МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Колективна монографія

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Колективна монографія

Київ
Європейський університет
2023

УДК [004.056(53+55):003(26+27)]+621.643.8
А 43

Рекомендовано до друку Вченою радою ПВНЗ «Європейський університет» (протокол № 3 від 28.09.2022)

Рецензенти:
В.А. Лахно – доктор технічних наук, професор
(Національний університет біоресурсів і природокористування України)
М.Г. Медведєв – доктор технічних наук, професор
(Таврійський національний університет імені В. І. Вернадського)
О.А. Чемерис – доктор технічних наук, старший науковий співробітник
(Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України)

А 43 Актуальні питання забезпечення кібербезпеки та захисту інформації: колективна монографія / за заг. наук. ред. А.М. Давиденко, Київ: Європейський університет, 2023. – 240 с.

ISBN 978-966-301-259-9

Монографія є результатом тривалих наукових досліджень і пошуків авторів у напрямі обґрунтування сучасних концепцій, моделей, механізмів, проблем та перспектив розвитку наукових засад забезпечення кібербезпеки та захисту інформації України та світу; узагальнено та висвітлено організаційно-технологічні аспекти функціонування та захисту об’єктів критичної інфраструктури; наведено теоретичні засади та розроблено практичні рекомендації щодо безпеки комп’ютерних мереж та інтернет ресурсів в умовах сучасних впливів; проаналізовано проблеми й обґрунтовано перспективи розвитку криптографічних та стеганографічних методів захисту інформації.

До монографії увійшли матеріали доповідей учасників VIII Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», що проходила 2-5 лютого 2022 року на базі «Едельвейс» Європейського університету.

УДК [004.056(53+55)::003(26+27)]+621.643.8

ISBN 978-966-301-259-9

ЗМІСТ

РОЗДІЛ 3.
КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

ПЕРЕДМОВА

Дозвольте висловити вдячність усім науковцям, які взяли участь у роботі над монографією, за самовіддану працю в цей нелегкий час. Сподіваємося, що цей вагомий науковий внесок дасть поштовх до нового розвитку теоретичних засад забезпечення кібербезпеки та захисту інформації в Україні та сприятиме швидшій перемозі України. Сьогодні небайдужість суспільства та наукової спільноти відіграє особливу роль у забезпеченні обороноздатності нашої держави. Сучасні умови існування як ніколи потребують об'єднання та формування наукових наробок щодо забезпечення кібербезпеки та захисту інформації на засадах розвитку інформаційних технологій в Україні та світі. Формування монографії було розпочато ще до військових дій як традиційне дослідження науковців в рамках постійно діючих семінарів та наукових конференцій ПВНЗ «Європейський університет» та Національного авіаційного університету під керівництвом професорів Тимошенко О.І. та Корченко О.Г., яке у процесі роботи було трансформовано відповідно до умов сьогодення. У монографії досліджено сучасні концепції, моделі, механізми, проблеми та перспективи розвитку наукових засад забезпечення кібербезпеки та захисту інформації України та світу; узагальнено та висвітлено організаційно-технологічні аспекти функціонування критичної інфраструктури; наведено теоретичні засади та розроблено практичні рекомендації щодо безпеки комп'ютерних мереж та інтернет ресурсів в умовах сучасних впливів; проаналізовано проблеми й обґрунтовано перспективи розвитку криптографічних та стеганографічних методів захисту інформації. Автори сподіваються, що їм вдалося дослідити проблематику і сформувати рекомендації щодо забезпечення розвитку технологій захисту інформації в Україні та світі, шляхом систематизації та обґрунтування ключових положень теорії і практики наукового забезпечення кібербезпеки та захисту інформації в Україні, та оцінити вплив світових тенденцій розвитку на захист інформації в цілому.

Монографія містить передмову та 3 розділи.

Перший розділ «Кібербезпека та захист інформаційної інфраструктури» присвячено опису теоретичних основ забезпечення кібербезпеки та захисту інформації в Україні. Розглянуто питання загроз та безпеки кіберпростору, ризики кібервійни; досліджено проблеми кіберзлочинності та наслідки її глобалізації; розглянуто поняття Інтернету речей (IoT) та загрози від пристроїв IoT; підняте питання кібершпигунства та стеження; наведено приклади кампаній з кібершпигунства, що здійснюються на рівні країн; розглянуто підхід та принципи безпеки з нульовою довірою (Zero trust security) та принципи його використання; описано основні функції та рішення, що використовуються світовими організаціями для підтримки моделі безпеки з нульовою довірою;

розглянуто помилки безпеки веб-додатків за версією організації Open Web Application Security Project (OWASP); з огляду на постійний та еволюціонуючий характер загроз кібербезпеці зазначена важливість їх подолання на основі багатостороннього підходу **(Тимошенко О. І., Литвиненко Л. О., Колодінська Я. О.).** Розглянуто можливість побудови базових інформаційних компонент для розширення засобів захисту системи доступу з метою використання опису складових частин системи захисту на природній мові. **(Корченко О. Г., Давиденко А. М., Висоцька О. О., Щербина В. П.)**. Досліджено що у більшості зломів систем безпеки використовується соціальна інженерія, а не електронний злом чи зняття інформації по каналам витоку інформації; зазначено що користувачі є найслабшою ланкою в системі безпеки і саме тому можливі атаки із застосуванням соціотехніки; проаналізовано що методи соціальної інженерії представляють найбільшу загрозу інформаційній та/або кібербезпеці, особливо якщо атаки здійснюються на об'єкти критичної інфраструктури; досліджено що для створення системи реагування на соціотехнічні атаки актуальним є оцінка наслідків таких атак. **(Дівізінюк М. М., Міщенко А. В., Лазаренко С. В., Клобуков В. В.)**. За рахунок використання літературно-концептуального дослідницького підходу в статті показано, що поняття конкурентної розвідки багатогранно, а штучний інтелект відіграє велику роль у вивченні та моніторингу конкурентів, іншим аспектом є важливість конкурентної розвідки для керівників підприємств. **(Obozna A. O., Iakovunyk O. V., Iakovunyk D. I.)**. Проаналізовано можливості застосування методу агентного моделювання для дослідження інформаційного протиборства у соціальних мережах **(Васильєва О. О., Бутвін Б. Л.)**. Досліджено зарубіжний досвід щодо здійснення організаційних заходів, спрямованих на розбудову державних систем забезпечення кібербезпеки, програми кібернавчання у США та ЄС для виявлення проблемних зон кіберзахисту інфраструктури, моделювання можливих кіберінцидентів і вироблення типових схем реагування на них, поліпшення міжвідомчої взаємодії. На основі проведеного аналізу досвіду розвинутих зарубіжних країн сформульовано рекомендації щодо створення в Україні відповідних структур, систем та заходів у сфері забезпечення кібербезпеки та протидії кібератакам (**Ткаченко О.В.**). Розглянуто важливість високого рівня безпеки функціонування електронних комунікацій в умовах кібератаки на державні комунікаційні послуги та послуги на базі електронних комунікацій (соціальні мережі, соціальні медіа, засоби масових комунікацій); відзначено що нові комунікації, нове обладнання розширюють можливості на рівні людина-суспільство-держава-кіберзловмисник, а тому від безпеки та стійкості залежить функціонування електронних комунікацій як окремо, так і в складі інформаційно-телекомунікаційних систем, інформаційної та критичної інфраструктури **(Гнатюк С. Є.)**. Розглянуто можливість розширення ролі кібергігієни серед користувачів послуг на базі електронних

комунікацій, які на сьогодні широко використовуються, а саме: Інтернет-шопінг, комунальні платежі, мобільний банкінг, передача персональних даних; досліджено, що рівень кіберзагроз зростає пропорційно рівню діджиталізації та віртуалізації комунікацій окремих громадян; досліджено що для запобігання та протидії кіберзлочинам серед населення необхідно збільшувати кількість заходів із попередження, роз'яснення та просвітництва широких верств населення питанням кібергігієни; аргументовано набуття актуальності питання допомоги населенню з питань кібердопомоги **(Скибун О. Ж.)**. Розглянуто математичну модель розподілу імовірностей порушень кібербезпеки без урахування їх категоричності **(Хохлачова Ю. Є, Скворцов С. О., Вишневська Н. С.)**.

Другий розділ «Безпека комп'ютерних мереж та інтернет ресурсів» присвячено аналізу безпеки комп'ютерних мереж та інтернет ресурсів. Проаналізовано, що збільшення числа комп'ютерних інцидентів, пов'язаних з зовнішнім втручанням в роботу систем, спонукало до розробки систем своєчасного виявлення такого втручання; досліджено, що сьогодні такі системи стали необхідним компонентом інфраструктури безпеки організацій, де виявлення і попередження атак є складовою повсякденної роботи фахівців з кібербезпеки; досліджено технології виявлення комп'ютерних атак, розглянуто системи виявлення вторгнень, методів аналізу виявлених атак, систем запобігання вторгнень; наведено і проаналізовано класифікацію, компоненти і архітектуру систем IDS; запропоновано методи захисту комп'ютерної мережі на базі систем виявлення вторгнень **(Пашорін В. І., Скляренко О. В., Милашенко В. М.)**. Досліджено що формування захищених віртуальних каналів на мережевому рівні моделі OSI дає оптимальне співвідношення між прозорістю та якістю захисту; аргументовано що для цього призначений IPsec (Internet Protocol Security) – набір протоколів для безпечної передачі даних IP мереж, який є доповненням до протоколу IP ver.4 та складовою IP ver.6; досліджено що стек протоколів IPSec використовується для автентифікації учасників обміну, тунелювання трафіку та шифрування IP-пакетів; проведено огляд та аналіз протоколів, алгоритмів, стандартів, режимів і типів перетворень, які використовуються для організації IPSec; зазначено що результати проведеного дослідження можуть бути використані для побудови спеціалізованої захищеної комп'ютерної мережі на прикладі IPsec **(Ніколаєвський О. Ю., Левченко С. В., Невзоров А. В., Скляренко О.А.)**. Доведено можливість побудови системи таємного Інтернет голосування, в якій повноцінний аудит доступний для всіх виборців та їх довірених осіб; зазначено, що під повноцінним слід розуміти такий аудит, при якому перевіряється все, що може викликати сумнів; на базі відкритого блоку серверів створено натурну модель системи для проведення експериментального голосування та розроблено детальну методику повноцінного аудиту; зазначено, що експеримент може проводити будь-хто в будь-який момент за посиланням в Інтернеті; таким чином, показано, що не лише

при традиційних технологіях таємного голосування можливий повноцінний аудит, завдяки якому у виборців немає сумнівів щодо збереження таємниці свого голосування та чесності результатів; зазначено, що для проведення повноцінного аудиту за описаною методикою не потрібно залучати висококваліфікованих спеціалістів, а цілком достатньо сучасної шкільної освіти, яка є обов'язковою у багатьох країнах **(Хлапонін Ю. І., Вишняков В. М., Пригара М. П., Шпак О. І.)**. Розглянуто процес аналізу подій з кібербезпеки, а саме аспект зменшення кількісті хибних спрацювань. Розглянуто шляхи зниження фінансових витрат на кібербезпеку та збільшення швидкості протидії зловмисника **(Венгерський П., Карпюк Р.)**. Розглянуто створення застосунку для аналізу мережевого трафіку (**Герей Т. М., Буковецький В. І., Матьовка Т. В., Різак В. М.)**.

Третій розділ «Криптографічні та стеганографічні методи захисту інформації» присвячено криптографічним перетворенням та іншим методам закриття інформації. Досліджено криптографічні алгоритми захисту інформації та програмне забезпечення, яке їх використовує; розроблено програмне забезпечення у вигляді прихованої програми для заміток «Нотатки» із безпечним зберіганням даних для вирішення проблеми конфіденційності інформації користувачів; зазначено, що дане програмне забезпечення складається з 3 компонентів і написане на мові програмування Python, програма «Нотатки» є основним компонентом, її основні функції: створювати, зберігати, видаляти та редагувати текстові замітки; зазначено, що використовуючи криптографічний алгоритм на основі RSA, програма для заміток зашифровує та розшифровує інформацію, що міститься в базі даних; описано що для приховування існування програми для заміток, вона впроваджена в програмний додаток «Калькулятор»; вказано, що даний додаток містить в собі повноцінний математичний функціонал, з якого відбувається запуск програми «Нотатки», при певних діях та правильній авторизації **(Боценюк Л. Р., Матьовка Т. В., Буковецький В. І., Різак В. М.)**. Наведено особливості поширених методів стеганографії; розглянуто вимоги до стеганосистем; зазначено, що особлива увага приділяється основним задачам та областям застосування методів відкритої стеганографії **(Мартинюк Г. В., Мелешко Т. В., Бичков В.В.)**. Здійснено класифікацію стеганоаналітичних методів за різними критеріями, окреслено місце та особливості методів стеганоаналізу на базі машинного навчання; описано способи формування тестових наборів контейнерів, переваги та недоліки кожного; продемонстровано широкий спектр наявних статистичних моделей характеристичних векторів, що концентрують зміни, внесені стеганографічним перетворенням; виділено та проаналізовано класифікатори, які застосовуються для вирішення задач стеганоаналізу; здійснено чисельні експерименти, що підтверджують перевагу ансамблевого класифікатора на базі лінійного дискримінанту Фішера над методом опорних векторів з лінійним ядром при

роботі з великорозмірними моделями; описано як наявні класифікатори розширюються на багатокласовий стеганоаналіз **(Кошкіна Н. В.)**. Зазначено що атомна енергетика відіграє дуже важливу роль в сучасному енерговиробництві; проаналізовано, що безперервна робота АЕС є головною метою підприємства «НАЕК Енергоатом»; описано криптографічні системи захисту інформації для об'єкту критичної інфраструктури Рівненської АЕС, що стандартизовані в Україні, та які запропоновано використовувати для захисту інформації, наприклад, ГОСТ 28147-89, FIPS-197, «Стрибог» тощо; досліджено що за допомогою криптографічних алгоритмів підприємство може захиститись від вторгнення, викрадення чи пошкодження спеціального обладнання та інформації, що може призвести до призупинення роботи АЕС, фінансових та матеріальних втрат для компанії; описано важливість впровадження криптографічної системи захисту інформації на АЕС **(Фесенко А. О., Мирутенко Л. В., Куроєдов А. С.)**. Наведено методики оцінювання коефіцієнту якості шуму, які зустрічаються на сьогодні для оцінки генераторів; проведено аналіз відомих методик на доцільність їх використання для сучасних генераторів рожевого шуму **(Мартинюк Г. В., Мартинайтус Є. О.)**.

З повагою, А. Давиденко

РОЗДІЛ 1.
КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

УДК 004.056.53

ЗАГРОЗИ ТА БЕЗПЕКА КІБЕРПРОСТОРУ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ: ПРОБЛЕМИ, ІНСТРУМЕНТИ, РІШЕННЯ

Тимошенко О.І.
д.ф.н., професор
ректор ПВНЗ «Європейський університет»
office@e-u.in.ua

Литвиненко Л.О.
к.т.н., доцент кафедри інформаційних систем
програмування та кібербезпеки
ПВНЗ «Європейський університет»
l.lytvynenko@gmail.com

Колодінська Я.О.
викладач кафедри математичних дисциплін
та інноваційного проектування
ПВНЗ «Європейський університет»
yanina.kolodinska@e-u.edu.ua

Анотація. У статті розглядаються питання загроз та безпеки кіберпростору, ризики кібервійни. Досліджуються проблеми кіберзлочинності та наслідки її глобалізації. Розглянуто поняття Інтернету речей (IoT) та загрози від пристроїв IoT. Піднімається питання кібершпигунства та стеження. Наведено приклади кампаній з кібершпигунства, що здійснюються на рівні країн. Розглянуто підхід та принципи безпеки з нульовою довірою (Zero trust security) та принципи його використання. Описано основні функції та рішення, що використовуються світовими організаціями для підтримки моделі безпеки з нульовою довірою. Розглянуто помилки безпеки веб-додатків за версією організації Open Web Application Security Project (OWASP). З огляду на постійний та еволюціонуючий характер загроз кібербезпеці зазначена важливість їх подолання на основі багатостороннього підходу.

Вступ.

Кіберпростір – це термін, що використовується для опису взаємопов'язаної мережі комп'ютерів та пристроїв, що надає можливості для здійснення та забезпечення електронних комунікацій та отримання інформації з використанням мережі Інтернет та (або) інших глобальних мереж, призначених

для передачі, аналізу та обробки даних. Він відіграє життєво важливу роль у нашому повсякденному житті, дозволяючи нам спілкуватися, працювати та отримувати доступ до інформації з будь-якої точки світу. Однак, ті самі особливості, які роблять кіберпростір таким корисним, водночас, роблять його вразливим до загроз і ризиків для безпеки. Авторами статті розглянуто основні підходи та принципи, при використанні яких можна запобігти потенційним загрозам у кіберпросторі, а також основні методи захисту від відомих видів кібератак.

У сучасному інформаційному суспільстві постійно зростають ризики кібервійни та загрози безпеці кіберпростору. Розповсюдження застосування мережі Інтернет та хмарних технологій, в тому числі, для критично важливої інфраструктури та військових операцій, сприяє нарощуванню кіберпотужностей як засобу ведення кібервійни. Види кіберзагроз можуть варіюватися від фейків і простих атак щодо відмови в обслуговуванні до значно складних кампаній, таких як крадіжка важливої інформації або маніпулювання даними. Так, прикладом таких кібероперацій може бути розгортання росією кіберкампанії з викраденням та оприлюдненням чутливих даних з метою втручання у американські президентські вибори 2017 році, у чому уряд США звинуватив росію.

Глобалізація кіберзлочинності є одним із факторів сьогодення, які підвищують рівень загроз безпеці кіберпростору. Кіберзлочинці використовують можливості сучасних інформаційно-комунікаційних та мережних технологій, діють через кордони, об'єднуючись у групи або мережі, що ускладнює їх відстеження і переслідування правоохоронними органами. До широко відомих прикладів витоку даних можна віднести злам Equifax у 2017 році [1], в результаті якого були викриті персональні дані 143 мільйонів осіб, та скандал Facebook-Cambridge Analytica у 2018 році [2], в ході якого були зібрані дані мільйонів користувачів без їхнього відома.

Окрім наведених вище загроз безпеці кіберпростору, потрібно відзначити збільшення ризиків кібератак через поширення пристроїв, підключених до Інтернету, відомих як "Інтернет речей". Такого роду пристрої часто мають слабкі протоколи безпеки, що робить їх легкою здобиччю для хакерів, які шукають будь-які можливості отримання доступу до мережі для викрадення конфіденційних даних. Так, у 2016 році кібератака на недостатньо захищений пристрій Інтернету речей спричинила масштабне відключення електроенергії в Україні. А у 2021 році росія здійснила ряд кібератак на Україну з метою ураження ключових державних і банківських інформаційних систем [3].

З огляду на складність і масштабність цих загроз, вирішення питань безпеки кіберпростору потребуватиме багатогранного підходу, який передбачає як технічні заходи, так і політичні ініціативи. Він може включати розробку більш надійних протоколів кібербезпеки і встановлення міжнародних норм і угод, які регулюватимуть використання кіберпотужностей у війні. Також виникають нагальні питання підготовки кваліфікованих кадрів з кібербезпеки та захисту інформації, постійного навчання і підвищення обізнаності як окремих осіб, так і організацій щодо способів захисту кофіденційної інформації та даних.

Отже, проблематика даного дослідження є важливою і актуальною з огляду

на нагальні виклики сьогодення та потребує детального вивчення. Метою статті є аналіз загроз і ризиків безпеці кіберпростіру, дослідження ролі та можливостей технічних засобів, політичних ініціатив у вирішенні цих питань, просвітницької діяльності, а також визначення шляхів та надання окремих рекомендацій щодо подолання і запобігання загрозам кібербезпеки в контексті сучасних викликів.

Ризики кібервійни.

Поняття кібервійни відоме як використання засобів кіберпотенціалу для ведення війни або збройного конфлікту у кіберпросторі. До способів ведення кібервійни можна віднести такі дії, як хакерство, крадіжка даних, порушення роботи критично важливої інфраструктури, тощо. З розповсюдженням Інтернету кібервійна стала ключовою загрозою для країн в усьому світі [3,4].

Перша зафіксована кібератака датується 80-ми роками XX століття, хоча історія кібервійн почалася значно раніше. З кожним роком витонченість і можливості кібератак постійно зростають, а їхній вплив на функціонування як військових, так і цивільних об'єктів стає все більш значним. Так, наприклад, у 2010 році комп'ютерний вірус «черв'як Stuxnet» був використаний для порушення роботи іранського ядерного об'єкта, а у 2017 році від атаки вірусу-здирника WannaCry постраждало понад 200 000 комп'ютерів у 150 країнах світу.

При виявленні і протидії кіберзагроз значні складнощі виникають з боку правових та етичних питань. Наразі не існує міжнародних законів чи угод, що стосуються саме кібервійни, а застосування існуючих законів до кібератак, як правило, є досить нечітким і неврегульованим. Деякі країни намагаються частково вирішити ці проблемні питання, окресливши певні норми. Так, США, росія і Китай, наприклад, розробили кібердоктрину і встановили норми використання кіберпотенціалу у війні. Однак, ці норми досить часто є конкуруючими і суперечливими, що значно ускладнює встановлення чітких рамок для регулювання кібервійни. З метою встановлення і забезпечення дотримання міжнародних норм і угод та із урахуванням складності і мінливості характеру кібервійни, необхідний багатогранний підхід із різноплановими діями, що включатимуть як технічні заходи і засоби протидії кіберзагрозам, так і дипломатичні зусилля з метою встановлення і забезпечення дотримання міжнародних норм і угод, а також підвищення обізнаності населення з кібергігієни. Технічна складова може включати, наприклад, розробку більш надійних протоколів кібербезпеки, а дипломатична - встановлення міжнародних норм і угод, які регулюватимуть використання кіберпотужностей у війні. Навчання кваліфікованих кадрів з кібербезпеки та підвищення обізнаності населення про ризики кібервійни є важливою складовою протидії кіберзагрозам.

Глобалізація кіберзлочинності.

Глобалізація кіберзлочинності стала ознакою кібервійн XXI століття, яка полягає в поширенні транскордонного характеру кіберзлочинності, до якої можуть бути причетні як окремі особи, так і організовані злочинні угруповання, що діють з різних країн. Наразі існує досить багато форм кіберзлочинності, а саме, крадіжка персональних даних, кібератаки з вимогою викупу та продажу

незаконних товарів або послуг у даркнеті. Наслідки від таких кібезлочинів можуть бути досить значними, як для окремих осіб, так і для організацій, зокрема, фінансові втрати або шкода репутації чи іміджу компанії. Глобальний характер кіберзлочинності створює значні виклики для правоохоронних органів, оскільки їм досить важко відслідковувати та переслідувати кіберзлочинців, які діють за кордоном. Можна навести цілий ряд прикладів кіберзлочинності за останні десятиріччя. Так, одним з них був виток даних компанії Uber у 2016 році, в результаті якого було отримано доступ до персональних даних мільйонів користувачів та викрадено їх [4]. Цей випадок показав ризики, які несе в собі відсутність належних заходів безпеки та важливість захисту персональних даних.

Глобалізації кіберзлочинності сприяють також використання криптовалют та даркнету, оскільки вони надають кіберзлочинцям можливість діяти анонімно та уникати виявлення. Організовані злочинні угруповання, зокрема, використовують криптовалюту як спосіб відмивання грошей та фінансування своїх операцій. Результатами кіберзлочинів є не тільки фінансові або іміджеві чи репутаційні втрати. Кібератаки можуть порушити роботу основних служб та критичної інфраструктури, чим завдати значної шкоди громадянам. Наприклад, атака комп’ютерного вірусу-вимагача на медичну організацію може призвести до втрати даних пацієнтів та неможливості надання необхідної медичної допомоги.

Враховуючи сучасні реалії глобализації кіберзлочинності виникає потреба у міжнародному співробітництві, обміні інформацією і ресурсами між правоохоронними органами різних країн. Серед міжнародних організацій, що відіграють важливу роль у сприянні обміну інформацією та розвитку правової бази для протидії кіберзлочинам, такі як Організація Об'єднаних Націй та Рада Європи. Однак, необхідність в подальших спільних міжнародних зусиллях та дієвих заходах для вирішення питань кібербезпеки постійно зростає, враховуючи значні виклики, пов'язані з відстеженням та переслідуванням кіберзлочинців через кордони.

Ризики та загрози від використання пристроїв Інтернету речей (IoT).

Останні десятирічя постійно зростають загрози від використання так званих Інтернет речей (IoT), що являють собою взаємозв'язані фізичні пристрої з вбудованими давачами та програмним забезпеченням, які дозволяють здійснювати передачу і обмін даними та керувати ними через Інтернет. На сьогодні IoT переживає стрімке зростання. Так, за прогнозами очікується, що до 2025 року кількість розумних пристроїв перевищуватиме 75 мільярдів. Таке інтенсивне зростання збільшує ризики для безпеки користувачів IoT, оскільки досить багато пристроїв Інтернету речей недостатньо захищені і вразливі до кібератак. Через відсутність регулярних оновлень безпеки пристроїв Інтернету речей їхні потенційні вразливості постійно зростають і вони стають відкритими для експлуатації хакерами. Використання простих паролів або одного і того ж для декількох пристроїв також полегшує хакерам доступ до IoT-пристроїв. Серед поширених кібератак на пристрої Інтернету речей можна зазначити розподілені

атаки типу «відмова в обслуговуванні» (DDoS – distributed denial of service), що перевантажують веб-сайт або мережу трафіком з декількох джерел. Так, у 2016 році масштабна DDoS-атака була здійснена з використанням скомпрометованих пристроїв Інтернету речей.

Враховуючи наведені можливі ризики, пов'язані з Інтернетом речей, для захисту від потенційних загроз потрібно вживати певні заходи, наприклад, проводити оновлення пристроїв найновішими патчами безпеки та використовувати надійні паролі. Виробники розумних пристроїв, в свою чергу, також мають працювати над підвищенням безпеки пристроїв Інтернету речей.

Через взаємопов'язаний характер IoT навіть одна вразливість певного пристрою може викликати потенційну загрозу для цілого ряду сумісних пристроїв, до яких хакери зможуть отримати доступ. Це ще раз підтверджує важливість розгляду безпеки всієї системи IoT, а не лише окремих пристроїв.

Підсумовуючи вище зазначене, стрімке зростання технологій IoT та поширення використання пристроїв Інтернету речей потребує розгляду супутних ризиків безпеки, які вони створюють та вживання заходів для захисту від потенційних загроз.

Шпигунство і стеження в кіберпросторі.

До інтернет шпигунства і стеження відносять використання кіберпростору з метою збору розвідувальних даних або відстеження діяльності осіб чи організацій з різних причин, включаючи національну безпеку або комерцію.

Як приклад, можна навести факт шпигунства Агентства національної безпеки США за європейськими лідерами через магістральні інтернет кабелі на території Данії [5]. Цей інцидент викликав обурення європейських лідерів і призвів до переоцінки американсько-європейських відносин.

Мали місце і численні повідомлення про кібершпигунську діяльність, яку приписували Китаю і росії. У випадку Китаю – надходили повідомлення про те, що китайські державні хакери шпигують за організаціями в різних секторах, в тому числі урядовому, оборонному, фінансовому і технологічному, які фінансуються державою. Наведемо деякі приклади ймовірних китайських кампаній з кібершпигунства:

- операція "Аврора": кампанія 2010 року, спрямована проти Google та інших технологічних компаній;
- операція Cloud Hopper: кампанія, спрямована проти провайдерів керованих послуг та їхніх клієнтів;
- операція APT10: кампанія, спрямована на провайдерів керованих послуг та їхніх клієнтів.

У нинішній час надходять численні повідомлення про те, що російські державні хакери націлені на організації в різних секторах, в тому числі уряд, оборону, енергетику і фінанси по всьому світу. Деякі приклади ймовірних російських кампаній з кібершпигунства включають наступні:

- операція "Pawn Storm": кампанія, спрямована на урядові, військові і медійні організації;

- операція SandWorm: кампанія, спрямована на урядові, військові та енергетичні організації;
- операція APT29: кампанія, спрямована на урядові та оборонні організації.

Використання кіберпростору для шпигунства і стеження не обмежується державами. Приватні компанії та хакери також можуть займатися цим з метою отримання фінансової вигоди або збору конкурентної розвідки. У деяких випадках хакери можуть продавати зібрану ними інформацію або використовувати її для вимагання грошей у компаній або приватних осіб.

Правові та етичні наслідки шпигунства і стеження є складними і залежать від контексту. В одних випадках шпигунство і стеження можуть бути виправданими мірами національної безпеки, а в інших, можуть розглядатися як порушення недоторканності приватного життя і громадянських свобод.

Для захисту від шпигунства і стеження комунікацій і даних можна використовувати шифрування та інші технології. Уряди також мають відігравати певну роль у регулюванні діяльності зі шпигунства і спостереження, щоб збалансувати потребу в безпеці із захистом громадянських свобод.

Безпека з нульовою довірою (Zero trust security) і OWASP.

Безпека з нульовою довірою – це модель кібербезпеки, яка передбачає, що всі суб'єкти та пристрої в мережі є потенційно ненадійними. Цей підхід відрізняється від традиційних моделей безпеки на основі периметра, які ґрунтуються на припущенні, що активи в межах периметра є безпечними. Натомість, безпека нульової довіри зосереджується на постійному моніторингу та оцінці ризиків, а також вимагає, щоб весь доступ до ресурсів був автентифікований та санкціонований.

Безпека з нульовою довірою включає наступні принципи.

