematical Modeling and Simulation of Systems (MODS'2020). MODS 2020. Advances in Intelligent Systems and Computing, vol 1265. Springer, Cham. https://doi.org/10.1007/978-3-030-58124-4_35

УДК 141 165.6/.8

РАССАМАКІН В. Я.,
доцент кафедри інженерії програмного забезпечення та кібербезпеки,
доцент, канд. техн. наук
Київський національний торговельно-економічний університет
rassamakin_vr@knute.edu.ua

WHO'S WHO У СВІТІ ХАКЕРІВ ВІД THALES ТА VERINT

Представлені результати досліджень, отриманих в рамках стратегічного партнерства Verint Systems і Thales Group з розробки передових і комплексних технологій для оцінки технічних загроз. Завдяки аналізу безлічі джерел інформації, як наявних в інтернет, або аналітиці технічних загроз, визначена безпрецедентна панораму основних кіберзагроз з точним описом методів здійснення атак, мотивації хакерів, окресленням найбільш цільових секторів діяльності державних, комерційних кампаній, об'єктів критичної інфраструктури, з підтвердженням атак, що здійснюються приблизно шістдесятьма символічними групами.

В умовах, коли ландшафт кіберзагроз стає все більш складним, і з ростом обсягу інформації, пов'язаної із загрозами, стає неможливим керувати всією складністю проблем без ефективних інструментів і методів. В цьому контексті співпраця вищезазначених партнерів і публікація результатів їх дослідження, викладене в [1] має величезне значення.

Verint Systems є провідний світовий постачальник програмного забезпечення для збору та аналізу даних безпеки та кіберрозвідки [2]. Його великий портфель продуктів інтелектуальної безпеки використовується у понад 100 країнах, допомагає державним установам, об'єктам критичної інфраструктури та бізнесу нейтралізувати та запобігти терористичним актам, злочинам та кіберзагрозам.

Thales Group – міжнародна промислова група, що випускає інформаційні системи для авіакосмічного, військового і морського застосування [3].

Для того щоб зробити результати досліджень реальним оперативним інструментом, ними були відібрані ті групи кіберзагроз, які, на їх погляд, заслуговують найбільшої уваги. Була розроблена ексклюзивна методика підрахунку балів і встановлені індивідуальні рейтингові карти для кожної групи нападників.

Після року розслідування групи аналітиків цих двох, представлених лідерів кібербезпеки визначили докладні профілі приблизно 60 основних груп кібератак, проаналізувавши 490 атакованих кампаній по всьому світу.

Аналітики Thales і Verint визначили чотири основні групи зловмисників, виходячи з їх мотивів і кінцевої мети. З 60, або близько того, проаналізованих основних атакуючих груп 49% спонсуються державою, які часто фокусуються на крадіжці конфіденційних даних з геополітичних цілей. 26% – «хактивісти», переслідують ідеологічні мотиви, за ними слідують кіберзлочинці (20%), рухомі жадібністю. Нарешті, кібертерористи складають 5% проаналізованих груп. (рис 1а)

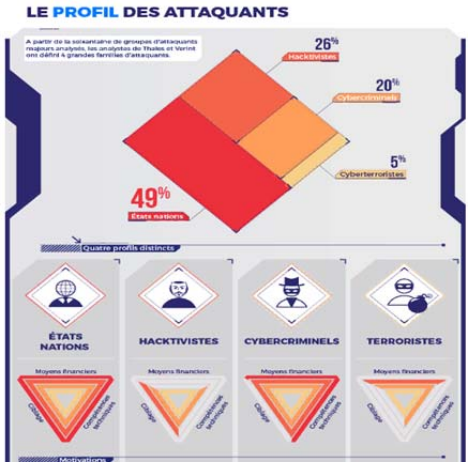
Великі економічні, політичні та військові держави найбільше страждають від значних кампаній. Таким чином, 12 країн з найвищим ВВП входять в число найбільш цільових держав, в першу чергу це США, Європейський Союз (зокрема, Великобританія, Франція і Німеччина), Китай, потім Індія, Південна Корея і Японія. (рис 1б)

Секторами, найбільш цільовими для цих великих кампаній, є держави і їх оборонозатність, за якими слідують фінансовий сектор, енергетика і транспорт. Зростають атаки на ЗМІ і медичний сектор (рис 1в)

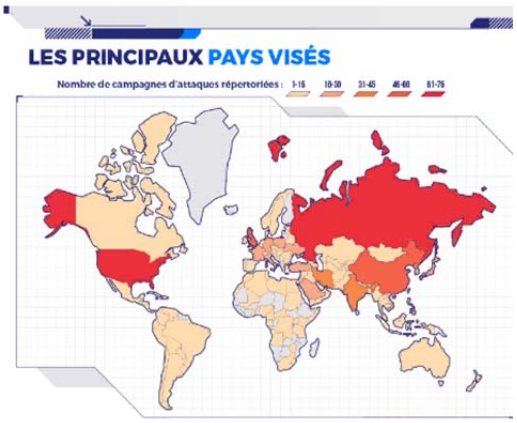
Найбільш поширені (способи) здійснення атак, які використовуються в більш ніж 50% нападів представлені на рис. 1д.

Також з’являється «супермаркет шкідливих програм» (шкідливе ПЗ як послуга), який дозволяє хакерам купувати і використовувати програмне забезпечення, розроблене іншими групами зловмисників.

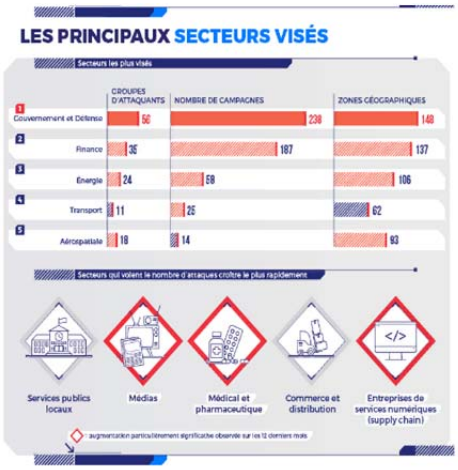
Нарешті, все більше і більше груп зловмисників тепер зосереджуються на недоліках постачальників, партнерів та постачальників, яких вони використовують в якості троянів для досягнення основних цілей (атаки через ланцюжок поставок).



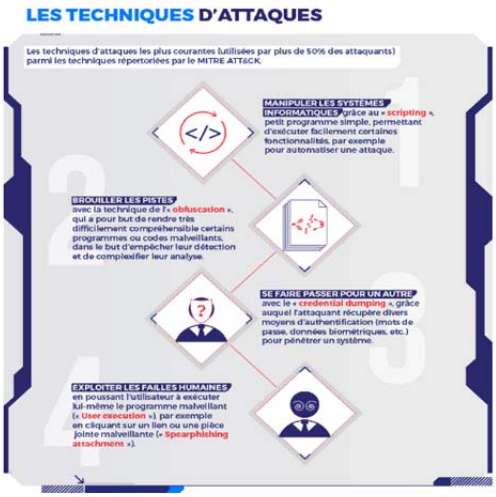
а



б



в



г

Рис. 1. 3 результатів досліджень Verint Systems і Thales Group, що відображують профілі атакуючих груп (а), цільові країни (б), основі цільові сектори (в) та методи атак (г)

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CyberThreat Handbook https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who
2. Verint Systems https://www.it-world.ru/company/42727.html
3. Thales Group https://novations.ua/thales-group/

УДК 004.056:005.8

ХАРЧЕНКО О. А.,
декан факультету інформаційних технологій, кандидат технічних наук, доцент
Київський національний торговельно-економічний університет
a.kharchenko@knute.edu.ua.
ЯРЕМИЧ В. Р.,
аспірант спеціальності 122 «Комп'ютерні науки»
Київський національний торговельно-економічний університет
v.yaremych@knute.edu.ua

КІБЕРРИЗИКИ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ЕЛЕКТРОННОЇ ТОРГІВЛІ

Швидкий розвиток інформаційних технологій та впровадження їх у різні сфери нашого життя вплинуло на розвиток у світі бізнесу механізмів торгівлі в глобальній мережі Інтернет. Відсутність діяльності будь-якого характеру у всесвітній мережі для підприємства нині розцінюється як недолік. Брак часу у споживачів змушує все більше придбань робити через Інтернет, а це, в свою чергу, зумовлює ще більший розвиток електронної торгівлі завдяки появі нових її різновидів [1].

Особливих темпів розвитку і впровадження електронна торгівля отримала у зв'язку з пандемією COVID-19, яка потрясла економічні ринки та вплинула на повсякденне життя багатьох людей і компаній по всьому світу. Для великої кількості людей, що перебувають на самоізоляції, покупки онлайн стали фактом життя. Через вірус люди замовляють товари в Інтернеті, які вони зазвичай купують в магазині [2].

Ведення торгівлі в глобальній мережі Інтернет несе як свої переваги, так і появу абсолютно нових ризиків для бізнесу таких як кібер-ризики.

Кібер-ризик – це ймовірність отримання прямих чи побічних збитків суб'єктом економічної діяльності внаслідок його функціонування у кіберпросторі.

Джерела виникнення операційних кібер-ризиків систематизували Й. Кебула та Л. Янг, виділивши чотири класи: дії людей; збій системи; помилки у внутрішніх процесах; зовнішні події [3].

За видами кібератаки на підприємство електронної торгівлі можна розподілити наступним чином:

1. Нецільові атаки – фішинг;
2. Цільові атаки – фінансове шахрайство, викрадення баз даних, DDoS-атаки, вимагання;
3. Внутрішні атаки – викрадення, знищення інформації, сприяння цільовим атакам.

У наслідок реалізації кібер-ризиків підприємство електронної торгівлі може уповільнити або зупинити бізнес-процеси, втратити конкурентну перевагу, втратити репутацію та отримати судові позови при крадіжці особистих даних. Все це може понести за собою втрату клієнтів та прибутку, зниження вартості бізнесу та необхідність витрат на усунення наслідків та оплату штрафів і санкцій від регулюючих органів.

За даними глобального огляду кількарічної давності, проведеного в 129 країнах об'єднанням ISACA, незалежною некомерційною міжнародною асоціацією, яка об'єднує спеціалістів з інформаційної безпеки, тільки 38% респондентів вважають, що вони підготовлені до кібернападів, 83% відносять кібернапади до однієї з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки [4].

Побоювання респондентів не були безпідставними і світ вразили масштабні кібератаки. Так у 2017 році по всьому світі було інфіковано більше 500 000 комп'ютерів вірусом-шифрувальником WannaCry.

Для України 2017 рік також не був простим. Проти України відбулася масштабна хакерська атака, що проходила у декілька етапів. Розпочалась атака з компрометації системи оновлення програми для подання звітності до контролюючих органів та обміну документами між контрагентами в електронному вигляді M.E.Doc. Наступний етап відбувся з використанням різновиду вірусу Petya та спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Зараженню піддалися інформаційні системи Міністерства інфраструктури, Кабінету Міністрів, сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та Служби спецзв'язку України [5]. Внаслідок цієї атаки було нанесено мільйонні збитки та виведено з ладу близько 10% персональних комп'ютерів в Україні [6].

Ці події показали всім необхідність дотримання кібербезпеки в будь-яких установах незалежно від їхнього розміру, так як жертвами атак були як і малі приватні підприємства, так і державні установи державного. Проте якщо підприємства й прийняли усі міри по дотриманню кібербезпеки та ізоляції певних частин своєї локальної мережі від глобальної мережі Інтернет після 2017 року, то пандемія COVID-19 принесла нові кібер-ризики пов'язані з необхідністю надання можливості співробітникам працювати з дому. Якщо раніше це було поодиноке явище, то під час пандемії воно прийняло масовий характер. Чому вірогідно були раді зловмисники. Більшість підприємств були вимушені відкрити доступ до своїх локальних мереж ззовні для роботи своїх користувачів з дому. Це потенційно збільшує вірогідність зламу мережі підприємства через домашній пристрій користувача внаслідок не дотримання ним цифрової гігієни.

В нещодавній доповіді Інтерполу повідомлялося, що з часу початку пандемії COVID-19 кіберзлочинність виросла більше, ніж будь-яка інша злочинна діяльність. А ФБР відзвітувало про збільшення кількості повідомлень про кіберзлочинність в чотири рази [7].

Все це говорить про те, що злочинці ніколи не зупиняють свою діяльність навіть під час пандемії. Тому відповідальним за кібербезпеку ні в якому разі не можна втрачати пильності і треба працювати над покращенням безпеки при роботі з дому, а користувачам обов'язково необхідно дотримуватися правил кібергігієни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тягунова Н. М., Гудзенко М. Ю. Інтернет-торгівля: сутність та особливості. *Вісник Полтавської державної аграрної академії*. 2013. № 3. С. 160–162. DOI: https://doi.org/10.31210/visnyk2013.03.34 (дата звернення 20.11.2020).
2. COVID-19: вплив на електронну комерцію. *Юридична газета online*. URL: https://yur-gazeta.com/publications/practice/medichne-pravo-farmacevtika/covid19-vpliv-na-elektronnu-komerciyu.html (дата звернення 20.11.2020).
3. Cebula J. J., Young L. R. A Taxonomy of Operational Cyber Security Risks. *Carnegie Mellon University*. URL : https://www.sei.cmu.edu/reports/10tn028.pdf (дата звернення 20.11.2020).
4. Стандарти ISO/IEC захистять від кіберзагроз. ДП «Укрметртестстандарт». URL: http://csm.kiev.ua/index.php?option=com_content&view=article&id=3631%3A-isoiec---&catid=122%3A2015-09-15-07-01-23&lang=uk (дата звернення 20.11.2020).
5. Хакерська атака на Україну: подробиці. *РБК-УКРАЇНА*. URL: https://www.rbc.ua/ukr/news/hakerskaya-ataka-ukrainu-podrobnosti-1498566985.html (дата звернення 20.11.2020).
6. Дмитрий Шимкив: «От кибератаки вируса-шифровальщика Petya.A пострадало приблизительно 10% компьютеров в Украине». ITC.ua. URL: https://itc.ua/news/dmitriy-shimkiv-ot-kiberataki-virusa-shifrovalshhika-petya-a-postradalo-priblizitelno-10-vseh-kompyuterov-v-ukraine/ (дата звернення 20.11.2020).
7. FBI says cybercrime reports quadrupled during COVID-19 pandemic. ZDNet. URL: https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/ (дата звернення 20.11.2020).

UDK 004.942

HONCHARENKO T. A.[1], LYASHCHENKO T. O.[2]
[1]PhD (Engineering), Associate Professor, Department of Information Technology
[2]Senior Lecturer, Department of Information Technology
Kyiv National University of Construction and Architecture
e-mail: geocad@ukr.net

CONCEPT OF DATA PROTECTION AND VERIFICATION OF BIM-MODELS FOR LIFECYCLE BUILDING TERRITORY

The study describes the data protection and verification of information models depending on the stage of the lifecycle of the building territory. An algorithm for verification of the information model at the construction stage is developed. The input and output data for modeling each stage of the object's lifecycle are described. Modeling a construction project in time over its lifecycle along the PRE-BIM, D-BIM, C-BIM, E-BIM, RE-BIM chain forms a complete description of a complex dynamic system chain forms a complete description of a complex dynamic system. The main directions for lifecycle of construction site that need to be monitored using the BIM- model are identified [1]. The composition of BIM models at each stage of the life cycle differs in the quantity and quality of information. To understand what checks are necessary for the BIM model at the construction stage, first of all, it is necessary to determine what information the model contains at this stage of the lifecycle [2]. The main directions for lifecycle of construction site that need to be monitored using the BIM-models are presented in Fig. 1.

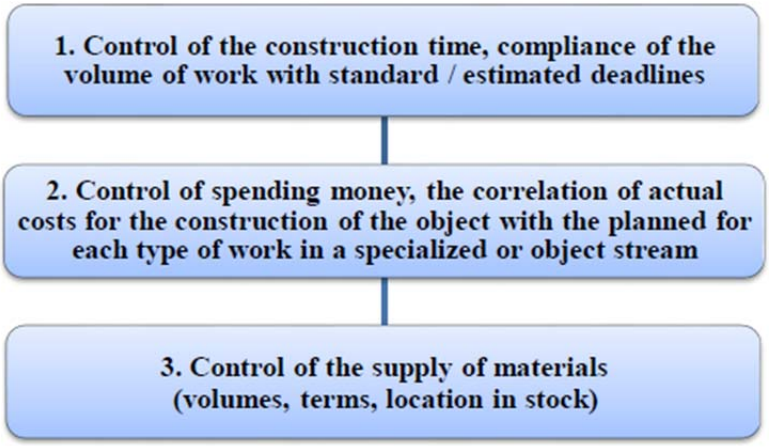


Fig. 1. The main monitoring directions of building territory using the data protection and verification of BIM-models

The presence of a BIM-model verification and data protection tools at the construction stage for the customer is a powerful management tool that will allow resolving conflicts and finding solutions that affect the further construction progress and its successful completion. Modeling a construction project in time over its lifecycle along the BIM chain forms a complete description of a complex dynamic system.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Honcharenko T. Verification of information models of construction objects. Management of Development of Complex Systems, 39, 2019, pp. 69–74; dx.doi.org\10.6084/m9.figshare.11340656
2. Churbanov A. E. The impact of information modeling technology on the development of investment construction process]. Vestnik MGSU, 2018, vol. 13, issue 7 (118), pp. 824–835.