- Найменші привілеї. Доступ до ресурсів надається за принципом необхідності, а користувачам надаються мінімальні привілеї, необхідні для виконання їхніх завдань.
- Мікросегментація. Мережа розділена на менші сегменти, при цьому доступ до ресурсів в межах сегмента контролюється гранульованими політиками.
- Безперервний моніторинг. Мережа безперервно контролюється на наявність ознак компрометації або несанкціонованого доступу.
- Багатофакторна аутентифікація. Доступ до ресурсів вимагає декількох форм аутентифікації, таких як пароль і маркер безпеки.

Cloudflare та Microsoft є великими прихильниками безпеки за принципом нульової довіри, обидві компанії пропонують рішення, які можуть допомогти організаціям впровадити модель безпеки з нульовою довірою.

Cloudflare пропонує цілий ряд сервісів безпеки та мережевих послуг, які можуть бути використані для захисту та оптимізації роботи веб-сайтів та додатків. Деякі з функцій, які можуть бути використані для підтримки моделі безпеки з нульовою довірою, включають:

- брандмауер веб-додатків (WAF) для захисту від поширених веб-вразливостей та атак;
- захист від DDoS-атак для захисту від розподілених атак на відмову в обслуговуванні;
- шифрування SSL/TLS для захисту зв'язку між клієнтами та серверами;
- управління доступом для дозволу або блокування доступу до ресурсів на основі різних критеріїв, таких як IP-адреса, агент користувача або місцезнаходження.

Корпорація Майкрософт пропонує ряд рішень, які можуть допомогти організаціям впровадити модель безпеки з нульовою довірою, в тому числі:

- Azure Active Directory (AD) для управління ідентичностями та доступом;
- Azure Private Link для безпечного підключення між ресурсами Azure і локальними мережами;
- Azure Security Center для захисту від загроз і забезпечення відповідності нормативним вимогам;
- Microsoft Defender для захисту від шкідливого програмного забезпечення та інших загроз на пристроях.

Таким чином, Cloudflare і Microsoft пропонують ряд сервісів і рішень, які можуть бути використані організаціями для реалізації моделі безпеки з нульовою довірою з метою захисту ресурсів і даних від несанкціонованого доступу і загроз.

Важливий внесок в сучасну світову безпеку вкладає некомерційна організація, яка займається питаннями безпеки веб-додатків Open Web Application Security Project (OWASP) [6]. Вона надає ряд інструментів і ресурсів, які допомагають розробникам і фахівцям з безпеки захистити веб-додатки. До того ж, OWASP проводить конференції і заходи для сприяння обміну інформацією та передовим досвідом у сфері безпеки веб-додатків.

Наведемо далі типовий топ-10 помилок безпеки за версією OWASP.

1. Ін'єкції. Уразливості типу «ін'єкція» виникають, коли зловмисник може надіслати шкідливий вхідний код в систему та виконати його як частину команди або запиту. Це може дозволити зловмиснику отримати несанкціонований доступ до даних або виконати шкідливий код в системі.

2. Порушення аутентифікації та управління сеансами. До цієї категорії відносяться уразливості, пов'язані з функціями аутентифікації та управління сеансами в додатках, наприклад, слабкі паролі, погане управління сеансами і відсутність належних засобів контролю аутентифікації.

3. Міжсайтовий скриптинг (XSS). Уразливості XSS виникають, коли зловмисник впровадить шкідливий код на веб-сторінку, який потім виконується браузером нічого не підозрюючого користувача. Це може дозволити зловмиснику викрасти конфіденційну інформацію або виконати довільний код на комп'ютері жертви.

4. Прямі посилання (unsafe pointers) на об'єкти. Цей тип вразливості виникає, коли додаток посилається на внутрішній об'єкт, такий як файл або запис в базі даних, використовуючи ідентифікатор, наданий користувачем. Якщо програма не перевіряє належним чином вхідні дані, зловмисник маніпулює ідентифікатором для отримання доступу до несанкціонованих даних.

5. Неправильна конфігурація безпеки. До цієї категорії відносяться вразливості, пов'язані з неправильною конфігурацією програми або її хостингового середовища. Сюди можна віднести такі проблеми, як паролі за замовчуванням, невиправлене програмне забезпечення та відкрита конфіденційна інформація.

6. Вразливість конфіденційних даних. Цей тип вразливості виникає, коли програма зберігає або передає конфіденційні дані у незахищений спосіб. Це може включати такі проблеми, як незашифрована передача даних, слабкі алгоритми шифрування та відсутність належного контролю за обробкою даних.

7. Підробка міжсайтових запитів (CSRF). CSRF уразливості виникають, коли зловмисник обманом змушує жертву зробити шкідливий запит до додатку від її імені. Це може дозволити зловмиснику виконувати дії від імені жертви, потенційно отримуючи доступ до конфіденційних даних або завдаючи шкоди додатку.

8. Використання компонентів з відомими вразливостями. До цієї категорії відносяться уразливості, пов'язані з використанням компонентів (таких як бібліотеки, фреймворки і плагіни), які мають відомі уразливості. Якщо додаток використовує застарілий або вразливий компонент, він може бути використаний зловмисником.

9. Недостатнє логування та моніторинг. Цей тип вразливості виникає, коли додаток не веде належним чином журнал і моніторинг активності, що ускладнює виявлення і реагування на інциденти безпеки.

10. Відсутність обмеження доступу до URL-адрес. До цієї категорії відносяться уразливості, пов'язані з відсутністю належного контролю доступу до URL-адрес або інших ресурсів програми. Якщо зловмисник отримує доступ до ресурсів з обмеженим доступом, він може отримати несанкціонований доступ до конфіденційних даних або виконати зловмисні дії.

Висновки.

У статті розглянуто ряд ключових викликів і питань, пов'язаних з кібербезпекою, включаючи кібервійни, глобалізацію кіберзлочинності, ризики що надходять від пристроїв Інтернету речей (IoT), шпигунство і стеження. Як один із засобів боротьби з цими загрозами, в статті описаний підхід безпеки з нульовою довірою. Описані ризики безпеки демонструють постійний та еволюціонуючий характер загрози, що підкреслює важливість застосування багатостороннього підходу [7].

Перспектива кібервійни та можливість порушення роботи критичної інфраструктури внаслідок кібератак підкреслюють необхідність розробки міжнародних норм та угод, які б регулювали цю сферу діяльності. Глобалізація кіберзлочинності та вплив кібератак на фізичних і юридичних осіб підкреслюють необхідність міжнародного співробітництва та обміну інформацією і ресурсами з правоохоронними органами. Ризики для безпеки, пов'язані з Інтернетом речей, а саме, потенційна можливість для хакерів отримати доступ до декількох пристроїв через одну вразливість підкреслюють важливість розгляду безпеки

системи в цілому, а не лише незалежних пристроїв. Використання кіберпростору для шпигунства і стеження піднімає правові та етичні питання, а також необхідність дотримання балансу між безпекою і громадянськими свободами. Принципи безпеки з нульовою довірою пропонують потенційний підхід до покращення ситуації в цілому, але й вимагають значних інвестицій в технології та ресурсів.

Оскільки використання кіберпростору продовжує розширюватися, важливо вирішувати ці питання вже зараз з метою захисту від потенційних загроз і забезпечення подальшої стабільності і безпеки цифрового світу. Перспективи і ризики кібербезпеки будуть продовжувати розвиватися з розвитком нових технологій, таких як квантові обчислення, які мають потенціал як для посилення, так і для підриву кібербезпеки. Важливо залишатися в курсі цих подій і продовжувати адаптувати наші підходи до кібербезпеки для того, щоб відповідати мінливому ландшафту загроз.

Впровадження принципів безпеки з нульовою довірою та використання підходів описаних в OWASP може допомогти організаціям захиститися від кіберзагроз та покращити загальний стан своєї безпеки. Однак, впровадження підходу безпеки з нульовою довірою та інших новітніх підходів може бути складним і вимагати значних інвестицій в технології та ресурси і, фактично, означає побудову внутрішніх мереж на зовсім інших принципах. Таким чином, організаціям важливо ретельно зважити свої потреби в безпеці та ресурси, які вони мають для впровадження нової моделі безпеки, виділяючи і ізолюючи, в першу чергу, найбільш чутливі внутрішні сегменти мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 2017 Equifax data breach. URL: https://en.wikipedia.org/wiki/2017_Equifax_data_breach.
2. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. URL: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
3. Digital technology and the war in Ukraine. URL: https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/.
4. The Uber data breach cover-up: A timeline of events. URL: https://www.techtarget.com/searchsecurity/news/252488361/The-Uber-data-breach-cover-up-A-timeline-of-events.
5. How Denmark became the NSA's listening post in Europe. URL: https://www.france24.com/en/technology/20210601-how-denmark-became-the-nsa-s-listening-post-in-europe.
6. Who is the OWASP Foundation. URL: https://owasp.org/.
7. Lakhno, V.A., Kasatkin, D.Y., Skliarenko, O.V., Kolodinska, Y.O. Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment// Machine Learning and Autonomous Systems. Smart Innovation, Systems and Technologies, vol 269. Springer, Singapore. – 2022 – p. 9-22. https://doi.org/10.1007/978-981-16-7996-4_2.

УДК 004.056.52:004.056.53:004.75

АНАЛІЗ ІНФОРМАЦІЙНИХ КОМПОНЕНТ СИСТЕМ РОЗМЕЖУВАННЯ ДОСТУПУ

Корченко О.Г.
д.т.н., професор, завідувач кафедри безпеки інформаційних технологій
Національного авіаційного університету
agkorchenko@gmail.com

Давиденко А.М.
д.т.н., с.н.с., професор кафедри безпеки інформаційних технологій
Національного авіаційного університету
провідний науковий співробітник Інституту проблем моделювання
в енергетиці ім. Г.Є. Пухова НАН України
davidenkoan@gmail.com

Висоцька О.О.
к.т.н., доцент кафедри комп'ютеризованих систем захисту інформації
Національного авіаційного університету
lek_vys@ukr.net

Щербина В.П.
старший викладач
кафедри безпеки інформаційних технологій
Національного авіаційного університету
smya@nau.edu.ua

Анотація. Розглядається можливість побудови базових інформаційних компонент для розширення засобів захисту системи доступу з метою використання опису складових частин системи захисту на природній мові.

Системи розмежування доступу [1-10] реалізують взаємозв'язок між об'єктом доступу і користувачем засобів, які представляє об'єкт користувачеві. В цьому випадку, такий взаємозв'язок реалізується у вигляді інтерфейсу між користувачем і об'єктом доступу. У більшості випадків, дані, якими оперує об'єкт, не мають форми відображення, яка збігалася б з даними, якими оперує користувач, особливо якщо таким користувачем є не процес, а людина, що вирішує свою прикладну задачу. Тому, система розмежування доступу, яка обмежується лише функціями інтерфейсу, повинна мати досить розвинену інформаційну структуру. Така інформаційна структура необхідна для вирішення завдань перетворення області інтерпретації даних користувача, які представлені у відповідній формі, в форму, яка прийнятна для об'єкта доступу. Відповідна система розмежування доступу повинна здійснювати і зворотні перетворення форм представлення даних. Очевидно, що відповідні перетворення форм представлення даних тісно пов'язані з описами предметних областей інтерпретації, якими користується користувач і областей, інтерпретації, які допустимі в об'єкті доступу. Якщо взяти до уваги, що таких користувачів з

різними областями інтерпретації їх прикладних задач у одного об'єкта доступу може бути багато, то стає очевидною досить велика складність вирішення завдання перетворень одних форм представлення даних в іншу і навпаки. У сучасних системах розмежування доступу завдання перетворення вхідних даних в необхідну для об'єкта форму розподілена за всіма складовими, які використовують систему доступу. Таким чином, для системи розмежування доступу виділена лише частина функціональних перетворень, які вирішують задачу узгодження даних, що виходять від користувача до об'єкта доступу і навпаки. До таких завдань, які визначені для системи розмежування доступу, можна віднести наступні: завдання надання користувачеві спадкоємного інтерфейсу; вихідне перетворення даних користувача в форму подання прийнятну для об'єкта; перетворення даних, що надходять від об'єкта доступу до користувача, в форму прийнятну для окремого користувача; формування додаткових коментарів до даних, призначених окремому користувачеві, якщо користувачем є людина і він сформував запит до таких коментарів; завдання ідентифікації користувача, метою вирішення якої є визначення окремого користувача, якщо таких користувачів може бути більше одного.

Наведені вище завдання це класичний набір функцій системи доступу, для випадку, коли не розглядаються завдання безпеки системи доступу, об'єкта доступу і забезпечення безпеки користувачів, які використовують відповідну систему розмежування доступу (SRD).

Для вирішення завдань безпеки SRD, для зручності, будемо говорити про безпеку SRD маючи на увазі безпеки всіх перерахованих складових, необхідна досить розвинена система інформаційного забезпечення тих підсистем, які безпосередньо орієнтовані на вирішення завдань захисту всіх компонент SRD. При коректному проектуванні SRD, причинами зміни рівня безпеки можуть бути, в першу чергу, зовнішні фактори, які можуть впливати на роботу SRD. Внутрішні чинники, які теж можуть негативно впливати на роботу SRD розглядати не будемо, так як до них будемо відносити такі чинники як виникнення несправності або виникнення дефектів, що впливають на штатні режими роботи SRD. Оскільки зовнішні фактори впливають негативно на SRD, вони ініціюють відповідні дії недетерміновано, то характерним для вирішення завдань захисту SRD є такі методи:

– методи прогнозування виникнення атак SRD з боку зовнішніх небезпек;

– методи адаптації SRD до зовнішніх умов, в яких функціонує SRD;

– методи розпізнавання негативних зовнішніх впливів на SRD або розпізнавання атак;

– методи визначення поточного рівня безпеки окремих компонент і системи SRD в цілому;

– методи протидії атакам, які були виявлені на різних етапах їх реалізації, включаючи кінцевий етап реалізації атаки, якщо остання є успішною.

З наведених базових методів вирішення завдань забезпечення безпеки видно, що для їх реалізації і ініціації не існує або досить складно визначити детермінований набір вхідних даних, які забезпечували б можливість однозначно визначити алгоритм реалізації відповідних методів вирішення задач, які в

сукупності вирішували б завдання забезпечення безпечного функціонування системи SRD. У зв'язку з цим, доцільно для вирішення наведених завдань використовувати засоби, які в максимально можливій мірі були б придатні для реалізації наведених вище методів вирішення окремих складових завдання забезпечення безпеки функціонування системи SRD. На основі раніше проведеного аналізу можливостей нейронних мереж, як засобів вирішення завдань розпізнавання, адаптації до постійно змінюваних зовнішніх впливів, які можуть бути основою для вирішення завдань прогнозування змін у зовнішніх впливах, а також ряду інших завдань, включаючи завдання визначення рівня безпеки і завдання ініціації засобів протидії атакам, в даній роботі в якості універсальних засобів вирішення завдання безпеки SRD в цілому, обрані засоби, які реалізуються на основі використання нейронних мереж.

Однією з важливих особливостей використання системи різних типів нейронних мереж є необхідність у використанні досить розвинену інформаційну систему, яка відображала б всі необхідні для функціонування нейронних систем дані. Крім того, в рамках відповідної інформаційної системи повинні існувати засоби, які забезпечували б попередню обробку відповідних даних, перш ніж останні можна було б подавати у функціональні блоки, які реалізовані на основі використання нейронних мереж. Цілком очевидно, що інформаційна система (IS) повинна ґрунтуватися на описах предметних областей, які описують інтерпретацію даних, які використовуються в усіх фрагментах SRD. Тому розглянемо основні компоненти IS, які необхідні для вирішення завдань інформаційного забезпечення системи безпеки SRD, яку скорочено будемо позначати символами BSD.

Словники є описами ідентифікаторів і інших компонент, які використовуються в SRD. Оскільки предметні області з боку користувачів або зовнішні предметні області можуть мати різний рівень абстракції, то немає сенсу прив'язуватися до однієї з можливих мов, якою могла б описуватися окрема предметна область. В даному випадку зміна рівня абстракції мови визначається кількістю нових базових ідентифікаторів, які вводяться в якості позначення реальних об'єктів або факторів, які мають своє самостійне значення в деякій предметній області інтерпретації. Прикладом такого типу зміни рівня абстракції в описі предметної області може служити використання професійної термінології. При цьому, така термінологія може бути ще й не загальноприйнятою. В цьому випадку, відповідну термінологію називають жаргоном. Отже, найбільш низьким рівнем абстракції буде мова, на якій будуються основні базові компоненти, що описують найбільш широко поширену предметну область. При використанні такого способу визначення зміни рівня абстракції мови, може мати місце ситуація, коли дві різні предметні області, які використовують різні базові елементи по відношенню один до одного, мають максимальний рівень абстракції. Для виключення можливості виникнення такої суперечливості, приймемо такі умови.

Умова 1. Вимірювання зміни рівня абстракції можливо тільки між двома описами предметних областей, які мають не менше половини загальних базових елементів.

Умова 2. Вимірювання величини зміни рівня абстракції можливо тільки між двома послідовно модифікованими описами предметних областей.

Умова 3. Зміна величини рівня абстракції між двома описами предметної області, які послідовно розглядаються не може перевищувати 10% від загальної кількості базових елементів, які були модифіковані при описі предметної області.

Беручи до уваги, що опис предметної області являє собою словник S_C, то наведені вище умови можна описати формально. Для цього приймемо, що послідовне перетворення S_C, яке призводить до зміни рівня абстракції певного опису предметної області, в загальному вигляді запишеться наступним співвідношенням:

$$A(S_C) = \{S_{C1} \to [F_{A1}(S_{C1}) = S_{C2}] \to ... \to [F_{A(n-1)}(S_{C(n-1)})] \to S_{Cn}, \quad (1)$$

де F_{Ai} – перетворення S_{Ci}, яке призводить до збільшення рівня абстракції опису предметної області S_{Ci}. У цьому випадку умова 1 запишеться у вигляді наступного співвідношення:

$$[S_{Ci} \cap S_{C,(i+1)} = 1/2(S_{Ci} \,\&\, S_{C,(i+1)})] \to U_{Ai}[F_{Ai}(S_{Ci})], \quad (2)$$

де U_{Ai} – функція визначає величину зміни рівня абстракції в $S_{C(i+1)}$, яке реалізується співвідношенням $F_{Ai}(S_{Ci}) \to S_{C,(i+1)}$.

Умова 2 формально описується наступним співвідношенням:

$\Delta Q_i = Q_{Ai}[S_{Ci}, F(S_{Ci})]$, де ΔQ_i - величина зміни рівня абстракції в $S_{C,(i+1)}$ по відношенню до S_{Ci}.

Умова 3 формально записується у вигляді наступного співвідношення:

$$Q_{Ai}(S_{C,(i+1)}) \le 0{,}1 \,|\, S_{Ci} \,|,$$

де $|\, S_{Ci} \,|$ – параметр, що характеризує S_{Ci} і який використовується для обчислення $Q_{Ai}(S_{Ci})$. У найпростішому випадку, цей параметр являє собою потужність множини S_{Ci}.

Умови 1 і 2 передбачають використання однієї і тієї ж предметної області, яка допускає на окремому етапі модифікації свій розвиток. Якщо ці умови не виконуються, то відповідні S_{Ci} і S_{Cj} є різними. В рамках прийнятого підходу до оцінки рівня абстракції опису S_{Ci} відсутня можливість порівнювати за параметром рівня абстракції S_{Ci} з S_{Ci+j}, якщо $j \ge 2$. Співвідношення (1) описує деяку еволюцію розвитку S_{Ci}, яка відбувається протягом змін S_C з S_{C1} до S_{Cn}. Оскільки опис предметної області S_C є базовим, для роботи системи BSD, то необхідно більш повно розглянути S_C. Всі процеси, які можуть відбуватися в рамках S_C і процеси, які пов'язані з перетвореннями самих словників S_C. Очевидно, що відповідні процеси повинні описуватися параметрами, які їх характеризують.

Процеси зміни рівня абстракції описуються в загальному випадку співвідношенням (1) і формальними уявленнями умов 1-3. Такий параметр, як

рівень абстракції S_C, який будемо позначати символом μ, являє собою характеристику одноразового перетворення $S_{Ci} \to S_{C(i+1)}$.

Процеси еволюційного розвитку S_C охоплюють цілий ряд перетворень семантичного словника S_C і, в загальному випадку, можуть бути представлені у вигляді наступного співвідношення:

$$E(S_C) = \{f_1[S_{C1}, d_1(t)] \to f_2[S_{C2}, d_2(t)] \to ... \to f_n[S_{Cn}, d_n(t)]\},$$

де f_i – функція, яка описує перетворення в словнику S_C з урахуванням інтерактивної взаємодії з системою доступу, яка розширена підсистемою безпеки доступу, $d_i(t)$ – інтерактивна взаємодія користувача, який використовує опис предметної області S_{Ci}, t – час реалізації відповідної взаємодії. Очевидно, що цей процес $E(S_C)$ повинен оцінюватися критеріями, які визначають його, як еволюційний процес. Всі процеси, які можуть відбуватися в S_C, ініціюються користувачем, при цьому, користувач може бути санкціонованим і несанкціонованим. Природно припустити, що всі процеси, які відбуваються в S_C, описуються параметрами, значення яких відрізняються між собою в разі їх ініціалізації санкціонованими користувачами і несанкціонованими користувачами. Більш того, процеси ініційовані несанкціонованим користувачем, можуть призводити до ситуацій, які є неприпустимими, що визначається наступними факторами, які виникають в S_C:

– суперечливістю, що виникає в S_C і що виявляється в різних формах (μ_e);

– конфліктами між компонентами S_C, що виникають в результаті несанкціонованої ініціації процесів в S_C, (η_e);

– порушення процесу функціональних перетворень, які регламентовані вище наведеними типами процесів і можуть складатися з циклічних модифікацій S_C, з дублювання елементів S_C і інших проявів відповідних порушень (χ_e).

Процеси локальних модифікацій S_C або $M(S_C)$ найчастіше пов'язані з необхідністю з боку легального користувача, розширити можливості в отриманні ресурсів з об'єкта доступу. Незважаючи на те, що така модифікація проводиться легальним користувачем, вона може привести до виникнення факторів типу ξ_i, особливо якщо S_C вже розширювалася на попередніх етапах функціонування системи: $P \leftrightarrow SD \leftrightarrow OD$, де P – користувач, OD – об'єкт доступу.

Процеси виродження $V(S_C)$ являють собою такі перетворення в S_C, які призводять до зменшення можливої різноманітності при формуванні запитів на обслуговування. Визначення величини параметра, який характеризує процес деградації, досить складне, оскільки просте зменшення компонент в S_C не приводить до зменшення можливих запитів до системи SD. Запити, які можуть формуватися на основі даних з S_C, будемо позначати z_i. Для формування запитів z_i крім даних з S_C, використовується система виведення нових формул запиту, яка включає в себе систему правил формування семантичних правильних

формул Ω і систему семантичних правил $P\Lambda$, що формально можна записати в такий спосіб:

$$[S_C, \Omega(S_C), P\Lambda(S_C), \Lambda] \to z_i, \qquad (3)$$

Перш ніж в конструктивному вигляді представляти співвідношення (3), розглянемо на якісному рівні інші процеси.

Процеси деградації $D(S_C)$ відрізняються від процесів $V(S_C)$ тим що $D(S_C)$ не призводять до зменшення кількості елементів в S_C, а лише призводять до зменшення кількості запитів, які можуть бути виведені на основі використання S_C. Оскільки z_i у співвідношенні з (3) залежить не тільки від S_C, то розглянемо, які перетворення в S_C можуть вплинути на можливість виведення z_i з Σ, де $\Sigma = \{S_C, \Omega(S_C), P\Lambda(S_C), \Lambda\}$. Оскільки кількість елементів в S_C у результаті $D(S_C)$ не зміниться, то $D(S_C)$ має впливати на $\Omega(S_C)$ і $P\Lambda(S_C)$, або хоча б на одну з цих компонент. Оскільки $P\Lambda$ і Ω являють собою системи правил, то процеси $D(S_C)$ здійснюють таке перетворення $(\Omega \,\&\, P\Lambda) \vee \Omega \vee P\Lambda$, яке унеможливлює їх використання при виведенні z_i. Цей фактор проявляється в тому випадку, якщо відповідні x_i з S_C змінюють свій інтерпретаційний опис $T(x_i)$ таким чином, що $\Omega(S_C)$, або $P\Lambda(S_C)$, або $(\Omega(S_C) \,\&\, P\Lambda(S_C))$ стають суперечливими, при реалізації співвідношення (3) або процедура z_i приводить до конфліктної ситуації в процесі $L_i(S_C, \Omega(S_C), P\Lambda(S_C), \Lambda) \to z_i$, де L_i – функція логічного висновку z_i.

Стабілізуючі процеси $C(S_C)$ представляють альтернативу для процесів дестабілізуючих, до яких можна віднести процеси $V(S_C)$ і $D(S_C)$. Справа в тому що $V(S_C)$ і $D(S_C)$ можуть ініціюватися зовнішніми, по відношенню до SD факторами, з метою компрометації SD або з метою реалізації атаки на SD. Таким чином, $C(S_C)$ являє собою процес протидії вторгненню в систему SD. Оскільки наслідком дестабілізації, до якої призводять $V(S_C)$ і $D(S_C)$, являє собою виникнення в S_C суперечливих і конфліктів, то $C(S_C)$ повинен їх усувати. Очевидно, що ця ініціація здійснюється не тільки в разі, коли необхідний z_i є таким, що не виводяться, а й у разі реалізації процесів визначення рівня безпеки системи BSD в цілому. Ці процеси реалізуються відповідно до алгоритмів забезпечення заданого рівня безпеки системи доступу в цілому. Як уже зазначалося, під безпечною системою доступу будемо мати на увазі трійку $BSD = < P, SD, OD >$.

Катастрофічні процеси $K(S_C)$ представляють собою процеси, яким в рамках BSD неможливо протидіяти. Всі розглянуті процеси являють собою певні послідовності перетворень, в даному випадку, перетворень в S_C. Оскільки дестабілізуючими процесами є $V(S_C)$ і $D(S_C)$, то формально, для визначення $K(S_C)$ можна записати співвідношення:

$$\{\{[V(S_C) \,\&\, D(S_C)] \vee \Phi[V(S_C), D(S_C)]\} \,\&\, \neg C(S_C)\} \to K(S_C),$$

де Φ – функція організації взаємодії між $V(S_C)$ і $D(S_C)$. Заперечення перед $C(S_C)$ означає, що $C(S_C)$ не може протидіяти санкціонованим змінам в S_C.

Система розмежування доступу в значній мірі ґрунтується на інформаційних компонентах. Особливістю інформаційних компонентів є їх залежність від опису їх інтерпретації $T(x_i)$, де x_i – інформаційний елемент, $T(x_i)$ – опис його інтерпретації. Базовими складовими інформаційних компонент є речення або фрази мови, яка використовується для формування $T(x_i)$. У більшості випадків, як такою мовою вибирається природна мова, особливо, якщо йдеться про систему за участю користувачів. Тому, важливими компонентами інформаційних засобів є синтаксис і семантика відповідної мови. Розглянемо ці компоненти в рамках обмежень, які випливають з особливостей і завдань системи безпеки доступом BSD.

Оскільки, базовими засобами безпеки, рівень якої визначається в рамках SRD, є нейронні мережі, то описи, які використовуються в системі доступу, повинні допускати свою кількісну інтерпретацію. Окремі інформаційні компоненти взаємопов'язані між собою. Тому, для коректного їх опису, необхідно розглянути структуру організації відповідних компонент. До складу такої структури входитимуть не тільки словник S_C, синтаксичні та семантичні правила Ω і $P\Lambda$, семантичні параметри Λ і правила перетворення інформаційних компонент Σ, але і об'єкти, які складають опис предметних областей, в яких вирішуються завдання забезпечення безпеки SRD. До таких компонентів можна віднести:

– компоненти опису предметних областей, які відображають інтереси користувачів і, для зручності, вони будуть ідентифікувати окремих користувачів, позначати їх будемо символом U_i;

– засоби захисту в частині їх інформаційного забезпечення IZ, які входять до складу системи BSD;

– підсистема інформаційного забезпечення об'єкта доступу IOD.

На рисунку 1 зображена структурна схема засобів інформаційного забезпечення системи безпеки системи доступу до об'єкта доступу. На рисунку використовуються наступні позначення:

– PIOSD-i – підсистема інформаційного забезпечення системи доступу;

– PIOPO-i – підсистема інформаційного забезпечення предметної області користувача;

– PSP – підсистема семантичних ознак;

– PCP – підсистема семантичних правил;

– IOSZ – інформаційне забезпечення засобів захисту об'єкта доступу;

– PPS – підсистема синтаксичних правил;

– PPV – підсистема правил виведення;

– SS – семантичний словник;

– PUB – підсистема управління безпекою.