UDC 004:332

TSIUTSIURA S. V.[1], YERUKAIEV A. V.[2], KOSTYSHYNA N. V.[3]
[1] Head of Department of Information Technologies, DSc (Eng.), Professor
[2] Associate Professor of Department of Information Technologies, PhD
[3] Postgraduade of Department of Information Technologies
Kyiv National University of Construction and Architecture, Ukraine
e-mail: orlova_natasha@ukr.net

THE SYSTEM OF FUZZY DERIVATION OF CLASSIFICATIONS OF FACTORS OF COMFORT OF LIVING IN APARTMENT BUILDINGS

One of the most acute problems of modern Ukraine is to provide our population with a high quality and high level of comfort, as well as pleasant conditions in multi-storey buildings. When designing such a living environment, it is necessary to meet a wide and diverse range of requirements. This applies not only to new buildings, but also to modernization projects. Today, the situation in the construction industry is gradually becoming stable, but there are still limitations at the level of the local living environment of Ukrainian people. The main purpose of urban organizations is to meet the needs of residents in their environment. Modern development of urban planning is a rather complex system consisting of other subsystems. There are many classifications of the city, one of the options of the hierarchy of classifications is described below. District – has limited boundaries and belongs to the objects of administrative management. The area is divided into several blocks (neighborhoods) – usually limited to pedestrian accessibility (shop, school, kindergarten, pharmacy), etc.

The adjacent territory is the closest surroundings of the house, its yard, – are distributed on a part of territories within the quarter [1].

In this article, the following factors were selected to study the comfort of the living environment: 1. Area; 2. Microdistrict; 3. Adjacent territory; 4. House.

Today, a very important problem is to determine and highlight the main properties of the comfort of our home.

Thus, the comfort of an apartment building depends on many qualitative and quantitative factors.

There are several different ways in which fuzzy relationships can be specified. The most common are: 1. In the form of a list; 2. Analytical form; 3. Graphic form; 4. Matrix form; 5. In the form of a fuzzy graph;

Terminal vertices – factors of influence (x1, x2 x3 x4)

The estimation of the coziness of a high-rise building can be considered by means of a tabular fuzzy relation [2]. This method is based on the representation of a fuzzy binary relation with a finite number of tuples [2].

X – We have ten positive integers X = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}.

X1 – Input values of the parameter. these include: city area, population, provision of transport conditions.

X2-X3 – Factors affecting the comfort of living between the area and the neighborhood. These include:

- Facilities of public services (schools, kindergartens, hospitals, grocery stores, pharmacies);
- Parking for private cars;
- Noise mode
- **X4-X5** – Factors that affect the comfort of living between the area and the adjacent territory or apartment
- Building density;
- Number of people living in the territory;
- Type of house;
- Age of the house;

– Technical condition of the house;
– View of the house
– **X6-X7** – External parameters of influence, namely:
– Insolation of the territory;
– Noise level;
– Landscaping.
– **X8-X9** – Internal factors of comfort:
– Quality of the house;
– Quality of the apartment;
– Landscaping.

X10 – Initial data of the comfort model for all the factors listed above.

Consider the binary fuzzy relation Q1, which is given on two universals X.

Next, we present a vague relationship, which contains a description of the situation on the comfort of an apartment building

As the first supermarket, let's take a few reasons that negatively affect the comfortable living in our living environment. X = {x1, x2 x3 x4}, in which x1 – not providing the district with social buildings, x2 – distance to passenger transport; x3- Type of house; x4- Age of the house.

As a second supermarket, consider several reasons that arise when solving common problems.

Y = {y1, y2 y3 y4}, where y1 – no social buildings are built; y2 = time spent on the road from one area to the destination; y3 = brick, panel, monolithic type of multi-storey building; we see that there is a connection between each element, with the reasons described above [3].

The peculiarity of this situation is that the relationship between the causes of the issues under consideration is considered. And it is quite ambiguous in building a fuzzy model. Having some data on various factors that adversely affect the comfort, this reason for the interaction can be more adequately represented in the form of a binary fuzzy relation P = {<xi, yj>, μp (<xi, yj>)}, which are given on the bases X and Y. In this case, the membership function of this binary fuzzy relation describes the degree of certainty that or other reason fixed.

Next, we present a specific fuzzy relation P, which is written as follows:

P = {(<x1, y1> 1), (<x1, y2> 0.1), (<x1, y3> 0.2), (<x2, y1> 0.8), (<x2, y1> 0.9), (< x1, y2> 0.1) (<x2, y3> 1), (<x3, y1> 0.7), (<x3, y2> 0.8), (<x3, y3> 0.5), (<x4, y1> 1), (<x4, y2> 0.5), (<x4, y3> 0.2)}.

Since we have a given fuzzy relation P binary finite, it is possible to specify.

At the moment, the typology of housing construction in Ukraine is impressive in its diversity. Today, there are about a third of multi-section buildings, but among designers and architects there is an opinion that this typology of construction will not satisfy the population with comfort. Based on the results of the study, all the characteristics that provide physical and psychological comfort in the most common types of buildings, namely: corridor, sectional, gallery. Still, it is advisable to supplement apartment buildings with modern innovations and nowadays it is quite relevant.

REFERENCES

1 Цюцюра М. І., Єрукаєв А. В., Костишина Н. В., Маляр В. А. (2020) Системний аналіз впливу психологічного стану комфортності багатоквартирного будинку. Управління розвитком складних систем. 42. 132–138.

2 Цюцюра М. І., Єрукаєв А. В., Гоц В. В., Костишина Н. В. (2019) Реалізація генетичного алгоритму шляхом застосування продукційних правил. Управління розвитком складних систем. 39, 64–68.

3 Tsiutsiura Svitlana, Pokolenko Vadym, Kostyshyna Nataliia (2020) Informative analysis of the modern state of comfort of apartment house Тези доповідей сьомої міжнародної науково-практичної конференції «Управління розвитком технологій». 152.

УДК 510.004

ПАШОРІН В. І.,
професор кафедри програмної інженерії та кібербезпеки
Київський національний торговельно-економічний університет.
КУКЛІНСЬКИЙ Д. В., ШАБАЛІН Д. С.,
здобувачі освіти ОС «бакалавр»
спеціальності 125 «Кібербезпека»
Київський національний торговельно-економічний університет
e-mail: 125-18-11-b-kuklinskiy@knute.edu.ua

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ

Суть безпеки інформації – забезпечити безперебійну роботу організації і звести до мінімуму збиток від подій, що таять загрозу безпеки, за допомогою їхнього запобігання і зведення наслідків до мінімуму.

Управління безпекою інформацією дозволяє колективно використовувати інформацію, забезпечуючи при цьому її захист і захист обчислювальних ресурсів.

Необхідно реалізувати заходи для виявлення і запобігання проникнення вірусів у системи і процедури інформування користувачів про їхню шкоду. Користувачам варто нагадати, що запобігання вірусів краще, ніж ліквідація наслідків від їхнього проникнення.

В основі захисту від вірусів повинні лежати високі знання і розуміння правил безпеки, належні засоби управління доступом до систем.

Варто застосовувати для перевірки комп'ютерів і носіїв інформації на наявність відомих вірусів або як запобіжний захід, або як повсякденна процедура.

Програмні засоби виявлення змін, внесених у дані, повинні бути по необхідності інстальовані на комп'ютерах для виявлення змін у виконуваних програмах.

Обслуговування систем. Заходи для обслуговування систем вимагаються для підтримки цілісності і доступності сервісів.

Необхідно визначити повсякденні технологічні процеси для зняття резервних копій з даних, реєстрації подій і збоїв, а також для спостереження за середовищем, у якій функціонує устаткування.

Резервні копії з критично важливих виробничих даних і програм повинні зніматися регулярно. Для забезпечення можливості відновлення всіх критично важливих виробничих даних і програм після виходу з ладу комп'ютера або відмови носія інформації, необхідно мати належні засоби резервного копіювання.

Процедури резервного копіювання для окремих систем повинні задовольняти вимогам планів забезпечення безпере-бійної роботи організації.

Для управління доступом до всіх інформаційних систем масового використання повинна існувати формальна процедура реєстрації і видалення облікових записів користувачів.

Доступ до таких інформаційних систем необхідно контролювати за допомогою формального процесу реєстрації користувачів, що повинний забезпечувати:

• перевірку, чи надано користувачу дозвіл на використання системи адміністратором;

• перевіряти, чи достатній рівень доступу до системи, наданий користувачу, для виконання покладених на нього посадових обов'язків і чи не суперечить він політиці безпеки, прийнятої в організації, чи не компрометує він принцип поділу обов'язків;

• надавати користувачам їх права доступу в письмовому виді;

Обов'язки користувачів. Користувачі повинні знати свої обов'язки по забезпеченню ефективного контролю доступу, особливо що стосується використання паролів і захисту устаткування користувачів.

Паролі є основним засобом підтвердження повноважень доступу користувачів до комп'ютерних систем.

Доступ до інформаційних систем необхідно здійснювати за допомогою надійної процедури входу в систему. Процедура входу в комп'ютерну систему (login) повинна зводити ризик несанкціонованого доступу до мінімуму, тому вона повинна давати мінімум інформації про систему, щоб уникнути надання зайвої допомоги незареєстрованному користувачу.

Захисту в системі підлягає:

- відкрита інформація, яка є власністю держави і у визначенні Закону України «Про інформацію» належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі – відкрита інформація);
- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі – конфіденційна інформація);
- інформація, що становить державну або іншу передбачену законом таємницю (далі – таємна інформація).

Саме з метою підвищення надійності та ефективності роботи платіжних систем Національний банк запрошує учасників платіжного ринку доєднатися до обговорення основних напрямів та вимог до захисту інформації та кіберзахист в платіжних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Урядовий портал, єдиний веб-портал виконавчої влади України. Затверджено постановою Кабінету Міністр України от 29 марта 2006 г. № 373. https://www.kmu.gov.ua/npas/32791826

2. Олійник А. В., Шацька В. М. Інформаційні системи і технології у фінансових установах: навч. посіб. Львів: Новий Світ-2000, 2006. 436 с. https://buklib.net/books/28699

3. Офіційне Інтернет-представництво Національного банку України. https://bank.gov.ua/ua/news/all/riven-informatsiynoyi-bezpeki-ta-kiberzahist-u-sferi-perekazu-koshtiv-planuyetsya-pidvischiti

4. Бурячок В. Л., Толюпа С. В., Семко В. В. Інформаційний та кіберпростори. Проблеми безпеки, методи та засоби боротьби: навч. посіб. Київ: Наш формат, 2016. 176 с.

5. Круглов В. В. Державно-приватне партнерство у сфері кібербезпеки [Електронний ресурс]. Режим доступу: http://www.pubadm.vernadskyjournals.in.ua/journals/2018/ 3_2018/13.pdf

6. Spencer Fm. (2017). Public-Private Partnerships (PPP)s for Cybersecurity Infrastructures. DOI: 10.13140/RG.2.2.22703.59044. https://www.researchgate.net/publication/332182533_Public-Private_Partnerships_PPPs_for_ Cybersecurity_Infrastructures

7. Shore Malcolm & Du, Yi & Zeadally, Sherali. (2011). A Public-Private Partnership Model for National Cybersecurity. Policy & Internet. Volume 3. DOI: 10.2202/1944-2866.1114. https://www.researchgate.net/publication/261543516_A_Public-Private_Partnership_Model_for_National_Cybersecurity

УДК 681.5

ПАЛАГУТА К. О.,
доцент кафедри інженерії програмного забезпечення та кібербезпеки,
доцент, канд. екон. наук
Київський національний торговельно-економічний університет
e-mail: palagutaea@knute.edu.ua.
ГАНАХ О. І.,
здобувач вищої освіти ОС «магістр» спеціальності 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: o_hanakh_foais_19_6m_m_d@knute.edu.ua

БЕЗПЕКА СИСТЕМ SMART HOME

Інтернет речей спростив створення розумного будинку, в якому можна дистанційно керувати замками дверей, світильниками, термостатами, пилососами, газонокосарками та навіть годівницями для домашніх тварин за допомогою смартфона та програми. Це також спростило контроль за будинком практично з будь-якого місця. Розумні системи безпеки є дуже доступними як засоби для самостійного використання, а також як повнофункціональні системи, що включають професійну установку та моніторинг. Користувач можете скористатися системою, яку він контролюєте самостійно, або заплатити абонентську плату за те, щоб будинок цілодобово контролювався професіоналами, які зв'язуватимуться з місцевими пожежними та поліцейськими підрозділами, коли спрацьовують сигнали тривоги. Існує безліч індивідуальних пристроїв, які дозволять контролювати будинок з будь-якого місця за допомогою телефону або планшета, включаючи внутрішні та зовнішні камери безпеки, дзвінки у відеодомофони, датчики руху та розумні замки.

Розумна домашня система безпеки може підключатися до мережі Wi-Fi, щоб користувач міг контролювати свої захисні пристрої за допомогою смартфона та програмного забезпечення. Системи початкового рівня зазвичай включають деякі датчики дверей і вікон, детектор руху та концентратор, який взаємодіє з цими пристроями за допомогою одного або декількох бездротових протоколів, таких як Wi-Fi, Z-Wave, Zigbee або власна мережа. Можна також додати додаткові датчики дверей, руху та вікон, щоб забезпечити покриття всього будинку, і побудувати комплексну систему, яка включає дверні замки, дверні відкривання гаражних дверей, внутрішні та зовнішні камери спостереження, ліхтарі, сирени, детектори диму / CO, датчики води і більше.

У ідеальному світі всі компоненти домашньої безпеки використовують один і той же стандарт бездротового зв'язку для зв'язку з основним концентратором, але такі фактори, як вимоги до потужності, діапазон сигналів, ціна та розмір, унеможливлюють практично застосування одного протоколу. Наприклад, менші компоненти, такі як датчики дверей / вікон, зазвичай використовують технологію Z-Wave або Zigbee, оскільки вони не вимагають багато енергії і можуть живитися від менших батарейок. Вони також працюють у сітчастій топології та можуть допомогти розширити діапазон мережевих пристроїв. Однак жоден протокол не забезпечує пропускну здатність, яку користувач отримує через Wi-Fi, саме тому він зазвичай використовується в камерах безпеки для забезпечення плавного потокового передавання відео та в інших пристроях. Більше того, пристрої Z-Wave та Zigbee підключаються та управляються за допомогою концентратора, тоді як пристрої Wi-Fi можна підключати безпосередньо до домашньої мережі та керувати ними за допомогою програми. Нарешті, пристрої Z-Wave та Zigbee використовують шифрування AES 128, і оскільки вони працюють у закритій системі із виділеним концентратором, вони забезпечують більший рівень безпеки, ніж пристрої Wi-Fi.

Практично будь-яка система безпеки Smart Home пропонує компоненти, які працюють разом у спільному середовищі та ними можна маніпулювати за допомогою індивідуальних правил. Наприклад, можна створити правила включення світла при виявленні руху, розблокування дверей, коли спрацьовує димова сигналізація, і зробити так, щоб камера починала записувати при спрацьовуванні датчика. Деякі системи зберігають записане відео локально на SD-карті або твердотільному накопичувачі, тоді як інші пропонують хмарне зберігання. Хмарне сховище дозволяє легко зберігати та отримувати доступ до записаного відео, але це може коштувати сотні доларів на рік. Деякі системи пропонують як хмарне, так і локальне сховище, а деякі – спеціальний накопичувач, який надає можливості відеореєстратора із тимчасовим записом, що полегшує пошук відеоподії, яка відбулася в певний момент часу.

Усі проаналізовані нами системи мають додаток, який дозволяє використовувати смартфон як командний центр для озброєння та зняття з охорони системи, створення правил, додавання та видалення компонентів та отримання сповіщень, коли спрацьовують тривоги. Більшість програм також дозволяють робити такі речі, як перегляд відео в прямому ефірі або записаного відео, блокування та розблокування дверей, зміна налаштувань термостата та приглушення сигналізації. Деякі програми навіть використовують служби локації телефону для автоматичного включення та зняття з охорони системи відповідно до фізичного місцезнаходження власника. Дорожчі системи, як правило, оснащені настінною панеллю, що виконує роль комунікаційного центру, з сенсорним дисплеєм. Дисплей дозволяє спілкуватися з професійною службою моніторингу при спрацьовуванні сигналізації та переглядати відео з будь-якої з встановлених камер безпеки.

Майже всі найновіші домашні системи домашньої безпеки пропонують підтримку голосового управління через Amazon Alexa, Google Assistant, а в деяких випадках і Apple Siri, що дозволяє розблокувати двері, змінити налаштування термостата, відкрити гараж і підняти або обеззброїти систему за допомогою голосової команди на підключений пристрій, такий як розумний динамік. Багато з них також пропонують підтримку аплетів IFTTT (If This Then That), які використовують тригери, сумісні з IFTTT, веб-службами та пристроями для створення дії. Наприклад, можна створити аплет, який повідомляє, якщо відкрити гаражні ворота, щоб увімкнути прожектор.

Зовнішня камера ідеально підходить для спостереження за тим, що відбувається поза домом. Ці пристрої захищені від атмосферних впливів і, як правило, потребують сусідньої розетки GFCI (переривник ланцюга замикання на землю) для живлення, хоча є кілька моделей, що працюють від акумуляторів. Як і їх внутрішні аналоги, зовнішні камери підключаються до вашої мережі Wi-Fi і дозволяють переглядати відео в реальному часі з вашого телефону. Більшість зовнішніх камер, таких як Arlo Ultra, пропонують виявлення руху за допомогою push-повідомлень та сповіщень по електронній пошті, нічного бачення та хмарного сховища для відео, а деякі, як Ring Floodlight Cam, виконують подвійний обов’язок як прожектори або ліхтарі. Деякі моделі можуть навіть відрізнити автомобіль, що проїжджає повз, тварину та людину.

Відео дзвінки пропонують простий спосіб побачити, хто біля дверей, не відкриваючи і навіть не наближаючись до дверей. Ці пристрої підключаються до мережі Wi-Fi і надсилатимуть сповіщення, коли хтось підійде до дверного отвору. Вони записуватимуть відео при натисканні на дверний дзвінок або при виявленні руху, і, як правило, пропонують двосторонній аудіозв’язок, що дозволяє розмовляти з відвідувачем з будь-якого місця за допомогою телефону. Більшість дзвіночків для відеодзвінків використовують існуючу проводку дверного дзвінка (два дроти низької напруги) і досить прості в монтажі, але є моделі на батарейках, які встановлюються за лічені хвилини. Деякі працюють з іншими розумними пристроями, такими як дверні замки та сирени, і підтримують голосові команди IFTTT та Alexa.

Розумний замок, як правило, є частиною надійної інтелектуальної системи захисту будинку, але для його використання не потрібно вкладати гроші в повноцінну систему. Якщо використовується концентратор домашньої автоматизації для управління такими речами, як освітлення та термостати, можна без особливих зусиль додати до системи розумний замок

Z-Wave або Zigbee. Деякі моделі використовують існуючий апаратний ключ із циліндрами та засувками та кріпляться до внутрішньої сторони дверей, тоді як інші вимагають видалення існуючих внутрішніх та зовнішніх клавіш та заміни засувки та засувки. Розумні замки можна відкривати та закривати за допомогою мобільного додатка, і вони надсилатимуть сповіщення, коли хтось замикає або відмикає двері, і більшість з них дозволяють створювати графіки постійного та тимчасового доступу для членів сім'ї та друзів на основі конкретних годин дня та днів тиждень. Серед функцій, на які слід звернути увагу, є геозонування, яке використовує служби локації телефону для блокування та розблокування дверей, голосова активація за допомогою голосових команд Siri (HomeKit), Google Assistant або Amazon Alexa, підтримка IFTTT та інтеграція з іншими розумними домашніми пристроями, такими як відеодзвінки, зовнішні камери, термостати, димові сигналізатори та підключене освітлення. На вибір є безліч моделей розумних замків, включаючи замки без дотику до клавіш, замки з сенсорним екраном, комбіновані замки та замки на сенсорній панелі, а також замки, які можна відкрити за допомогою біометричного зчитувача відбитків пальців.

Як і будь-який продукт, який підключається до Інтернету та використовує бездротові технології, розумні системи безпеки будинку вразливі до злому, особливо системи, які не мають шифрування. Хакери можуть сидіти біля будинку та використовувати ноутбук та програмне забезпечення для перехоплення бездротових сигналів, що надходять від системи Smart Home, що дозволяє їм придушувати тривоги та вимикати датчики. Інші пристрої дозволяють хакерам генерувати радіошум, який може перешкоджати зв'язку між датчиками та концентратором. Крім того, пристрої, які підключаються через Wi-Fi, такі як камери безпеки та розумні дверні замки, можна зламати, щоб отримати доступ до домашньої мережі. Потім кваліфікований хакер може використовувати пристрої Wi-Fi та інші мережеві ресурси для здійснення атак DDoS з розподіленою відмовою в обслуговуванні проти великих мереж. Можливо, ще більш тривожною є ідея про якісь незнайомі відеоспостереження з внутрішніх і зовнішніх камер охорони.

Існує кілька кроків, щоб переконатися, що система домашньої безпеки захищена від зловмисних кібер-зловмисників. Слід замінити системний пароль за замовчуванням на унікальний, що містить поєднання літер, цифр та символів. Якщо можливо, час від часу потрібно змінювати пароль. Потрібно переконатися, що домашня мережа захищена. Слід перевірити налаштування безпеки на власному бездротовому маршрутизаторі та розглянути моделі, які додають додатковий рівень програмного захисту, наприклад Bitdefender Box 2. Деякі постачальники систем безпеки використовують технологію стрибка частоти для запобігання затухання сигналу, тоді як інші використовують вбудоване шифрування. Потрібно слідкувати за журналами камери, щоб побачити, коли вони були доступні. Слід переконатися, що системне програмне забезпечення та всі підключені пристрої оновлені. Оновлення мікропрограми часто вирішують проблеми безпеки і можуть допомогти захистити систему від проникнення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lakhno V. A., Hrabariev A. V., Petrov O. S., Ivanchenko Y. V., & Beketova G. S. (2016). Improving of information transport security under the conditions of destructive influence on the information-communication system. Journal of theoretical and applied information technology, 89(2), 352–361.
2. Methodology Forming for the Approaches to the Cyber Security of Information Systems Management / A. Adranova, L. Yona, J. Kryvoruchko, A. Desiatko, K. Palahuta, A. Blozva // Journal of Theoretical and Applied Information Technology (ISSN: 1992-8645, E-ISSN: 1817-3195). 2020. P. 1993–2005.
3. Smart Home Market Reports 2020. URL: https://www.reportlinker.com/smart-home/reports (дата звернення: 25.11.2020)
4. Best smart home systems 2020: Reviews and buying advice. URL: ttps://www.techhive.com /article/3206310/best-smart-home-system.html (дата звернення: 25.11.2020)

УДК 004.49

ШЕСТАК Я. І.,
директор ІОЦ-ГЦІТ КНТЕУ
Київський національний торговельно-економічний університет

КІБЕРБЕЗПЕКА, ОРГАНІЗАЦІЙНІ ЗАХОДИ БЕЗПЕКИ

Тривалий час вже аналізують різні компанії безпеку підприємств. Будують моделі різних структур комерційних підприємств, фінансових структур, банків, громадських установ, навчальних закладів, та особливо вразливих підприємств державного значення. У різних країнах розпочато роботу з моделювання об'єктів та організацію атак для подальшого аналізу уражень підприємств, фінансових структур чи важливих державних установ. Так довгий час 5-10 років компанії вивчали вплив різних факторів на розвиток загроз у кіберпросторі. Всі вони фінансувалися окремими компаніями, які розвивали сегмент захисту кіберпротору та державами, які використали багато ресурсів на створення систем моніторингу, контролю та перевірки безпеки на державному рівні за визначеними критеріями які були визначені як загроза державної безпеки. Найбільше у розвитку таких систем взяли участь Америка та Китай. За даними з вікіпедії **Національне управління кібербезпеки** (англ. *National Cyber Security Division*, NCSD) – підрозділ управління кібербезпеки і комунікацій Директорату національної безпеки і програм міністерства внутрішньої безпеки США. Сформовано 6 червня 2003 року на базі Управління захисту найважливіших об'єктів інфраструктури, Національного Центру захисту інфраструктури, Федерального Центру комп'ютерних інцидентів і Національної системи комунікацій. Місією NCSD є співпраця з приватним сектором, урядом, військовими та розвідувальними органами для оцінки ризиків і зниження вразливостей і загроз у сфері інформаційних технологій і пристроїв, що впливають на функціонування критично важливих IT-інфраструктур уряду США і приватного сектора. NCSD також здійснює аналіз вразливостей, раннє попередження та допомогу в реагуванні на комп'ютерні інциденти для державного і приватного секторів. NCSD виконує більшість завдань міністерства, покладених на нього в рамках комплексної національної ініціативи з кібербезпеки. Бюджет NCSD в 2011 фінансовому році склав $378 млн. В Китаї і по сьогодні дані по роботі у межах кіберпростору – таємні та не оприлюднюються, але є певна інформація яка дає право на ґрунтовне свідчення про певні розробки систем, є зафіксовані короткострокові атаки, що дають змогу визначити вплив і перевірку захищеності різних структур з боку КНР. У вікіпедії не багато інформації, але представляю: За оцінкою американського аналітика Джеймса Малвенона, організація військово-кібернетичних операцій Китаю має прихований і децентралізований характер, операції виконуються постійно мінливим складом офіційних, громадських, і полугражданских груп. За його словами, в цих цілях використовуються також «патріотичні хакерські об'єднання».

У структурі НВАК щонайменше з 2004 року є підрозділ 61398, призначене для проведення хакерских атак на комп'ютерні мережі противника. Крім спеціальних підрозділів НВАК, китайське керівництво використовує для проведення кібершпіонажу і кібератак також групи хакерів, найбільшою з яких є так званий «Альянс червоних хакерів» (*Red Hacker Alliance*), чисельність якого оцінюється приблизно в 80 тисяч чоловік. За оцінками російських експертів в сфері інформаційної безпеки В. С. Овчинского і Є. Ларіної, «Альянс червоних хакерів» є неформальною, але керованою владою КНР мережею, що включає хакерів не тільки з самого Китаю, але і з китайської діаспори у всьому світі, тісно взаємодіючої з Третім і Четвертим управліннями Генерального штабу НВАК.

Ці дані довгий час були таємні, розголосу ні підлягали і не застосовувалися у межах країни, або відносно об'єктів, що становили загрозу. У кіберпросторі важче визначити розташування об'єктів загрози, методів маскування і засобів влаштування атак. Тому довгий час багато компаній не знали, що їх ресурси використовувалися для організації атак,

розсилання спаму та інших небезпечних вірусів блокувальників-здирників. За ці роки почали писати віруси більш витонченіше, не гребуючи взагалі ніякими перепонами. Так почали використовувати маскування під важливе листування від керівників, адміністраторів чи важливі повідомлення від постачальників програмного забезпечення. З аналізу вірусів які спричиняли загрози 94% з них для використання у операційних системах Windows, інші 5% – призначені були для операційних систем: MacOs, Unix, Linux та операційних систем комутаційного обладнання і 1% – програмне забезпечення власних розробок, де не враховані досвід і принципи захисту від загроз.

Так багато можемо обговорювати проблеми сьогодення з побудови захищених систем, але для цього потрібен досвід, надбання та знання різних систем протидії. Важливо зазначити, що адміністратори, або як зараз пропонують компанії побудувати захищену систему, чи провести повний аудит підприємства, але багато є в цьому проблем про які важко пояснити курівникам підприємств з побудови безпечної роботи, організаційних та регламентних заходів щодо забезпечення безпеки інформації. На прикладах великих організацій різних форм власності раніше, коли ще не була розвинена комп'ютерна інфраструктура, мережа, були організовані секретні підрозділи які займалися контролем витоку інформації, співпрацювали з служби безпеки України та Інтерполу.

В Україні політика щодо кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи. За інформацією Департаменту кіберполіції, щороку кількість кіберзлочинів в Україні збільшується в середньому на 2,5 тисячі. Згідно зі звітом, який міститься на веб-сайті цього правоохоронного органу, працівники Департаменту кіберполіції були залучені до розслідування більше ніж 11 тисяч виявлених кримінальних проваджень, вчинених у сфері високих інформаційних технологій.

Довгий час цього вистачало, але сьогодні кордони відкриті і у багатьох країнах створили органи контролю небезпечних активностей у кіберпросторі. Багато країн мають ці органи які покликані визначити активності трафіку (спам), організацію обмеженого доступу до небезпечних секторів у державних межах, побудова захисту і забороні використання небезпечних чи заборонених державними актами ресурсів. Ресурси компаній сьогодні рідко використовують локальні сервери це пов'язано з дороговизною підтримки, модернізації, розширення ресурсів, забезпечення захисту баз даних, та власне утримування IT фахівців такого рівня, використовуючи хмарні технології та правильну організацію потоків інформації – дозволить безпечно, економно використовувати ресурси. Важливим організаційним фактором у захисті клієнтів є свідомість працівників, дотримання елементариних правил користування робочим майном. Так я б не рекомендував використовувати у приватному листуванні корпоративну пошту, заборонив би використовувати соціальні мережі, обмін інформації за допомогою флеш накопичувачів, довести до відома працівників, що робочий ресурс є ресурс компанії, а не приватні засоби розповсюдження інформації. Ще рекомендував би переглядати повідомлення налаштованого антивіруса, який повідомляє про загрози вашій і корпоративній безпеці. Для роботи рекомендую обирати системи які пройшли перевірку з кібер захисту, а організаціям які перевіряють системи і надають право на розповсюдження даного програмного забезпечення, надстройку чи структуру яка дозволить безпечно працювати в умовах кіберзлочинності, посилання на видані документи зазначати на своїх веб ресурсах. Зробити реєстр перевірених систем, що дають можливість безпечно працювати комерційним чи державним підприємствам. Надавати можливість проходити довгострокові навчальні курси адміністраторів на полігонах створених державним сектором для організації забезпечення захисту підприємств. Вважаю, що на рівні юристів, бухгалтерів необхідно забезпечити всі установи висококваліфікованими IT фахівцями з розширеними знаннями з кіберзахисту. Кібер полігон небхідно проходити всім відповідальним для отримання практичних навичок, досвіду моніторингу загроз, виявлення проблем та вибору засобів їх ліквідації.

УДК 004.49

ТИЩЕНКО Д. О.,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
e-mail: tyshchenko_d@knute.edu.ua
БАРОЯН В. А.,
здобувач вищої освіти ОС «бакалавр» /PhD, спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: 125-18-11-b-baroian@knute.edu.ua

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ PGP ПРИ ВИКОРИСТАННІ ЕЛЕКТРОННОЇ ПОШТИ

Система PGP забезпечує конфіденційність і сервіс автентифікації, які можна використовувати для електронної пошти і додатків зберігання файлів. Система PGP швидко одержала визнання і сьогодні використовується дуже широко. Серед причин такого швидкого визнання можна виділити наступні.

Система PGP широко доступна у версіях, що виконуються на великій кількості платформ, включаючи DOS/Windows, UNIX, Macintosh і багато інших. Крім того, існує комерційна версія, покликана задовольнити користувачів, які вважають за краще мати підтримку виробника.

Система PGP використовує загальновідомі популярні алгоритми, які витримали перевірку практикою і вважаються виключно надійними. Зокрема, до пакета включено алгоритми шифрування з відкритим ключем RSA, DSS і алгоритм Діфі-Хелмана, алгоритми традиційного шифрування CAST-128, IDEA, 3DES і AES, а також алгоритм хешування SHA-1. Система PGP має дуже широку галузь застосування – від корпорацій, які хочуть мати стандартизовану схему шифрування файлів і повідомлень, до простих користувачів, які потребують захисту свого листування з іншими користувачами в мережі інтернет або іншій мережі [2].

Система PGP не була розроблена урядовою або іншою офіційною організацією, і тому непідконтрольна їм. У документації PGP часто використовується термін «секретний ключ», що означає ключ, який становить пару з відкритим ключем у схемі шифрування з відкритим ключем. Сервіс системи PGP, якщо не розглядати керування ключами, складається з п’яти функцій: автентифікації, конфіденційності, стиснення, сумісності на рівні електронної пошти і сегментації

Відправник створює повідомлення за допомогою алгоритму SHA-1, внаслідок чого виходить 160-бітовий хеш-код повідомлення. Одержаний хеш-код шифрується за допомогою алгоритму RSA з використанням особистого ключа відправника, і результат додається на початок повідомлення. Одержувач використовує RSA з відкритим ключем відправника, щоб розшифрувати і відновити хеш-код. Одержувач генерує новий хеш-код одержаного повідомлення і порівнює його з розшифрованим хеш-кодом. Якщо хеш-коди збігаються, повідомлення вважається справжнім [1].