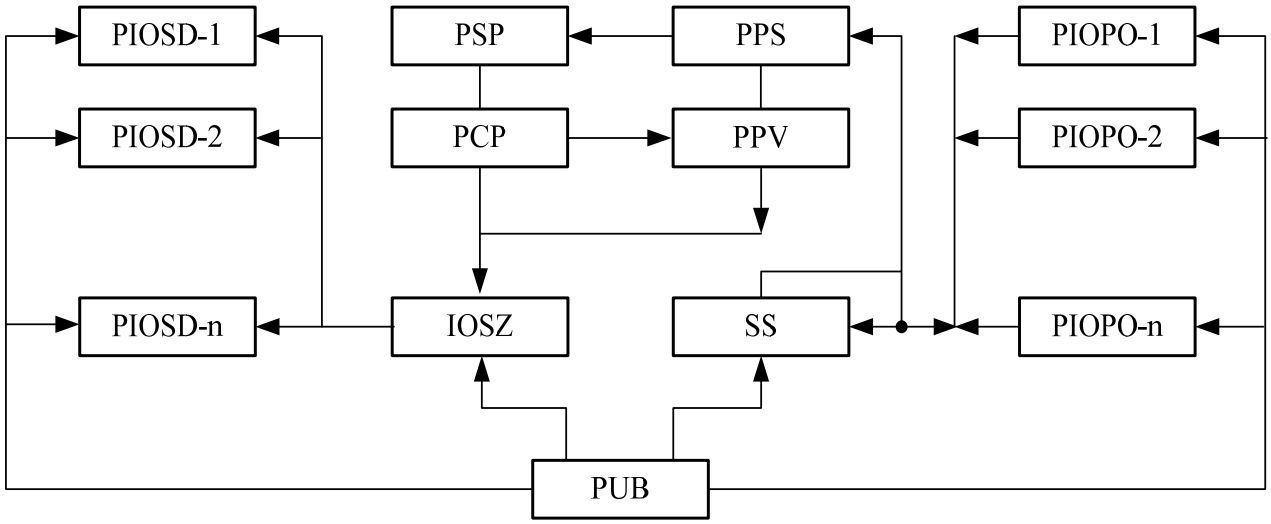


Рис. 1. Структурна схема засобів інформаційного забезпечення системи розмежування доступу *SRD*.

Підсистема PIOSD-i містить опис предметної області системи розмежування доступу. Предметна область системи розмежування доступу являє собою опис всіх засобів, які використовуються або можуть використовуватися для вирішення завдань безпосередньо пов'язаних з реалізацією доступу користувача до об'єкта доступу і засобів або опису предметної області, який пов'язаний з вирішенням завдань забезпечення безпеки системи доступу. Оскільки перша група завдань дуже тісно переплітається з другою групою завдань, то будемо розглядати завдання зі згаданих груп під кутом зору забезпечення безпеки системи доступу. Природно припустити, що міра розширення засобів захисту в системі доступу впливає на величину безпеки функціонування відповідної *SRD*. Тому розглянемо засоби, які можуть використовуватися в рамках *SRD* для забезпечення безпеки функціонування системи. До таких засобів, які відповідають різним аспектам забезпечення безпеки і відображають різні підходи до забезпечення безпеки системи доступу в цілому, можна віднести наступні:

– засоби ідентифікації користувача (*SIP*);

– засоби автентифікації користувача на основі різних інформаційних підходів (*SAI*);

– засоби автентифікації на основі поділу таємної інформації (*SAI*);

– засоби виявлення аномалій в *SRD*, на основі використання нейронних мереж (*VAN*);

– засоби виявлення аномалій в *SRD*, на основі імовірнісних моделей (*VAV*);

– засоби контролю доступу на основі використання різних моделей доступу (*SKD*) та інші.

Кожний з наведених вище засобів, по суті, являє собою окремий фрагмент предметної області системи (*SRD*) розширеної до системи *BSD*. Очевидно, що для кожної окремої *SRD* немає необхідності використовувати всі існуючі засоби для забезпечення безпеки *SRD*, оскільки, вимоги до рівня безпеки для різних *SRD* можуть бути різними. У зв'язку з цим, необхідно вирішити задачу визначення і

розробки методів оцінки рівня безпеки, який забезпечується кожним окремим засобом.

Другим важливим завданням є завдання встановлення взаємозв'язків між окремими засобами. На підставі таких взаємозв'язків можна будувати впорядковану структуру системи *BRD*, в яку входять окремі засоби безпеки. В рамках цієї структури упорядкування може вестися по відношенню до величини безпеки, яку забезпечує кожний із засобів.

Третє завдання, яке необхідно вирішувати, це побудова для кожного з засобів або для кожного фрагмента відповідної області предметної інтерпретації індивідуальних інформаційних розширень, за допомогою яких можна пов'язувати між собою засоби захисту різних типів. Справа в тому, що кожний із засобів володіє власною специфікою вирішення завдань захисту, яка описується відповідною моделлю. Щоб специфіки різних засобів пов'язати між собою, необхідно використовувати не тільки їх інформаційні розширення, а й інформаційні моделі відповідних засобів, оскільки, тільки на інформаційному рівні можна реалізувати взаємозв'язки між різними типами математичних моделей засобів захисту системи доступу.

Черговою задачею, яку необхідно вирішувати і яка безпосередньо пов'язана з попередніми завданнями, є завдання формування формальних засобів опису інформаційних моделей, що дозволить здійснювати необхідні узагальнення побудованих інформаційних моделей. Таке узагальнення дозволить спростити методи вирішення завдань формування структури системи захисту, в яку може входити цілий ряд окремих засобів захисту *SRD*.

Для випадку схем сильної ідентифікації окремі елементи предметної області можуть в рамках семантичного словника описуватися наступним чином:

$SP =<$ санкціонований користувач $>$

$\mathrm{NP} =<$ несанкціонований користувач $>$

$SD =<$ система доступу $>$

$(r_1,...,r_n) =<$ випадкові числа, n$>$

$K =<$ ключ криптографічний $>$

$(A_1,...,A_k) =<$ алгоритми криптографічні блокові, k$>$

$A_1 =< x_1(A_1) >\rightarrow$ { опис блочного алгоритму A_1 }

$A_m =< x_m(A_m) >\rightarrow$ { опис блочного алгоритму A_m }

$S_1 =< x_1(S_1) >\rightarrow$ { опис схеми доступу S_1 }

$S_k =< x_k(S_k) >\rightarrow$ { опис схеми доступу S_k }.

У наведеному вище фрагменті семантичного словника присутній приклад опису предметної області. Такі інтерпретаційні розширення, як $< x_i(A_i) >$ та $< x_i(S_i) >$, являють собою скорочений опис алгоритму і схеми доступу, які використовується тільки в рамках наведеного прикладу опису фрагмента опису S_C.

Використання семантики, в традиційних підходах, обмежується автоматизацією процесів відображення необхідної для користувача інформації при формуванні дружнього інтерфейсу. У цьому випадку, функції семантики розглядаються значно ширше. Це розширення орієнтоване на обґрунтування

можливості використання особливостей семантики об'єктів, які досліджуються, для опису, спеціальних семантичних параметрів, які дозволяють проводити кількісний аналіз семантичних чинників. У зв'язку з цим, виникає необхідність, на певному рівні семантичних описів, перейти від особливостей відображення семантики до формальних оцінок відповідних особливостей. Головними особливостями семантичних описів є наступні:

– якісний характер таких описів;

– наявність кількісної невизначеності, яка відображається у відповідних описах;

– суб'єктивність уточнень або інтерпретації невизначеності описів.

Інтерпретаційні розширення, які використовуються для опису базових елементів системи, є основою для обчислення семантичних параметрів окремих елементів описів і фрагментів таких описів інформаційних компонент. У зв'язку з цим, однією з важливих вимог до складання словників предметної області є вимога до однозначності описів інтерпретаційних розширень і відповідно однозначності базових елементів. Це означає, що конструкції інтерпретаційних розширень повинні містити певну кількість елементів, в основному слів природної мови. Такі вимоги забезпечуються в першу чергу нормалізацією таких описів. Нормалізований опис відрізняється від ненормалізованого тим, що число синтаксичних правил побудови описів і множина слів предметної області, істотно обмежені в порівнянні з різноманітністю синтаксичних правил і допустимих до використання слів, при формуванні подібних не нормалізованих описів. Такі скорочення стосуються різних неоднозначностей, синонімів і синтаксичних схем, які, з точки зору, надмірності, можуть бути заборонені до використання. Обмеження допустимих схем синтаксичних правил ґрунтується на визначенні обмеженої кількості класів слів, які визначаються на основі аналізу загальноприйнятих значень відповідних слів, зокрема, в предметній області, яка описується відповідними розширеннями. До таких класів відносяться наступні типи слів, які прийняті до використання

– слова ідентифікатори об'єктів, процесів та інших базових елементів (клас B),

– слова, які ідентифікують перетворення елементів або їх стан (клас D),

– слова, які ідентифікують різні ознаки базових об'єктів У і слова класу D (клас H).

Зрозуміло, що клас B складають слова, які в граматиці природної мови є іменниками. Для складання фрагментів S_c, використовується ряд умов, які стосуються способів формування інтерпретаційних розширень.

Умова 4. Текстове представлення опису інтерпретаційного розширення $j\,(X_i)$ має виконуватися тільки з використанням множини певних слів K, в якому всі слова однозначно розподілені на класи B, D і H.

Умова 5. Структури фрагментів $\varphi\,(j\,(X_i))$ повинні відповідати структурам, які визначаються синтаксичними правилами Ω.

Умова 6. Різні слова, які мають різну семантичну значимість, повинні описуватися різною кількістю слів в $j\,(X_i)$.

Ця умова є одним з ключових положень, завдяки якому виникає можливість переходу від якісної характеристики семантики слова до визначення її кількісного значення.

Умова 7. При використанні в черговому j (X_i) слів зі словника S_c має зберігатися наступне співвідношення:

$$(j > i) \rightarrow [X_i \in j_k(X_i)].$$

Якщо ця умова має місце для конкретного X_j, то при обчисленні кількісних значень семантичних параметрів, j_k (X_j) розширюється шляхом доповнення j_k (X_j) описом $j_i(X_j)$. Ця процедура може бути рекурентною, якщо $j_i(X_j)$ містить X_k, які задовольняють умові 4. або $(K < i)$.

Схеми синтаксичних правил описують допустимі послідовності класів слів, які можуть використовуватися при формуванні фрагментів описів або цілих речень, які описують певну ситуацію в предметній області. Перш за все, правила Ω не повинні суперечити синтаксису граматики природної мови. Оскільки в результаті використання Ω, можуть бути побудовані два типи конструкції: фрази і речення, то відповідні правила повинні орієнтуватися на побудови фраз і речень φ. Очевидно, що за межами цих конструкцій, говорити про використання правил Ω, при побудові окремих описів не має сенсу.

Висновки: В роботі розглянуто основи побудови базових інформаційних компонент для розширення засобів захисту системи доступу з метою використання опису складових частин системи захисту на природній мові. Для цього проаналізовано основні інформаційні компоненти. Показані і формалізовані семантичні умови існування таких компонент. Запропоновано схему засобів системи розмежування доступу і проведено дослідження взаємозв'язків між семантичними параметрами для розширення функціональних можливостей при здійсненні контролю доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. K. Chen, E. Dowson, J. Golic, eds. A new identification algorithm//Cryptography: Policy and Algorithms. Lecture Notes in Computer Science, vol. 1029, pp. 244-249, 1995.
2. U. Feige, A. Fiat, A. Shamir. Zero-knowledge proofs of identity// Journal of Cryptology, vol. 1, no. 2, pp. 77-94, 1988.
3. N. Heintze, J.D. Tygar. A Model for Secure Protocols and their Compositions// IEEE Symposium on Security and Privacy, pp. 2-13, 1994.
4. A. Davydenko, «Formalization level of abstraction of state information resourses access systems», Scientific letters of academic society of Michel Baludansky, vol.4, no. 1, pp. 35-38, 2016.
5. А. М. Давиденко, О. А. Суліма О.А. Структурні підходи до методів оцінки рівня безпеки інформаційних систем//Моделювання та інформаційні технології. Зб. наук. праць, Вип. 83, С.11-21, 2018.
6. А. М. Давиденко, О. А. Суліма О.А. Аналіз функціональних можливостей окремих компонент засобів захисту інформаційних систем// Моделювання та інформаційні технології. Зб. наук. праць, Вип. 84, С.103-111, 2018.

7. О. Корченко, А. Давиденко, О. Висоцька, Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних// Захист інформації, Том 21, №1, С. 40-51, 2019.

8. О. Г. Корченко, Системи захисту інформації, К.: НАУ, 2004, С. 264.

9. A. Davydenko, O. Vysotska, T. Shmelova, «Methods of Primary Processing Handwriting Samples at User Authentication Using a Probabilistic Neural Network», 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019), Kyiv, Ukraine, 2019., pp. 723-735.

10. Ю. Ткач, С. Казмірчук, Д. Мехед, В. Базилевич. Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу //Захист інформації, №2, С. 137-142, 2017.

УДК 004.056.53

ОЦІНКА НАСЛІДКІВ СОЦІОТЕХНІЧНИХ АТАК НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Дівізінюк М.М.
д-р фіз.-мат. наук, професор
головний науковий співробітник
ДУ «Інститут геохімії навколишнього середовища НАН України»
divizinyuk@ukr.net

Міщенко А.В.
д-р техн. наук, професор
професор кафедри засобів захисту інформації
Національний авіаційний університет
td@airport.kiev.ua

Лазаренко С.В.
д-р техн. наук, доцент
професор кафедри засобів захисту інформації
Національний авіаційний університет
zzi.lazarenko@nau.edu.ua

Клобуков В.В.
канд. техн. наук
асистент кафедри засобів захисту інформації
Національний авіаційний університет
kvv@nau.edu.ua

Анотація. У більшості зломів систем безпеки використовується соціальна інженерія, а не електронний злом чи зняття інформації по каналам витоку інформації. Користувачі є найслабшою ланкою в системі безпеки і саме тому можливі атаки із застосуванням соціотехніки. Методи соціальної інженерії представляють найбільшу загрозу інформаційній та/або кібербезпеці, особливо якщо атаки здійснюються на об'єкти критичної інфраструктури. Для створення системи реагування на соціотехнічні атаки актуальним є оцінка наслідків таких атак.

Об'єкти критичної інфраструктури та їх вразливості.

Об'єкти критичної інфраструктури – підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв [2].

Закон України «Про основні засади забезпечення кібербезпеки України» використовує термін «Критично важливі об'єкти інфраструктури», визначаючи їх як юридичні особи, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей [1].

В наш час діяльність об'єктів критичної інфраструктури (далі – ОКІ) пов'язана з процесами зберігання та обробки інформації з обмеженим доступом, несанкціонований доступ або розкриття (оприлюднення) якої завдасть значної шкоди репутації ОКІ, фінансовому положенню, зниженню роботоспроможності, додаткових витрат ресурсів тощо.

Крім витоку інформації, атаки на ОКІ можуть бути направлені на виведення їх з ладу, порушення функціонування або руйнування.

Таким чином, основними вразливостями ОКІ є виток інформації з обмеженим доступом, виведення з ладу, порушення функціонування або руйнування. Порушення цих чинників має вплив на національну безпеку і оборону, природне середовище, економіку та може призвести до значних матеріальних та фінансових збитків.

Актуальність соціотехнічних атак.

На поточний момент загрозу інформаційній та/або кібербезпеці представляють методи соціальної інженерії, що застосовуються для злому існуючих засобів захисту. Основною причиною цього є те, що застосування соціальної інженерії не вимагає значних фінансових витрат і досконалого знання інформаційних технологій.

Соціальна інженерія – метод несанкціонованого доступу до інформації або до систем зберігання інформації без використання технічних засобів. Він заснований на використанні слабкостей людського фактору. На сьогодні поширеною практикою використання психологічних слабкостей людини є соціотехніка. Дослідження показують, що людям притаманні деякі поведінкові схильності, які можна використати для маніпулювання. Більшість зломів систем безпеки відбуваються завдяки використанню соціальної інженерії, а не електронному злому [4]. Тому, важливим є своєчасне реагування та запобігання соціотехнічних атак.

Саме поняття соціотехніки визначається, як використання зовнішніх факторів для впливу на поведінку групи людей. У контексті кібербезпеки під соціотехнікою розуміються різні прийоми введення в оману внутрішніх користувачів з підштовхуванням їх до виконання певних дій або розголошення конфіденційної інформації. У результаті зловмисник, через непідозрюваних внутрішніх користувачів, отримує доступ до внутрішніх ресурсів і особистих даних, наприклад, банківських реквізитів, паролів тощо.

Розглянемо діаграму загроз інформаційної та/або кібербезпеки (рисунок 1.)

Рис. 1. Загрози інформаційної та/або кібербезпеки (у відсотках).

Проаналізувавши діаграму можливо зазначити, що більшість загроз реалізується завдяки людському фактору.

Атаки із застосуванням соціотехніки можливі завдяки тому, що користувачі часто є найслабшою ланкою в системі безпеки. Зловмисники, які застосовують соціотехніку, можуть перебувати як усередині, так і за межами підприємства або установи, однак найчастіше вони не контактують з потерпілими обличчя до обличчя [3].

Головна мета соціотехнічних атак — отримати несанкціонований доступ до захищених інформаційно-комунікаційних систем та інформації (паролі, персональні дані тощо). Для цього неавторизовані користувачі найчастіше діють згідно з наведеною на рисунку 2 схемою Шейнова В.П.

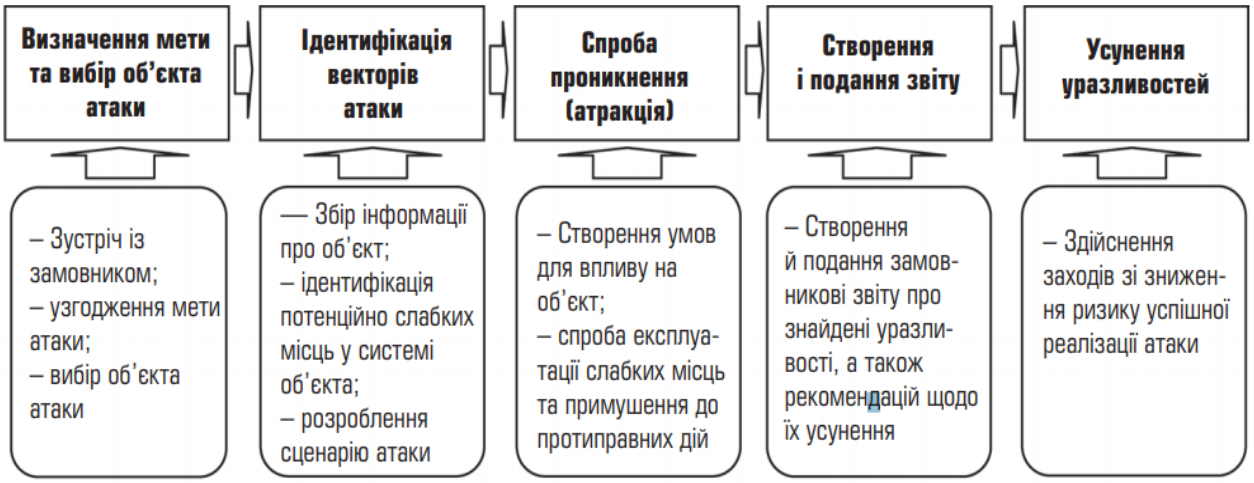


Рис. 2. Алгоритм дій порушників методом соціальної інженерії.

Щоб реалізувати схему Шейнова В.П., порушник має:

1) Визначити мету операції, з'ясувавши, якого роду інформація становить об'єкт полювання і де вона знаходиться (зберігається).

2) Зібрати інформацію про об’єкт розвідки, що дасть змогу вивчити його психологію (джерелом інформації може бути практично все: результати аналізу трафіку, пошти, навіть касових чеків). Під «об’єктом» розуміється потерпілий, на якого націлено атаку неавторизованого користувача.

3) Розробити план дій, провести моральну підготовку та тренування (опрацювати сценарій, зіставити кожне його слово з психологічною моделлю потенційного потерпілого).

4) Виявити найбільш привабливі цілі (мішені) впливу.

5) Створити умови, необхідні для здійснення впливу на об’єкт розвідки, тобто змусити потерпілого до дій, потрібних зловмисникові. Наприклад, ключем до маніпулювання може стати гостра потреба потенційного потерпілого в грошах, про що зловмиснику вдалося дізнатися на етапі збору інформації. Заходи мають активізувати атакованого до невідкладних дій щодо отримання (добування) грошей.

6) Сформувати звіт і подати його замовникові.

На поточний момент атаки, засновані на методах соціотехніки, можливо розділити на п’ять основних напрямків:

- мережеві атаки;
- телефонні атаки;
- пошук інформації в смітті;
- персональні підходи;
- зворотна соціотехніка.

Крім знання можливих видів атак, потрібно також розуміти, що повинні отримати зловмисники. Зловмисниками рухають ті ж потреби, що і всіма людьми: гроші, соціальний статус і самооцінка. Іншими словами, зловмисники хочуть отримати чужі гроші або ресурси, отримати визнання в суспільстві чи своїй групі і підняти себе в своїх очах.

На жаль, зловмисники досягають цих цілей незаконними методами, шляхом викрадання інформації або завдання шкоди інформаційно-комунікаційним системам.

Оцінка наслідків соціотехнічних атак.

При розробці заходів захисту ОКІ від соціотехнічних атак в першу чергу проводиться оцінка рівня захищеності об’єктів від ризику стороннього кібернетичного впливу та можливих наслідків таких атак [4, 5, 8].

При мережевих атаках (з використанням електронної пошти, спливаючих додатків і служб миттєвого обміну повідомленнями, фішингові атаки) – наслідками є ураження інформаційних систем шкідливим програмним забезпеченням (комп’ютерними вірусами, вбудовування в корпоративне середовище поштового механізму тощо).

У наш час співробітникам ОКІ часто доводиться використовувати та обробляти електронні дані, запити, отримані з внутрішніх і зовнішніх джерел. Завдяки цьому зловмисники можуть налагоджувати відносини з співробітниками компаній через глобальну мережу «Інтернет», залишаючись при цьому анонімними.

Зловмисник, який використовує методи соціотехніки, обманним шляхом переконує співробітника надати йому потрібну інформацію, приводячи обґрунтовані правдоподібні аргументи. Отриману інформацію зловмисник може використовувати для подальшого проведення атак за допомогою шкідливих програм.

Можливі наслідки наведено в таблиці 1.

Таблиця 1.

Мережеві атаки, пов'язані з використанням електронної пошти, служби миттєвого обміну повідомленнями, спливаючих додатків і діалогових вікон, та можливий збиток від них

Цілі атаки	Опис	Збитки
Крадіжка корпоративної, особистої інформації	Видаючи себе за внутрішнього користувача, зловмисник намагається отримати корпоративну або особисту інформацію.	Виток конфіденційної інформації Втрата репутації
Крадіжка фінансової інформації	Використовуючи методи фішингу (або спрямованого фішингу), зловмисник запитує конфіденційну корпоративну інформацію, таку як облікові записи.	Фінансові втрати Виток конфіденційної інформації Втрата репутації
Завантаження шкідливого ПЗ	Зловмисник обманним шляхом переконує користувача натиснути гіперпосилання або відкрити вкладення, що призводить до зараження корпоративної мережі шкідливим ПЗ.	Зниження працездатності Втрата репутації
Завантаження шкідливих програм зловмисника	Зловмисник обманним шляхом переконує користувача натиснути гіперпосилання або відкрити вкладення, в результаті чого завантажується програма зловмисника (наприклад поштового механізму), яка споживає ресурси корпоративної мережі.	Витрачання ресурсів Втрата репутації Фінансові втрати

Як і у випадку з іншими різновидами шахрайства, найефективнішим способом захисту від атак зловмисників, заснованих на методах соціотехніки, є скептичне ставлення до будь-яких несподіваних вхідних листів. Для поширення цього підходу на ОКІ в політику безпеки слід включити конкретні принципи використання електронної пошти, що охоплюють перераховані нижче елементи:

- вкладення в документи;
- гіперпосилання в документах;

- запити особистої або корпоративної інформації, які виходять із середини компанії;
- запити особистої або корпоративної інформації, які виходять із-за меж компанії.

Крім того, в опис цих принципів слід включити приклади атак, заснованих на фішингу. Ознайомившись з прикладами, користувачам буде простіше виявляти інші спроби фішингу.

При телефонних атаках (фрікери, вішинг, претекстінг) – наслідками може бути запит інформації або доступ по телефону, крадіжка ПІН-кодів, кредитних і телефонних карток.

Телефонний зв'язок забезпечує унікальні можливості для проведення соціотехнічних атак. Це дуже звичний і в той же час знеособлений засіб спілкування, оскільки потерпілий не може бачити зловмисника. Комунікаційні функції, що підтримуються більшістю комп'ютерних систем, можуть також зробити привабливою ціллю корпоративні телефонні станції.

Зловмисник, атакуючий корпоративну телефонну станцію, може переслідувати наступні цілі:

- запросити інформацію (як правило, видаючи себе за легального користувача), що забезпечує доступ до самої телефонної системи або дозволяє отримати віддалений доступ до комп'ютерних систем;
- отримати безкоштовні телефонні дзвінки;
- отримати доступ до комунікаційної мережі.

Всі ці дії об'єднує загальний сценарій: зловмисник телефонує в компанію і намагається дізнатися телефонні номери, що дозволяють отримати доступ до самої корпоративної телефонної станції або опосередкований доступ через неї до телефонної мережі загального користування.

Запит інформації або доступу по телефону – порівняно безпечний для зловмисника вид атаки. Якщо потерпілий починає щось підозрювати або відмовляється виконувати запит, зловмисник може просто повісити трубку або завершити дзвінок.

Можливі наслідки наведено в таблиці 2.

Таблиця 2.

Атаки, пов'язані з використанням корпоративної телефонної станції та служби підтримки, та можливий збиток від них

Цілі атаки	Опис	Збитки
Отримання доступу до мереж або конфіденційної інформації	Видаючи себе за легального користувача, зловмисник намагається отримати доступ до корпоративних мереж та конфіденційної інформації.	Виток конфіденційної інформації Зниження працездатності Втрата репутації Витрата ресурсів

Цілі атаки	Опис	Збитки
Отримання інформації про телефонну систему	Видаючи себе за інженера з обслуговування телефонних систем, зловмисник намагається отримати доступ до корпоративної телефонної станції з метою здійснення зовнішніх телефонних дзвінків.	Витрата ресурсів Фінансові втрати
Використання корпоративної телефонної станції для доступу до комп'ютерних систем	Використовуючи корпоративну телефонну станцію, зловмисник отримує доступ до комп'ютерних систем для крадіжки або зміни інформації, зараження систем шкідливим ПЗ або використання ресурсів в своїх цілях.	Зниження працездатності Втрата репутації Витрата ресурсів

При пошуку інформації в смітті – паперові відходи можуть містити відомості, які зловмисник може використати безпосередньо (наприклад номери облікових записів і ідентифікатори користувачів) або, які полегшують йому проведення подальших атак (списки телефонів, схеми структури організації тощо).

Електронні засоби зберігання інформації бувають для зловмисників ще більш кориснішими. Якщо на ОКІ не діють правила збору відходів, що передбачають утилізацію списаних носіїв даних (викинутих жорстких дисків, компакт-дисків флеш накопичувачів тощо), можливо знайти найрізноманітніші відомості. Сучасні електронні носії даних надійні і довговічні, тому служби захисту інформації, що відповідають за захист ІТ-систем, повинні забезпечити дотримання політик, які передбачають гарантоване знищення носіїв або інформації з таких носіїв.

Співробітники повинні розуміти всі наслідки, до яких може привести викидання паперових документів або електронних носіїв інформації в сміттєву корзину. Саме по собі «пірнання в смітті» не завжди є чимось незаконним, тому співробітники повинні знати, що потрібно робити зі сміттям. Наприклад, паперове сміття завжди слід подрібнювати в паперорізальних машинах, а електронний носій - знищувати або видаляти записані на ньому дані. Сміттєві контейнери слід розміщувати в захищеній області, недоступною стороннім особам.

Можливі наслідки наведено в таблиці 3.

Таблиця 3.

Атаки, засновані на пошуку інформації в смітті, та можливий збиток від них

Цілі атаки	Опис	Збитки
Паперове сміття в сміттєвих корзинах, розташованих поза організації	Вивчаючи документи, витягнуті з зовнішніх сміттєвих контейнерів, зловмисник дізнається важливу корпоративну інформацію.	Виток конфіденційної інформації Втрата репутації
Паперове сміття в сміттєвих корзинах, розташованих усередині організації	Видаючи себе за прибиральника зловмисник викрадає документи з сміттєвих кошиків, розташованих в самій організації.	Виток конфіденційної інформації Втрата репутації
Викинуті електронні носії	Зловмисник краде дані та додатки, що зберігаються на викинутих електронних носіях, а також самі носії.	Виток конфіденційної інформації Витрата ресурсів Втрата репутації

Персональний підхід:

- *залякування* (зловмисники, які обрали цю стратегію, часто змушують потерпілих виконати певні дії, видаючи себе за осіб, наділених владою);

- *переконання (*найпопулярніші форми переконання - лестощі і посилання на відомих людей);

- *виклик довіри* (цей підхід зазвичай вимагає досить тривалого часу і пов'язаний з формуванням довірчих відносин з колегою або начальником заради отримання у нього потрібної інформації);

- *допомога* (зловмисник, який вибрав цей підхід, пропонує співробітникові ОКІ допомогу, для надання якої, нібито потрібна особиста інформація співробітника. Отримавши цю інформацію, зловмисник викрадає ідентифікаційні дані потерпілої);

- *віртуальні методи (*для проведення атаки зловмисникові потрібно встановити контакт з потерпілою. Як правило, для цього він використовує електронні способи взаємодії, такі як електронна пошта або спливаючі вікна.

У більшості випадків ці атаки спрямовані на конкретних людей і проводяться з метою отримання ідентифікаційних даних потерпілого).

- *фізичні методи* (менш популярний, але більш ефективний для зловмисника спосіб підготовки до проведення атаки є встановлення безпосереднього особистого контакту з потерпілим).