Комбінація SHA-1 і RSA забезпечує ефективну схему цифрового підпису. Зважаючи на надійність RSA, одержувач упевнений в тому, що тільки власник відповідного секретного ключа міг створити цей підпис. Надійність SHA-1 дає одержувачу впевненість у тому, що ніхто інший не міг створити інше повідомлення з відповідним хеш-кодом і, отже, з підписом з оригінального повідомлення. Підписи можуть також генеруватися за допомогою DSS/SHA-1 [2].

Хоча підписи зазвичай приєднуються до повідомлень або файлів, для яких вони створюються, часто буває так, що підтримуються і відокремлені підписи. Відокремлений

підпис може зберігатися і передаватися окремо від самого повідомлення. Це стає корисним у цілому ряді випадків. Користувач може мати окремий протокол підписів усіх посланих і одержаних їм повідомлень. Відокремлений підпис виконаної програми може згодом допомогти виявити зараження програми вірусом. Нарешті, такі підписи можуть використовуватися тоді, коли підписувати документ повинна не одна, а кілька сторін, як, наприклад, у разі контракту. Підпис кожної сторони виявляється тоді незалежним і, таким чином, застосовується тільки до даного документа. Інакше підписи повинні бути вкладеними так, що друга сторона підписувала б документ разом з підписом першої сторони і т.ін. [1].

У сучасних автоматизованих системах керування, комп'ютерних системах і мережах, різних інформаційних і телекомунікаційних системах, інформаційно- телекомунікаційних системах висуваються високі вимоги до забезпечення цілісності, спостережливості і автентичності (справжності) інформації на всіх етапах їх життєвого циклу.

Досвід застосування і проведені дослідження показали, що ці високі вимоги, особливо з реалізації функції причетності (неспростовності), можуть бути забезпечені тільки за рахунок застосування електронного цифрового підпису. Електронний цифровий підпис (ЕЦП), по суті, являє собою додані до інформації дані, обчислені за допомогою криптографічного перетворення інформації, що захищається, і параметри, наявність яких дозволяє упевнитися в цілісності інформації і дійсності її джерела, а так само забезпечити захист від підробки з боку отримувача.

Електронний цифровий підпис є цифровим еквівалентом підпису (штампа, печатки, водяного знаку і т.д.), наявність якого в повідомленні, чи даних програми дозволяє з високою імовірністю визначити джерело (джерела) цього повідомлення чи даних і юридично довести, що з зазначеною припустимою імовірністю P_n тільки він міг сформувати цей підпис, але підробити його в процесі заданого часу, при обмежених ресурсах, зловмисник може з імовірністю, що не перевищує заданої величини P_z. Причому ЕЦП у такий спосіб обчислюється на основі інформації, що захищається, з використанням особистого (конфіденційного) ключа конкретного суб'єкта чи об'єкта, що є його джерелом чи відправником. Перевірка цілісності і дійсності виконується з використанням відкритого ключа, причому знання відкритого ключа не дозволяє підробити ЕЦП з імовірністю, що перевищує P_z [2].

При використанні PGP шифрується, принаймні, частина переданого блока. Якщо потрібен тільки цифровий підпис, то шифрується профіль повідомлення (з використанням особистого ключа відправника). Якщо має місце сервіс конфіденційності, шифрується (з використанням одноразового симетричного ключа) повідомлення плюс підпис (за наявності останньої). Таким чином, частина або весь вихідний блок повідомлення є потік довільних 8-бітових байтів. Проте багато систем електронної пошти дозволяють використовувати тільки блоки, що складаються з символів тексту ASCII. Щоб задовольнити таке обмеження, PGP забезпечує сервіс конвертації «сирого» 8- бітового двійкового потоку в потік друкованих символів ASCII[1].

Засоби електронної пошти часто обмежують максимально допустиму довжину повідомлення. Наприклад, багато засобів електронної пошти, доступних через інтернет, допускають пересилання повідомлень завдовжки не більше 50000 байт. Будь-яке повідомлення, яке має більшу довжину, повинно бути розбито на сегменти меншої довжини, кожний з яких посилається окремо. Щоб відповідати такому обмеженню, PGP автоматично розбиває дуже довгі повідомлення на сегменти, достатньо малі для того, щоб їх можна було переслати за допомогою електронної пошти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Столингс В. Криптография и защита сетей. Принципы и практика. М.: Вильямс, 2014. 672 с.

2. Семенов Ю. А. Протоколы Интернет. Энциклопедия. М.: Горячая линия – Телеком, 2015. 405 с.

УДК 004.056.5

КОСТЮК М. А.,
аспірант кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
e-mail: hell.gunshe@gmail.com

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ПІД РЕГУЛЮВАННЯМ GDPR

В світлі розвитку нових IT-технологій, поняття інформаційної безпеки значно розширилося. Говорячи про інформаційну безпеку, часто мають на увазі інформаційну безпеку в найзагальнішому сенсі, як комплекс заходів, покликаний зменшити число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації. З цієї точки зору інформаційна безпека – це економічний параметр, який повинен враховуватися у роботі підприємства, а інформацію (або дані) можна розглядати як певний товар або цінність, що підлягає захисту, а відтак вона має бути доступною лише для авторизованих користувачів чи програм. Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність [1]. Величезна кількість інформаційних систем створюється із направленням на закордонні на міждержавні ринки, тому слід відзначити, що забезпечення кібербезпеки в такій ситуації набуває більш серйозних масштабів. Проте під час забезпечення кібербезпеки необхідно також враховувати обмеження, що створюються на законодавчому рівні. Одним із таких обмежень, наприклад, є набір правил GDPR. Загальний регламент про захист даних (GDPR) – це регламент у законодавстві ЄС про захист даних та конфіденційність у Європейському Союзі (ЄС) та Європейському економічному просторі (ЄЕЗ). Він також стосується передачі особистих даних за межі країн ЄС та ЄЕЗ. Основна мета GDPR – надати контролю особам над їхніми персональними даними та спростити регуляторне середовище для міжнародного бізнесу шляхом уніфікації регулювання в ЄС.[2]

Існує 7 ключових принципів, що лежать в основі GDPR:

- Законність, справедливість та прозорість
- Обмеження призначення
- Мінімізація даних
- Точність
- Обмеження зберігання
- Цілісність та конфіденційність (безпека)
- Підзвітність

Для моніторингу безпеки та операцій у інформаційних системах, що відповідають вимогам GDPR, більше уваги приділяється як запобіганню, так і уникненню порушень безпеки та конфіденційності. Крім того, важливо мати можливість швидко реагувати, коли проблема виникає, розуміти її та вживати заходів. Як мінімум, інформаційним системам, які обробляють персональні дані, потрібно:

- Швидко виявляти та реагувати на проблеми, щоб дотримуватися правил повідомлення та зменшити штрафи, демонструючи ефективний контроль, нагляд та стримування порушень;
- Досягнути наочного дотримання GDPR, а також задоволення потреб бізнесу.

При розробці нових інформаційних систем необхідно одразу впроваджувати правила GDPR тому що при побудові фундаменту системи набагато простіше організувати всі ключові принципи, що прописані регламентом. Більш того, з юридичної точки зору, порушення правил GDPR несе за собою неабиякі наслідки для підприємства, що володіє

інформаційною системою, а саме штрафи до 20 мільйонів доларів (або 4% від минулорічного доходу, дивлячись що більше), а також інші юридичні обмеження.

Для того аби привести інформаційні системи у відповідність з GDPR необхідно дотримуватись наступних рекомендацій:

- Оцінювати наслідки захисту персональних даних до розробки нового функціоналу. Це обов'язкова процедура, яка дозволить врахувати всі ризики при розробці і вбудувати захист інформації користувача в ядро системи.
- Обмежити перелік зібраних персональних даних.
- Необхідно вести реєстр даних. Потрібно вести детальний облік всієї особистої інформації користувачів: знати її місце розташування, відповідального за файли або процес, рівні доступу до даних, ризики і значимість файлів та інше.
- Розробити нову політику конфіденційності. У документі описати простою мовою все, що перерахували вище, включаючи права користувача, підрядників, які беруть участь в обробці персональних даних, і заходи безпеки, які приймаються для збереження конфіденційності. Крім того, вам потрібно чітко розмежувати згоду з правилами користування та згоду на збір інформації для різних цілей.
- Отримайте згоду на обробку даних від старих користувачів. Якщо у вас немає доказів, що користувач, наприклад, усвідомлено підписався на розсилку, надішліть йому лист з роз'ясненням і проханням підтвердити підписку.[3]
- Отримайте згоду на використання сайтом cookies. Додайте спливаюче вікно з поясненням, навіщо ви використовуєте cookies, розмістіть там посилання на Privacy Policy і кнопку ОК. Вікно не повинно зникати, поки користувач не натисне на кнопку.
- Додайте в особистому кабінеті користувача вкладку для перегляду даних і відправлення запитів. Там повинно бути вказано все, що система знає про користувача, а також форма запиту на редагування або видалення інформації.
- Використовуйте для обробки ПЗ, яке відповідає умовам privacy by design і privacy by default. Перше означає, що ПЗ використовує шифрування і анонімізація користувачів. Друге, що при встановленні програми користувачеві повинні пропонуватися максимальні налаштування безпеки.
- Впровадити систему інформаційної безпеки в компанії. Зберігати дані на захищених серверах, необхідно розмежувати рівні доступу.
- Фіксувати всю роботу з даними. За вимогами GDPR всіх заходів, які приймаються для захисту даних, повинні бути задокументовані. Описувати, що саме відбувається: від оцінки наслідків захисту і ведення реєстру до технічних рішень, положень та внутрішніх правил. [4]

Таким чином дотримуючись простих правил, представлених регламентом GDPR, можливо побудувати досить просту та надійну систему, що матиме всі необхідні елементи захисту даних від основних кібератак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Архівовано 21 серпень 2011 у Wayback Machine., Інформаційні технології-методи захисту-система управління інформаційною безпекою, офіційний переклад, ст. 3.

2. The Proposed EU General Data Protection Regulation. A guide for in-house lawyers, Hunton & Williams LLP, June 2015, p. 14.

3. Стаття 13. Інформація, яку необхідно надати у разі збирання персональних даних від суб'єкта даних | GDPR-Text.com. GDPR. Режим доступу: https://gdpr-text.com/read/article-13/?col=2&lang1=ukr&lang2=en&lang3=rumain

4. Art. 99 GDPR – Entry into force and application | General Data Protection Regulation (GDPR). General Data Protection Regulation (GDPR) (en-US). Mode of Access: https://gdpr-info.eu/art-99-gdpr

УДК 004.056.5

САЛЕОМОН А. А.,
здобувач вищої освіти ОС «бакалавр» спеціальності 125 «Кібербезпека»
Київський національний торговельно-економічний університет
e-mail: A_Saleomon_FOAIS_18_12_B_d@ knute.edu.ua.
САШНЬОВА М. В.,
доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національного торговельно-економічний університет
e-mail: m.sashnova@knute.edu.ua

АНАЛІЗ СИСТЕМИ ЗАХИСТУ НА ПІДПРИЄМСТВІ «САМСУНГ ЕЛЕКТРОНІКС УКРАЇНА»

На сьогоднішній день на підприємстві існує значна кількість загроз, адже представники відділу безпеки компанії Самсунг, а саме її українського підрозділу, допустили декілька вагомих помилок, якими може скористатися потенційний зловмисник.

Підприємство «Самсунг Електронікс Україна» використовує перевірене програмне забезпечення, яке впроваджує захист найбільш високого рівня. Це може дозволити компанії зберегти дані про своїх клієнтів і працівників. Але той факт, що служба безпеки організації генерує абсолютно банальні паролі для облікових записів своїх працівників, а також не слідкує за безпекою в мережі Інтернет (у агентів служби підтримки є можливість шукати інформацію в браузері під час консультації клієнтів), значно підвищує ризик реалізації загроз з боку зловмисників [1]. Якщо конкурентна організація відправить свого шпигуна працювати на даному підприємстві, вони зможуть дізнатися практично все, що потрібно для удару по репутації конкурента. Особливо під час пандемії, коли працівники працюють зі своїх домівок. Представники компанії-конкурента зможуть проаналізувати кожен компонент інформаційної системи та нанести вагомі збитки організації.

Оцінивши дані чинники, можна зробити висновок, що ризик реалізації загроз у комунікаційних системах підприємства «Самсунг Електронікс Україна» є доволі високим. Основною причиною є практично вільний доступ до стратегічно важливої інформації, якою може володіти практично кожен працівник. Для того, що більш широко та об'єктивно оцінити потенційні загрози, необхідно їх класифікувати за певними ознаками. Перш з все, за природою їх виникнення.

Загрози за природою виникнення:

1) Об'єктивні (природні):

– Призупинення роботи певних комп'ютерних пристроїв, які є робочими для агентів служби підтримки (деякі комп'ютери та ноутбуки знаходяться у жахливому стані, але представники компанії Самсунг все одно готують їх до подальшої роботи, закладаючи в них величезну кількість робочих даних. Якщо ноутбук припинить свою роботу, що не буде сюрпризом, адже він працює по 12 годин на добу майже кожного дня, це може вплинути на подальшу роботу всієї інформаційної системи);

– Прийом на роботу некваліфікованих співробітників (дана загроза полягає у тому, що у колл-центрах люди надовго не затримуються, тому компанія кожного місяця проводить тренінги та намагається наймати щонайбільше працівників на посаду оператора служби підтримки. Необхідно пройти лише невеличкий тест на перевірку знань по методичним вказівкам. Таким чином на підприємство з особливою легкістю можуть потрапити шпигуни конкуруючої компанії або звичайні некваліфіковані працівники, що у процесі псують репутацію компанії).

2) Штучні загрози:

– Ненавмисні:

• перезавантаження Телеграм-бота (телеграм-бот є основним джерелом прийому та обробки телефонних дзвінків. Ним користується велика кількість людей, а саме до однією сотні працівників компанії майже щохвилинно. Тому до перезавантаження бота всі звикли. Це перезавантаження полягає у тому, що бот зупиняє свою роботу, а разом із цим і роботу всієї інформаційної системи) [3];

• помилки під час входу до системи (вхід до робочої системи є комплексним і складається з великої кількості компонентів. Деякі працівники можуть некоректно увійти до системи, що не дасть їм можливості обробляти дзвінки клієнтів компанії. Це може вплинути на робочі показники абсолютно всіх операторів, адже потік клієнтів з кожною годиною росте, а нові працівники за зміні не з'являються. Це призведе до перезавантаження лінії, що залишить деяких клієнтів без обслуговування зі сторони агентів служби підтримки щодо певних технічних питань, і суттєво вплине на репутацію підприємства).

– Навмисні:

• атака на програмне забезпечення з метою отримання доступу до системи (дана процедура може бути з легкістю реалізована правопорушниками, а тим паче тими, що знайомі з «внутрішньою кухнею» компанії. Робочі паролі створюються за певними шаблонами, про які всім відомо, тому отримання доступу до даних у такій ситуації – лише питання часу) [2];

• навмисне перезавантаження системи з метою зупинки діяльності інформаційної системи;

• поширення вірусних програм (під час консультацій агенти служби підтримки можуть використовувати браузер с метою пошуку інформації з приводу певних пристроїв компанії Самсунг. Цим можуть скористуватися зловмисники, адже використання інших ресурсів, які повідомляють про використання cookies-файлів, є дуже небезпечним, якщо паралельно з цим відкриті робочі вікна та вкладки, де зберігається конфіденційна інформація).

Ознайомившись з потенційними загрозами, можна побудувати модель порушника.

Мета моделі порушника: авторизація для одержання доступу до ресурсів ІТС з метою ознайомлення, модифікації, знищення, зміни режимів використання або загального функціонування системи, а також установка програмних засобів копіювання інформації або модифікації системного забезпечення з метою перезавантаження систем.

Категорії осіб, до яких може належати порушник:

1) Користувачі продукції Самсунг;
2) Працівники служби підтримки компанії Самсунг;
3) Представники відділу моніторингу та служби безпеки підприємства;
4) Керівники різних рівнів;
5) Представники конкуруючої фірми;
6) Представник партнерської організації;
7) Персонал компанії;
8) Фізичні особи (в тому числі люди, що раніше працювали на підприємстві).

Кваліфікація зловмисника може напряму залежати від мотивів, які він переслідує. Його обізнаність у програмному продукті сягатиме рівня розробників системи, але така підготовка може і не знадобитися, якщо найслабша ланка у захисті виявилася достатньо вразливою, щоб нею скористувався навіть початківець. Якщо порушник є експертом, йому відома інформація про принципи роботи системи, включаючи секретну. Можна припускати, що він є законним користувачем системи, або навіть працівником компанії, яку атакує. Головне – підозрювати всіх і кожного, адже переваги зловмисника полягають в його переміщеннях. Він може з'явитися в будь-який час та у будь-якому місці периметра системи. Важливо вміти помічати сліди, що залишив порушник, якщо вони наявні.