Метою персонального підходу може бути отримання злочинцем персональних даних.

Можливі наслідки атак, заснованих на фізичному доступі, наведено в таблиці 4.

Таблиця 4.

Атаки, засновані на фізичному доступі, та можливий збиток від них

Цілі атаки	**Опис**	**Збитки**
1	2	3
Крадіжка облікових даних мобільного користувача	Зловмисник підглядає, як легальний користувач вводить в систему облікові дані або інші відомості. Це може передувати крадіжці мобільного комп'ютера.	Виток конфіденційної інформації
Крадіжка облікових даних співробітника, який працює віддалено (вдома)	Зловмисник представляється службою технічної підтримки, щоб отримати доступ до мережі користувача, що працює віддалено (вдома), і запитує у користувача ідентифікатор та пароль, нібито для тестування оновленої конфігурації системи.	Виток конфіденційної інформації
Вхід в корпоративну мережу через мережу співробітника, який працює віддалено (вдома)	Видаючи себе за представника служби підтримки, зловмисник отримує доступ до мережі співробітника, який працює віддалено (вдома), і використовує її для підключення до корпоративної мережі. У разі успіху зловмисник отримує вільний доступ до мережі та ресурсів об'єкту.	Виток конфіденційної інформації Втрата репутації Зниження працездатності Витрата ресурсів Фінансові втрати
Поточний доступ до мережі співробітника, який працює віддалено (вдома)	Зловмисник або локальний користувач отримує доступ в Інтернет по широкосмуговому з'єднанню, використовуючи для цього незахищену домашню мережу іншого користувача.	Витрата ресурсів Фінансові втрати

1	2	3
Доступ в офісну будівлю компанії без супроводу	Зловмисник проникає в офісну будівлю компанії слідом за авторизованим співробітником.	Виток конфіденційної інформації Втрата репутації Зниження працездатності Фінансові втрати Витрата ресурсів
Доступ в офіс співробітника компанії	Зловмисник отримує доступ в офіс співробітника ОКІ, де намагається скористатися комп'ютерним обладнанням або знайти цікаві для себе відомості в паперових документах.	Виток конфіденційної інформації Витрата ресурсів Фінансові втрати

При зворотній соціотехніці – наслідками може бути крадіжка облікових, персональних, конфіденційних даних, завантаження шкідливого ПЗ тощо.

Про зворотну соціотехніку говорять тоді, коли потерпілі самі пропонують зловмисникові потрібну йому інформацію. Це може здатися малоймовірним, але насправді особи, що мають авторитет в технічній або соціальній сфері, часто отримують ідентифікатори і паролі користувачів та іншу важливу особисту інформацію просто тому, що ніхто не сумнівається в їх порядності. Наприклад, співробітники служби підтримки ніколи не запитують у користувачів ідентифікатор або пароль (їм не потрібна ця інформація для вирішення проблем). Проте, багато користувачів заради якнайшвидшого усунення проблем добровільно повідомляють ці конфіденційні відомості. Зловмиснику навіть не треба питати про це.

У потерпілого немає підстав підозрювати зловмисника в чому-небудь, так як при таких атаках створюється враження, що ситуація знаходиться під її контролем [4]. Головним способом захисту від атак, заснованих на зворотній соціотехніки, є включення в політику безпеки принципу, що вимагає вирішення всіх нештатних ситуацій тільки через службу підтримки.

Захиститися від атак, заснованих на зворотній соціотехніці, найскладніше.

Можливі наслідки наведено в таблиці 5.

Таблиця 5.

Атаки, засновані на методах зворотної соціотехніки, та можливий збиток від них

Цілі атаки	Опис	Збитки
Крадіжка облікових даних	Зловмисник отримує ідентифікатор та пароль авторизованого користувача.	Виток конфіденційної інформації Втрата репутації Зниження працездатності Фінансові втрати Витрата ресурсів
Крадіжка інформації	Використовуючи ідентифікатор і пароль авторизованого користувача, зловмисник отримує доступ до файлів компанії.	Виток конфіденційної інформації Фінансові втрати Витрата ресурсів Втрата репутації Зниження працездатності
Завантаження шкідливого ПЗ	Зловмисник обманним шляхом переконує користувача натиснути гіперпосилання або відкрити вкладення, що призводить до зараження корпоративної мережі шкідливим ПЗ.	Зниження працездатності Втрата репутації
Завантаження ПЗ зловмисника	Зловмисник обманним шляхом переконує користувача клацнути гіперпосилання або відкрити вкладення, в результаті чого відбувається завантаження програми зловмисника, яка споживає ресурси корпоративної мережі.	Витрата ресурсів Втрата репутації Фінансові втрати

Найпростіший та дешевий для зловмисника спосіб отримати потрібну йому інформацію – безпосередньо спитати у співробітника або направити запит на її отримання.

Реагування на соціотехнічні атаки.

З метою зменшення наслідків соціотехнічних атак, або взагалі уникнення їх, на ОКІ повинні бути впроваджені заходи з реагування на соціотехнічні атаки. Виходячи з наслідків існують базові методи реагування на атаки, до яких відносяться [7]:

- тестування системи захисту об’єктів інформаційної діяльності;
- поінформованість персоналу;
- активний захист, у тому числі блокування каналів витоку інформації.

Якісне та оперативне реагування на соціотехнічні атаки підвищує ефективність процесів управління політикою безпеки на ОКІ та допомагає фахівцям служб захисту (адміністраторам безпеки, менеджерам з кібербезпеки тощо) швидко, в масштабах реального часу, приймати рішення щодо локалізації таких атак та усунення їх наслідків.

Заходи із запобігання соціотехнічних атак потребують виконання наступних етапів [6]:

- проведення аналізу сучасного стану соціотехнічної безпеки ОКІ;
- з'ясування існуючих засобів та заходів реагування та запобігання соціотехнічних атак, що використовуються на ОКІ;
- проведення аналізу існуючих проблем з оцінювання ефективності реагування на соціотехнічні атаки;
- на основі проведеного аналізу формування вимог до оцінки ефективності реагування на соціотехнічні атаки;
- на підставі сформованих вимог, визначити методи, способи та заходи виявлення та запобігання соціотехнічних атак.

Висновки.

У роботі наведені основні вразливі чинники об'єктів критичної інфраструктури, порушення яких має вплив на національну безпеку і оборону, природне середовище, економіку та може призвести до значних матеріальних та фінансових збитків.

Проведено аналіз основних напрямків здійснення соціотехнічних атак на об'єкти критичної інфраструктури. Наведено можливі наслідки (збитки) від соціотехнічних атак (мережевих; телефонних; пошуку інформації в смітті; персональному підході та зворотній соціотехніці).

Досліджено основні поняття соціотехнічної безпеки, проведено аналіз сучасних заходів та засобів реагування на соціотехнічні атаки.

За результатами проведеного аналізу доведено необхідність впровадження на об'єктах критичної інфраструктури заходів запобігання соціотехнічних атак, які зможуть надати можливість службам захисту інформації оперативно виявляти, знешкоджувати та здійснювати оцінку таких атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України».
2. Постанова Кабінету Міністрів України від 23.08.2016 № 563 «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».
3. Роуз М. Соціальна інженерія [Електронний ресурс] / Роуз Маргарет// Режим доступу до ресурсу: http://searchsecurity.techtarget.com/definition/social-engineering.
4. Митник К.Д. Мистецтво обману / Митник К. Д.// Посібник. NYC: Wiley Books. 2008. – 273 с.
5. Бурячок В.Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / Бурячок В.Л., Корченко О.Г., Хорошко В.О., Кудінов В.А. // Захист інформації. – К.: НАУ, 2013. – Т. 15, № 1. – С. 5–14.

6. Лазаренко С.В. Підвищення ефективності реагування на соціотехнічні атаки/ Лазаренко С.В., Козловський В.В., Мартинюк Г.В., Баланюк Ю.В.// Перспективні няпрями захисту інформації: матеріали VI міжнародної науково-практичної конференції, 02 – 06 вересня 2020 р.: тези доп. – м. Одеса: Одеська національна академія зв'язку ім. О.С. Попова - 2020. – С. 122-124.

7. Лазаренко С.В. Реагування на соціотехнічні атаки об'єктів критичної інфраструктури / Лазаренко С.В., Щербак Т.Л., Фурсенко О.М., Ткач Б.В.// Комп'ютерні системи та мережні технології: Збірник тез доповідей XIII міжнар. наук.-практ. конф., 15-17 квітня 2021 р.: тези доп. – К.: НАУ, 2021. – С. 71-72.

8. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно структурний аналіз) / Бутузов В.М.// Монографія. – К.: КІТ, 2010. – 145 с.

УДК 658.64

THE ROLE OF COMPETITIVE INTELLIGENCE IN BUSINESS MANAGEMENT

Obozna A.O.,
Phd of Economics
postmaster@mikolaiv.e-u.in.ua

Iakovunyk O.V.,
Head of MB
helensj532@gmail.com

Iakovunyk D.I.,
Lecturer
denisyakovunik2016@gmail.com
Mykolaiv branch of the European University
Ukraine, Mykolaiv

Abstract. It is possible to provide a conceptual framework and analysis of the role of competitive intelligence in the study of competitors, synthesizing information from market participants: suppliers, customers, industry competitors, as well as own company personnel. The work uses a literary and conceptual research approach. A review of foreign literature showed that the concept of competitive intelligence is multifaceted, where artificial intelligence plays a big role in the study and monitoring of competitors, and also showed how important competitive intelligence is for business managers.

Benjamin Gilad is a pioneer in the field of competitive intelligence, strongly recognizing the relationship between competitive intelligence and strategy, conducting and supporting research on key trends that affect the practice of competitive intelligence and its ability to support key decision makers and their organizations.

Modern marketing includes data scientists and analytics functions that collect and analyze vast amounts of customer data, whether transactional (still the dominant form) or textual (social media analysis) to develop an optimal *«customer experience»*. New technological tools can help, but they cannot replace what savvy strategists are doing.

Competitive intelligence (CI) is the activity of a company that involves the collection and analysis of information about competitors, competitive products and services. All information and analytical work is carried out exclusively within the framework of ethical standards.

Competitive intelligence serves as a strategic tool that facilitates the identification of potential opportunities and threats [Du Toit, 2013] [1] and stimulates innovation activity [Rodriguez-Salvador et al., 2013] [2]. This is the process of accumulating information about the future and determining medium and long-term prospects to support decision-making and prepare operational joint actions.

Competitive intelligence and business intelligence can reduce uncertainty and risk, as well as increase the likelihood of target audience acceptance of proposed policies and early identification of opportunities.

Competitive intelligence is presented in three main areas (Fig. 1):

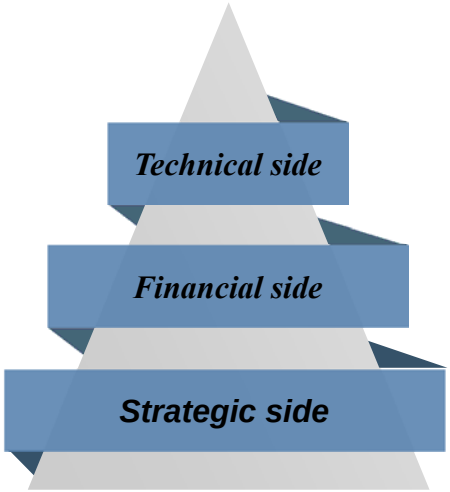


Fig.1. Main areas of Competitive intelligence.

▶*Technical side.* It involves the collection of all information about products, services, new developments.

▶*Financial side*. It implies the study of pricing, the collection of information about the current financial situation of competitors, the study of reports from open sources. Such competitive intelligence helps to find out the financial strength of your own company.

▶*Strategic side.* It involves the study of corporate policy, the organization of the work of competitors and other information related to the functioning of a competitor company [15].

The study of the competitive environment, conducted in all three directions, allows you to conduct a thorough competitive intelligence and solve the following tasks (Fig. 2):

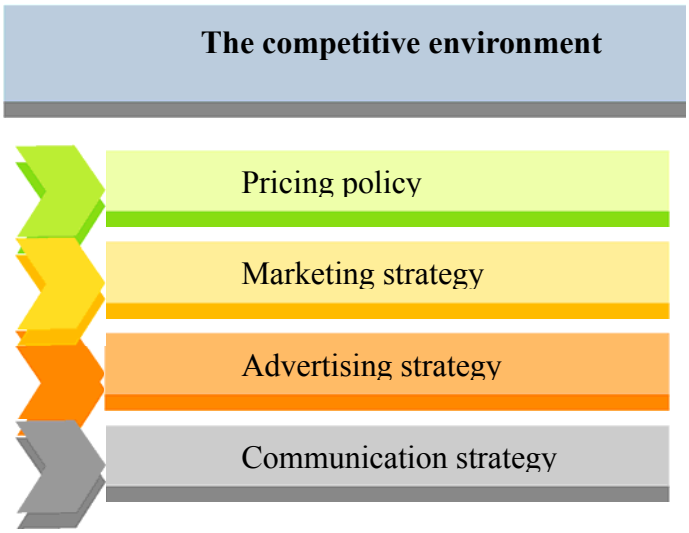


Fig.2. Tasks of the competitive environment.

- find new opportunities for business development and competitiveness;
- determine the pricing policy of competitors;
- improve marketing strategy;
- build a forecast of market changes;
- improve advertising strategy;
- find new methods of business management;
- predict the actions of competitors;
- improve the quality of customer service and communication strategy;
- change the positioning of the company;
- improve the trade offer.

The more information you know about your competitors, the clearer your company's position in the market will be.

Competitive intelligence produces useful information that aids in decision making and provides a competitive advantage for businesses. For competitive intelligence to be effective, it must be properly located within the enterprise [3].

Unlike corporate espionage, competitive intelligence involves the ethical collection of information from both published and unpublished sources, such as [4]:

- online search (competitor websites, job postings, business information aggregators, your competitor's social media platforms);
- -press releases;
- sales team (they collect information organically when someone calls potential customers);
- industry events, conferences and trade shows;
- suppliers and distributors who operate in your industry and may serve competitors;
- the competitors themselves.

All methods of analyzing your business rivals can be divided into 3 groups: *intelligence* on your own, *investigation* through an agency and *industrial espionage*. The latter is an illegal method, so for now we are only interested in legal methods.

It is extremely important to remember that effective competitive intelligence goes beyond your internal data - otherwise you will just be doing day-to-day market research. To write a competitive intelligence report, it is important to look beyond your company and all external sources.

The article by Marie-Luce Kühn, Wilma Viviers, N. Syudass and J. Kalof «*Ecosystem for monitoring the business environment beyond the «first world»*: the case of South Africa"[5] provides an insight into the ecosystem of the CI, its elements and methods for evaluating the latter. Since most of the work on CI focuses on the analysis of practical activities, the concept considered by the authors allows us to conclude that the actual practice of CI is determined by the presence of an appropriate ecosystem to support organizations.

In particular, the elements of such an ecosystem include (Fig. 3):

- consultants and other CI service providers;

- universities that recruit new talent to organizations, offer training programs for existing staff, and provide hands-on support for CI implementation;
- associations that develop educational and professional standards;
- organizations (private, public, non-governmental) for which CI is part of their daily activities.

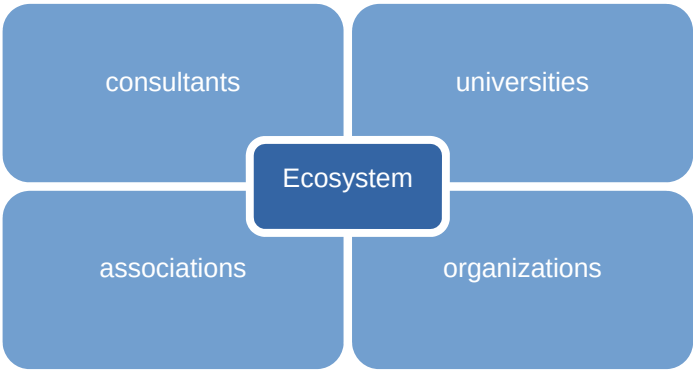


Fig.3. The elements of an ecosystem.

The concept of a business ecosystem was proposed in [Moore, 1993], which noted that companies should not be considered as players in a separate industry, but as part of a business ecosystem that unites many industries [13].

Ecosystem participants evolve through collaborative innovation: collaborating (and competing) to develop new products, meet customer needs, and ultimately master the next generation of innovations.

The ecosystem includes suppliers, distributors, consumers, government agencies, processes, products, and competitors. [Hayes, 2019]: Everyone affects and is influenced by others, which leads to continuous evolution and requires participants to be flexible and adaptive in order to survive (similar to a biological ecosystem) [7].

Other authors have also found this concept useful. For example, in [Hult et al., 2020, p. 38] the international business ecosystem is defined as a set of business entities, including stakeholders, organizations and countries involved in exchange, production, business activities and cross-border trade based on a combination of competition with partnership [14]:

- Academic organizations
- Consulting firms
- Governmental support
- Associations of the competitive intelligence.

Association of Strategic and Competitive Intelligence Professionals (SCIP) SCIP, founded in 1986, [6] is the world's largest professional association in the field of CI with an established ecosystem and areas of work, including, in addition to CI itself, sales, marketing, strategy development, business development, management products, creating innovations. It brings together competitive and market intelligence professionals, consultants, strategists, educators, students and non-profit experts from various employment modes. Over time, sophisticated analytics came to the fore.

The new approach, called «*integrated intelligence*» (integrated intelligence) [7], involves the use of artificial intelligence. There is a trend of moving away from gathering information about competitors towards areas that increase the added value of information products, including analysis and consideration of broader aspects of the operating environment (consumers, government, technology, economics, etc.).

Nanette Bulger proposed the concept of «*comprehensive intelligence*» [Bulger, 2016], which does not contradict the above definition, but expands its scope and range of required skills [9]. Initially, CI focused directly on the study of competitors. Subsequently, the new competencies required to assess the current economic and political situation in specific regulatory conditions were integrated into the concept.

Today, competitive and market intelligence requires an understanding of marketing features, market segmentation, the formation of a competitive environment, and the assessment of rivals [Calof, 2016] [9].

How Competitive Intelligence Works?

Competitive intelligence involves the ethical collection of information from both published and unpublished sources, such as [10]:

- on-line search (competitor websites, business information competitor)
- press releases
- sales team
- suppliers and distributors
- competitors.

Competitive analytics (CI) tools can give us insight into our competitors' digital marketing strategies, which can help us outperform them in creating new actionable strategies, such as (Fig.4):

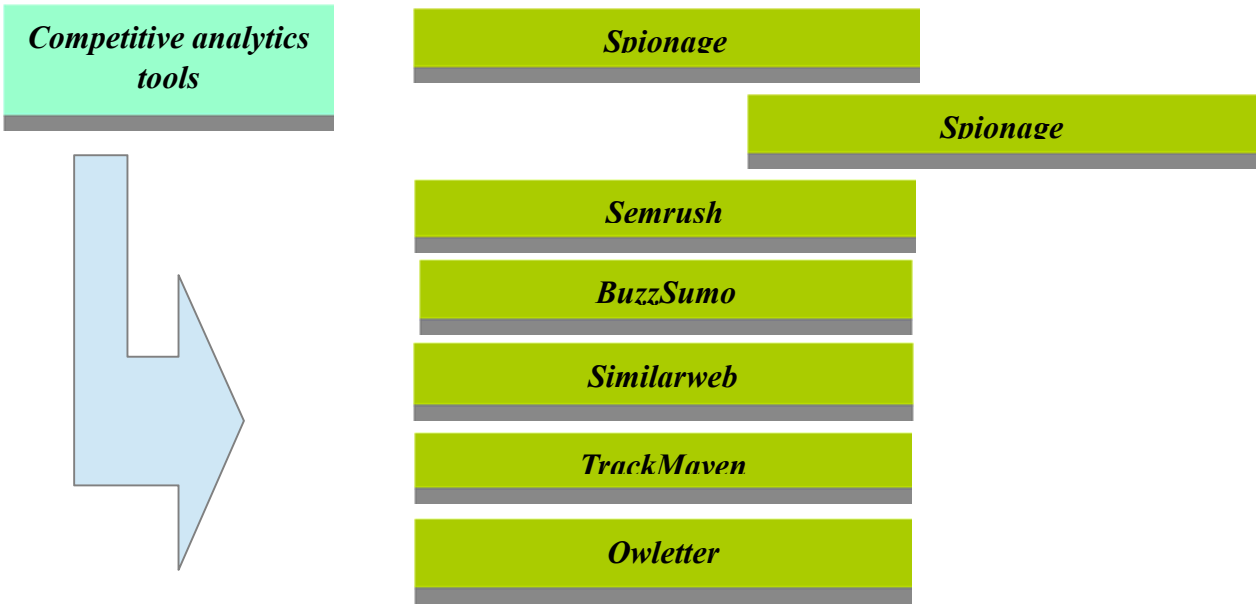


Fig. 4. Competitive analytics (CI) tools.

- *Open SEO* Stats is a tool when we see any competitor's website.

- *Spionage* helps you understand your competitors' search marketing strategies by identifying which keywords your websites rank for most effectively.
- *BuzzSumo* - effective content related to major topics, niche or industry.
- *Semrush* will give you an estimate of which keywords will provide the best ROI
- *Similarweb* - web research where you can learn more about your competitor's audience
- *TrackMaven* provides personalized metrics and reports to track competitors
- *Owletter* is a good tool for SMBs who want to focus on monitoring their competitors' email marketing performance.

Competitive intelligence, like digital marketing in general, is not a one-time process. It takes time and consistency. By having the right tools and striving to monitor and adjust our strategies over time, we can learn how to stay ahead of the competition, attract the perfect audience, and win loyal customers.

The Internet is the key source of information for the CI. This is followed by primary sources such as company employees, customers, and industry experts. Most often, respondents use a set of five analytical methods. SWOT analysis and competitor analysis are the most popular.

Optimization of corporate innovation activities is formed by the introduction of information about innovations. *Science and Technology Intelligence* (STI) is an important branch of Competitive Intelligence (CI) that collects information about technologies using data mining tools from patents, scientific literature, technology exhibitions and other sources of information about who, where, why and how quickly develops or uses new technologies [7].

There are many TCR models that describe the necessary data to develop and support innovative concepts. One of the most effective approaches was proposed in the mid-1990s. including six *NOMMAR* factors [7] (Fig. 5):

- *Need*: Is there evidence of a significant unmet need in the community?
- *Option*: Will there be a technology that will successfully meet this need?
- *Market*: Is there a market for such an offering, given competitors' product portfolios, production costs, and the operational and organizational changes that such an innovative product or service might entail?

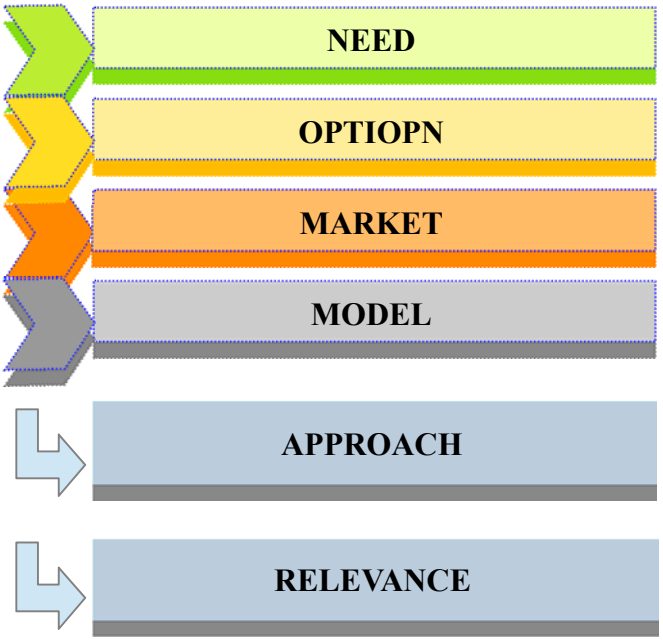


Fig.5 Model NOMMAR factors.

- *Model:* Is there a known business model that adequately describes how this product can be profitably developed, produced and maintained?
- *Approach:* Is there an approach that is highly likely to enable the organization to successfully enter the relevant market?
- *Relevance*: if possible, is it necessary; is it in line with the overall corporate strategy?

To solve this problem, the methods of competitive technological intelligence (KTR) were used. The KTR methodology includes the collection, analysis and processing of scientific and technological information to form the relevant knowledge that is used in the course of decision-making in the organization [Colakogly, 2011; Rodriguez et al., 2019] [11].

Competitive technology intelligence is an important methodology for analyzing new technologies to improve the quality of strategic decisions in innovation activities produced by additive technologies - known as 3D printing (rapid prototyping and free-form objects), remains a relatively new technology. For this purpose, multiple linear regression analyzes of scientific articles and patents submitted on the Scopus and PatSnap platforms were performed [Mancilla-de-la-Cruz J., Rodriguez Salvador M., Ruiz-Cantu L. (2020)] [12].

Not only start-up businesses, but also experienced business structures resort to studying their rivals. Competitive intelligence methods are used in their work by such Silicon Valley giants as Google, Apple, Facebook, Microsoft and Amazon and showed the following results (Fig.6):

- 65% prefer free analysis tools,
- 25% prefer paid ones,
- 10 % the rest combine them in their work.

The study of the competitive environment allows you to conduct competitive intelligence and solve the following tasks:

- find new opportunities for business development and competitiveness;
- determine the pricing policy of competitors;
- improve marketing strategy;
- build a forecast of market changes;
- improve advertising strategy;
- find new methods of business management;
- predict the actions of competitors;
- improve the quality of customer service and communication strategy;
- change the positioning of the company.

The market is changing very quickly, so all research must be done efficiently and quickly.

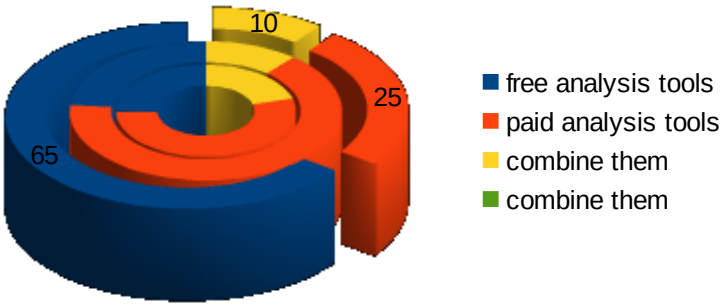


Fig. 6 Analysis of the results of use CI.

It is necessary to conduct competitive intelligence regularly in order to increase the competitiveness of own company and make informed management decisions. To get answers when making decisions, they use the latest marketing techniques today (Fig.7):

- neuromarketing
- pop-up
- CRM Marketing
- onboarding
- crowd marketing
- Cohort analysis
- Referral Marketing
- performance marketing.

Referral marketing is an activity aimed at promoting a company, its products and services through existing and potential buyers.

The concept of performance marketing is based on the fact that investments should be justified and bring results in the shortest possible time, ideally immediately. This approach allows you to achieve goals when the budget is limited, and sales are needed now.

Crowd marketing is a type of hidden advertising in which a brand or its products are mentioned in social networks, forums or answer aggregators in order to promote the brand.

With the help of *onboarding,* the company disposes users from the first steps of acquaintance, «immerses» them in work and sets them up for further communication.

Pop-up is an effective way to attract the attention of website visitors.

CRM Marketing systems are focused on interaction with customers and potential customers, activity tracking.

Cohort analysis allows you to explore changes in the behavior of groups of users over time. The data obtained helps to improve the marketing strategy, refine the customer journey and sales. With cohort analysis, we can:

- analyze the impact of marketing decisions on the level of retention;
- find the most effective channels to attract customers;
- evaluate the effectiveness of advertising campaigns;
- find ways to increase the engagement of users with low activity and minimize customer churn;
- see the need to connect a new promotion channel;
- assess the impact of seasonality on the level of sales;
- get to know the target audience better.

Neuromarketing - use of the neuromarketing method, which allows you to track and analyze the reaction of customers.

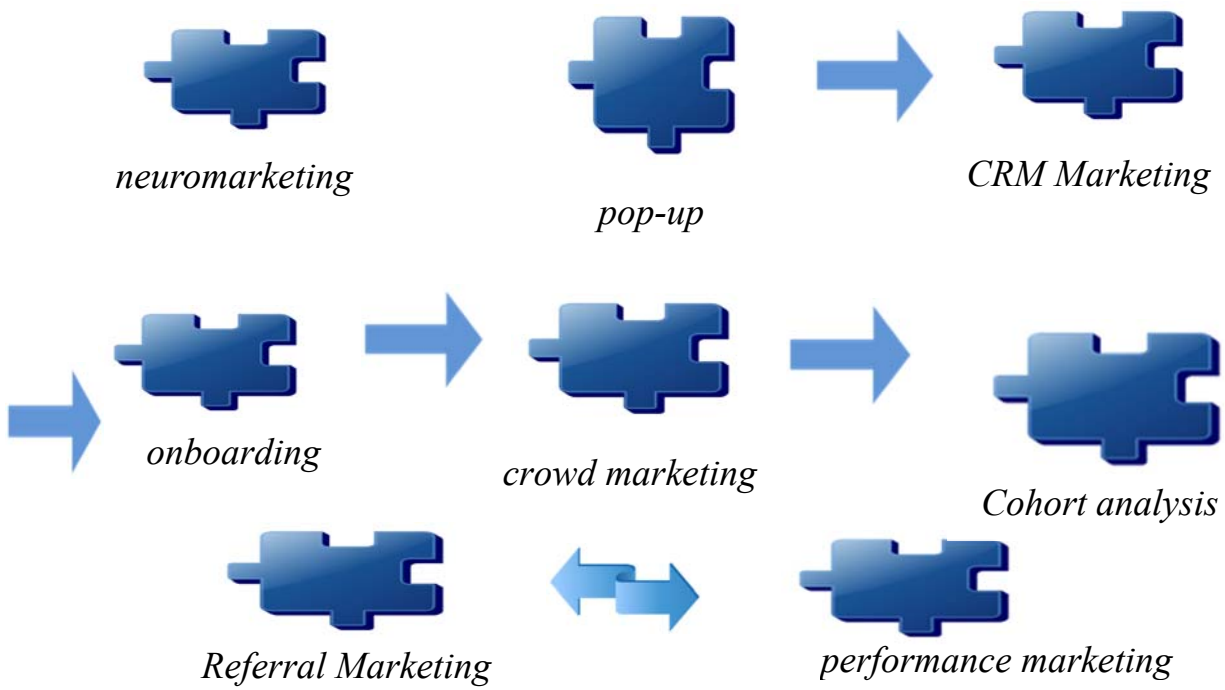


Fig. 7 Innovation marketing techniques.

The Benchmarking method should also be noted separately.

Benchmarking is the process of comparing your performance with the best companies in the market and industry, and then implementing changes to achieve and maintain competitiveness.

In general, the key ideas of benchmarking are as follows (Fig.8):

- Identifying best-in-class organizations;
- Obtaining the necessary information using appropriate methods of collecting information for self-assessment;
- Work on self-improvement through the implementation of changes aimed at achieving and exceeding established standards.

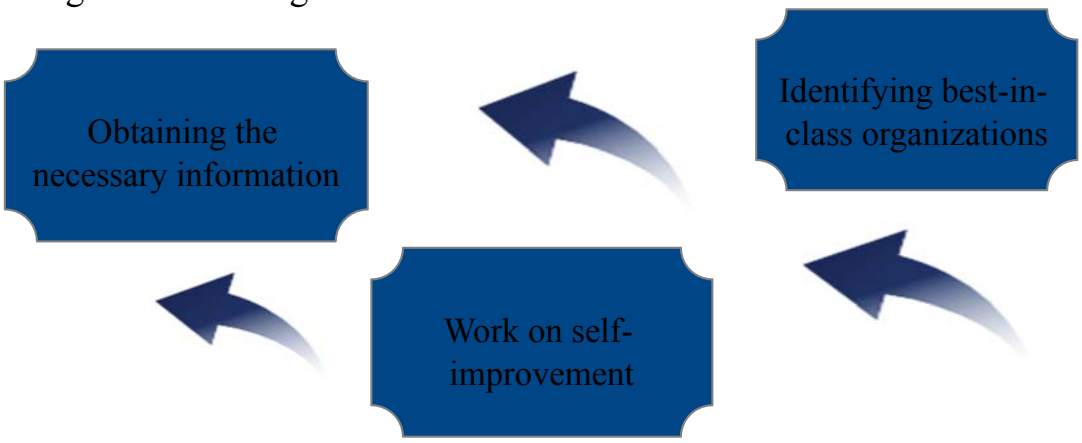


Fig.8 Key ideas of benchmarking.

Competitive intelligence is an effective marketing tool designed to analyze the competitive environment by collecting information about competitors. But it is important to remember that regular monitoring will greatly expand the vision of strategic planning for future development and success.

REFERENCES.

1. Du Toit A. (2013) Comparative Study of Competitive Intelligence Practices between Two Retail Banks in Brazil and South Africa // Journal of Intelligence Studies in Business. Vol. 3. № 2. P. 30–39.

2. Rodriguez-Salvador M., Salinas-Casanova L. (2012) Applying Competitive Intelligence: The Case of Thermoplastics Elastomers // Journal of Intelligence Studies in Business. Vol. 2. № 3. P. 41–47.

3. Tshilidzi Eric Nenzhelele Competitive Intelligence Location in Small and Medium-Sized Enterprises https://www.researchgate.net/publication/281020039_Competitive_Intelligence_Location_in_Small_and_Medium-Sized_Enterprises.

4. https://www.ringcentral.co.uk/gb/en/blog/definitions/competitive-intelligence/

5. Calof J., Smith J. (2009) The integrative domain of foresight and competitive intelligence and its impact on R&D management // R&D Management. Vol. 40. № 1. P. 31–39.

6. https://www.scip.org/page/Scaling-Competitive-Intelligence-Platforms.

7. Foresight and STI Governance. 2020. Vol.14 (3). SPECIAL ISSUE “COMPETITIVE INTELLIGENCE”

8. Bulger N.J. (2016) The Evolving Role of Intelligence: Migrating from Traditional Competitive Intelligence to Integrated Intelligence // The International Journal of Intelligence, Security, and Public Affairs. Vol. 18. № 1. P. 57–84. DOI: 10.1080/23800992.2016.1150691.

9. Calof J.L. (2016) Government sponsored competitive intelligence for regional and sectoral economic development: Canadian experiences // Journal of Intelligence Studies in Business. Vol. 6. № 1. P. 48–58.

10. Competitive Intelligence Tools to Suppress Competition https://www.affde.com

11. Colakogly T. (2011) The problematic of competitive intelligence: How to evaluate and develop competitive intelligence? // Procedia Social and Behavioral Sciences. Vol. 24. P. 1615–1623.

12. Mancilla-de-la-Cruz J., RodriguezSalvador M., Ruiz-Cantu L. (2020) The Next Pharmaceutical Path: Determining Technology Evolution in Drug Delivery Products Fabricated with Additive Manufacturing. Foresight and STI Governance, vol. 14, no 3, pp. 55–70. DOI: 10.17323/2500-2597.2020.3.55.70

13. Moore J. (1993) Predators and Prey: A New Ecology of Competition // Harvard Business Review. May/June 1993. Режим доступа: https:// hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition, дата обращения 11.05.2020.

14. Kuhn M.-L., Viviers W., Sewdass N., Calof J. (2020) The Business Anticipatory Ecosystem outside the «First World»: Competitive Intelligence in South Africa. Foresight and STI Governance, vol. 14, no 3, pp. 72–87. DOI: 10.17323/2500-2597.2020.3.72.87

УДК 004.942

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА У СОЦІАЛЬНИХ МЕРЕЖАХ НА ОСНОВІ АГЕНТНОЇ ПАРАДІГМИ

Васильєва О.О.
аспірант
olga.vasiljeva37@gmail.com

Бутвін Б.Л.
д.т.н., професор
butvin_bl@ukr.net

Анотація. В роботі проаналізовано можливості застосування методу агентного моделювання для дослідження інформаційного протиборства у соціальних мережах.

Метою дослідження є обґрунтування використання агентної парадигми для моделювання деструктивних соціальних процесів, які відбуваються в соціальних мережах, що дає змогу в подальшому здійснювати управління соціальними процесами в соціальних мережах та досягти необхідного рівня інформаційного впливу.

У суспільстві соціальні мережі, засновані на Інтернет-технологіях, стали наразі одним із найвпливовіших каналів поширення інформації. Через соціальні мережі відбувається як міжособистісне спілкування їх учасників, так і просування інформації, ідей та думок. Іноді ці процеси носять деструктивний, руйнівний характер, що стимулює людство навчитися управляти цими процесами.

Загалом моделювання соціальних мереж насамперед використовується для здійснення [1]:

– аналізу структури мережі (наприклад, пошуку лідерів думок, пошуку прихованих спільнот та прихованих зв'язків тощо);

– дослідження соціальних процесів (наприклад, поширення чуток);

– дослідження процесу формування та розвитку соціальної мережі (наприклад, дослідження впливу репутації учасників соціальної мережі на динаміку зміни її структури у часі).

З погляду інформаційної безпеки важливими питаннями, на які може допомогти знайти відповіді підходи до адекватного моделювання соціальних мереж, є такі:

як впливає структурна позиція суб'єкта впливу на його ефективність у поширенні інформаційних впливів;

як впливає структура мережі на її робастність щодо зовнішніх інформаційних впливів;

через скільки часу суб'єкт інформаційного впливу зможе впливати на задану кількість вузлів.

Саме тому моделювання соціальних мереж – це **актуальне** наукове завдання, яке використовується для дослідження соціальних процесів, таких як поширення інформації та/або інформаційних впливів, формування репутації учасників соціальної мережі, процесу інформаційного управління та протиборства тощо.

Для управління деструктивними процесами, які відбуваються в соціальних мережах, слід розуміти, як організовані соціальні мережі, як вони ростуть, як у них поширюється інформація і як знайти найбільш впливові вузли, що забезпечують її швидке поширення. Саме тому для дослідження соціальних процесів, авторами розглядається модель динамічної соціальної мережі.

Сам термін «соціальна мережа» у 1954 р. запропонував англійський соціолог Джеймс Барнс у збірці робіт «Людські стосунки». Цим терміном він висловив думку про те, що суспільство - це складне переплетення особистісних соціокомунікаційних стосунків. Барнс досліджував взаємозв'язки між людьми (членами соціуму) за допомогою візуальних діаграм, в яких окремі особи зображались крапками, а зв'язки між ними - лініями.

Ще до створення інтернету соціолог Марк Грановеттер (амер.) і математик Лінтон Фріман (амер.) опублікували основоположні матеріали за цією тематикою [2]. М. Грановеттер визначив, що всередині соціальних мереж слабкі зв'язки (сусіди, знайомі, знайомі знайомих, формальні контакти на роботі) мають більше значення, ніж сильні (родичі, друзі). Таке явище пояснюється це тим, що інформація швидше і ширше розповсюджується саме через слабкі зв'язки. Більш сильну теоретичну аргументацію на користь тези про силу слабких зв'язків запропонував Рональд Берт (амер.) у своїй теорії «структурних дір» [3].

Наприкінці XX - початку XXI ст. з'явилися віртуальні соціальні утворення. У 1995 р., під авторством Ренді Конрадса, з'явилася Classmates.com – перший інтернет- сайт, який пропонував можливості роботи із соціальними мережами. Слідом за ним у 1997 році з'явився SixDegrees.com. Починаючи з 2001 року, з'являються сайти, у яких використовувалася технологія під назвою «Коло друзів». Ця форма соціальних мереж, яка й нині використовується у віртуальних спільнотах, набула широкої популярності в 2002 році з появою сайту Friendster.

Слід також визначити саме поняття «соціальна мережа». В кожній предметній галузі можна надати своє власне визначення. Так для соціальних мереж, які функціонують в кіберпросторі, в сучасних дослідженнях використовують терміни «електронна соціальна мережа», «соціальна інтернет-мережа», «віртуальна соціальна мережа» та «комп'ютерна соціальна мережа», які є семантично рівноправні. В даній роботі автор буде використовувати більш зручний, загальний та найпоширеніший термін – «соціальна мережа», хоча він визначається контекстно.

З *технологічної* точки зору соціальна мережа - це інтерактивний, з великою кількістю користувачів веб-сайт, контент якого наповнюється самими учасниками. Сайт є автоматизованим соціальним середовищем, яке дозволяє спілкуватися групі користувачів, об'єднаних загальним інтересом. Теоретично як соціальну мережу можна розглядати будь-яку онлайнову спільноту [4].

О. Онищенко, В. Горовий, В. Попик визначають соціальні мережі як «технологічні комплекси організації і управління обмінами електронною інформацією між суб'єктами соціальних відносин, призначені для забезпечення горизонтального спілкування зацікавлених у ньому абонентів, об'єднаних спільними інтересами, інформаційними потребами і навичками спілкування» [5].

Однією з задач соціальних мереж є процес комунікації, при чому наразі вже не лише невербальної, оскільки типи соціальних мереж поповнилися як аудіо-, так і відео контентними. Отже, слід визначити, яким саме чином здійснюється комунікація, та хто є її основними суб'єктами.

За Д. Брасом можна виділити такі властивості суб'єктів соціальних мереж та зв'язків між ними (див. Таблицю 1).

Таблиця 1.

Типові показники деяких суб'єктів соціальних мереж

Властивості	**Визначення**
Degree (ступінь)	кількість прямих посилань на з іншими суб'єктами
In-degree (ступінь вихідних посилань)	кількість посилань на суб'єкта від інших суб'єктів
Out-degree (ступінь вхідних посилань)	кількість посилань суб'єкта на інших суб'єктів
Range / diversity (різноманітність)	кількість зв'язків з не пов'язаними між собою суб'єктів
Closeness (близькість)	ступінь того, наскільки один суб'єкт може легко дійти до іншого суб'єкта
Betweenness (посередність)	ступінь, в якій суб'єкт є посередником між двома суб'єктами в найкоротшому шляху від одного до іншого
Centrality (центральність)	ступінь, а якою суб'єкт є центральним в мережі
Prestige (престиж)	міра, що відображає центральність суб'єкта з урахуванням спрямованості зв'язків. В даному випадку престижний суб'єкт є не джерелом відносин, а об'єктом, на якого дані відносини спрямовані
Ролі	
Star (зірка)	суб'єкт в значній мірі центральний в соціальній мережі
Liason (зв'язковий)	суб'єкт, який має зв'язки з двома чи більше не пов'язаними між собою групами, при цьому не є членом жодної з них
Bridge (міст)	суб'єкт, який є членом двох і більше груп
Gatekeeper (хранитель воріт)	користувач, який є одноосібним посередником або контролює потік двох частин соціальної мережі
Isolate (ізольований)	суб'єкт, який не має або має відносно мало зв'язків з іншими суб'єктами

В даній таблиці вказані параметри аналізу структурної організації соціальної мережі та рольові позиції суб’єктів, які в свою чергу також організують дану структуру.

Крім характеристик самих акторів і їх рольових позицій для аналізу і розуміння функціонування соціальних мереж важливим є поняття зв'язку. Самі зв'язку, як і власне учасники мережі, мають свої властивості і особливості. Найбільш повний список, який демонструє типи взаємодії між суб’єктами соціальної мережі, представлений в роботі Д. Браса (див. Таблицю 2).

Таблиця 2.

Типи взаємодії між суб’єктами соціальної мережі

Властивості	Визначення
indirect links (непряме посилання)	Шлях від одного суб’єкта до іншого опосередкований одним або більше осіб
frequency (Частота)	Кількість посилання на суб’єкта
stability (стабільність)	Поява посилання на суб’єкта з певною періодичністю
multiplexity (множинність)	Поява зв'язків між двома суб’єктами в двох і більше різних контекстах
strength (сила)	Кількість часу, емоційної близькості та взаємних послуг
direction (напрямок)	Частота звернення одного суб’єкта до іншого
symmetry (симетрія)	Частота обопільних звернень суб’єктів

Разом з тим навіть сама докладна характеристика суб’єктів соціальних мереж та їх соціальних відносин недостатньо розкриває психологічні аспекти їх поведінки в рамках соціальної мережі.

Процес комунікації в соціальних мережах може здійснюватися **між окремими користувачами** – друзі, підписники, фоловери, як в односторонньому, так і в двосторонньому напрямку. Так, наприклад, соціальна мережа Instagram або Twitter не передбачають обов’язкової двосторонньої комунікації, тобто, якщо один користувач стає підписником іншого алгоритм роботи мережі не передбачає обопільної дії. В свою чергу соціальна мережа Facebook, або російські мережі «ВКонтакте» та «Одноклассники» застосовують здебільшого алгоритм обопільної «дружби».

Інший вид **комунікації – групова** – здійснюється в межах створених груп - це віртуальні співтовариства, об'єднання певного числа користувачів на основі певних спільних інтересів. При цьому, кожна група керується одним або декількома адміністраторами, які, як правило, поширюють в ній певний контент відповідної спрямованості конкретної групи. В даному випадку процес обміну інформацією скоріш за все буде представлений у вигляді відцентрованих променів, тобто від одного або декількох адміністраторів до певної кількості користувачів. Але надалі частина користувачів може активно вступати в так

звані багатосторонні дискусії-обговорення (залучена одночасно велика кількість користувачів).

Слід також зазначити, що різні соціальні мережі передбачають різні підходи до групової комунікації. Так, наприклад, в тих же «ВКонтакте», «Одноклассники» та Facebook групи існують в зазначеному вище вигляді, а такі соціальні мережі як Instagram, Twitter, LinkedIn чи відеохостинг YouTube не передбачають групових профайлів. Тут функція групової комунікації належить так званим «лідерам думок» або блогерам, які активно з використанням технологій контентної реклами залучають до себе на акаунти велику кількість підписників. «Лідери думок» в даному випадку відіграють роль адміністраторів, тобто одноосібно формують контент, однак групову комунікацію в коментарях можуть підтримувати всі користувачі.

Аналізуючи наведений факт з точки зору теорії «***двоступеневих думок***», запропонованої Г.Г. Почепцовим [7], адміністратори груп та «лідери думок» сприймаються користувачами як компетентні фахівці в тій чи іншій області, а їх думка, доведена до цільової аудиторії за допомогою віртуального інформаційного повідомлення, не піддається сумніву.

Основні проблеми дослідження мережевих структур полягають в тому, що їх безпосереднє вивчення ускладнене дуже великими розмірами та постійними змінами, що відбуваються у структурі мереж — відмирають старі зв'язки, виникають нові зв'язку й вузли. Так можна виділити три основні взаємопов'язані процеси, що становлять парадигму їх дослідження:

1. Процес генерації значної кількості об'єктів соціальної мережі, який має динамічний (стохастичний) характер.
2. Нестаціонарний і досить різноманітний характер взаємних інформаційних зв'язків (ІС) об'єктів соціальної мережі між собою.
3. Процес знищення (загибелі) як самих об'єктів соціальної мережі, так і їх зв'язків, також має нестаціонарний і стохастичний характер.

Саме тому одним з ефективним методом дослідження великих мереж є їхнє моделювання. При цьому досвід авторів показує, що застосування класичних методів, таких як модель гонки озброєнь Річардсона, системна динаміка Форрестера, теорія диференційних рівнянь, зустрічає значні труднощі в їх практичній реалізації з урахуванням розглянутих вище особливостей. Тому авторами пропонується розглянути агентну парадигму (agent — based modelingand simulation) як один з методів імітаційного моделювання. Саме агентне моделювання дозволяє дослідити динаміку соціальних процесів та поведінку користувачів (агентів), які відбуваються в соціальних мережах.

Можна виділити основну особливість даного методу, що складається у наступному: будуються сценарії можливих варіантів розвитку подій у майбутньому, на підставі чого формуються, а потім відбираються стратегічні альтернативи, які працюють у кожному сценарії і служать підставою для прийняття рішень про вибір інтегрованої стратегії.

Агентний підхід дозволяє проводити багатоваріантний ситуаційний аналіз системи, що моделюється. Сутність агентного підходу при побудові сценаріїв

полягає в побудові середовища активних агентів, визначенні алгоритмів їхнього функціонування та взаємодії, та виявлення нових закономірностей, зв'язків, когнітивних зв'язків, а також комплексу математичних моделей формування сценаріїв на комп'ютерному моделюючому комплексі.

В імітаційній агентній моделі її складові – агенти – функціонують незалежно один від одного та від системи загалом. Вони діють за своїми законами, на основі яких й формуються загальні правила функціонування системи загалом, тобто побудова моделі «від низу до верху».

Для створення агентної моделі соціальної мережі, перш за все, необхідно сформувати близький до реальності віртуальний інформаційний простір, «населений» віртуальними агентами. Розглядаючи модель інформаційного протиборства авторами запропоновано наступні типи агаентів:

– першоджерело – ***перший тип агентів***, які публікують контент для подальшої популяризації;

– акаунти–боти – ***другий тип агентів*** (бот — це спеціальна програма, що виконує автоматично і за заданим розкладом певні дії через ті ж інтерфейси, що й звичайний користувач)– використовуються для штучного нарощування «лайків» чи коментарів з метою підняття рейтингу публікації серед користувачів мережі, **дають змогу посилити вплив у інформаційному середовищі** шляхом залучення нових цільових аудиторій **(**бот поширює новину, але майже нічого не змінює**, він на відміну від троля є механічним, троль — креативним)**;

– акаунти-тролі – ***третій тип агентів***— звичайна дійова особа, яка надає кольорового забарвлення новинам. Вони оперують великими групами і подають новину з різних ракурсів. За цим типом агентів можуть знаходитись блогери, лідери думок, які репостять «вірусний» контент на власні сторінки, тим самим одразу (в один клік) збільшуючи потенційні цільові аудиторії (перегляди, лайки, репости) в рази;

– ***четвертий тип агентів*** – реальні люди, які є потенційною цільовою аудиторію інформаційної операції, вони «споживають» контент та сприймають його достовірним, тобто підпадають під інформаційний та психологічний вплив і стають «інфікованими» даним контентом, вірять, що інформація правдива та популяризують її далі в мережі, базуючись на своїй вірі.

При побудові агентної моделі однією з основних задач ***є визначення взаємодії агентів між собою***, яким чином дані агенти ***формуються*** (виникають), що впливає на передачу інформації від одного агенту до іншого, якою може бути динаміка цієї передачі.

Передбачається, що агенти в соціальній мережі можуть:

1. самозароджуватися;
2. породжувати нових агентів шляхом репостінгу (repost);
3. «вмирати» — зникати з простору агентів (припинити передавати контент);
4. отримувати лайки (like) від інших агентів.

Випливаючи з можливих дій агентів також різниться взаємодія між ними, яка може відбуватися за такими алгоритмами:

від одного агенту до іншого – взаємодія між четвертим типом агентів;

від одного агенту до групи агентів – взаємодія між третім та четвертим типом агентів, між першим та четвертим типом агентів та між другим та четвертим типом агентів;

від однієї групи агентів до іншої- взаємодія між другим типом агентів.

Характер зв'язків між агентами може бути як прямим, так і зворотнім.

У такій системі рішення задачі можуть формуватися за рахунок взаємодії великої кількості агентів, що безперервно взаємодіють один з одним, а також формується колективна поведінка.

У результаті виділення типових агентів – акаунтів-користувачів – в соціальній мережі, виявлення закономірностей їх взаємодії та притаманних даним агентам характеристик, стає очевидним, що така умовна інформаційна система не належить до формальних моделей, є неоднорідною, а поведінка її елементів – акаунтів користувачів – нераціональною. Саме в таких випадках, коли інформаційна система є децентралізованою та не діє за глобальними правилами і законами, а навпаки, ці глобальні правила і закони є результатом індивідуальної активності членів групи, слід застосовувати агентний підхід.

Нижче пропонується розглянути реалізацію генерації безлічі об'єктів соціальної мережі як стохастичного нестаціонарного процесу за допомогою агентного моделювання (АМ) в програмному середовищі професійної версії AnyLogic 7.02.

Динамічне створення і видалення агентів соціальної мережі.

AnyLogic дозволяє динамічно додавати і видаляти активні об'єкти соціальної мережі за рахунок застосування реплікованих об'єктів, що використовуються зокрема для моделювання агентів. AnyLogic підтримує реплікацію об'єктів - дуже простий і зручний спосіб створення заданої кількості активних об'єктів мережі одного типу. AnyLogic позбавляє від необхідності додавання на діаграму великої кількості ідентичних об'єктів, оскільки такий підхід є втомливим і дозволяє створювати тільки системи з постійною кількістю об'єктів. Замість цього, ви можете просто створити реплікований об'єкт, який буде представляти собою одразу кілька активних об'єктів одного типу.

За допомогою реплікації об'єктів можна:

• створювати задану кількість активних об'єктів одного типу одним об'єктом;

• створювати масштабовані системи, задаючи кількість елементів реплікованого об'єкта за допомогою параметра;

• моделювати системи з динамічно змінюваною структурою, додаючи і видаляючи елементи реплікованого об'єкта під час роботи моделі соціальної мережі.

Щоб мати можливість динамічного додавання або створення об'єктів соціальної мережі, необхідно оголосити вкладений об'єкт реплікованим, ввівши в його властивості кількість початкову кількість примірників даного об'єкта (або 0, якщо Ви не хочете, щоб екземпляри об'єкта створювалися при запуску моделі, а хочете додати їх пізніше самостійно).

Припустимо, у Вас є реплікований об'єкт people типу Person, що знаходиться на діаграмі агента Main. Тоді AnyLogic автоматично створить два методи, що

дозволяють динамічно додавати і видаляти елементи цього реплікованого об'єкта під час виконання моделі:

Person add_people - додає новий об'єкт типу Person в реплікований об'єкт і повертає його для того, щоб можна було зробити додаткову ініціалізацію цього об'єкта;

void remove_people (Person personToRemove) - вилучає вказаний елемент з реплікованого об'єкта і видаляє його.

На рисунку 1 наведено графічне уявлення інформаційних зв'язків соціальної мережі.

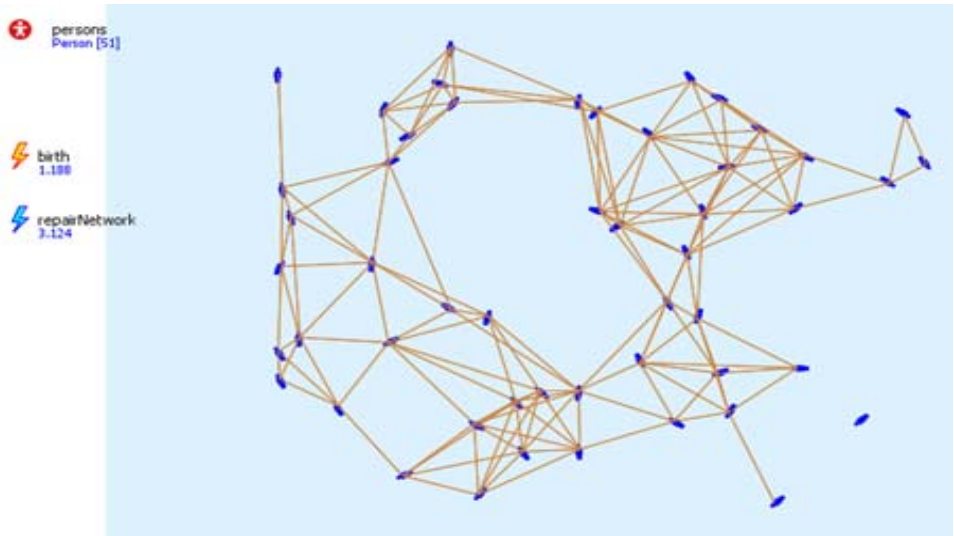


Рис. 1. Графічне уявлення інформаційних зв'язків соціальної мережі.

Другим нестаціонарним і досить різноманітним завданням є формування взаємних інформаційних зв'язків (ІЗ) об'єктів соціальної мережі між собою. AnyLogic як середовище дослідження соціальної мережі підтримує кілька типів мереж агентів:

1. Випадкова мережа – агенти з'єднуються випадково, у кожного агента встановлюється вказана кількість зв'язків з іншими учасниками соціальної мережі.
2. Мережа згідно відстані – один з одним з'єднуються ті агенти соціальної мережі, відстань між якими не більше заданого радіуса з'єднання.
3. Мережа на основі решіткового впорядкованого кільця – зв'язки агентів утворюють кільце, в якому кожен агент з'єднується із заданою кількістю найближчих агентів.
4. Малий світ – це рішуче впорядковане кільце, де деякі зв'язки були розірвані і встановлені інформаційні зв'язки з віддаленими агентами.
5. Безрозмірна мережа – деякі агенти є концентраторами (лідерами думок) з безліччю з'єднань, а деякі – «відлюдниками» з невеликим числом з'єднань з іншими агентами соціальної мережі.

На рисунку 2 наведено фрагмент соціальної мережі «малий світ» з інформаційними зв'язками та оцінкою кількості інформаційних зв'язків об'єктів соціальної мережі.

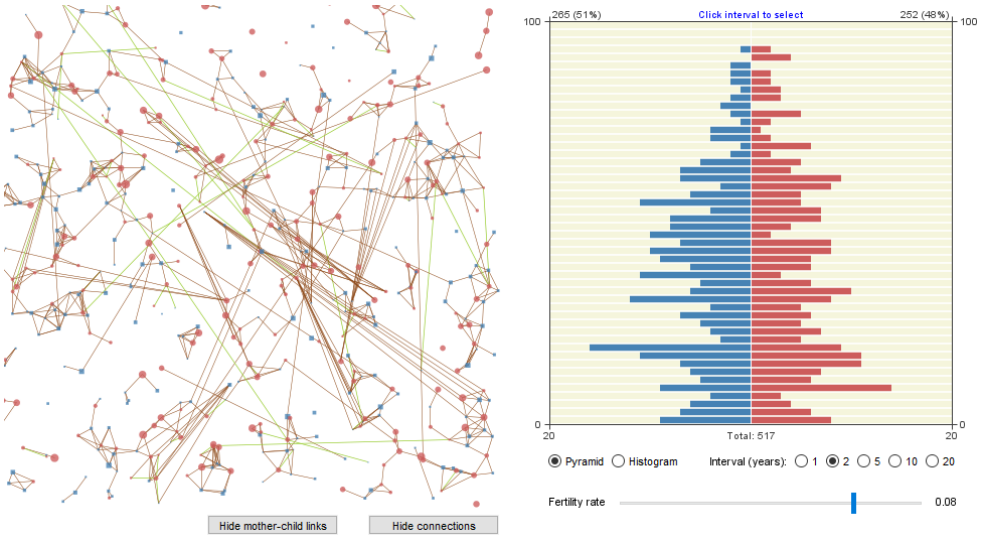


Рис. 2. Фрагмент соціальної мережі «малий світ» з інформаційними зв'язками та оцінкою кількості інформаційних зв'язків об'єктів соціальної мережі.

Слід врахувати, що ці методи створюються в типі агента Main, так що вони можуть бути викликані безпосередньо з будь-якого місця моделі мережі.