Опис програмних засобів захисту інформації. В компанії існує декілька етапів входу до робочої системи. Перш за все, працівник повинен налагодити VPN-з'єднання за допомогою корпоративного сервісу власної розробки Самсунг. Після цього відкривається можливість увійти до корпоративної пошти, використавши робочу e-mail-адресу та надзвичайно

простий пароль, який згенерувала служба безпеки компанії. Згодом необхідно відкрити клієнтські бази даних, що ведуться у додатку SAP CRM. Паролі до бази даних є більш складними, як і логін окремого користувача, але можна помітити шаблонність їх генерування (використовується один і той же шаблон для кожного працівника). Також рекомендується використовувати сервіс miniweb. Працівники відділу безпеки генерують для співробітників спеціальні токени, які є не змінюють свого значення та є видимими для користувачів. За цим токеном також стоїть процес автентифікації, де необхідно ввести логін та пароль свого акаунту, що прив'язаний до сервісу.

Методи шифрування даних на підприємстві не розсекречувалися, адже ця інформація є недоступною для сторонніх осіб. Але представників служби підтримки не ознайомлюють з тим, яким чином необхідно користуватися корпоративними інструментами передачі даних, тому вони можуть використовувати сторонні браузери або хмарні технології для передачі стратегічно важливої для компанії інформації [4]. У таких ситуаціях можливе перехоплення даних або їх крадіжка.

Опис апаратних пристроїв, що можуть забезпечувати захист інформації. На підприємстві використовуються спеціальні пластикові карти, які являються пропусками при вході у будівлю та певні офісні приміщення. Такі карти є практично у кожного співробітника компанії, адже без них практично неможливо потрапити в офіс. Використання таких карт практикується у більшості офісів країни, але не так багато людей дійсно задумувалися про їх вразливості. Найлегший спосіб – просто використати карту будь-якої людини, що працює на підприємстві. Доступ не буде заблоковано, адже конфіденційні дані зчитуються саме з картки, а не з персонального ідентифікатора певної людини. Слід розуміти, що викрадення такої картки сторонніми особами є справжньою проблемою. Картку можна клонувати або просто зчитати дані програмним шляхом [6]. Деякі картки є дійсно добре захищеними, адже їх шифрують з метою забезпечення найбільш безпечного функціонування, але шифрування може погіршити продуктивність та швидкість роботи пристрою. У таких випадках можна використовувати методи диверсифікації ключів.

Підводячи підсумки, можна з упевненістю заявити, що «Самсунг Електронікс Україна» впровадили достатньо високий рівень захисту. Їх програмні засоби захисту інформації є дуже надійними, але у такому випадку необхідно очікувати атаки саме зі сторони інсайдерів. Саме ця область є найбільш вразливою, адже працівники компанії мають доступ до величезної кількості важливих даних, які з легкістю можна передати у карантинних реаліях (майже кожен агент працює зі свого дому) [5]. Складські приміщення недостатньо захищені. Необхідно впроваджувати спеціальні термінали з багатофакторною автентифікацією, а не сподіватися, що людське око, хоч і за допомогою камер, зможе зафіксувати зловмисні дії. Також слід впроваджувати нові правила безпеки на підприємстві, проінструктувавши співробітників. Особливу увагу слід зосередити на відповідальності, що понесе та чи інша людина у разі порушення політики безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kevin Mitnick. «The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data», 18–50 (2017).

2. Georgia Weidman. «Penetration Testing: A Hands-on Introduction to Hacking», 179–360 (2014).

3. Habr: веб-сайт у форматі тематичних колективних блогів, що створений для публікації новин та статей, що пов'язані і інформаційними технологіями. URL: https://habr.com/ru/feed

4. Mark Goodman. «Future Crimes: Inside the Digital Underground and the Battle for Our Connected World», 103–132 (2015).

5. Peter Kim, «The Hacker Playbook 2: Practical Guide To Penetration Testing», 328–362 (2014).

6. Cybersecurity Interviews: подкаст в однойменному додатку, під час якого дискутують на тему безпеки інформації окремих підприємств. URL: https://podcastgo.pl/listen/?appleid=1179376133

УДК 004.056

ТИЩЕНКО Д. О.,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
e-mail: tyshchenko_d@knute.edu.ua.
ФРАНЧУК Т. М.,
здобувач вищої освіти ОС «магістр» /PhD; спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: t.franchuk.fit.121.2m.20.m.z@knute.edu.ua.
КОПА В. О.,
здобувач вищої освіти ОС «бакалавр» /PhD; спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: 125-18-11-b-kopa@knute.edu.ua

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ЕЛЕКТРОННОЇ ПОШТИ

В сучасному світі інтернет відкриває необмежені можливості для швидкого і конфіденційного зв'язку, забезпечує умови для дистанційної роботи чи навчання і є незамінним засобом для передачі інформації та електронного документообороту.

Електронна пошта стає все більш важливим елементом для повсякденної діяльності. Підприємствам потрібні спеціалісти для налаштування надійності електронної пошти, щоб допомогти співробітникам правильно її використовувати, зменшити ризик навмисного або ненавмисного неправильного її використання, і щоб гарантувати, що офіційні документи, які передаються за допомогою електронної пошти, правильно обробляються.

У процесі розширення використання систем електронної пошти в сучасному діловому світі стрімко зростає і кількість конфіденційних даних, які передаються по мережі інтернет. В результаті стає актуальною проблема автоматизації та захисту документообігу, що здійснюється за допомогою засобів електронної пошти.

Можна виділити основні загрози, пов'язані з електронною поштою [1]:

1. Фальшиві адреси відправника. Адресі відправника в електронній пошті в інтернеті не можна довіряти, тому що відправник може вказати фальшиву зворотну адресу, або заголовок може бути модифікований в ході передачі листа, або відправник може сам з'єднатися з SMTP-портом на машині, від імені якої він хоче відправити лист, і ввести його.

2. Перехоплення листа. Заголовки і вміст електронних листів передаються в чистому вигляді. В результаті вміст повідомлення може бути прочитано або змінено в процесі передачі його через інтернет.

3. Поштові бомби. Поштова бомба – це атака за допомогою електронної пошти. Система, на яку здійснюється атака переповнюється листами до тих пір, поки вона не вийде з ладу.

Деякі провайдери дають тимчасові логіни для тестування підключення до інтернету, і ці логіни можуть бути використані для початку подібних атак.

Типові варіанти виходу поштового сервера з ладу[3]:

– Поштові повідомлення приймаються до тих пір, поки диск, де вони розміщуються, максимально не переповниться. Наступні листи не приймаються. Якщо цей диск є також основним системним диском, то вся система може аварійно відключитися.

– Вхідна пошта переповнюється повідомленнями, які потрібно обробити і передати далі, до тих пір, поки не буде досягнутий граничний розмір черги. Наступні повідомлення не потраплять в чергу.

– У деяких поштових систем можна встановити максимальне число поштових повідомлень або максимальний загальний розмір повідомлень, які користувач може прийняти за один раз. Наступні повідомлення будуть відкинуті або знищені.

– Може бути перевищена квота диска для даного користувача. Це завадить прийняти наступні листи, і може перешкодити йому виконувати інші дії. Відновлення може виявитися важким для користувача, так як йому може знадобитися додатковий дисковий простір для видалення листів.

– Великий розмір поштової скриньки може зробити важким для системного адміністратора отримання системних попереджень і повідомлень про помилки.

– Отримання поштових бомб в список розсилки може привести до того, що його члени можуть анулювати свою підписку.

Також виділяють листи з погрозами. Якщо ви вказали вашу поштову адресу на певному веб-сайті, він може продати вашу адресу для поштового спаму. Деякі веб-браузери самі вказують вашу поштову адресу, коли ви відвідуєте веб-сайт, тому ви можете навіть не зрозуміти, що ви його дали. Для безпечної атаки може використовуватися анонімний ремейлер. Коли хтось хоче надіслати образливий або лист із погрозами і при цьому приховати свою особистість, він може скористатися анонімним ремейлером. Якщо людина хоче надіслати електронного листа, не розкриваючи свою домашню адресу тим, хто може загрожувати йому, він може теж використовувати анонімний ремейлер. Якщо він почне раптом отримувати небажані листи за своєю поточною адресою, він може відмовитися від нього і взяти новий [1].

Враховуючи вищезазначене, можна відзначити способи захисту електронної пошти [2]:

1. Захист від фальшивих адрес. Від цього можна захиститися за допомогою використання шифрування для приєднання до листів електронних підписів. Якщо канал зв'язку зашифрований, то системні адміністратори на обох його кінцях все-таки можуть читати або змінювати повідомлення. Було запропоновано багато різних схем шифрування електронної пошти, але жодна з них не стала масовою. Одним з найпопулярніших додатків є PGP. Раніше використання PGP було проблематичним, так як в ній використовувалося шифрування, що підпадає під заборону на експорт з США. Комерційна версія PGP включає в себе плагіни для декількох популярних поштових програм, що робить її особливо зручною для включення в лист електронного підпису та шифрування листів клієнтом. Останні версії PGP використовують ліцензовану версію алгоритму шифрування з відкритими ключами RSA.

2. Захист від перехоплення. Від цього можна захиститися за допомогою шифрування вмісту повідомлення або каналу, по якому він передається. Якщо канал зв'язку зашифрований, то системні адміністратори на обох його кінцях все-таки можуть читати або змінювати повідомлення.

Всі співробітники підприємств повинні використовувати електронну пошту так само, як і будь-який інший офіційний засіб організації. З цього випливає, що коли лист надсилається, як відправник, так і одержувач повинен гарантувати, що взаємодія між ними здійснюється відповідно до прийнятих правил захисту. Захист листів, поштових серверів і програм повинен відповідати ступеню важливості інформації, яка передається по мережі.

Тобто має здійснюватися централізоване управління сервісами електронної пошти. Повинна бути розроблена політика, в якій вказувався б потрібний рівень захисту. Для вирішення задач із забезпечення безпеки інформації, що надсилається через електрону пошту в усьому світі все активніше застосовуються технології криптографічного захисту з використанням відкритих ключів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гутман Б., Бегвілл Р. Політика безпеки при роботі в Інтернеті – технічне керівництво. Режим доступу: [http://citforum.ru/internet/security_guide/glava8.shtml#8_7]

2. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту Видавництво: ТИД Діа Софт, 2014. С. 414.

3. Кузнецов А. А. Захист ділового листування (секрети безпеки). М.: Іспит, 2016. 239 с.

УДК 004.056.5

ПАШОРІН В. І.,
професор кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет.
ШАПОЧНІКОВА А. О., БОЙКО Т. В., ОЛЕКСЮК В. А.,
здобувачі вищої освіти ОС «бакалавр» спеціальності 125 «Кібербезпека»
Київський національний торговельно-економічний університет
e-mail: vpashorin@knute.edu.ua
125-18-11-b-shapochnikova@knute.edu.ua

ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ SWOT-АНАЛІЗУ

Введення оцінки виявлених загроз є значущим етапом розвитку SWOT-аналізу, який може фундаментально вплинути на безпеку інформаційних систем організації.

На цьому етапі повинні бути досягнуті найбільш об'єктивні результати на підставі чого буде обрано оптимальний підхід до інформаційного захисту організації.

SWOT – це абревіатура для позначення внутрішніх сильних і слабких сторін організації, можливостей загроз, виявлених у зовнішньому середовищі організації.

SWOT-аналіз є одним з методів стратегічного аналізу початкового стану підприємства. SWOT-аналіз може бути включений в число найбільш реалізованих аналітичних методів.

Хоча організація не може впливати на зовнішні фактори так сильно, як на внутрішні, SWOT-аналіз повинен вжити відповідних заходів для їх мінімізації (у разі виникнення загроз) або вжити відповідних заходів для їх усунення перевага їх (у разі можливості).

Аналітичні групи досвідчених співробітників виявляють і оцінюють фактори в аналізованих областях. Можна створити спеціальну команду для кожної області, тобто кожна область буде проаналізована іншою командою, яка є найбільш обізнаною і досвідчений в даній області.

У членів команди повинно бути достатньо часу і компетенцій в разі, якщо вони отримують певну інформацію в ході обговорення з керівництвом організаціїї.

Виявлення та оцінка сильних і слабких сторін виконується в два послідовних кроки, які більш детально описані нижче:

1. Підготовка до SWOT – аналізу;
2. Виявлення та оцінка сильних і слабких сторін організації та її напрямків;
3. Виявлення та оцінка можливостей і загроз з боку зовнішнього середовища;
4. Розробка SWOT-матриці.

Підготовка до SWOT – аналізу пропонується виконувати в чотири етапи в наступному порядку:

1. Чіткий виклад мети SWOT-аналізу;
2. Визначення областей, що підлягають аналізу;
3. Створення аналітичних груп;
4. Стандартизація методології роботи та мотивації членів команди.

Мета SWOT-аналізу повинна бути сформульована, якщо вона ще не була сформульована, замовиком аналізу.

Для визначення областей, що підлягають аналізу в разі застосування SWOT-аналізу до всієї організації, доцільно розділити організацію на області, які потім аналізуються незалежно.

Організація може бути розділена відповідно до функціональних областей, процедурних областей або відповідно до системи « 7s « McKinsey.

Поділ організації на функціональні області може мати: системи управління; організаційні структури; інформаційні мережі; культура організації; людські ресурси та їх розвиток; наукові дослідження та розробки, обладнання; фінанси та економіка; аналіз наступних областей проводиться в тому випадку, якщо організація розділена по технологічних областях; основні процеси; процеси управління; допоміжні процеси.

SWOT-аналіз підходить для визначення можливостей збору інформації та методів, які будуть використовуватися (або які рекомендується використовувати). У членів команди повинно бути достатньо часу і компетенцій на випадок якщо вони придбають певну інформацію в ході обговорення з керівництвом організації.

Оцінка загроз в першу чергу спрямована на визначення актуальності наслідків загроз із зовнішнього середовища для аналізованої території в разі їх виникнення. Виявляється ймовірність виникнення окремих загроз.

Рівень ризику того, що дана загроза вплине на аналізовану область діяльності організації, потім буде розраховуватися як добуток загрози і значущості її наслідків для організації і ймовірності її виникнення. Чим вище рівень ризику, тим більше стратегічне значення він має. Потім ризики для аналізованої території шикуються відповідно до їх рівнями.

Ризик найвищого рівня – це ризик № 1. Двома ключовими напрямками діяльності є:

• Облік факторів, що мають стратегічне значення;

• Генерації альтернативних стратегій.

Облік факторів стратегічної значущості – це врахування сильних і слабких сторін високої значущості, а також можливостей і загроз високої цінності (тобто вигод і ризиків високого рівня), які мають стратегічне значення.

Таким чином, мова йде про вибір тих факторів (сильних і слабких сторін, можливостей і загроз), які будуть використовуватися для вироблення альтернативних стратегій.

Генерація альтернативних стратегій заснована на поєднанні сильних і слабких сторін (внутрішні фактори) з виявленими загрозами і можливостями (зовнішні фактори). Таким чином, розробка чотирьох стратегій є логічним продовженням SWOT-матриці.

SWOT матриця включає в себе наступні чотири стратегії:

- Стратегія пошуку. Ці стратегії спрямовані на подолання (усунення) слабких сторін шляхом використання можливостей.
- Стратегія отримання вигоди. Ці стратегії використовують переваги сильних сторін на користь можливостей, ідентифікованих у зовнішньому середовищі.
- Стратегія уникнення. Це оборонна стратегія, спрямована на усунення (подолання) слабких місць і запобігання зовнішньої загрози.
- Стратегія протистояння. Ці стратегії можуть бути реалізовані, якщо організація достатньо сильна, щоб протистояти загрозі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Grasseova M. (2006). The implementation of SWOT analysis in long-term plan-ning. Defence and Strategy, 2(6), 48–55. ISSN 1214-6463

2. Rehak D., Dubec R., & Grasseova M. (2008). Assessment of external environmental elements within SWOT analysis utilizing the evaluation of risks and benefits. Paper presented at the Symposium on Risk Analysis / Management Cybernetics / Economics (19th International Conference on Systems Research Informatics & Cybernetics), Baden-Baden, Germany

УДК 004.056.5

ЧУДІК М. І.,
здобувач вищої освіти ОС «магістр»
спеціальність 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: chudik199813@gmail.com.
ЖИРОВА Т. О.,
старший викладач, кафедра інженерії програмного забезпечення та кібербезпеки
Київський національний торгово-економічний університет

ПЕРЕОСМИСЛЕННЯ КІБЕРБЕЗПЕКИ У ПОСТПАНДЕМІЧНОМУ СВІТІ

Однозначно, страх і відчуття терміновості є одними з найпотужніших засобів для експлуатації людей, коли мова заходить про кібербезпеку, і це було чітко видно в перші дні пандемії COVID-19.