Керування зв'язками агентів.

Взаємодія агентів в агентних моделях соціальних мереж може бути реалізована різними способами. Якщо зв'язки між агентами досить постійні, то агенту потрібно запам'ятовувати тих агентів, які перебувають з ним в якомусь зв'язку. Сенс таких зв'язків може бути, наприклад, таким: друг, колега, батько, дитина тощо. На рисунку 3 наведено меню типу взаємодії та графічні результат оцінки взаємодії агентів соціальної мережі.

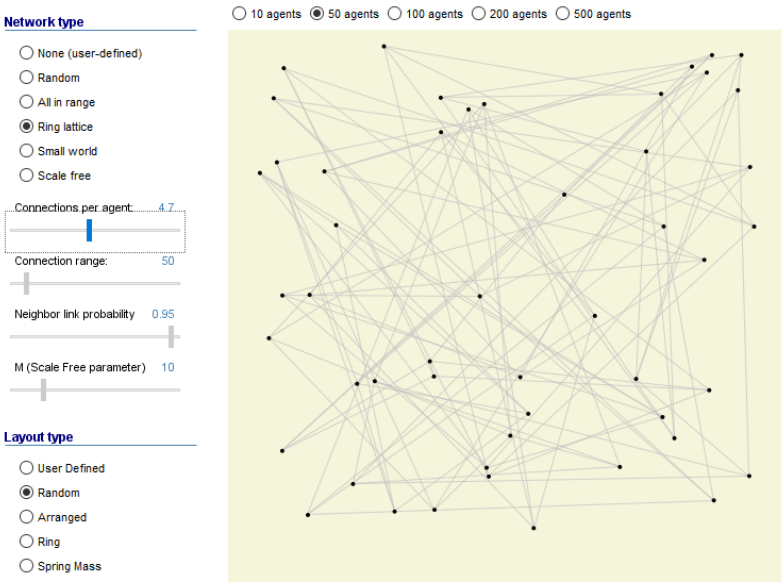


Рис. 3. Меню завдання типу взаємодії агентів соціальної мережі.

Списки взаємодій використовуються, коли агент надсилає повідомлення своїм контактам. Якщо вам потрібно створити більше мереж взаємодій, ви можете додати більше зв'язків агентів.

AnyLogic надає такі методи для встановлення зв'язків між агентами:

LinkedList < Agent > getConnections - повертає список всіх пов'язаних агентів або null, якщо зв'язків встановлено не було;

int getConnectionsNumber – повертає кількість пов'язаних агентів;

Agent getConnectedAgent (int index) – повертає зв'язаного агента з вказаним номером index;

connectTo (Agent a) – додає зазначеного агента до списку зв'язків цього агента, і навпаки;

boolean isConnectedTo (Agent a) – перевіряє, чи пов'язаний цей агент з зазначеним агентом;

boolean disconnectFrom (Agent a) – від'єднує цього агента від зазначеного агента, повертає false, якщо вони не були пов'язані;

disconnectFromAll () – від'єднує цього агента від усіх інших агентів.

На рисунку 4 наведено результати оцінки активності агентів соціальної мережі (чоловіків і жінок).

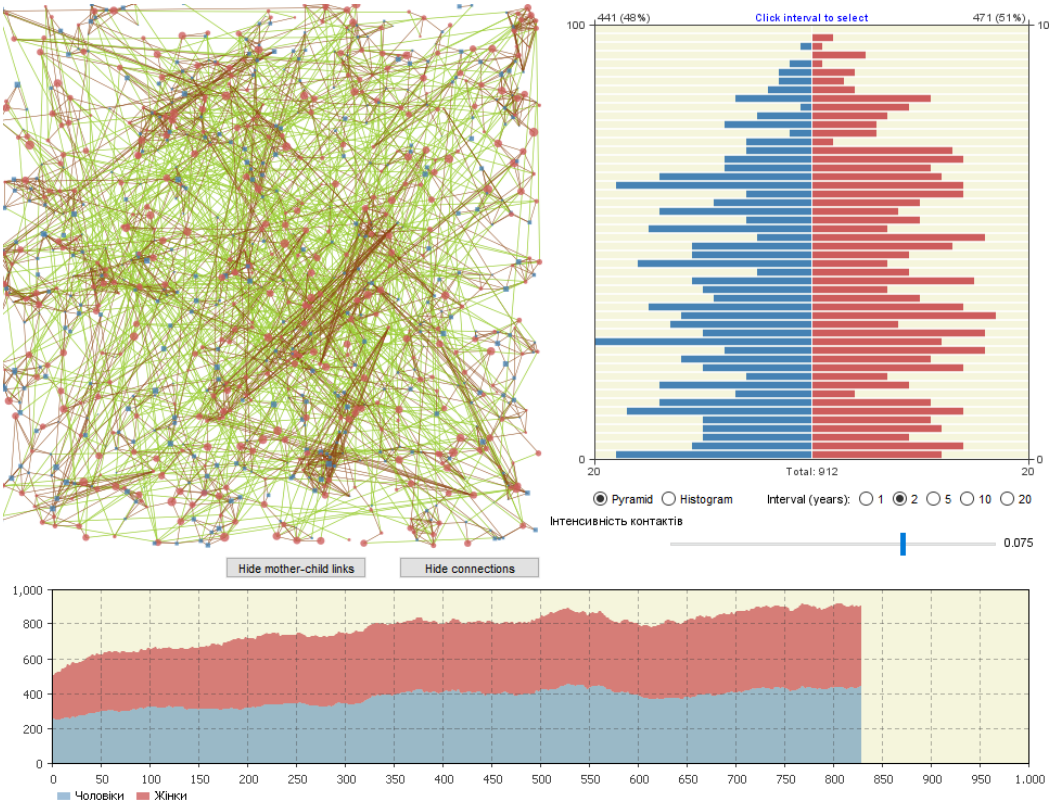


Рис. 4. Результати оцінки активності агентів у соціальній мережі (чоловіків і жінок).

Висновок. На сьогодні є очевидним, що пошук дієвих механізмів дослідження соціальних мереж є надзвичайно актуальним і важливим завданням. Це нелінійне динамічне середовище, яке не можливо зарегламентувати чи описати чіткими математичними формулами. Для такого середовища

запропоновано використання агентної парадигми. Особливістю даної парадигми є багаторівнева абстракція опису процесу взаємодії в соціальних мережах. Це порівняно новий клас моделей, який дозволяє вирішувати завдання високого рівня складності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mark Granovetter. Professor in the School of Humanities and Sciences [Електронний ресурс]. - http://www.stanford.edu/dept/soc/people/mgranovetter/index.html; 37 Freeman, Linton C. Research Professor. - Режим доступу: http://moreno.ss.uci.edu/
2. Burt, Ronald S. «StructuralHoles: The Social Structure of Competition». - Cambridge : Harvard University Press. - (1992).
3. Галіч Т. О. Соціальні Інтернет-мережі та віртуалізація суспільного життя с. 150 / Т. О. Галіч // Соціологія майбутнього: науковий журнал з проблем соціології молоді та студентства. - Х., 2010. - Вип. 1. - С. 145-152.
4. Онищенко О. С. Соціальні мережі як чинник розвитку громадянського суспільства : монографія / О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.; НАН України, Нац. б-ка України ім. І. Вернадського. - К., 2013. - 220 с.
5. D. Brass A Social Network Perspective on Human Resources Management Networks in the Knowledge Economy (pp.39-79) Publisher: JAI Press https://www.researchgate.net/publication/234021381_A_Social_Network_Perspective_on_Human_Resources_Management

УДК 004.056.53

ЗАРУБІЖНИЙ ДОСВІД ЩОДО РОЗВИТКУ СИСТЕМ ПРОТИДІЇ ЗАГРОЗАМ КІБЕРТЕРОРИЗМУ НА ДЕРЖАВНОМУ РІВНІ

Ткаченко О.В.,
заступниця Генерального директора,
Консалтингова компанія «СІДКОН»
tkachenko@sidcon.com.ua

Анотація. Ефективний кіберзахист та інформаційний суверенітет держави можуть бути забезпечені на основі конкурентоспроможних національних інформаційних технологій та створення спеціалізованих кібервійськ, здатних відбивати атаки кібертерористів на державні критичні інфраструктурні системи та захищати від кібератак органи державної влади та управління.

Світовий досвід показує, що на сьогодні близько 70 країн світу активно займаються питаннями забезпечення кібербезпеки, в тому числі у військовій сфері [1]. Це пов'язане з тим, що останніми роками переважна більшість країн світу зіштовхнулась з проблемами кіберзлочинності, зокрема з кібератаками на об'єкти критичної інфраструктури.

Вступ

Близько 50 країн мають власні системи кібербезпеки, які створені за останнє десятиріччя. У розвинутих країнах світу на державному рівні отримали розвиток централізовані системи протидії загрозам кібертероризму, до яких відносяться США, Китай, Німеччина, Великобританія та ін.

Поряд з цим, в умовах зростання геополітичної ролі кіберпростору та протистоянь у ньому значним чином зросла роль кібервійськ у сфері глобальних конфронтацій. Ці кібервійська створюються провідними державами світу (США, Великобританією, країнами ЄС, Китаєм тощо). Завданням цих кібервійськ є розвідувальна робота в мережі, захист власних мереж, блокування та «обвал» структур противника з використанням можливостей кіберпростору [2]. Найпотужнішими та найактивнішими вважаються кібервійська США та КНР [3].

США

США мають технологічну перевагу серед інших держав світу в галузі інформаційних технологій, а тому є безумовним лідером у сфері протидії кібертероризму.

США одні з перших країн світу оперативно зреагували на кіберзагрози та нові можливості використання кіберпростору з метою ефективного захисту від кібератак, створивши у 2009 р. на базі Агентства національної безпеки (АНБ) і підрозділів військово-повітряних сил спеціалізоване Кіберкомандування (кібервійсько) (U.S. Cyber Command). Практично відразу аналогічні структури стали з'являтися і в інших країнах.

Поряд із спеціалізованим Кіберкомандуванням (U.S. Cyber Command), у США також створені кіберкомандування військово-морського флоту, морське кіберкомандування, військове кіберкомандування.

Головною метою функціонування Кіберкомандування США є планування та координація дій щодо захисту інформаційних мереж Міністерства оборони, а також, в особливих випадках, проведення повномасштабних військових операцій у кіберпросторі з метою протидії кібератакам. Поряд з цим, обов'язки щодо захисту цивільної інформаційної інфраструктури в США покладено на Міністерство внутрішньої безпеки та Агентство національної безпеки (АНБ) [4].

Іншими словами, Кіберкомандування США не виконує завдання з оборони від кібератак досить вразливої цивільної критичної інформаційної інфраструктури країни, яка охоплює системи управління мережами енергопостачання, транспортом, інформаційні мережі фінансових організацій тощо, концентруючись виключно на обороні елементів військової інфраструктури Міністерства оборони.

Зокрема, вищевказаний підрозділ «Cyber Command» забезпечує функціонування інформаційних систем з блокування хакерів та запобігання збору інформації на комп'ютерах Міністерства оборони, для чого здійснюються закупівля і установка захисних систем, обмеження доступу, криптографічний захист і т.п.

Кіберкомандування у структурі збройних сил США розпочало роботу в 2010 р., а на повну потужність вийшло тільки наприкінці 2018 р.

У цілому, ключова роль у здійсненні державного управління кібербезпекою США належить Міністерству внутрішньої безпеки (МВБ) – загальнодержавному органу, який повинен забезпечувати координацію всіх зусиль щодо захисту внутрішньої території та критично важливих об'єктів (КВО) США.

Так, забезпечення кібербезпеки покладено на Управління кібербезпеки та комунікацій МВБ (Office of Cyber Security and Communications), у складі якого створено Національний центр кібербезпеки та комунікацій (National Cybersecurity and Communications Integration Center).

Завданнями Національного центру кібербезпеки та комунікацій є:

- раннє попередження про кібератаку;
- захист від несанкціонованого доступу до комп'ютерних мереж;
- розслідування кіберзлочинів;
- координація діяльності федеральних органів влади з реагування на комп'ютерні надзвичайні події;
- вжиття оперативних заходів з виявлення та локалізації джерел кіберзагроз.

Ще одним структурним елементом вказаного підрозділу є Центр екстреного реагування (Комп'ютерна група реагування) на комп'ютерні інциденти (надзвичайні ситуації) в США (US-CERT), який було утворено у 2004 р. та який здійснює заходи зі зміцнення системи національної кібербезпеки, координує обмін інформацією та оперативно протидіє кіберризикам, що загрожують державі.

Водночас, відповідно до раніше підписаної Президентом США Директиви «Presidential Policy Directive / PPD-20» згаданий вище підрозділ «Cyber Command» займається не лише оборонними, а й наступальними кібероперацiями. У межах «Cyber Command» створені підрозділи для планування і здійснення кібератак на противника – кібертерористів, а також для захисту Пентагону від ворожих кібератак.

Про наступальні операції у кіберпросторі представники Пентагону відкрито заговорили у лютому 2019 р. У той же час, керівництво Кіберкомандування США офіційно підтвердило, що їх фахівці провели кібератаку проти російської інфраструктури. А в грудні 2019 р. глава Кіберкомандування США Пол Накасоне знову повідомив, що в якості заходів запобігання втручанню у вибори американського Президента в 2020 р. вони знову проведуть кібератаки проти Російської Федерації.

Взагалі, за даними експертів, кіберпростір в якості зони бойових дій став активно використовуватися американськими військовими ще з 90-х років.

Отже, в США фактично здійснюють протидію кібертероризму спеціалізоване Кіберкомандування – у військовій сфері та Міністерство внутрішньої безпеки та Агентство національної безпеки (АНБ) – для кіберзахисту критичної інформаційної інфраструктури держави. Агентство національної безпеки (ANB) є основним суб’єктом з кібербезпеки в секторі національної безпеки. Крім того, в США також створено так зване Національне агентство геопросторової розвідки. Поряд з цим, в Адміністрації Президента є посада Координатора з кібербезпеки (Cybersecurity Coordinator).

У цілому, у США проблемами кіберзахисту та кібернападу передусім опікується профільний персонал Агентства національної безпеки, Федерального бюро розслідувань, Центрального розвідувального управління, Міністерства внутрішньої безпеки, Розвідувального управління Міністерства оборони США та ін.. Агентством бойового забезпечення Міністерства оборони США у сфері кібербезпеки є Агентство із захисту інформаційних систем (DISA), до 1991 р. відоме як Агентство із захисту комунікацій. Перед DISA поставлено завдання забезпечення безпеки інформаційних технологій та комунікацій, підтримки та захист військових мереж.

Крім того, у 2018 р. в США згідно із законом «Про забезпечення кібербезпеки та інфраструктуру безпеки» було створено Агентство з кібербезпеки і захисту інфраструктури (Cybersecurity and Infrastructure Agency – CISA), яке займається захистом інфраструктури США як від кібер-, так і від фізичних атак [5]. У склад CISA входить Національний центр інтеграції кібербезпеки і комунікацій (NCCIC), який реагує на будь-які кіберзагрози, гарантує кібербезпеку веб-сайтів уряду та інших державних органів США тощо.

CISA також координує зусилля з кібербезпеки між урядом та приватними компаніями. У разі кібератаки на критичну інфраструктуру США CISA доручено координувати зусилля з реагування та сприяти ефективній комунікації з протидії та нейтралізації кібератаки.

На відміну від багатьох європейських країн, де власники та оператори критичної інфраструктури юридично зобов’язані повідомляти про великі

інциденти з кібербезпекою визначеним державним органам, у США обмін інформацією щодо вразливостей та оцінки ризиків між федеральним урядом і приватним сектором є добровільним. Відповідно основна відповідальність за захист критичної інфраструктури, реагування на кібератаки та відновлення після них лежить на власниках та операторах цих потужностей.

Всі провідні країни світу регулярно підтримують належний рівень кібербезпеки: активно беруть участь у навчаннях щодо протидії кібератакам. Військовий досвід США (Cyber Storm) та ЄС (Cyber Europe) доводить, що подібні програми навчання мають значний ефект для виявлення проблемних зон кіберзахисту інфраструктури, моделювання можливих кіберінцидентів і вироблення типових схем реагування на них, поліпшення міжвідомчої взаємодії. Наприклад, у Великій Британії створено Інститут віртуальних досліджень (virtual Research Institute).

Як відомо, в 2011 р. між США та Великобританією було укладено угоду про проведення масштабних тренінгів і програм навчання американських і європейських IT-експертів, спрямованих на боротьбу з терористичними IT-загрозами.

КНР

Дані про потенціал, чисельність та завдання китайських кібервійськ практично відсутні. У так званій «Білій книзі з питань оборони КНР» йдеться мова про створення та активну діяльність китайських кібервійськ та про розбудову інформаційного потенціалу збройних сил Китаю, у тому числі армії кібершпигунів, в умовах зростання ролі цифровізації для розвитку міжнародної економіки та суспільства.

За переконанням міжнародних експертів, кібервійська КНР володіють потенціалом знищувати критично важливу інфраструктуру, отримувати доступ до банківських, комерційних, військових та оборонних баз даних зарубіжних країн. При цьому у Китаї широко залучаються до виконання військових або розвідувальних кібероперацій працівники приватних компаній.

У 2011 р. КНР офіційно визнала існування спеціальних кіберпідрозділів у своїй армії. Відповідальним за наступальні дії в кіберпросторі є підрозділ армії КНР, який має назву «Підрозділ 61398».

Базою для вербування нових хакерів до військових кіберпідрозділів армії КНР стають хакерські клуби, за якими керівництво Китаю уважно спостерігає. Щоправда, схожим шляхом прямують також і США, і країни ЄС.

У КНР кібервійська здійснюють регулярні та координовані кібератаки на інформаційні системи інших держав, зокрема США. Китай – найбільш активна держава у світі за фільтрацією інформації та за частотою здійснення кібератак на іноземні організації.

Німеччина

Відповідальним державним органом у сфері кібербезпеки Німеччини виступає Федеральне управління інформаційної безпеки (BSI) [6], яке взяло участь у спільній ініціативі з Федеральним управлінням захисту громадян та

допомоги в надзвичайних ситуаціях (ВВК) щодо створення інтернет-платформи із захисту важливих об'єктів інфраструктури від кібератак.

У складі Федеральної розвідувальної служби Німеччини (BND) функціонує підрозділ по боротьбі з кібератаками, який здійснює кіберзахист державних органів та промислових підприємств країни. При цьому за кількісним складом цей державний підрозділ по боротьбі з кібератаками на порядок менше, ніж аналогічні структурні підрозділи в США або Китаї.

Поряд з цим, в Міністерстві оборони Німеччини створений спеціальний підрозділ – Computer Network Operations (CNO) – для ведення «наступальних» кібероперацій в Інтернеті.

Німеччина активно співробітничає із США в рамках двосторонніх зустрічей, присвячених питанням кібербезпеки.

Ізраїль

Однією з найбільш підготовлених держав у світі щодо протидії кібертероризму, поряд з США і Китаєм, виступає Ізраїль. Донедавна відповідальними за кібербезпеку Ізраїлю державними органами виступали: Національне кібербюро Ізраїлю та Національний департамент кібербезпеки. Національне кібербюро активно співпрацювало з іншими державними органами, приватним сектором, науковцями, промисловими компаніями, пов'язаними з кібербезпекою.

Зокрема, у 2015 р. в Ізраїлі було створено Національний департамент кібербезпеки (The National Cyber Bureau) як координаційний орган, діяльність якого спрямована на посилення кіберзахисту.

Крім цього, у лютому 2015 р. уряд Ізраїлю схвалив рішення про створення ще й Національного управління з кіберзахисту як центрального оперативного органу Національного кібербюро.

У подальшому з метою інституційної оптимізації процесів забезпечення кібербезпеки 17 грудня 2017 р. ізраїльським урядом було прийнято рішення про об'єднання Національного кібербюро та Національного департаменту кібербезпеки в єдину Національну службу кібербезпеки, яка на сьогодні відповідає за всі аспекти кіберзахисту: від формування засад державної політики та нарощування технологічного потенціалу з метою ефективного кіберзахисту до оперативної роботи спеціальних підрозділів у цій сфері, а також за усі аспекти кіберзахисту в цивільному секторі.

20 червня 2018 р. офіс Прем'єр-міністра Ізраїлю опублікував законопроєкт про кібербезпеку та національний директорат з кібербезпеки. Цей проєкт став останньою стадією процесу, що розпочався у 2010 р. із створення в Ізраїлі національного органу з кібербезпеки як частини національної стратегії кібербезпеки.

Законопроєкт слугує правовою основою для створення Ізраїльського національного директорату з кібербезпеки (INCD). INCD визначається як орган оперативної безпеки, підпорядкований офісу Прем'єр-міністра, що повинен опікуватися захистом кіберпростору та утвердженням Ізраїлю як світового лідера в галузі кібербезпеки. На INCD покладається завдання захисту держави

від кіберзагроз, посилення спроможності Ізраїлю в боротьбі з кібератаками та просування ізраїльської кіберполітики, а також сприяння міжнародному співробітництву в кіберсфері. Працівники INCD матимуть право вимагати у будь-якої організації інформацію або документи, необхідні для виявлення кібератак, їх подолання або запобігання їм. INCD керуватиме національною командою реагування на комп'ютерні надзвичайні ситуації (CERT), яка вже працює.

З 2002 р. в Ізраїлі функціонує Національне агентство з інформаційної безпеки (NISA), яке працює в межах Служби загальної безпеки (GSS) і визначає критерії регулювання в тих чи інших сегментах державного та приватного секторів у кіберсфері. Завданням NISA є визначення цілей щодо кібербезпеки, розробка плану їх досягнення та контроль за виконанням плану спільно з відповідним міністерством.

За готовність країни до надзвичайних ситуацій та управління кризовими ситуаціями в цивільному секторі кіберсфери відповідають Міністерство громадської безпеки, Міністерство оборони та Командування армією оборони Ізраїлю.

Поряд з цим, у 2010 р. при службі безпеки (ШАБАК) Ізраїлю був створений відділ з інформаційної безпеки, який контролює критично важливі національні інфраструктури та який спеціалізується на запобіганні кібертероризму, проведенні спеціальних операцій у кіберпросторі.

Армія оборони Ізраїлю (IDF) також десятиліттями займається питаннями кібербезпеки та кіберзагрозами, однак згідно зі своїми підходами до оборонної політики не оприлюднює деталей щодо бачення національної безпеки та політики у військовій сфері; зазвичай ці питання не обговорюються з громадськістю. Але у серпні 2015 р. Стратегію IDF вперше було опубліковано.

У цьому документі окреслено кілька аспектів позиції IDF щодо кібербезпеки, зокрема вказано, що кіберпростір – це військова сфера; зроблено акцент на пріоритетності подальшої розбудови кіберзахисту; визнано наявність загроз у кіберпросторі та необхідність ініціювання на організаційному рівні створення кіберкоманд у межах IDF.

Крім того, кіберрозвідка в Ізраїлі належить до військового та оборонного секторів.

Ізраїль має одну з найбільших у світі баз радіоелектронної розвідки (SIGINT).

Головним кібервійськом Ізраїлю, як однієї з найбільш підготовлених держав у світі щодо протидії кібертероризму, є підрозділ військової розвідки Ізраїлю 82005. До завдань підрозділу 8200 входять: перехоплення розвідданих, дешифрування, прослуховування ворожих цілей та організація кібератак. Другим за вагомістю кібервійськом Ізраїлю є управління С41 збройних сил Ізраїлю. Основним завданням даного управління є захист військових мереж від кібератак. Підрозділ 8200 та управління С41 працюють координовано [7].

Національне управління з питань надзвичайних ситуацій спільно з Армією оборони Ізраїлю IDF проводить навчання, націлене, зокрема, на відбиття кібератак на критичну інфраструктуру Ізраїлю.

У 2012 р. в Ізраїлі був розроблений симулятор кібератак спеціально для тренування військових, а також співробітників державних організацій, які забезпечують захист стратегічно важливих, критичних комп'ютерних систем країни. За допомогою симулятора фахівці моделювали різні кібератаки для того, щоб оцінювати ефективність кіберзахисту критичних інформаційних систем країни.

Також у 2012 р. в Ізраїлі була створена кіберполіція як суб'єкт забезпечення національної безпеки.

В Ізраїлі розвивається державно-приватне партнерство у сфері забезпечення кібербезпеки. У 2016 р. в Ізраїлі розпочав роботу Ізраїльський консорціум кіберкомпаній (IC3) – група провідних ізраїльських компаній у сфері кібербезпеки. Члени IC3 співпрацюють з провідними урядовими установами у сфері кіберзахисту, передовими технологічними компаніями, стартапами та міжнародними кіберрозвідувальними організаціями.

Естонія

Естонія є одним із беззаперечних лідерів в ЄС у сфері впровадження цифрових сервісів та електронного урядування.

Національний план розвитку оборони Естонії на 2017-2026 роки, виходячи з Національної військової стратегії, передбачає розвиток Кіберкомандування. Міністерство оборони є координаційним органом з питань кіберзахисту у сфері національної оборони Естонії.

У лютому 2014 р. у межах Міністерства оборони Естонії засновано відділ, який безпосередньо займається кібербезпекою та який координує розвиток інформаційних систем та інформаційних технологій у сфері компетенції Міністерства оборони, займається плануванням політики у кіберсфері в межах юрисдикції Міністерства оборони та контролює виконання такої політики.

Окрім Міністерства оборони, національний кіберзахист підтримує Відділ кіберзахисту Естонської ліги оборони – підрозділ, до складу якого входять фахівці з кібербезпеки як державних, так і приватних інституцій. Естонська ліга оборони (Kaitseliit) – це добровольча воєнізована озброєна національна організація оборони, яка діє в межах завдань Міністерства оборони і включає підрозділ з кіберзахисту.

Головним учасником процедур виявлення та попередження кіберзагроз, спричинених кіберрозвідкою, екстремізмом, кібертероризмом та спробами диверсій, є Служба внутрішньої безпеки Естонії (Kaitsepolitseiamet, KAPO), основними функціями якої є розвідка та кримінальні розслідування.

У цілому, основними державними органами Естонії, відповідальними за кібербезпеку, є: Управління інформаційних систем (RIA), CERT Estonia, підпорядкований Управлінню інформаційних систем, та Департамент захисту важливих об'єктів інфраструктури (CIIP). Щорічно Управління інформаційних систем Естонії публікує доповіді про кібербезпеку.

У 2009 р. у рамках Комітету з безпеки при Уряді Республіки Естонія була створена Рада з кібербезпеки, основне завдання якої полягає в розвитку стратегічного рівня співпраці між різними міністерствами і відомствами країни

та контроль за реалізацією Стратегії кібербезпеки країни. Головує у цій Раді генеральний секретар Міністерства економіки та комунікацій.

Управління інформаційних систем (RIA) Естонії, створене в 2011 р. як Естонський центр компетенції та координації кібербезпеки, організовує захист критичної інформаційної інфраструктури та здійснює контроль за кібербезпекою інформаційних систем держави. RIA підпорядковується Міністерству економіки та комунікацій, яке координує державну політику Естонії у сфері кібербезпеки.

У межах RIA сформовано окрему структуру – Департамент захисту важливих об'єктів інфраструктури (CIIP), завданням якого є організація захисту об'єктів критичної інфраструктури Естонії. RIA також бере участь у розробці національних стратегій та політики в галузі кібербезпеки. У випадку порушення вимог кібербезпеки під час надання життєво важливих послуг RIA може накладати штрафи.

Крім того, у сфері забезпечення кібербезпеки Естонії основною організацією, відповідальною за проведення навчання та підвищення рівня інформування про кіберінциденти, є Фонд розвитку освіти у сфері інформаційних технологій (HITSA), раніше відомий як Фонд «Стрибок тигра».

Окрім цього, у 2012 р. відділи Департаменту поліції та прикордонної охорони (PBGB) Естонії з розслідування кіберзлочинів були об'єднані в єдиний департамент. У поліції є посада web-констеблів (поліціянти, які працюють в Інтернеті).

Служба внутрішньої безпеки Республіки Естонія також постійно вдосконалює свої можливості щодо запобігання загрозам національній безпеці, пов'язаним з кібератаками та кібершпигунством.

Відповідальність за загальну координацію державної політики у сфері кібербезпеки наразі покладено на Міністерство економіки та комунікацій Естонії, хоча до 2011 р. цим питанням опікувалося Міністерство оборони.

Естонія взяла участь у Об'єднаному центрі передових технологій з кібероборони НАТО (NATO CCDCOE).

В Естонії активно практикується державно-приватне партнерство у сфері кібербезпеки. Національною платформою для співробітництва з державним та приватним секторами у сфері кібербезпеки виступає X-Road.

Литва

У грудні 2014 р. сейм Литви прийняв Закон «Про кібернетичну безпеку», яким було передбачено створення Національного центру кібернетичної безпеки, відкриття якого відбулось у липні 2016 р. Цей центр вирішує питання кібербезпеки державних інформаційних ресурсів та критичної інформаційної інфраструктури.

У цілому, організаційна структура системи кібербезпеки Литви визначена зазначеним Законом про кібербезпеку (останні зміни у закон внесено у червні 2018 р.)

Поряд з цим, у 2011 р. уряд Литви затвердив Постанову №766 «Про затвердження Програми розвитку електронної інформаційної безпеки (кібербезпеки) на 2011-2019 рр.».