Усе почалося в березні з шахрайства та фішингу, пов'язаного із надзвичайною ситуацією COVID-19, таких як уособлення таких авторитетних осіб, як ВООЗ та інші глобальні та урядові установи. Початок пандемії також чітко продемонстрував безпорадність звичайних користувачів перед кіберзлочинцями. Пандемія, безумовно, змінила світ, і це включає кібербезпеку. Розмірковуючи про останні місяці в постпандемічному світі, з'являються деякі конкретні моменти.

1. Карантин створив нові виклики для кібербезпеки.

Під час перебування на карантині, люди вдома почали проводити в Інтернеті набагато більше часу, ніж раніше. Дані показують, що в березні-травні обсяг збільшився на 20% для середнього домогосподарства. Це свідчить про збільшення кількості суб'єктів, що генерують Інтернет-трафік, але, на диво, кількість нових пристроїв, що з'являються в будинках кінцевих користувачів, зменшилась майже на 50%, оскільки користувачі перестали купувати непотрібне обладнання. Громадська поведінка та рекомендації щодо карантину, та щодо ізоляції разом із зупиненими або уповільненими поштовими операціями додали загального спаду.

Корпораціям, малим та середнім підприємствам довелося швидко адаптувати свої бізнес-процеси, щоб вони відповідали новим реаліям. Зазвичай підприємства надавали пріоритет безперебійному наданню послуг над безпекою віддалених робочих просторів та пристроїв, що означало, що люди починали працювати вдома, майже не захищенні перед кіберзагрозами.

Віддалений доступ до корпоративних ресурсів через віртуальні приватні мережі традиційно призводить до жорсткіших політик віддаленого доступу; однак перехід до віддаленої роботи призвів до більш дозвільних політик доступу, що створює ризики для безпеки, що побічно ставлять під загрозу корпоративні мережі.

І хоча темп зростання нових пристроїв сповільнився, останні дані свідчать про те, що він повернувся майже до попереднього обсягу. Зростаюча кількість пристроїв у домашніх мережах та відсутність безпеки можуть створити можливості для доступу стороннім людям. Коли додаються різноманітні пристрої із виходом в мережу з слабкими політиками безпеки, спільними паролями Wi-Fi та швидко побудованою інфраструктурою, щоб забезпечити безперебійну безперервність бізнесу, відбувається момент, коли одна вразливість або помилковий крок у конфігурації може відкрити двері для зловмисників.

Нові хвилі шкідливого програмного забезпечення, котре використовує пристрої або користувачів як проксі-сервери для досягнення більш цінних активів у корпоративних мережах, є одними із найбільших потенційних загроз у постпандемічному світі. Ситуація також дуже зручна для суб'єктів промислового шпигунства, які планують цілеспрямовані

напади на вибраних жертв. Таким чином, забезпечити безпеку домашніх мереж, а також залишатися сегментованими та прозорими для звичайних користувачів є викликом найвищого значення.

2. Штучний інтелект – засіб для усунення розриву між реальним часом та інформацією про нові загрози

Хоча численні схеми захисту виявились корисними та ефективними в певних ситуаціях від відомих векторів атак та загроз, одна з найбільших проблем – це подолання невідомого. Штучний інтелект є одним із засобів, який можна використовувати для подолання розриву між виявленням та захистом від невідомих або швидкозмінних загроз. Хоча зібраний досвід та знання, як правило, є безперечними джерелами істини для захисту, в даний час вони в основному успішно констатують вже відоме: певна загроза трапилася (зараз чи раніше), і ось як захистити від неї.

Одним із прикладів того, як штучний інтелект використовується у швидко змінних умовах пандемії та постпандемії, є розпізнавання веб-сайтів без категорій або без міток з незаконними намірами, які пов'язані із звичайними тригерами, такими як страх. За даними MarkMonitor, існує понад 100 000 зареєстрованих доменів COVID-19. Аналіз веб-сайтів без категорій, до яких користувачі отримували доступ протягом 50 днів, показує, що приблизно від 20% до 35% веб-сайтів містять вміст, який, хоча і не є безпосередньо небезпечним, однаково вводить в оману або демонструє ознаки можливого незаконного наміру.

Хоча розвідка загроз є джерелом підтвердження зловмисності, використання штучного інтелекту передбачить потенційну зловмисність до того, як вона стане відомою або зареєстрованою в базах знань. І хоча існують певні чітко визначені політики, проблем тут може бути мало чи взагалі не бути. Однак у світі зі змішаними правами та правилами щодо віддаленої роботи – або, принаймні, для забезпечення того, щоб існували ризики – AI має великі можливості для подолання та допомоги у вирішенні численних проблем.

3. Після пандемії з'являтимуться нові загрози для кібербезпеки

За попередні місяці спільнота кібербезпеки спостерігала численні вектори атак, які використовують тему COVID-19 або як приманку, або як спосіб приховати зловмисну діяльність від простої ідентифікації та виявлення. Тому, оскільки зараз зараження COVID-19 в деяких країнах зменшується, зміни в найбільш поширених моделях нападів неминучі. Однак, здається, ці зміни натхнені не спробами швидкого та легкого використання теми пандемії (як на початку, коли актори загроз швидко створювали шахрайські кампанії), а використанням складних та добре розроблених кампаній у ретельно підібраний час.

Останнім часом співтовариству з кібербезпеки стало відомо про численні спроби імітувати інформаційні програми, а також про те, що шкідливі дії можуть відбуватися під красивою картою зараження або вигаданим «радаром зараження». Іншими словами, такі програми виконують роль троянів віддаленого доступу на пристроях користувачів. Коли троян встановлено на пристрої, актор загрози не тільки здатний фіксувати та маніпулювати конфіденційними даними, але також може виконувати цілий ряд шпигунських дій. Незважаючи на те, що такі кампанії спостерігалися у всьому світі, здається, що спроби розпочати подібні атаки зростають лише в певних регіонах і лише тоді, коли в цьому регіоні спостерігається черговий сплеск інфекцій COVID-19. Іншими словами, кампанії із загрозами безпосередньо корелюють із кількістю заражень та сприйняттям пандемії громадськістю – коли люди відчувають більше занепокоєння, актори загроз посилюють свою експлуатацію теми COVID-19.

Очікується, що до тих пір, поки COVID-19 не буде викорінено принаймні в одному регіоні (як епідемія) до тих пір, широка громадськість не стане менш занепокоєна загрозою, яку вона несе, ми, ймовірно, все ще побачимо безліч ще більш складних прикладів використання COVID-19 як прикриття для здійснення зловмисних дій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Churbanov A. E. The impact of information modeling technology on the development of investment construction process]. Vestnik MGSU, 2018, vol. 13, issue 7 (118), pp. 824–835.

УДК 004.056.5

КАРПЕНКО В. О.,
здобувач вищої освіти ОС «бакалавр» спеціальність 125 «Кібербезпека»
Київський національний торгововельно-економічний університет

ФІШИНГ. БЕЗПЕКА В ІНТЕРНЕТІ

Концепція фішингу вперше була описана в 1987 році в документі з конференції під назвою «Безпека системи: перспективи хакера».

В документі описувалась техніка зловмисників, яка полягає в імітації авторитетних організацій або сервісів.

Саме слово є омофоном англійського слова «Fishing» (рибалка), оскільки техніка використовує ту ж логіку «вилову».

Фішингові повідомлення спонукають до негайних дій, не залишаючи часу на роздуми. Шахрайські повідомлення найчастіше надходять від імені відомих брендів і впливають на емоційне сприйняття інформації.

Такі посилання ведуть на сторінки збору даних, які потім будуть використані проти тебе. Зловмисники у фішингових електронних листах або на сайтах частіше за все збирають таку інформацію:

– імена користувачів і паролі;
– ідентифікаційні номери;
– номери банківських рахунків;
– PIN-коди (особисті ідентифікаційні номери);
– номери кредитних карток;
– дівоче прізвище матері;
– дату народження і т. д.

Фішинг існує впродовж багатьох років, за цей час кіберзлочинці розробили широкий спектр методів інфікування жертв.

Найчастіше зловмисники, які займаються фішингом видають себе за банки чи інші фінансові установи, щоб змусити жертву заповнити фальшиву форму та отримати дані облікових записів.

У минулому для виманювання даних користувачів кіберзлочинці часто використовували неправильно написані або оманливі доменні імена.

Сьогодні зловмисники використовують більш складні методи, завдяки чому фальшиві сторінки дуже схожі на свої легітимні аналоги.

Наприклад, замість @google.com може бути @gogel.com чи @goo.gle.com або замість @company.com використовують @campany.com. Особливою популярністю зараз користуються фішингові email-повідомлення з темою: «Змінити пароль» чи «Підтвердити акаунт», «Змінити умови підписки», «Встановити оновлення на MacOS».

Починаючи з березня цього року, кіберзлочинці розгортають фішингові атаки COVID-19 проти співробітників компаній, зокрема й в галузі охорони здоров'я.

Рекомендовано налаштувати двофакторну аутентифікацію (2FA) сервісів.

У такому випадку, крім логіну та паролю, необхідно також ввести унікальний код, який буде приходити по SMS. Також можна використовувати спеціальні програми для генерації кодів.

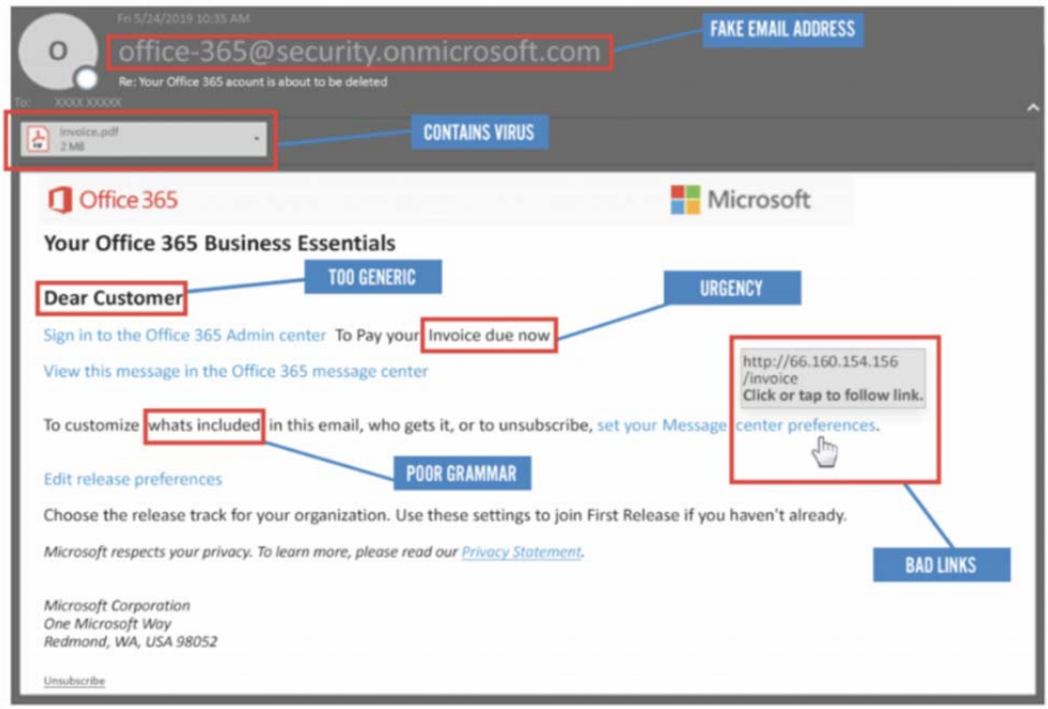


Рис. 1. Приклад фішингового повідомлення

Висновок: З розвитком інтернет-технологій і розширенням інтернет-простору збільшується ймовірність зіткнення з шахрайством. Фішингові повідомлення спонукають до негайних дій, не залишаючи часу на роздуми. Шахрайські повідомлення найчастіше надходять від імені відомих брендів і впливають на емоційне сприйняття інформації. Для того, щоб захистити себе від шахраїв-фішерів треба завести собі декілька поштових адрес, одну з яких використовувати лише для особистого спілкування, іншу – для публічного доступу; взяти собі за звичку ніколи не відповідати на спам; замислитиися про наслідки перш ніж перейти за запропонованим посиланням, воно може вести на фішингові сайти; користуватися спам-фільтрами; своєчасно оновлювати свій інтернет-браузер.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке фішинг та як не стати жертвою зловмисників. Вісімнадцять три нулі [Електронний ресурс]. URL: https://18000.com.ua/blogs/shho-take-fishing-ta-yak-ne-stati-zhertvoyu-zlovmisnikiv/ (дата звернення: 26.11.2020)

2. Фішинг. ESET [Електронний ресурс]. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/ (дата звернення: 26.11.2020)

3. Фішинг: що це таке і як себе убезпечити? Zillya антивірус [Електронний ресурс]. URL: https://zillya.ua/fishing-shcho-tse-take-i-yak-sebe-ubezpechiti (дата звернення: 26.11.2020)

УДК 004.056.5

БАЙ А. С.,
здобувач вищої освіти ОС «бакалавр» спеціальності 122 «Комп'ютерні науки»
Київський національний торговельно-економічний університет

НАЙБІЛЬШ КРИТИЧНІ ВРАЗЛИВОСТІ ВЕБДОДАТКІВ

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.

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]. URL: https://www.owasp.org/index.php/Main_Page
2. OWASP top 10 [Електронний ресурс]. 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]. URL: https://habr.com/ru/post/342986/

УДК 004.056.5

ВАСИЛЬЄВА В. Ю.,
здобувач вищої освіти ОС «бакалавр» спеціальність 125 «Кібербезпека»
Київський національний торгововельно-економічний університет
v.vasylyeva.FIT.125.20@knute.edu.ua

ЯК УБЕЗПЕЧИТИ СЕБЕ ВІД ХАКЕРСЬКИХ АТАК ТА ЗАХИСТИТИ ДАНІ

У 21-му столітті все більше зростає роль інформаційної безпеки, адже ми живемо у столітті інформаційних технологій та постійного прогресу. На жаль, в Україні дуже низький рівень кібербезпеки, через постійні хакерські проникнення та низький рівень розуміння людей про важливість захисту своїх данних. І хоча зараз в Україні існує нормативна база щодо кібербезпеки, її реалізація демонструє недостатню ефективність.

Жертвами хакерів можуть стати не лише люди, але й цілі держави. Кібербезпека – одна з основних проблем, що викликає занепокоєння. І чим швидше людство розвиває інформаційні технології, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем.

Спочатку з'ясуємо хто такі хакери і звідки беруться хакерські атаки. Спочатку хакерами називалися досвідчені ІТ-фахівці, чиєю головною функцією вважалося виправлення помилок в програмному забезпеченні

Причини хакерських атак бувають різні: конкуренція, атака з метою заволодіти даними компанії або організації, шахрайство. Яскравий приклад хакерської атаки – вірус Petya, через який були заморожені десятки українських банків, сайтів, медіаресурсів, сайтів державних і недержавних підприємств, не працювали лікарні, перекрився весь інтернет. Всього, за офіційними даними Microsoft, було заражено майже 13 тисяч комп'ютерів.

На перший погляд може здатися, що кібератаки не можуть завдати великої шкоди та не забирають людських життів. Але це лише на перший погляд: пропаганда – розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору, збір інформації – злом приватних сторінок, втручання в роботу обладнання – атаки на комп'ютери або сервери.

Зараз дуже багато кібератак, тож кожен має дбати про свої данні, щоб мінімізувати відсоток зникнення важливої інформації або її викоритсання іншими людьми.

Будьте уважні, роблячи онлайн-покупки. Не робіть покупки за допомогою чужого пристрою, використовуючи свій пароль чи логін, адже їх можна бути відновити та вкрасти ваші дані, особливо якщо ви платили онлайн і вводили номер своєї картки.

Не приєднуйте незнайомі USB-пристрої до свого комп'ютера. На них може зберігатися вірус, який повністю знищить всі дані зз вашого пристрою.

Мабуть, одна їз найважливіших порад це стежити за своїми підписками, хто додається в друзі в соціальних мережах. Багато хакерів є гарними психолагами, тому можуть ввійти у довіру, і навіть не взламуючи вашу сторінку.

Коли Ви регеструєтесь десь, використовуйте більш складні паролі. Використовуйте більш складні шифровки, наприклад, великі і маленькі букви в слові, цифри комбінуйте з буквами, використовуйте довгі фрази для пароля.

Важливим кроком є ліцензійний антивірус! Захист комп'ютера антивірусом завжди буде актуальний, особливо якщо згадати, скільки шкоди завдають віруси.

Якщо є порушення у роботі комп'ютерів, то слід негайно від'єднати їх від мереж (Інтернет, Wi-Fi).

Перевіряйте свою пошту, але ніколи не відкривайте повідомлення від неівдомих людей, адже там Вас може чекати вірус.

Кращі хакери рекомендують встановити систему захисту від DDoS-атак (безкоштовні програми Deflect, CloudFlare, Google Project Shield).

Напевно, кожен з вас помічав, що інколи під час постингу фотографій географічне місце розташування ставиться автоматично. Це спричинено тим, що у налаштуваннях соцмереж ця графа досить часто заповнюються за умовчанням.

А тому хто завгодно і з будь-якими намірами може дізнатися, де ви відпочиваєте, де живете та де буваєте. Експерти радять видаляти геолокації з ваших особистих постів задля забезпечення власного захисту.

Номер телефону Прикріпляти до свого персонального, а тим паче до бізнес-аккаунту, мобільний номер телефону – звичайна практика, досить зручна та розповсюджена. Проте, незважаючи на практичність такої функції, варто пам'ятати про підводне каміння. Номер телефону може посприяти злому персональної сторінки для використання облікового запису.

Кібератаки будуть постійно переслідувати нас, адже ми розвиваємося, використовуємо пристрої будь-де: розрахуватися в метро чи магазині, купити білет у театр, поповнити мобільний рахунок, соціальні мережі і тд.

Ми, як покоління 21 століття, повинні врешті-решт зрозуміти, що треба починати з себе- треба захищати свої данні. Найголовніше- слідкуати за своїми соцальними мережами, не надавати багато інфрмації про місцезнаходження, обновлювати паролі пошти та на банківських картках. Якщо ми почнимо з себе, то массові кібератаки зменшать свою кількість в рази.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гутман Б., Бегвілл Р. Політика безпеки при роботі в Інтернеті – технічне керівництво. Режим доступу: [http://citforum.ru/internet/security_guide/glava8.shtml#8_7]
2. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту Видавництво: ТИД Діа Софт, 2014. С. 414.
3. Кузнецов А. А. Захист ділового листування (секрети безпеки). М.: Іспит, 2016. 239 с.
4. Wi-Fi Alliance® introduces security enhancements. // Wi-Fi Alliance. 2018. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements.
5. DAN GOODIN. Serious flaw in WPA2 protocol lets attackers intercept passwords and much more // Ars Technica. https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping
6. Handbook of CRM: Achieving Excellence in Customer Management / Adrian Payne, 2005. 438 p.
7. How to Secure Your CRM (Customer Relationship Management) Data From Hackers [Електронний ресурс]. Режим доступу: https://www.cloudbric.com/blog/2018/01/secure-crm-data-hackers
8. PHP: Password Hashing – Manual [Електронний ресурс]. Режим доступу: https://www.php.net/manual/en/faq.passwords.php
9. How to Hash and Verify Passwords with Argon2 in Go – Alex Edwards [Електронний ресурс]. Режим доступу: https://www.alexedwards.net/blog/how-to-hash-and-verify-passwords-with-argon2-in-go
10. Ways to Protect Your Company From a CRM Data Breach [Електронний ресурс]. Режим доступу: https://www.nimble.com/blog/crm-data-breach-protection
11. How to Secure Your CRM (Customer Relationship Management) Data From Hackers [Електронний ресурс]. Режим доступу: https://www.cloudbric.com/blog/2018/01/secure-crm-data-hackers
12. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: наук.-практ. посіб. Київ: К.І.С, 2015. 220 с.

УДК 004.05

ЛИТВИНЕНКО В. В.,
здобувач вищої освіти ОС «бакалавр» спеціальність 125 «Кібербезпека»
Київський національний торгововельно-економічний університет
e-mail: v.lytvynenko.FIT.125.20@knute.edu.ua

ФІШИНГ ТА ЙОГО ВПЛИВ НА ІНТЕРНЕТ-КОРИСТУВАЧІВ

Більшість людей, які стабільно користуються інтернетом, хоч раз стикалися з шахрайством у мережі. Ми все більше дізнаємося про різні види махінацій у сіті, але актуальність боротьби з ними продовжує зростати. І це не дивно, адже потрапляють на гак зловмисників не тільки новачки, а й досвідчені користувачі.

Фішинг – один з багатьох існуючих інтернет-шахрайств, найпопулярніша схема в інтернеті, метою якої є заволодіння особистими даними користувачів, таких як логін і пароль. Завдяки цим даним зловмисники можуть легко оволодіти вашими платіжними даними або пробратися до вашої конфіденційної інформації, після чого можна стати жертвою шантажу.

Отже, як працює дана схема? Фішингові повідомлення виступають у ролі наживки, вони можуть надійти електронною поштою, у соціальних мережах, месенджерах – усюди, де є можливість зв'язатися з жертвою. Наживка має вигляд повідомлення від надійної організації та містить посилання на, з першого погляду, знайомий сайт, що виступає як пастка.

Перейшовши за посиланням, користувача просять увійти в його обліковий запис або увести платіжні дані, такі як номер банківської картки, CVV-код, PIN-код. Після надання потребуючих даних інформація надсилається шахраям, які тепер можуть використовувати її на власний розсуд. Слід зауважити, що злодії оперують різними інструментами: фішингові сайти, e-mail розсилка, фішингові landing page, таргетована реклама, вікна, що вспливають, та ін., тож потрібно бути дуже уважним, щоб не стати жертвою інтернет-махінацій.

Розпізнати дану схему не так і важко, важливо лише залишатися обачним, користуючись всесвітньою павутиною. Часто можна отримувати повідомлення, що починаються з «Вітаємо! Ви виграли…». Вам повідомляють про виграш у лотереї або розіграші, та, щоб отримати приз, потрібно лише авторизуватися, залишив свої дані на невідомому ресурсі. З іншого боку, пропозиція залишити особисту інформацію може йти від уже добре відомого сайту. У такому випадку потрібно обов'язково звернути увагу на посилання.

Шахраї не можуть створити аналогічний лінк, тож, якщо це їх рук справа, адреса буде відрізнятися від оригінальної: крадії змінюють, дописують літери або міняють їх місцями, додають символи, слова або фрази.

Також є ймовірність отримати даний лінк від знайомого чи друга, чий аккаунт зламали. Якщо посилання визиває підозру, краще не ризикувати та утриматися від натискання. Якщо ви думаєте, що неможливо повестися на дану аферу, то статистика каже про протилежне: фішинг працює не на якість, а на кількість.

Не так давно одна з британських компаній, що спеціалізується на кібербезпеці, провела цікавий експеримент. Відвідувачам кофейні запропонували безкоштовну каву в обмін на лайк корпоративної сторінки у соціальній мережі. У той час, поки відвідувач робив замовлення та чекав на нього, співробітники займалися аналізом профілю споживача та дізнавалися про нього багато цікавої інформації. Видаючи замовлення, бариста видавав інформацію про дату народження, ім'я родичів, освіту клієнта, та таким чином призводив останнього у стан легкого шоку. І все це через таку дрібницю – лайк! Таким інтерактивним методом компанія акцентувала увагу громадян на важливість захисту особистих даних.

Рис. 1. Приклад фішингового сайту

Задля того, щоб захистити себе та свою конфіденційну інформацію, потрібно:

1. Пам’ятати, що нікому і ні при яких обставинах не можна передавати свої особисті дані.
2. Установити хороший антивірус, що допоможе виявити сайт з недобросовісними цілями.
3. Звертати увагу на дизайн сайту та його адресу.
4. При відвідуванні банківських сайтів слідкувати, щоб було встановлене захисне з’єднання.
5. Прибирати листи з невідомих адрес, що «діють на емоції» до папки «спам».
6. Не ризикувати заходити до банківських аккаунтів, користуючись громадським Wi-Fi.

Підбиваючи підсумки, хочеться наголосити на тому, що, окрім фішингу, існує безліч схем для крадіжок особистої інформації користувачів та заподіяння ним шкоди, тож головне – убезпечити себе від таких інтернет-махінацій. Поширюючи інформацію про кібербезпеку, ви уберігаєте себе та своїх близьких від небажаних ситуацій в інтернеті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lakhno V. A., Kravchuk P. U., Malyukov V. P., Domrachev V. N., Myrutenko L. V., & Piven O. S. (2017). Developing of the cybersecurity system based on clustering and formation of control deviation signs. Journal of Theoretical and Applied Information Technology, 95(21), 5778–5786.

2. Дослідження основних тенденцій сучасної розробки вебсайтів / А. М. Десятко, Н. О. Котенко, Т. О. Жирова, В. І. Чубаєвський. Кібербезпека: освіта, наука, техніка = Cybersecurity: Education, Science, Technique. Київський університет ім. Бориса Грінченка. 2019. С. 6–15.

УДК 004.056

КОЛЕСНИК Д. С.,
здобувач вищої освіти ОС «бакалавр» спціальності 122 «Комп'ютерні науки»
Київський національний торговельно-економічний університет
e-mail: d_kolesnyk_foais_18_8_b_d@knute.edu.ua

POPULAR TYPES OF CYBERATTACKS AND METHODS TO PREVENT THEM

Nowadays, people cannot imagine their lives without the Internet. The smartphone is the first thing we pick up when we wake up and the last thing we see in front of us when we go to bed. Today, the Internet is a place for communication, learning, entertainment and work. Every day we pour Tebibyte of information about ourselves into the network, sometimes without even knowing it. IT technologies are evolving rapidly, especially in the current realities of the Covid-19 pandemic. However, at the same time with the development of data transmission technology, develop technology of data theft, or rather cyberattacks.

The purpose of this work is to acquaint the simple user with the types of attacks on the information system and methods of their prevention. So, consider 6 popular types of cyberattacks:

1. Virus and extortion virus

A virus is usually called malware that infects a computer or other computing device when a user opens an email attachment or links to a malicious site. A ransomware virus is a specialized virus that encrypts all files in the system, when infected, and does not give the user data until the ransom is paid.

To reduce the likelihood of being infected with such viruses, you need to be vigilant and learn to recognize suspicious files and questionable requests. In addition, you need to use protective software on your devices.

2. Potentially unwanted programs (PUP)

Potentially unwanted programs are Trojans, spyware, or adware. They are usually installed together with another useful program that the user has decided to download. Such programs can secretly record all keystrokes, scan files on your hard drive and read browser cookies.

To protect yourself from this threat, do not download or install applications, browser extensions, or other applications from untrusted websites. You should also set up regular backups of your device to an external drive or online backup service.

3. Phishing

Phishing is a way of hacking with e-mails, in which the user tries to deceive and force to transfer the login and password from any service or other important information. To do this, the letter can be issued as a message from the bank or a message from an acquaintance.

Using an e-mail protection program will help detect suspicious links and block spam and messages with malicious attachments, and multi-factor authentication (when a user is asked for additional code via SMS when logging in to a service) will help protect your account even if the password has been stolen.

Also talking about phishing, I would like to mention such a type of cyberattack as **Mailbombing**.

It is considered the oldest method of attack, although its essence is simple and primitive: a large number of e-mail messages make it impossible to work with mailboxes, and sometimes with entire mail servers. Many programs have been developed for this purpose, and even an inexperienced user could make an attack by specifying only the victim's e – mail, message text, and the number of required messages. Such programs allow you to hide the real IP address of the sender, using an anonymous mail server for sending. This attack is difficult to prevent, as even the mail filters of the providers can not identify the real sender of spam. The provider can limit the number of letters in the id one sender, but the address of the sender and subject are often generated random manner.

4. Account hacking

A hacker can also access a user's account with a «frontal attack» when a special program goes through many login and password options – usually using a dictionary and other passwords stolen earlier.

To prevent this, you need to block the login to the account after a certain number of login attempts, or set a multi-stage authentication and. You can also protect yourself from automatically trying to log in using a test that distinguishes a human from a robot, such as reCAPTCHA.

5. Man-in-the-Middle

Type of attack where an attacker intercepts a channel of communication between the two systems, and gets access to all the information, which is transmitted. When getting access to this he ivni attacker can modify information needed him a way to achieve their goals. The aim of such attacks – illegal receipt, theft or falsification of transmitted information, or is getting access to the resources of the network. Such attacks are extremely difficult to track, as the attacker is usually inside the organization.

6. DoS and DDoS attacks

These attacks are more commonly used against corporations and firms, but ordinary users often become part of such an attack.

DoS attack that is his aim to make the server does not respond to inquiries. This type of attack does not involves receiving some secret information, but sometimes it happens claim idmohoyu to initialize other attacks. For example, some programs due to errors in their code can cause exceptional situations and when disabling services are able to execute the code provided by the attacker or the attack avalanche type when the server is not can handle a huge number of incoming packets.

DDoS is a subtype of DoS attack that has the same purpose as DoS, but is not carried out from one computer, but from several computers on the network. In these types of attacks used or the occurrence of errors, which lead to the denial of service, or operation of protection, which leads to blocking of the service, and the result also to failure in service.

So, what are the main methods of protection against cyberattacks:

- Timely update the software used
- Use antivirus protection
- Monitor network settings
- Reserve critical systems and resources
- Apply automated analysis tools security and vulnerability detection in software
- Use WAF
- Use antivirus
- Apply a strict password policy
- Use different accounts and passwords for access to various resources
- Use two-step authentication
- Delete old accounts

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цюцюра М. І., Моспан О. В. Інформаційна безпека та її забезпечення у соціальних мережах. Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). Київ: Київ. нац. торг.-екон. ун-т, 2019. С. 63–64.

2. Киберограбление Века – ТОПЛЕС [Електронний ресурс]. URL: https://youtu.be/uYpBIrhW114

3. Закон України Про основні засади забезпечення кібербезпеки України [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. Cyberattack [Електронний ресурс]. URL: https://en.wikipedia.org/wiki/Cyberattack

5. Хакерска Атака [Електронний ресурс]. URL: https://cutt.ly/RhmuG2g

УДК 004.056

ПАШОРІН В. І.,
професор кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет
ЛІЩУК О. В., ВОЛЧАТОВ І. С., ФІЛАТОВ О. І.,
здобувачі вищої освіти ОС «бакалавр» спеціальності 125 «Кібербезпека»
Київський національний торговельно-економічний університет
e-mail: o_lishchuk_foais_18_12_b_d@knute.edu.ua

ЗАХИСТ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ НА РІВНІ ОПЕРАЦІЙНОЇ СИСТЕМИ

Для захисту інформації та моніторингу подій в корпоративній мережі на підприємстві використовують серверну операційну систему. Призначення серверної операційної системи – це управління додатками, що обслуговують всіх користувачів корпоративної мережі, а нерідко і зовнішніх користувачів.

Windows Server дає багато інструментальних засобів для стеження за мережевою діяльністю і використанням мережі. ОС дозволяє:

- переглянути сервер і побачити, які ресурси він використовує;
- побачити користувачів, підключених в даний час до сервера і побачити, які файли вони відкрили;
- перевірити дані в журналі безпеки;
- перевірити записи в журналі подій;
- вказати, при яких помилках адміністратор повинен бути попереджений, якщо вони відбудуться.

Всякий раз, коли користувач починає сеанс на робочої станції, екран початку сеансу затребувана ім’я користувача, пароль і домен. Потім робоча станція посилає ім’я користувача і пароль в домен для ідентифікації. Сервер в домені перевіряє ім’я користувача і пароль в базі даних облікових карток користувачів домену. Якщо ім’я користувача та пароль ідентичні даним в обліковій картці, сервер повідомляє робочу станцію про початок сеансу. Сервер також завантажує іншу інформацію при початку сеансу користувача, як наприклад установки користувача, свій каталог і змінні середовища.

За замовчуванням в усіх користувачів облікові картки в домені дозволяють входити в систему. Тільки картками груп адміністраторів, операторів сервера, операторів управління печаткою, операторів управління дисконтними картками і операторів управління резервним копіюванням дозволено це робити.

Для всіх користувачів мережі підприємства передбачено своє ім’я та пароль.

Кожен клієнт, який використовує мережу, має облікову картку користувача в домені мережі. Облікова картка користувача містить інформацію про користувача, що включає ім’я, пароль та обмеження щодо використання мережі, що накладаються на нього. Облікові картки дозволяють згрупувати користувачів, які мають аналогічні ресурси, в групи; групи полегшують надання прав і дозволів на ресурси, досить зробити тільки одну дію, дає права або дозволу всій групі.

Windows Server дозволяє визначити, що увійде в ревізію і буде записано в журнал подій безпеки щоразу, коли виконуються певні дії або здійснюється доступ до файлів. Елемент ревізії показує виконану дію, користувача, який виконав його, а також дату і час дії. Це дозволяє контролювати як успішні, так і невдалі спроби будь-яких дій.

Журнал подій безпеки для умов підприємства є обов’язковим, так як в разі спроби злому мережі можна буде відстежити джерело.

Насправді протоколювання здійснюється тільки у відношенні підозрілих користувачів і подій. Оскільки якщо фіксувати всі події, обсяг реєстраційної інформації буде рости занадто швидко, а її ефективний аналіз стане неможливим. Стеження важливо в першу чергу як профілактичний засіб. Можна сподіватися, що багато користувачів утримаються від порушень безпеки, знаючи, що їх дії фіксуються.