Програма забезпечення інформаційної безпеки (кібербезпеки) Литви має три основні цілі: забезпечити безпеку державних інформаційних ресурсів; забезпечити ефективне функціонування критичної інформаційної інфраструктури; забезпечити кібербезпеку населення Литви та осіб, які перебувають у Литві. Згодом ці цілі були доопрацьовані у вказаному вище Законі Литви про кібербезпеку, ухваленому у 2014 р.

З 1 січня 2018 р. у Литві розпочала діяти нова система національної кібернетичної безпеки, відповідно до якої створена Служба інформаційної безпеки, в структурі якої виділяються три кіберпідрозділи щодо кіберзахисту та управління мережами, які підпорядковані Міністерству національної оборони. Частина співробітників Служби інформаційної безпеки – це військовослужбовці.

Розробку політики кібербезпеки, її реалізацію організовує, контролює та координує Міністерство національної оборони Литовської Республіки. Політика кібербезпеки реалізується Національним центром кібербезпеки, Державною інспекцією захисту даних, Литовською поліцією та іншими державними органами влади Литви, функції яких пов'язані з кібербезпекою.

У свою чергу, Уряд Литви у сфері забезпечення кібербезпеки держави:

- затверджує Національну стратегію кібербезпеки;
- затверджує інституційний склад Ради з питань кібербезпеки;
- затверджує методику ідентифікації критичної інформаційної інфраструктури та перелік критичної інформаційної інфраструктури;
- затверджує організаційні та технічні вимоги до кібербезпеки, що висуваються до суб'єктів кібербезпеки;
- затверджує Національний план управління кібербезпекою;
- здійснює контроль за управлінням кризами кібербезпеки.

Рада з питань кібербезпеки є постійним колегіальним незалежним дорадчим органом, який аналізує ситуацію із забезпеченням кібербезпеки в Литовській Республіці та вносить пропозиції до установ, які розробляють і впроваджують політику кібербезпеки, суб'єктів кібербезпеки, науково-дослідних і освітніх установ та суб'єктів господарювання, які беруть участь у діяльності в галузі інформаційних технологій (так звані «актори кібербезпеки»), щодо покращення ситуації із забезпеченням кібербезпеки.

Раду з питань кібербезпеки очолює представник Міністерства національної оборони.

Найбільше завдань з реалізації політики кібербезпеки у Литві покладається на Національний центр кібербезпеки, який підпорядкований Міністерству національної оборони та який:

- здійснює нагляд за дотриманням суб'єктами кібербезпеки вимог щодо кібербезпеки;
- наказує суб'єктам кібербезпеки надавати інформацію, необхідну для оцінки відповідності суб'єктів кібербезпеки й керованих ними комунікаційних та інформаційних систем організаційним і технічним вимогам кібербезпеки;

- застосовує технічні заходи для вимірювання кіберстійкості державних інформаційних ресурсів та критичних інформаційних інфраструктур щодо потенційних кіберінцидентів;
- видає накази щодо забезпечення кібербезпеки та усунення виявлених недоліків та прогалин з питань кібербезпеки;
- надає вказівки суб'єктам кібербезпеки, за винятком постачальників цифрових послуг, проводити незалежні аудити комунікаційних та інформаційних систем або послуг, що надаються за допомогою таких систем;
- здійснює моніторинг та аналіз кіберінцидентів на національному рівні;
- здійснює та контролює технічні заходи кібербезпеки в державних інформаційних ресурсах та критичній інформаційній інфраструктурі;
- здійснює організаційне управління та реагування на кіберінциденти в комунікаційних та інформаційних системах суб'єктів кібербезпеки на національному рівні;
- застосовує заходи кібербезпеки у випадку кіберінцидентів;
- бере участь в управлінні кризами кібербезпеки тощо.

Державна інспекція захисту даних Литви здійснює функції національного регулятора у сфері захисту персональних даних.

Великобританія

Велика Британія є лідером у багатьох питаннях забезпечення кібербезпеки, хоча окремого спеціального закону про кібербезпеку країна не ухвалювала.

Головним державним органом Великобританії, на який покладено завдання захисту критичної інфраструктури від загроз кібертероризму, є Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI) – міжвідомча організація, яка підпорядкована та фінансується Службою безпеки Великобританії (MI-5), контррозвідувальним органом країни, що здійснює заходи забезпечення захисту держави від загроз національній безпеці (тероризму, шпигунства, поширення зброї масового знищення).

У країні існує добре розвинена система державно-приватного партнерства, яке є частиною Стратегії з кібербезпеки Великобританії. Так, наприклад, Центр захисту національної інфраструктури (CPNI) організує для компаній, що працюють у 14 секторах економіки, регулярні обміни інформацією та кращими практиками у сфері забезпечення кібербезпеки.

Крім того, у Великобританії у 2013 р. у зв'язку із збільшенням кількості кібератак на інформаційно-комунікаційні системи країни та на основі державно-приватного партнерства і системи обміну інформацією з питань кібербезпеки (Cyber Security Information Sharing Partnership, CISP) було створено Центр з протидії кіберзагрозам (Cyber Security Operations Centre). Метою створення цього Центру є попередження та нейтралізація кібератак на об'єкти критичної інфраструктури, а також швидке реагування на ці атаки.

Окрім цього, у Великобританії існують Національна рада Безпеки та Офіс страхування з питань кібернетичної та інформаційної безпеки (Office of Cyber

Security and Information Assurance) [8], а також Національний центр кібербезпеки (NCSC).

З огляду на важливість партнерства між урядом та приватним сектором у розробці стандартів кібербезпеки на веб-сайті NCSC створено спеціалізовану сторінку, де перераховані зусилля, спрямовані на розвиток можливостей міжсекторальної кібербезпеки у Великій Британії, зокрема навчальні заходи з підготовки майбутніх спеціалістів з кібербезпеки, освітні заходи для існуючих фахівців з кібербезпеки.

Кібербезпека також належить до сфери компетенції міжурядової групи Government Emerging Technology and Innovation Analysis Cell (ETIAC), створеної з метою виявлення технологічних загроз і визначення можливостей, пов'язаних з національною безпекою. Крім того, питаннями кібербезпеки у своїй діяльності опікуються й такі усталені структури Великобританії, які займаються питаннями «сканування горизонтів» і «сценаріїв «що якщо»: зокрема, урядова група Government Futures Group (GFG) і консультативна група при секретарі кабінету (Cabinet Secretary's Advisory Group, CSAG).

За дотримання правил кібербезпеки у Великобританії в основному відповідають такі регуляторні органи:

1) **GCHQ** – провідна агенція з питань розвідки, кібербезпеки та безпеки, місією якої є захист Великої Британії від основних загроз національній безпеці. Для виявлення, аналізу та нівелювання кіберзагроз співробітники агенції використовують передові технології, технічні винаходи та широкі партнерські зв'язки. У випадку кіберзагроз національній безпеці залучаються органи безпеки та розвідки Великої Британії;

2) **Національний центр кібербезпеки (NCSC)**, який створений у 2016 р. та який об'єднав компетенції відділу забезпечення інформації GCHQ, Центру оцінювання кібербезпеки, CERT-UK та Центру захисту національної інфраструктури. NCSC є єдиним контактним пунктом для малого і середнього бізнесу, великих організацій, державних установ, широкої громадськості та урядових підрозділів. Центр співпрацює з іншими правоохоронними органами, оборонними відомствами, службами розвідки та безпеки Великої Британії та міжнародними партнерами;

3) **Національний підрозділ з кіберзлочинності (NCCU).**

Польща

У Польщі функціонують три суб'єкта державної системи кібербезпеки: Міністерство адміністрації та впровадження цифрових технологій (цифровізації), Міністерство національної оборони та Служба внутрішньої безпеки.

Зокрема, у 2011 р. у Польщі створено Міністерство адміністрації та цифровізації, до основних завдань якого відносяться:

- розробка та реалізація стратегічних документів і правових актів у сфері кібербезпеки, здійснення національного та міжнародного співробітництва;

- розробка керівних принципів щодо розробки заходів з метою кіберзахисту інформаційних систем держави;
- забезпечення кібербезпеки у військовій сфері;
- підготовка аналізу щодо стану кібербезпеки на національному рівні та кіберризиків для держави;
- побудова національної освітньої платформи з метою забезпечення кібербезпеки.

У межах Міністерства адміністрації та цифровізації Польщі у 2016 р. був створений Національний центр кібербезпеки. Його ключовим завданням стало попередження кіберзагроз, реакція на них та координація дій з іншими державними органами у цій сфері.

Польща також взяла участь в ініціативі Міжнародного телекомунікаційного союзу «Міжнародне багатостороннє партнерство проти кіберзагроз» (ITU-IMPACT).

Канада

У Канаді створені та функціонують такі державні органи, які забезпечують кібербезпеку: Центр реагування на надзвичайні ситуації у кіберпросторі (Canadian Cyber Incident Response Centre), Офіс омбудсмена з питань персональних даних (Office of the Privacy Commissioner of Canada) та Управління захисту важливих об’єктів інфраструктури та готовності до надзвичайних ситуацій Міністерства державної безпеки (Office of Critical Infrastructure Protection and Emergency Preparedness).

При цьому Управління захисту важливих об’єктів інфраструктури та готовності до надзвичайних ситуацій Міністерства державної безпеки Канади разом з Shared Services Canada (SSC) сприяють комунікації між державними органами та бізнесом. Центр реагування на надзвичайні ситуації у кіберпросторі Канади співпрацює з провайдерами інтернет-послуг з метою сприяння у визначенні загроз у кіберпросторі та розробки ефективних заходів з їх протидії.

Іспанія

До суб’єктів кібербезпеки Іспанії відносяться:

- **Національна рада з кібербезпеки**, яка надає очолюваній Прем’єр-міністром Раді національної безпеки підтримку та допомогу в спрямуванні та координації політики національної безпеки з питань кібербезпеки та сприяє координації та співпраці між громадськістю і владою та між державними органами і приватним сектором у зазначеній сфері;
- **Спеціалізований ситуаційний комітет за підтримки Ситуаційного центру Департаменту національної безпеки**, що керує кризовими ситуаціями в галузі кібербезпеки, які за своєю суттю або масштабами виходять за межі засобів реагування на надзвичайні ситуації у зазначеній сфері;
- **Національний криптологічний центр (CCN)** – організація в структурі Національного центру розвідки (CNI), створена в 2002 р.

для забезпечення безпеки інформаційно-комунікаційних технологій у різних органах державного управління та безпеки Іспанії для інформаційних систем, які обробляють, зберігають або надсилають таємну інформацію;

- **Національний центр захисту критичної інфраструктури (CNPIC)** – орган, відповідальний за сприяння всім діям щодо захисту критичної інфраструктури, за які на національному рівні відповідає Державний секретаріат з питань безпеки, а також за координацію цих дій і нагляд за їх виконанням. Основна мета діяльності цієї інституції – координація механізмів, необхідних для гарантування безпеки критичної інфраструктури. CNPIC підтримує державно-приватне партнерство, яке надає змогу мінімізувати вразливості критичної інфраструктури Іспанії. CNPIC відповідає також за поширення інформації щодо кіберзагроз і кіберінцидентів щодо критичної інфраструктури та забезпечує координацію і співпрацю між різними секторами економіки та між державними і приватними інституціями у цій сфері. Поряд з цим, CNPIC створює робочі групи, які розробляють секторальні плани з кібербезпеки щодо критичної інфраструктури;
- **Іспанський національний інститут кібербезпеки (INCIBE)** – організація, яка підпорядкована Міністерству економіки та цифрових трансформацій Іспанії, Державному секретарю з питань цифрової трансформації та штучного інтелекту і є базовою установою у сфері розвитку кібербезпеки та довіри у цифровому суспільстві – серед широких кіл громадськості, у сегментах іспанської академічної та дослідницької мережі, а також бізнесу, особливо секторів економіки, що мають стратегічне значення;
- **Об'єднане командування з кіберзахисту (Міністерство оборони) Іспанії**, яке відповідає за планування та виконання дій, пов'язаних з кіберзахистом у мережах, інформаційних системах та телекомунікаціях Міністерства оборони, а також забезпечує адекватну реакцію на загрози в кіберпросторі.

Отже, на сьогодні Іспанія може похвалитися рядом спеціалізованих організацій з кібербезпеки та міцною позицією у сфері забезпечення Кіберзахисту не лише в Європі, а й у всьому світі.

Австралія

В Австралії створена низка відповідальних за кібербезпеку державних органів: відділ кіберполіції та кіберрозвідки, Міністерство Генерального прокурора, Управління радіотехнічної оборони та Національний центр швидкого реагування на надзвичайні ситуації у кіберпросторі (CERT Australia).

Австралією укладені ряд документів щодо міжнародного співробітництва у сфері кібербезпеки, зокрема, із співробітництва у сфері реагування на надзвичайні ситуації кібербезпеки між Міністерством внутрішньої безпеки США та Міністерством Генерального прокурора Австралії.

Через платформи Govdex та Govshare в Австралії заохочують державні органи та приватний сектор обмінюватись знаннями та ресурсами з метою пошуку ефективних та інноваційних рішень щодо забезпечення кібербезпеки.

Висновки

Отже, дослідження зарубіжного досвіду щодо здійснення організаційних заходів, спрямованих на розбудову державних систем забезпечення кібербезпеки, дозволило дійти висновку, що в основі такої системи знаходиться окремий центральний державний орган, який формує політику забезпечення кібербезпеки, здійснює законотворчу та нормативну діяльність у цій сфері, координує діяльність щодо кіберзахисту інших державних органів, забезпечує партнерство з приватним сектором, займається питаннями міжнародного співробітництва щодо протидії кібертероризму та іншим кіберзлочинам.

За прикладом розвинутих зарубіжних країн в Україні доцільно створити державний центр захисту критичної інфраструктури, розвивати методи та види державно-приватних партнерських ініціатив у сфері забезпечення кібербезпеки, а також необхідним є регулярне проведення кібернавчань низки державних органів України, які відповідають за функціонування критичної інфраструктури держави, щодо протидії кібератакам. Подібні програми кібернавчання у США та ЄС мають значний ефект для виявлення проблемних зон кіберзахисту інфраструктури, моделювання можливих кіберінцидентів і вироблення типових схем реагування на них, поліпшення міжвідомчої взаємодії.

Література

1. Шпачук В. В. Суб’єкти державного управління кібербезпекою країни: зарубіжний досвід. Державне управління: удосконалення та розвиток. 2019. №2. http://www.dy.nayka.com.ua/pdf/2_2019/7.pdf
2. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. К.: НІСД, 2014. 328 с.
3. Кращі практики управління кібербезпекою: оглядовий звіт: Проєкт ЄС-ПРООН з парламентської реформи. 2019. 129 с.
4. Кіберезпека та ризики цифрової трансформації компаній : практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН», 2021. 372 с.
5. В США з'явилось агентство оборони, присвячене кібербезпеці. https://futuro.in.ua/news/2140-v-ssha-zyavylos-ahentstvo-kiberbezpeky.html
6. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших: Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України: Європейський інформаційно-дослідницький центр. 2016. 37 с. https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf
7. Ізраїль, Фінляндія та Швеція найбільше підготовлені до кібервійн. https://tyzhden.ua/izrail-finliandiia-ta-shvetsiia-najbilshe-pidhotovleni-do-kibervijn/
8. Кольцов М., Аушев Є. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні (Policy Paper): USAID. 2017. 28 с.

9. Кібервійна та безпека об’єктів критичної інфраструктури: практичний посібник / Ю. І. Когут; за ред. док-ра тех. Наук, проф. А. С. Довгополого. – Київ : Консалтингова компанія «СІДКОН»; ВД Дакор, 2021. 332 с.

10. Кібертероризм (історія, цілі, об’єкти) : практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН», 2021. 304 с.

11. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології) : практичний посібник / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН»; ВД «Дакор», 2022. 284 с.

12. Цифрова трансформація економіки та проблеми кібербезпеки : практич. посіб. / Ю. І. Когут. – Київ : Консалтингова компанія «СІДКОН», 2021. 368 с.

УДК 351.862.48

СТІЙКІСТЬ ДЕРЖАВНИХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ У КРИЗОВИХ СИТУАЦІЯХ

Гнатюк С.Є.
кандидат технічних наук
керівник відділу, Адміністрація Державної служби
спеціального зв'язку та захисту інформації
sgnatuk30@gmail.com

Анотація. Розглядається важливість високого рівня безпеки функціонування електронних комунікацій в умовах кібератаки на державні комунікаційні послуги та послуги на базі електронних комунікацій (соціальні мережі, соціальні медіа, засоби масових комунікацій). Відзначено, що нові комунікації, нове обладнання розширюють можливості на рівні людина-суспільство-держава-кіберзловмисник, а тому від безпеки та стійкості залежить функціонування електронних комунікацій як окремо, так і в складі інформаційно-телекомунікаційних систем, інформаційної та критичної інфраструктури.

Подальший розвиток суспільства характеризується збільшенням рівня цифровізації та віртуалізації суспільства, а також широке впровадження інформаційно-комунікаційних технологій у виробничі процеси, процеси моніторингу та управління як на об’єктовому рівні, так і на рівні цілих сфер економіки починає створює передумови для уразливості збоку нових видів загроз – кібернетичних, які починають домінувати над традиційними. Так, в умовах посилення впливу кіберзагроз на стійкість та сталість функціонування складових елементів критичної інфраструктури в усіх сферах (економічної, політичної, соціальної та гуманітарної) суспільства зростає загроза збільшення кількості кризових явищ, які впливають на широке коло питань, що стосуються як взаємовідносин на рівні людина-суспільство-влада, так і на рівні ефективності управління з боку центральної та місцевої влад у звичайний період та в кризових ситуаціях.

Неоголошена кібервійна проти нашої держави триває, і свідченням цього є кібератаки, які не припиняються. Так, є періоди відносного затишшя, які змінюються сплесками активності хакерів, однак загальної картини це не змінює. Ми бачимо постійне зростання кількості кіберінцидентів і кібератак на 10-12% за квартал. Про це на сторінці у Facebook написав голова Держспецзв’язку Юрій Щиголь [4]. Так, за інформацією розміщеною на сайті Державної служби спеціального зв’язку та захисту інформації, зазначено: вночі з 13 на 14 січня 2022 року була здійснена масована кібератака на державні інформаційні ресурси – одна з найпотужніших за роки агресії. Від неї постраждали майже 70 сайтів центральних і регіональних органів влади. Також частина сайтів, у тому числі портал Дія, були відключені спільно з адміністраторами, щоб уникнути

можливості поширення атаки на інші ресурси. Фахівці Держспецзв'язку разом із колегами з інших служб досліджують цей інцидент. Зараз збираються цифрові докази, аналізуються логфайли для того, щоб зрозуміти весь ланцюжок реалізації цієї атаки. Від кібератак сьогодні потерпають майже всі країни, саме тому основним завданням є швидке відновлення інфраструктури та забезпечення збереження інформації. Наразі триває діяльність із відновлення роботи ресурсів. Частина з них вже відновили свою роботу, інші – запрацюють найближчим часом.

Наразі не виявлено жодних загроз для даних про громадян. Такі дані зберігаються не на сайтах, а у відповідних реєстрах. Доступ до них здійснюється через спеціальну захищену систему обміну даними між реєстрами Трембіта. І ще одне – ми не залишаємося наодинці з ворогом, який використовує фактично необмежені ресурси для агресії проти нашої держави у кіберпросторі. Ситуацію добре бачать і розуміють наші європейські та американські партнери, які запропонували нам свою допомогу. Важливим завданням було – встановити метод реалізації атаки, зібрати цифрові докази та якомога швидше відновити роботу вебресурсів. Протягом дня у медіа з'являлися повідомлення про використання хакерами конкретної вразливості системи керування контентом. Це було лише однією з версій, які опрацьовували фахівці.

Зараз ми можемо зі значною ймовірністю стверджувати, що відбулася так звана supply chain attack. Тобто атака через ланцюжок поставок. Зловмисники зламали інфраструктуру комерційної компанії, що мала доступ із правами адміністрування до вебресурсів, які постраждали внаслідок атаки [3].

При цьому необхідно враховувати, що у бізнесі та приватних комунікаціях ситуація із кіберінцидентами є навіть загрозливішою, адже малий та середній бізнес не мають достатніх ресурсів для протидії кіберзлочинам, на відміну від великих компаній та державних установ. Що стосується пересічних громадян, то ситуація ще гірша, і це зумовлено низьким рівнем цифрової грамотності та кібергігієни. Ось чому питання кіберзахисту є досить важливим в умовах збільшення рівня віртуалізації усіх сфер суспільства та соціальних процесів. Крім того, питання цифровізації інформації, інформаційних та комунікативних процесів разом із інформаційно-комунікаційними технологіями та програмами і проектами з інформатизації формують сучасний порядок денний цифрового відкритого суспільства та цифрової економіки, демократії та урядування. Таким чином, електронні комунікації постають головним суб'єктом інформаційно-телекомунікаційних систем та автоматизації процесів управління, моніторингу та контролю виробничих процесів у багатьох сферах економіки. Отже, збільшення рівня цифровізації та інформатизації виробничих процесів та процесів надання послуг для громадян починає формувати критичну комунікаційну та інформаційну інфраструктуру від стійкості та сталості, функціонування якої починає залежати функціонування усієї іншої інфраструктури, особливо це стосується таких сфер як: електронні комунікації, енергетика, транспорт, банки, е-комерція, е-послуги, державні послуги та управління державою на всіх рівнях. Зважаючи на високий рівень небезпеки, який визначається активізацією кіберзагроз в сучасних реаліях ведення

гібридних війн, питання забезпечення національної стійкості в кризових ситуаціях може відбуватися в «ефективній співпраці, координації між цивільними та військовими структурами», а також «готовності та рівню співпраці між публічними та приватними секторами». На сьогодні великий відсоток критичної інфраструктури знаходиться у приватній власності, а тому для забезпечення високого рівня стійкості необхідна тісна співпраця та взаємодія державних інституцій, які займаються питаннями протидії кіберзагрозам та приватним компаніям, які є власниками та користувачами критичної інфраструктури. Крім того, необхідно враховувати, що питання кіберзагроз та кіберзахисту носить глобальний характер і не обмежується національними кордонами, а тому досить ефективним форматом їх вирішення є об'єднання зусиль окремих держав, транснаціональних компаній та наукових центрів. На сьогодні досить багато різних проєктів та форм співпраці продукується в рамках Європейського Союзу та блоку НАТО. Так, у рамках Східного Партнерства (далі - СхП) заплановано заходи із «EU4Digital: Cybersecurity East», метою яких є «розробка технічних механізмів та механізмів співпраці для зміцнення кібербезпеки і кращої підготовленості до кібератаки відповідно до стандартів ЄС». В рамках СхП участь у заходах беруть Азербайджан, Вірменія, Білорусь, Грузія, Республіка Молдова, Україна, а також інституції ЄС. Основними напрямами пропонується такі: «посилення національного управління кібербезпекою і правової бази в країнах СхП; посилення захисту критично важливої інформаційної інфраструктури в країнах СхП; збільшення операційних можливостей управління інцидентами, пов'язаними з кібербезпекою, в країнах СхП.» [EU4Digital]. У результаті вказаних заходів повинні підвищитись «довіра і безпека» через «розвиток трастових послуг в цифрову економіку і кібербезпека для підвищення стійкості критично важливої інфраструктури як найважливіших будівельних блоків для сумісних транскордонних електронних послуг в регіоні Східного партнерства». Так, окрім інституціонального, законодавчого та нормативно-правового забезпечення кібербезпеки та стійкості на національному рівні Україна приймає участь у практичних заходах, а саме «тижневі командно-штабні навчання «Непорушна стійкість-2020»(проведені у вересні 2021 року), до участі в яких було залучено представників державних силових відомств України та держав-членів НАТО» [2], а саме «три дні 50 учасників з команд Держспецзв'язку, Служби безпеки України, Нацбанку, Міністерства оборони та Департаменту Кіберполіції «наживо» змагалися на віртуальному полігоні з нападниками, роль яких виконували фахівці естонської спеціалізованої компанії CybExer Technologies OU» [1]. Основним результатом цих змагань стало напрацювання навичок «командної роботи», ефективної комунікації та взаємодії підрозділів різних відомств та компаній власників критичною інфраструктурою «для забезпечення стійкості нашої критичної інфраструктури та державних інформаційних ресурсів» [1]. Підводячи підсумки вказаних навчань, віце-прем'єр-міністр з питань європейської та євроатлантичної інтеграції України О. Стефанишина відзначила: «Україна є дуже важливим партнером НАТО і багатьох країн-членів Північноатлантичного альянсу щодо питань, які стосуються боротьби з гібридними загрозами. Ці навчання – це перший елемент

національної соціальної стійкості. І результати сьогоднішніх навчань будуть покладені в основу імплементації концепції з питань стійкості і ухвалення подальших рішень Уряду, парламенту, Президента України» [2]. У свою чергу Танель Танг, представник Групи ЄС з підтримки України, наголосив, що «залучаючи найкращі знання та експертів ЄС, ми допомагаємо підготувати українських експертів із кібербезпеки до нових викликів» [1].

Таким чином, провідні експерти ЄС з питань кібербезпеки передають практичний досвід під час проведення практичних семінарів та навчань. Набутий практичний досвід повинен стати у нагоді під час формування Плану заходів із реалізації заходів щодо національної стійкості за окремими напрямами, сферами, об'єктами усіх сфер економіки. Крім того, проведення таких заходів на регулярній основі сприятиме зростанню рівня міжгалузевих взаємовідносин, а також покращить комунікації між силовими структурами країни під час проведення антикризових заходів та здійснення ефективного управління під час виникнення кризових явищ та ситуацій у країні (на регіональному та загальнодержавному рівнях). Крім того, проведення регулярних тренінгів та навчань на державно-приватному рівні дасть змогу побудувати ефективну національну систему стійкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Головне завдання кібернавчань – напрацювати ефективні механізми і навички для забезпечення кіберстійкості критичної інфраструктури та державних інформаційних ресурсів. URL : https://cip.gov.ua/ua/news/golovne-zavdannya-kibernavchan-napracyuvati-efektivni-mekhanizmi-i-navichki-dlya-zabezpechennya-kiberstiikosti-kritichnoyi-infrastrukturi-ta-derzhavnikh-informaciinikh-resursiv1. (Дата звернення 24.09.2021).
2. Українські силовики спільно з представниками НАТО завершили навчання «Непорушна стійкість-2020». URL : https://m.day.kyiv.ua/uk/news/180921-ukrayinski-sylovyky-spilno-z-predstavnykamy-nato-zavershyly-navchannya-neporushna. (Дата звернення 23.09.2021).
3. Юрій Щиголь: фахівці Держспецзв'язку досліджують кібератаку на сайти державних органів, щоб зрозуміти весь ланцюжок її реалізації. URL: https://cip.gov.ua/ua/news/yurii-shigol-fakhivci-derzhspeczv-yazku-doslidzhuyut-kiberataku-na-saiti-derzhavnikh-organiv-shob-zrozumiti-ves-lancyuzhok-yiyi-realizaciyi. (Дата звернення 14.01.2022).

УДК 351.862.48

КІБЕРБЕЗПЕКА ТА КІБЕРГІГІЄНА КОРИСТУВАЧІВ ПОСЛУГ НА БАЗІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Скибун О.Ж.
к.держ. упр.
начальник 1 управління ДЕК
Адміністрації Держспецзв'язку
skybun@i.ua

Анотація. Розглядається можливість розширення ролі кібергігєни серед користувачів послуг на базі електронних комунікацій, які на сьогодні широко використовуються, а саме: Інтернет-шопінг, комунальні платежі, мобільний банкінг, передача персональних даних. Так, рівень кіберзагроз зростає пропорційно рівню діджиталізації та віртуалізації комунікацій окремих громадян. Для запобігання та протидії кіберзлочинам серед населення необхідно збільшувати кількість заходи із попередження, роз'яснення та просвітництва широких верств населення питанням кібергігієни. Також набуває актуальності питання допомоги населенню з питань кібердопомоги.