Права користувача визначають дозволені типи дій для цього користувача. Дії, регульовані правами, включають вхід в систему на локальний комп'ютер, вимикання, установку часу, копіювання і відновлення файлів сервера і виконання інших завдань.

В домені Windows Server права надаються і обмежуються на рівні домену; якщо група знаходиться безпосередньо в домені, учасники мають права у всіх первинних і резервних контролерів домену. Для кожного користувача підприємства обов'язково встановлюються свої права доступу до інформації, дозвіл на копіювання та відновлення файлів.

Для домену визначені всі аспекти політики пароля: мінімальна довжина пароля (6 символів), мінімальний і максимальний вік пароля і винятковість пароля, який охороняє користувача від зміни його пароля на той пароль, який користувач використовував недавно.

Коли дозволене блокування облікової картки – облікова картка блокується у разі кількох безуспішних спроб початку сеансу користувача, і не більше, ніж через певний період часу між будь-якими двома безуспішними спробами початку сеансу. Облікові картки, які заблоковані, не можуть бути використані для входу в систему.

Якщо користувачі примусово відключаються від серверів, коли час їхнього сеансу минув, то вони отримують попередження саме перед кінцем встановленого періоду сеансу. Якщо користувачі не відключаються від мережі, то сервер зробить відключення примусово. Однак відключення користувача від робочої станції не відбудеться. Години сеансу на підприємстві не встановлені, так як в успішній діяльності зацікавлені всі співробітники і часто деякі залишаються працювати понаднормово або у вихідні дні.

Коли користувачу потрібно змінити пароль, а він не встиг змінити його вчасно, то цей пароль блокується. При простроченні пароля користувач повинен звернутися до адміністратора системи за допомогою в зміні пароля, щоб мати можливість знову входити в мережу. Якщо користувач не входив в систему, а час зміни пароля підійшло, то він попереджений про необхідність зміни, як тільки він буде входити.

Windows надає можливість захистити зашифровані файли і папки на томах NTFS завдяки використанню шифрованого файлової системи EFS (Encrypting File System). При роботі в середовищі Windows можна працювати тільки з тими томами, на які є права доступу.

При використанні файлової системи EFS можна робити шифрування даних за допомогою пари ключів. Будь-який користувач, який захоче отримати доступ до певного файлу, повинен мати особистий ключ, за допомогою якого дані файлу будуть розшифровуватися. Система EFS так само забезпечує схему захисту файлів в середовищі Windows.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом СТСЗІ СБ України від 28.04.1999 № 22.

2. Петров О. С. Основи безпеки інформаційних систем. Луганськ: Вид-во СНУ ім. В. Даля, 2004. 148 с.

3. Panek Crystal. Windows Server Administration Fundamentals Sybex; John Wiley & Sons, Inc., 2020. 389 p. ISBN 978-1-119-65065-2.

УДК 004.056

МУКВІЧ А. Л.,
здобувач вищої освіти ОС «магістр»
спеціальності 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: mukvichandriy@gmail.com.
ЖИРОВА Т. О.,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет

КІБЕРБЕЗПЕКА У СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СВІТІ – КЛЮЧОВІ ТЕНДЕНЦІЇ ТА ЗАГРОЗИ

1. Перша умова для безпечної роботи в Мережі – дотримання базових норм кібергігієни

Сучасна Глобальна мережа містить у собі цілу низку серйозних загроз, включаючи загрози зараження вірусами, крадіжку паролю та персональних даних, зламу інтернет-гаманця та ін. Краща стратегія захисту – знати заздалегідь, звідки саме чекати загрози та який алгоритм дій виконати для уникнення зустрічі з нею. Приміром, досвідчений користувач ніколи не видасть свій пароль зловмиснику, з самого початку знаючи, що легітимні працівники банків ***ніколи*** не роблять подібних запитів. Схожі аналогії актуальні для будь-якого типу мережевої загрози.

2. Антивірус бореться з наслідками, в той час як кібергігієна – з першопричиною

Кібергігієна як спосіб захисту має вищу ієрархію та більшу цінність, аніж різноманітне антивірусне ПЗ. Набагато дешевше просто не допустити зараження власного пристрою шляхом дотримання простих правил безпеки (відмова від завантаження невідомих файлів без підпису та видавця, ігнорування фішингових сторінок і т.д.), аніж боротися з самими наслідками цього зараження, покладаючись на потужність антивірусного ПЗ. Простий доказ тому – процедура лікування або видалення вірусу може коштувати значних витрат часу та ресурсів, і навіть за короткий час свого існування у пристрої вірус здатен спричинити суттєву шкоду.

3. Антивірусне ПЗ з різних причин апріорі не здатне захистити користувача від усіх видів загроз

Таблиця 1

Перелік типових обставин, при яких антивірусне ПЗ може виявитись неефективним при боротьбі з загрозами

№ п/п	Обставина	Опис обставини
1	*Користувач має справу з загрозою «нульового дня»*	Розробка нових вірусів не припиняється ні на хвилину. У тому разі, якщо з моменту розробки шкідливого ПЗ минуло надзвичайно мало часу (наприклад – менше доби), розробники захисного ПЗ просто фізично не встигають як слід вивчити цю загрозу та підібрати до неї захист (або внести її код у базу антивірусних сигнатур). У такому разі користувач лишається майже беззахисним перед хакером

Закінчення табл. 1

№ п/п	Обставина	Опис обставини
2	*З моменту розробки вірусу хоч і минуло достатньо часу, однак його не було додано у склад сигнатур*	Даний чинник доволі сильно залежить від типу антивірусу, його можливостей та потужності. Однак враховуючи статистику (кожен рік з'являється близько 90 млн нових одиниць шкідливого ПЗ), додати усі 100% загроз у антивірусну базу – завдання майже невиконуване для будь-якого розробника будь-якого розробника
3	*Антивірус не володіє функцією евристичного аналізу*	Для протидії вірусам, шкідливий код яких відсутній у базі сигнатур, існує метод захисту відомий як «евристичний аналіз» – це означає, що антивірус досліджуватиме поведінку програм, наявних на комп'ютері, на предмет її схожості з типовою поведінкою шкідливого ПЗ. Однак цей підхід має цілий ряд недоліків: він відсутній на багатьох антивірусах, він може визначити як вірус цілком безпечну програму, він не завжди гарантує безпечне для ПК вилучення вірусу і т.д.
4	*Антивірус не здатен до самозахисту*	Особливо потужні та розвинені віруси здатні самостійно знаходити наявне на пристрої антивірусне ПЗ та знешкоджувати/видаляти/паралізувати його служби й процеси ще до того, як антивірус встигне спрацювати першим. Рішення такої проблеми може бути лише комплексним – у поєднанні кібергігієни та використанні потужного, перевіреного антивірусного ПЗ

4. Розгортання заходів кібербезпеки в масштабах держави відбувається на кількох окремих рівнях.

Це – рівень Уряду, який задає стратегію кібербезпеки в цілому, рівень об'єктів критичної інфраструктури та державних корпорацій, які передусім потребують захисту, а опісля – рівень приватних компаній та груп, що мають відчувати підтримку держави та водночас дотримуватись правил та норм інформаційної безпеки, наявних у законодавстві.

Така схема організації розгалуженого захисту країни є достатньо ефективною та дозволяє: розподілити пріоритети захисту, виявити та нейтралізувати потенційні уразливості у інфраструктурі вищого рівня, розподілити повноваження: який орган і що має захищати, а також створити законодавство, здатне відповідати світом кібернетичним загрозам світу.

УДК 004.056

КУПІНА В. Я.,
здобувач вищої освіти ОС «бакалавр»
спеціальності 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
e-mail: 121-7-17-kupina@knute.edu.ua

КІБЕРБЕЗПЕКА ТА СЗД. ПІДХІД NETAPP: ПРІОРИТЕТ НА ІНФОРМАЦІЮ

Інформація – найважливіший актив і зброя, вона ж є основою епохи, де принцип «довіряй, але перевіряй» змінюється на «перевіряй і ніколи не довіряй». Ми живемо в епоху «нульової довіри»,а це означає те, що існує необхідність пильного контролю даних. Давно минули часи, коли існує необхідність пояснювати, що зберігання інформації на сервері – запорука їх втрати, пошкодження чи викриття.

Правильний підхід збереження та безпеки даних вимагає:

- Знання, де зберігаються дані організації
- Класифікація даних
- Безпечної утилізації тих даних, які більше не потрібні
- Розуміння, яким співробітникам і до яких даними необхідний доступ
- Використання мультифакторної авторизації для адміністративного доступу і доступу до даних
- Використання шифрування
- Відстеження і реєстрація доступу

Все це реалізовано у провідного постачальника систем зберігання NetApp. Раніше компанія спеціалізувалася тільки на рішеннях, в основі яких була ONTAP – власна операційна система компанії для сховищ даних, таких як NetApp FAS і AFF. Однак незважаючи на те, що система дійсно добре працює, її неможливо застосувати до всіх нових продуктів NetApp. Це заважало розвитку нових рішень. У 2019 NetApp розповіла про зміни в стратегії розвитку і випуску нових продуктів на основі Data Fabric. В 2020 компанія диверсифікується і стає серйозним гравцем на ринку ще й хмарних рішень. NetApp позиціонує сімейство своїх продуктів як основу для безперешкодного переміщення даних з локального середовища в хмару, а потім – управління ними з єдиним, призначеним для користувача, інтерфейсом, незалежно від використовуваних хмарних платформ. Чому NetApp? І в локальному середовищі, і в хмарах збережено основні принципи кібербезпеки. Адаптивні рішення для шифрування і управління ключами дозволяють захищати важливі дані як on-premises, так в хмарах та між ними. Іншими словами, шифрування по-справжньому ефективне тільки тоді, коли воно працює в будь-який інфраструктурі. Також воно буде ефективним, лише якщо працює, як з даними на локальних ресурсах, так і в процесі переміщення даних. Другий принцип забезпечення кібергігієни та кібербезпеки – місце розташування. Тільки знаючи, де знаходяться ваші дані, ви можете обирати, які з них зберігати, які класифікувати і до яких надавати доступ. У свою чергу, класифікація забезпечує основу для дотримання норм, безпеки та ефективності. Визначення, які дані найбільш важливі, відповідно до таких норм, як Стандарт захисту даних в галузі платіжних карт (PCI-DSS) і Європейський Загальний закон про захист даних (GDPR), дозволяє впровадити відповідні заходи безпеки. Розташування – головний елемент управління ризиками. Останній принцип – доступ. Рішення NetApp Data ONTAP забезпечує визначені ролі з управління доступом для кластерів і віртуальних сховищ (SVM). Воно також дозволяє створювати додаткові ролі і налаштовувати права доступу до певних команд і директив. Завдяки системам збереження даних впроваджуються надійні методи кібербезпеки підприємства, а завдяки досконалим рішенням – все це відбувається без втрати ефективності, швидкості доступу до інформації. Систематизуючи дані, системи зберігання забезпечують безпечність, чистоту, надійність та ефективність використання ресурсів.

УДК 004.056.5

PASHORIN V.,
Professor of Software Engineering and Cybersecurity department
SALEOMON A.,
Applicant for education in the specialty of 125 «Cybersecurity»
Kyiv National University of Trade and Economics
e-mail: A_Saleomon_FOAIS_18_12_B_d@ knute.edu.ua

AN INTEGRATED APPROACH TO PROVIDE A SECURITY OF PERSONAL DATA IN THE ORGANIZATION

Technological companies are extremely popular because of innovations they provide into modern society. But it's not enough to sell a specific product – a company needs to support a client and to give him an opportunity to ask for a solution if problem existed. That's why this organization decided to create and open a call center in Kyiv. The main topic of this research is to create an approach to secure and protect customer's data in this specific call center. People in this company are using great applications and services to protect Data Bases from third-party individuals, but the main problem is all about the attitude of local security service. They generate easy and simple passwords, which are similar to every worker. Server room and warehouses are not protected as they should. Almost every agent (customer support agent) knows nothing about security of customer data. Those are main factors that hackers can use to get an access. [1] To get the job of a customer support agent all you need to do is to get through 2 weeks of study and to pass an easy test. It's because of staff turnover. Every call center faces this type of problem. People don't like this job and leave it after few months of hard work. To get new people, a company needs to provide an easy way to pass the test and to get started as an agent. This is not good, because new workers can be as bad, as it really possible, and that can make an impact on the reputation of the company. Other organizations can use it in their favor. They can get a spy to work there and to find all the information they need. That is very easy to do, because local workers have so much access to any kind of data: Data Bases, corporate services and even passwords of almost anybody who works there less than a month. Hackers can passively make an impact on a system by loading all the data without deleting it or changing their structure. The situation around coronavirus changed most of things in the organization. People started working from home. A spy could get into corporation as an agent and the easiest way to get the data is to copy. He does not even need a key-logger or a specific virus to get an access. [2] In this situation security service needed to change the way their authentication system works and the level of access to information. Of course, there is a way to solve these problems. A security service needs to implement a multi-factor authentication to get an access to the room (they need to locate a terminal, which is sensitive to the specific magnetic card, and to add a feature of entering a password as a second type of the authentication itself). A multi-factor authentication is a strong way to protect the actual data from stealing. That's why an organization has to implement it for every corporate service to restrict an access to third parties. They also need to create a strong random password generator and password manager to make sure that those are reliable. Telegram-bot is often used to regulate and control phone calls, which were made by a client. This bot is very unstable, because 40–50 workers use it in the same time and it is very likely to be stopped this way. In this situation I would recommend to use Avaya. This service is reliable and Samsung has an experience of using it in the past. I would also recommend giving specific privileges of using software to every worker. Finally, security policy needs to be converted and adapted to the newest and the freshest ways of saving and protecting data. Every agent needs to be told about rules he should follow and responsibility for the violation.

REFERENCES

1. Kevin Mitnick. «The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data», 18–50 (2017).

2. Georgia Weidman. «Penetration Testing: A Hands-on Introduction to Hacking», 179–360 (2014).

УДК 004.056

ГАЛИЧ І. В.,
здобувач вищої освіти ОС «бакалавр»
спеціальності 121 «Інженерія програмного забезпечення»
Київський національний торговельно-економічний університет
i.halych.fit.121.20.m@knute.edu.ua

КІБЕРБЕЗПЕКА В РАМКАХ ЗАКОНУ «ПРО НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ»

Національна безпека України – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [1]. З кожним роком кібербезпека збільшує свою вагу не тільки на рівні кожного окремого громадянина, а і на рівні цілої держави. Це потребує правового регулювання на рівні національної безпеки. На теперішній момент загрози національній безпеці України та відповідні пріоритети державної політики у сфері кібербезпеки визначає Стратегія кібербезпеки України.

Стратегія кібербезпеки України – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1]. Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [2].

Для досягнення цієї мети можна сформулювати такі кроки як:

- Створення національної системи кібербезпеки;
- Збільшення ефективності боротьби з загрозами у воєнній сфері;
- Кіберзахист державних електронних інформаційних ресурсів, а також інформаційної інфраструктури;
- Захист інтересів громадянина, суспільства та держави в кіберпросторі.

Також визначенні основні загрози національної безпеки в даній сфері:

- невідповідність інфраструктури і сучасним вимогам;
- недостатня ефективність та рівень координації суб'єктів сектору безпеки і оборони України.

Суб'єктами сектору безпеки і оборони встановленні:

- Міністерство оборони України (відбиття воєнної агресії у кіберпросторі)
- Державна служба спеціального зв'язку та захисту інформації України (формування та реалізація державної політики)
- Служба безпеки України (попередження та виявлення злочинів)
- Національна поліція України (забезпечення захисту прав і свобод громадянина)
- Національний банк України (формування вимог кіберзахисту у банківській сфері)
- розвідувальні органи (здійснення розвідувальної у кіберпросторі)

Пріоритетом та напрямом забезпечення кібербезпеки України є розвиток безпечного, стабільного і надійного кіберпростору. Підсумувавши, на рівні національної безпеки питання кібербезпеки чітко визначене, як із сторони можливих загроз та напрямів покращення і розподілення відповідальності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про національну безпеку України: Закон України [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016#n11

Наукове електронне видання

КІБЕРГІГІЄНА. КІБЕРБЕЗПЕКА. БЕЗПЕКА ДЕРЖАВИ

МАТЕРІАЛИ НАУКОВИХ СЕМІНАРІВ

(Київ, 27 листопада 2020 року)

Видавець і виготовлювач
Київський національний торговельно-економічний університет
вул. Кіото, 19, м. Київ, Україна, 02156
Електронна пошта knute@knute.edu.ua

Свідоцтво суб'єкта видавничої справи серія ДК № 4620 від 03.10.2013 р.