Стрімкий розвиток науки та техніки в сфері електронних комунікацій (технологій, мереж, програмного забезпечення, кінцевого програмованого обладнання споживачів) відкриває ще більше можливостей для цифровізації та інформатизації усіх сфер та процесів на глобальному, національному, регіональному та об'єктовому рівнях через збільшення переліку та обсягів надання послуг на базі електронних комунікацій. Так, міжнародні електронні комунікації та глобальна мережа передачі даних дають змогу передавати та отримувати інформацію (цифрову різних форматів) у реальному часі з усіх куточків світу, що створює глобальний віртуальний простір без національних кордонів та застережень на культурному, національному та на рівні віри. Водночас подальше зростання рівня впровадження програм та проектів «Цифрова держава» та «Цифрове суспільство», в рамках яких збільшуються обсяги інформації (цифрової), які передаються, отримуються, обробляються та зберігаються в інформаційно-телекомунікаційних системах державного та приватного рівнів (на різних платформах, базах даних та сервісах). Показовим є збільшення обсягів надання електронних адміністративних послуг через єдині платформи, комунікації надавач/споживач послуг (ЖКХ, опалення, водопостачання та водовідведення, постачання газу, теплової енергії та електроенергії тощо), телемедицина (eHealth), дистанційне навчання, сервіси з покупок та доставки товарів широкого вжитку і продуктів харчування із торгових мереж, банківська сфера (е-банкінг) тощо. Разом з рівнем цифровізації та глобалізації суспільства, відносин на рівні громадянин-суспільство-держава зростає кількість кіберзагроз, кіберінцидентів та кібернебезпек. Отже, можна говорити про те, що «кожен громадянин може розраховувати на власну безпеку

в кіберпросторі», адже «кожен громадянин» повинен «усвідомити правила поведінки в кіберпросторі», бо тільки він сам відповідальний за захист, користуючись «корпоративною поштою, підключаючись до конференцій, обмінюючись файлами» [3] тощо. У зв'язку з цим виникає запит на стійкість та сталість функціонування створених інформаційних ресурсів, не зважаючи на зовнішні та внутрішні чинники впливу, в першу чергу, через зростання рівня кіберзагроз, кіберінцидентів та кібернебезпек. Оскільки «одними з найвразливіших місць віртуального світу є мобільний телефон із доступом до соціальних мереж, месенджерів, та десятків мобільних додатків часто невідомого походження, де люди з легкістю діляться приватною інформацією, яка, на перший погляд, не є критичною» [1]. Вказане відбувається у зв'язку зі збільшенням кількості громадян/споживачів послуг, які почали повсякденне використання цифрових технологій. Так, «загальна кількість комп'ютерних пристроїв, включаючи ноутбуки, настільні ПК, планшети і мобільні телефони, які знаходяться у використанні, в 2021 році досягне 6,2 млрд. штук» [2]. При цьому слід зважати на рівень кібер (комунікативної, комп'ютерної, ІТ, цифрової) компетентності та навичок тих осіб, які володіють та користуються таким кінцевим обладнанням. Особливістю сучасного світу є те, що у вирі новітніх технологій добре почуває себе наймолодше (цифрове) покоління, яке з народження має доступ до цифрових технологій) і у більшості випадків не отримує досвід від попередніх поколінь, а само їм його надає. Ось чому кібер компетентності та навички, хоча і відіграють важливу освітню роль, але головним запобіжником у сучасному цифровому світі проти кіберзагроз, кіберінцидентів та кібернебезпек визначається кібергігієна, яка при належному рівні виступає запобіжником для попередження кіберзлочинів через людський фактор (коли шахраї використовують соціальну інженерію та психологію впливу). Тим самим рівень кібергігієни впливає на «кількість Інтернет-шахрайств, фактів втручання в особистий простір, поширення неправдивих відомостей тощо нині набуває рис епідемії», коли нехтуються (свідомо чи через незнання) так званих «базових правил цифрової безпеки при роботі у світовій мережі та використанні різноманітних сервісів, що їх пропонують сучасні технології» [4]. Високий рівень кібергігієни сьогодні є запорукою безпеки людини (не тільки у кіберпросторі, а і на фізичному рівні), адже «хороша кібергігієна означає дотримання розумних щоденних практик щодо здоров'я та безпеки вашої інформації в Інтернеті» [5]. Тобто, основні рекомендації з кібергігієни повинні використовуватися людиною практично на підсвідомому рівні. Тільки так можна зменшити вплив кібершахраїв на людину в кіберпросторі. Але при цьому не треба забувати, що кібершахраї постійно збільшують арсенал, методи та інструменти впливу на людину з метою заволодіння її персональними даними, паролями та коштами, а тому підвищення рівнів кібер компетентності та кібергігієни повинно відбуватися регулярно на постійній основі. Якщо говорити про державних службовців, військових та працівників великих фірм та корпорацій, то для них проводяться відповідні курси підвищення кваліфікації, тренінги та навчання. Головна проблема постає серед інших верств населення, особливо старшого віку та тих людей, які не є

постійними учасниками кіберкомунікацій. Ось тут і потрібна допомога з боку держави. Наприклад у цьому році Міністерство цифрової трансформації України та Координатор проектів ОБСЄ в Україні презентували новий освітній серіал «Основи кібергігієни», ознайомлення з яким дасть можливість «знати й застосовувати правила кібергігієни на роботі й у повсякденні; розуміти суть соціальної інженерії та психології впливу; безпечно користуватися браузером та загалом мережами Wi-Fi; розмежовувати використання особистої та службової поштових скриньок; розбиратися у використанні програмного забезпечення; вміти відповідально поширювати інформацію в соціальних мережах; опанувати правила безпечної роботи з мобільними пристроями; ознайомитися з роллю фізичної безпеки в кіберзахисті організації; розбиратися у видах маніпуляцій з інформацією у кіберсфері» [6]. Також необхідно враховувати потребу не тільки у навчанні, а і в практичній допомозі через створення відповідних «центрів надання кібердопомоги», якими необхідно охопити усю територію країни, адже на сьогодні відсутній механізм допомоги населенню в наданні практичної допомоги із кінцевим обладнанням (ноутбуки, настільні ПК, планшети і мобільні телефони, смартфони, айфони) в частині антивірусних заходів та перевірки встановленого програмного забезпечення.

Таким чином, можна зробити наступні висновки, що для збільшення ефективності протидії кібершахраїв необхідно виконання двох важливих умов, а саме: створення умов для постійного підвищення рівнів кібер компетентностей і навичок та формування кібервідповідальності через кібергігієну широких верств населення, в першу чергу старшого віку та тих, для кого цифрові технології не є основним засобом (знаряддям праці). Крім цього, формування кібербезпеки та кібергігієни необхідно починати формувати з раннього дитинства. Отже, для вжиття усіх необхідних заходів потрібно сформувати, затвердити та впровадити відповідний План заходів щодо розвитку кібер компетентностей та кібергігієни у населення (на коротку, середню та довгу перспективи) і чітко його дотримуватися та виконувати. Також необхідно створити мережу «центрів надання кібердопомоги», куди б міг звернутися будь-який громадянин та отримати допомогу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безпека в Інтернеті: найпростіші правила захисту даних. URL: https://www.bbc.com/ukrainian/blogs-51444737 (дата звернення: 10.01.2022).
2. Яким буде нове покоління смартфонів. URL: https://www.dsnews.ua/future/dvoynaya-moshchnost-i-novyy-um-kakim-budet-sleduyushchee-poslednee-pokolenie-smartfonov-16052021-425130 (дата звернення: 09.01.2022).
3. Жора В. Може, у кіберНАТО ми будемо швидше, ніж у реальному. URL: https://www.ukrinform.ua/rubric-technology/3249583-viktor-zora-zastupnik-golovi-derzavnoi-sluzbi-specialnogo-zvazku-ta-zahistu-informacii-ukraini.html90щ (дата звернення: 09.01.2022).
4. Кібергігієна – це важливо! URL: https://kpi.ua/2020-10-28 (дата звернення: 10.01.2022).

5. Кібергігієна … Що це? І 5 речей, які слід знати про це. URL: https://itech.co.ua/novyny/kiberhihiiena-shcho-tse-i-5-rechej-iaki-slid-znaty-pro-tse/ (дата звернення: 11.01.2022).

6. Мінцифри навчить держслужбовців основ кібергігієни. URL: https://www.kmu.gov.ua/news/mincifra-navchit-derzhsluzhbovciv-osnov-kibergigiyeni. (дата звернення: 12.01.2022).

7. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : розпорядження Кабінету Міністрів України від 3 березня 2021 р. № 167-р. Урядовий кур'єр від 16.03.2021 № 50.

УДК 004.056.5

ОЦІНКА ІМОВІРНОСТЕЙ ПОЯВ ПОРУШЕНЬ КІБЕРЗАХИСТУ У КОНТРОЛЬОВАНОМУ ЗАХИЩЕНОМУ ПРОСТОРІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ

Хохлачева Ю.Є.
к.т.н., доцент
yuliiahohlachova@gmail.com

Скворцов С.О.
к.т.н., доцент
ssamailer@gmail.com

Вишневська Н.С.
старший викладач
кафедри безпеки інформаційних технологій,
Національний авіаційний університет

Анотація. Розглянуто математичну модель розподілу імовірностей порушень кібербезпеки без урахування їх категоричності.

Стрімкий розвиток науково-технічного процесу в галузі інформаційно-комунікаційних технологій пов'язаний з повсюдним впровадженням їх у всі сфери діяльності суспільства: військову, екологічну, економічну, політичну, наукову, соціальну, фінансову та інші. У результаті відкрилися широкі можливості несанкціонованого доступу до інформаційних ресурсів та систем передачі інформації неавторизованим користувачем.

Небезпечний характер сучасних загроз (атак різного виду та різного характеру) інформації, що переходить в розряд стратегічних ресурсів на предмет інформаційної та кібернетичної безпеки, зумовлює протидію та оцінку імовірності їх принциповим аспектам укріплення стратегічної стабільності суспільства, національної, регіональної та міжнародної безпеки.

Тому пріоритетним напрямом забезпечення достовірності, цілісності, конфіденційності та інших характеристик інформації є оцінка імовірності порушень захисту (кіберзахисту) у інформаційних об'єктах інформаційно-комунікаційних систем (ІКС), а також контроль безпеки (КБ) на об'єкти ІКС або системах зв'язку і при цьому необхідність у виявлені порушень безпеки (кібербезпеки).

Математична модель розподілу імовірностей порушень безпеки (кібербезпеки) без урахування їх категоричності слідує біноміальному розподілу. Як до своєї межі, до біноміального розподілу прагне і гіпергеометричний розподіл.

При біноміальному розподілу кількість порушень безпеки, як випадкова величина, може прийняти тільки цілі значення $x=0,1,2,3,\ldots,n$. Згідно теореми

Бернуллі, імовірністю випадкової події є межа, до якої (з імовірністю, рівної ≈ *1*) майже завжди прагне частість випадкової події при $n>\infty$. Отже, частість:

$$\omega = \frac{x}{n}. \tag{1}$$

Може бути при досить великому *n* прийнята в якості оцінки вірогідності.

Зауважимо, що частість ω сама є випадковою величиною у зв'язку з випадковістю вибірок контролю, а отже:

$$\left|\omega - p\right| = \Delta, \tag{2}$$

де Δ – випадкова похибка (відхилення частості від істинного значення імовірності).

У зв'язку з цим частість ω потребує оцінки її точності та надійності її наближення до імовірності *p*. Це завдання можна успішно вирішити, якщо скористатися теорією довірчих інтервалів. Зауважимо, що при великих *n* (у всякому разі при $n>30$) і при *p*, недуже близькому до *0* або *1*, біноміальний розподіл може відрізнятися від поріального з тими ж параметрами розподілу (математичним очікуванням і дисперсією):

$$a = np \tag{3}$$

та

$$\sigma^2 = np(1-p) = npq, \tag{4}$$

де значення *q* називається рівнем значущості.

З лінійності нормального розподілу випливає, що розподіл частості ω також буде «майже» нормальним з параметрами:

$$a(\omega) = \frac{a}{n} = p \tag{5}$$

та

$$\sigma(\omega) = \frac{\sigma}{n} = \sqrt{\frac{p(1-\mathrm{p})}{n}}. \tag{6}$$

Тоді довірчий інтервал до невідомого значення імовірності можна визначити за формулою:

$$p(\mathrm{z}_q\sqrt{\frac{p(1-\mathrm{p})}{n}} \le p \le \omega + \mathrm{z}_q\sqrt{\frac{p(1-\mathrm{p})}{n}}) = \mathrm{p}, \tag{7}$$

де z_q – імовірнісний коефіцієнт стандартного нормального розподілу, який знаходиться з вирішення рівняння:

$$2\varphi(\mathrm{z}_q) = \mathrm{p} = 1 - \mathrm{q},$$

де $\varphi(\mathrm{z})$ – нормована функція Лапласа.

Значення z_q для різних значень *q* наведені в таблиці 1.

Таблиця 1

Нормовані значення коефіцієнтів z_q

q, %	10	5	1	0.27	0.1	0.01
z_q	1.64	1.96	2.58	3.00	3.29	3.89

Так як стандарт $\sigma(\omega)$ визначається по засвідченим даним, то формула (6) приймає вигляд:

$$\sigma(\omega)=\sqrt{\frac{\omega(1-\omega)}{n}}. \qquad (8)$$

Тоді остаточна конструкція довірчого інтервалу для невідомого значення імовірності *p* може бути побудована за виразом:

$$p(\omega-z_q\sqrt{\frac{\omega(1-\omega)}{n}}\le p\le\omega+z_q\sqrt{\frac{\omega(1-\omega)}{n}})=\mathrm{p}. \qquad (9)$$

Так, наприклад, при довірчій імовірності p=0,95 (q=5%), z_q=1,96 і за виразом (9) отримаємо:

$$p(\omega-1{,}96\sqrt{\frac{\omega(1-\omega)}{n}}\le p\le\omega+1{,}96\sqrt{\frac{\omega(1-\omega)}{n}})=0{,}95. \qquad (10)$$

Отже імовірність того, що невідоме значення імовірності *p* буде заключено в інтервалі, довжина якого:

$$L=2z_q\sqrt{\frac{\omega(1-\omega)}{n}}=4\sqrt{\frac{\omega(1-\omega)}{n}}, \qquad (11)$$

дорівнює *0,95* (або *95%*), де *1,96* можливо округлити до *2*.

Зазвичай вважають, що довірчої імовірності, рівної *0,95* цілком достатньо для практичного використання.

Слід зауважити, що така оцінка імовірності *p* має результати лише за умови $n\omega(1-\omega)>9$. Якщо $n\omega(1-\omega)\le 9$, довірчий інтервал для *p* будується інакше. Найбільш просте в цьому випадку скористатися x^2 розподіленням. Отже, довірчий інтервал для імовірності *p* будується за виразом:

$$\frac{1}{2n}X^2_{q/2}(f_1)<\mathrm{p}<\frac{1}{2n}X^2_{q/2}, \qquad (12)$$

де f_1 та f_2 – числа ступенів свободи рівні $f1$=2x, f_2=2(x+1).

Величини X^2 отримують із спеціальних імовірнісних таблиць за прийнятою довірчою імовірностю *p* і числу ступенів свободи f_1 та f_2.

Наприклад, при ω*=0,06* і $n=200(n\omega(1-\omega)=200*0.06*0.94=11.3>9)$ для довірчої імовірності *p=0,95* за формулою (10) отримаємо довірчий інтервал *0,027<p<0,093*.

Якщо ж $\omega=0,03$ і $n=200(n\omega(1-\omega)=5,8<9)$, то довірчий інтервал для імовірності p необхідно будувати за формулою (12). Очевидно, що в цьому випадку $x=6$. Тоді $f_1=2x=12$, а $f_2=(2x+1)=14$.

З імовірнісних таблиць для довірчої імовірності $p=0,90$ ($q/2=5\%$) отримуємо $X^2_{q/2=5\%}=23.7$. Отже, довірчий інтервал для p в даному випадку буде $0,013<p<0,059$.

Цілком можливо, що систему контролю безпеки інформаційно-комунікаційної системи отримані довірчі інтервали можуть не влаштовувати. Отже, будь-яке їх звуження, спричинить за собою звуження довірчої імовірності, що також небажано. Тому єдиний шлях поліпшення оцінок – поліпшення КБ, уточнення діючих факторів.

Ще раз зазначимо, що при $n\omega(1-\omega)<9$ заміни біноміального розподілу нормальним призводить до дуже великих похибок в оцінці імовірності p. Тоді в практиці КБ до цього питання слід підходити з максимальною коректністю та обережністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки. – Житомир: ЖНАЕУ, 2016. – 616 с.

РОЗДІЛ 2.
БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ ТА ІНТЕРНЕТ РЕСУРСІВ

УДК 004.056.53

АНАЛІЗ ТЕХНОЛОГІЙ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ НА БАЗІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Пашорін В.І.
к.т.н., професор
завідувач кафедри інформаційних систем
програмування та кібербезпеки
ПВНЗ «Європейський університет»
v.pashorin@e-u.edu.ua

Скляренко О.В.
к.ф.-м.н., доцент
завідувач кафедри математичних дисциплін
та інноваційного проектування
ПВНЗ «Європейський університет»
olena.skliarenko@e-u.edu.ua

Милашенко В.М.
декан факультету інформаційних систем та технологій
ПВНЗ «Європейський університет»
viktor.mylashenko@e-u.edu.ua

Анотація. Збільшення числа комп'ютерних інцидентів, пов'язаних з зовнішнім втручанням в роботу систем, спонукало до розробки систем своєчасного виявлення такого втручання. Сьогодні такі системи стали необхідним компонентом інфраструктури безпеки організацій, де виявлення і попередження атак є складовою повсякденної роботи фахівців з кібербезпеки. Дана стаття присвячена дослідженню технологій виявлення комп'ютерних атак, огляду систем виявлення вторгнень, методів аналізу виявлених атак, систем запобігання вторгнень. Авторами наведено і проаналізовано класифікацію, компоненти і архітектуру систем IDS. Запропоновано методи захисту комп'ютерної мережі на базі систем виявлення вторгнень.

Вступ.

З огляду на постійне збільшення числа комп'ютерних атак, пов'язаних із зовнішнім втручанням в роботу систем, виникає необхідність у розробці та вдосконаленні систем та методів своєчасного виявлення різного роду інцидентів та втручань у комп'ютерну мережу. На сьогодні наявність таких систем важко переоцінити, вони стали невід'ємним компонентом інфраструктури безпеки більшості організацій. Файєрвол може успішно захистити внутрішню мережу від

різноманітних атак за умови, що його фільтри правильно налаштовані. Однак, навіть правильні фільтри конфігуруються статично, так що для ефективного захисту потрібно заздалегідь передбачати всі можливі атаки, а це, впринципі, неможливо. Будь-який новий тип атаки має всі шанси «просочитися» через фаєрвол і досягти внутрішніх серверів мережі, що захищається. Виявити сліди атак, які змогли подолати бар'єр фаєрволу, можна шляхом моніторингу мережевого трафіку і моніторингу подій, що відбуваються в комп'ютерній системі або мережі з метою пошуку серед цих подій ознак можливих атак. Інакше кажучи, виявлення атак – це процес реагування на підозрілу діяльність, спрямовану на обчислювальні або мережеві ресурси. Моніторинг трафіку виконується за допомогою програм-аналізаторів мережевих протоколів, а також маршрутизаторів, що підтримують протокол NetFlow, а моніторинг подій за допомогою систем виявлення вторгнень IDS (Intrusion Detection System).

Технології виявлення атак.

Аналізатори протоколів, або мережеві сніфери, дозволяють захоплювати трафік локальних мереж та представляти його у зручному для аналізу вигляді [1].

Система NetFlow збирає статистику про трафік у мережі, але не про кожен пакет, а про потік пакетів (послідовність пакетів, що належать одному й тому з'єднанню між певними програмами двох певних комп'ютерів, наприклад Skype-сеанс між двома користувачами, передача файлу з сервера на клієнтський комп'ютер, читання даних з сервера браузером клієнтського комп'ютера), звідси і назву протоколу (net – мережа, flow – потік) і передає її для аналізу програмним системам NetFlow, які автоматизують пошук атак та загроз. NetFlow збирає різноманітну статистику про потік, таку як час початку та закінчення потоку, обсяг даних, переданих з початку потоку, середня швидкість передачі даних, ну і, природно, всі параметри, що визначають потік, тобто адреси, порти і т. д. Важливо підкреслити, що на відміну від аналізаторів трафіку і систем виявлення атак, NetFlow збирає так звані метадані про трафік, не заглядаючи в поля даних пакетів. Часто статистику NetFlow порівнюють із телефонним рахунком, який показує, з ким і скільки розмовляв цей абонент, але не розкриває, про що він говорив. Однак, знання метаданих часто буває достатньо для того, щоб розпізнати атаку. Для цього застосовується загальний принцип моніторингу мережі — порівняння її поточної поведінки з «нормальною», тобто такою, що стійко повторювалась у минулому і ми знаємо, що при цьому атак у мережі не спостерігалося. Атака зазвичай генерує не зовсім звичайний зразок трафіку і існують рекомендації для розпізнавання таких аномалій. Перелічимо основні з них.

– Виявлення вузлів із незвичайно великою кількістю запитів на з'єднання. Якщо який-небудь вузол раптом увійшов до найбільш активних щодо встановлення сеансів, це має викликати підозри. Така активність характерна для DoS/DDoS-атак, вузлів, заражених хробаками, сканування портів та деяких інших видів зловмисної діяльності. Так, комп'ютер, заражений черв'яком, зазвичай намагається заразити таким кодом якнайбільше інших комп'ютерів і тому намагається з ними з'єднатися. Спам-хост намагатиметься надіслати

якнайбільше листів і тому встановлювати велику кількість з'єднань в одиницю часу з портом 25 (SMTP-порт, на який надсилається пошта).

– Виявлення вузлів з надзвичайно інтенсивним трафіком. У цьому випадку хост, який зазвичай не входив до найактивніших, починає посилати або отримувати незвичайно велику кількість даних в одиницю часу, тобто генерувати занадто інтенсивний трафік. Це також може бути DoS-атака або активність хробака, який намагається заразити інші хости.

– Аналіз SYN та інших прапорів заголовка TCP. Наявність незвичайно великої кількості пакетів із встановленим прапором SYN або іншими прапорами заголовка TCP може свідчити про DoS-атаку. Програмні системи аналізу даних NetFlow автоматизують процедури виявлення аномальної активності в мережі, перевіряючи потоки на відповідність численним зразкам різноманітних атак, насамперед атак відмови в обслуговуванні та скануванні мережі та портів. Дані, віднесені системою до підозрілої активності, виділяються в особливу групу та надаються адміністратору мережі.

Системи виявлення вторгнень.

Розглянемо процес виявлення несанкціонованого доступу чи спроби несанкціонованого доступу до ресурсів. Саме собою виявлення вторгнень не запобіжить доступу до ресурсів. Тим не менш, це метод, який можна використовувати для виявлення злочинної діяльності, надання допомоги у збиранні доказів і, можливо, найголовніше, індикація атак, що відбуваються. Сьогоднішня IDS – це набагато більше, ніж просто виявлення вторгнення. Більшість IDSS матимуть змогу виконувати одну або декілька з таких дій:

• розпізнавання шаблонів, пов'язаних із відомими атаками;
• статистичний аналіз аномальних схем руху;
• оцінка та перевірка цілісності певних файлів;
• моніторинг та аналіз активності користувачів та системи;
• аналіз мережевого трафіку;
• аналіз журналу подій.

Система виявлення вторгнень – це програмний або апаратний засіб, який виконує безперервне спостереження за мережним трафіком та діяльністю суб'єктів системи з метою попередження, виявлення та протоколювання атак.

На відміну від фаєрволів, які будують захист мережі виключно на основі аналізу мережевого трафіку системи виявлення вторгнень враховують у своїй роботі різні підозрілі події, що відбуваються в системі.

Існують ситуації, коли мережевий екран виявляється проникним для зловмисника: наприклад, коли атака йде через тунель VPN зі зламаної мережі, або коли ініціатором атаки є користувач внутрішньої мережі, тощо. І справа тут не в поганій конфігурації міжмережевого екрану, а в самому принципі його роботи. Файєрвол конфігурується на блокування трафіку з заздалегідь передбачуваними ознаками, наприклад за IP-адресами або протоколами. Так що факт злому зовнішньої мережі, з якою у нього був встановлений захищений канал і яка раніше поводилася цілком коректною, у правилах екрану відобразити не можна. Так само, як і несподівану спробу легального внутрішнього користувача копіювати файл із паролями або підвищити рівень своїх привілеїв.

Подібні підозрілі дії може виявити лише система, яка стежить не лише за трафіком, а й за всіма зверненнями до важливих ресурсів окремих комп'ютерів, а також за інформацією про перелік підозрілих дій (сигнатур атак) користувачів.

Іншою важливою відмінністю IDS від фаєрволів є те, що в обов'язки IDS не входить блокування підозрілого трафіку. IDS тільки намагається виявити підозрілу активність та підняти тривогу. Крім цього IDS протоколює підозрілі пакети, поміщаючи їх в журнал.

IDS вміють виявляти різні види мережевих атак, виявляти спроби несанкціонованого доступу або підвищення привілеїв, появу шкідливого ПЗ, відстежувати відкриття нового порту і так далі. IDS перевіряє не тільки параметри сесії (IP адресу, номер порту і стан зв'язку), а і зміст пакетів аж до прикладного рівня, аналізуючи дані, що передаються.

Ефективність таких системи багато в чому залежить від застосовуваних методів аналізу отриманої інформації. У перших системах виявлення атак, використовувалися статистичні методи виявлення атак. В даний час до статистичного аналізу додався ряд нових методів, починаючи з експертних методів і закінчуючи використанням нейронних мереж.

Статистичний метод. Основні переваги статистичного підходу - використання вже розробленого і зарекомендованого апарату математичної статистики і адаптації до поведінки суб’єкта. Спочатку для всіх суб'єктів аналізованої системи визначаються еталонні профілі стану або поведінки. Будь-яке відхилення реального профілю від еталонного визнається як несанкціонована діяльність в системі.

Однак статистичні методи не чутливі до порядку проходження подій; в деяких випадках одні й ті ж події в залежності від порядку їх слідування можуть характеризувати аномальну або нормальну діяльність. Слід також враховувати, що статистичні методи не можуть застосовуватися в тих випадках, коли відсутній шаблон типової поведінки (еталонний профіль).

Експертні методи складаються з набору правил перевірки вхідної інформації, які формуються для системи людиною – експертом. Ці правила можуть бути записані, наприклад, у вигляді послідовності дій в системі, або у вигляді послідовність біт даних в мережевому трафіку (сигнатури). При виконанні будь-якого з цих правил приймається рішення про наявність несанкціонованої діяльності. Важливою перевагою такого підходу є практично повна відсутність помилкової тривоги. Основним недоліком є неможливість виявлення невідомих атак. При цьому навіть невелика зміна послідовності дій для вже відомої атаки може стати серйозною перешкодою для функціонування системи виявлення атак.

Нейронні мережі. В цьому методі передбачено, що спочатку нейромережу, яка є складовою системи виявлення атак, навчають правильної ідентифікації атак на попередньо підібраній вибірці прикладів атак. Після навчання мережа запускається в режимі розпізнавання і самостійно проводить аналіз вхідної інформації та перевіряє чи узгоджуються отримані дані з характеристиками атак, які вона навчена розпізнавати. У ситуації, коли у вхідному потоці не вдається розпізнати нормальну поведінку, фіксується факт атаки.

Джерелом інформації для IDS систем можуть бути: мережевий трафік; журнали реєстрації подій в системі; дії суб'єктів (здебільш виконуваних процесів) системи. Механізми реагування на можливе вторгнення можуть бути досить різноманітними, наприклад, сповіщення адміністратора безпеки (подача звукового сигналу, передача повідомлення на консоль управління, відправки SMS-повідомлення на мобільний телефон), розрив з'єднання, виклик зовнішньої програми, блокування (від блокування конкретної IP-адреси до блокування окремих видів діяльності), переналаштування системи.

IDS – це тільки частина інфраструктури захисту мережі і, як і всі інші компоненти, сама по собі вона не забезпечує абсолютного захисту. Цікавим є порівняння, якщо МЕ – це «броньовані двері» на вході до ІТС, то IDS – це сигналізація, що спрацьовує при спробі зламати ці двері.

Класифікація систем IDS.

Класифікація IDS може бути виконана:

• за способом реагування;

• за способом виявлення атаки;

• за способом збору інформації про атаку.

Класифікація IDS за способом реагування розрізняють пасивні та активні IDS. Пасивні IDS просто фіксують факт атаки, записують дані в файл журналу і видають попередження. Активні IDS намагаються протидіяти атаці, наприклад, шляхом реконфігурації МЕ або генерації списків доступу маршрутизатора [2].

Класифікація IDS за технологією виявлення атак. Існує два підходи до аналізу подій, які можна вважати як можливу атаку: виявлення зловживань (misuse detection) і виявлення аномалій (anomaly detection).

У *технології виявлення зловживань* передбачається, що апріорі відомо, яка послідовність біт даних в мережевому трафіку є ознакою атаки, тому аналіз подій тут полягає у пошуку таких "небажаних" послідовностей біт – сигнатур. Дана технологія виявлення атак дуже схожа на технологію виявлення вірусів. Сигнатури атак також зберігаються в БД, аналогічної тій, яка використовується в антивірусних системах. При цьому IDS може виявити всі відомі атаки, для яких в базі даних вже є інформація про їх характерну послідовність біт. Однак системи даного типу не можуть виявляти нові, ще невідомі види атак.

У *технології виявлення аномалій* визначають ненормальну (незвичайну) активність на хості або в мережі, що і дозволяє зробити висновок про ймовірний інцидент. Детектори аномалій тут створюють профілі нормальної активності, за результатами зібраних даних у період тестового нормального функціонування і потім аналізують діяльність системи і фіксують відхилення від нормальної діяльності. Прикладом аномального поведінки може служити велике число з'єднань за короткий проміжок часу, високе завантаження центрального процесора. При такій технології є можливість виявити нові атаки. Однак аномальна поведінка не завжди є атакою. Наприклад, одночасну посилку великого числа запитів від адміністратора мережі може ідентифікувати як атаку типу «відмова в обслуговуванні».

При використанні з такою технологією можливі два випадки:

• виявлення аномального поведінки, яке не є атакою, і віднесення його до класу атак;

• пропуск атаки, яка не підпадає під визначення аномального поведінки.

Найбільш популярна *класифікація за способом збору інформації про атаку*, тобто в залежності від того де здійснюється збір інформації: в мережі, на конкретному комп'ютері чи на певних додатках, що працюють на комп'ютері. Існує два основних види IDS: рівня мережі (network-based), які аналізують мережевий трафік, і рівня хоста (host-based), які аналізують дії суб'єктів і журнали подій в рамках однієї комп'ютерної системи. Останнім часом виникла необхідність моніторингу безпеки навіть на рівні окремих додатків, що встановлені на комп'ютері і тому, як вид, окремо виділяють IDS рівня додатків (application-based).

IDS рівня мережі (NIDS – network-based IDS) працює як сніффер, «прослуховуючи» увесь трафік в мережі завдяки тому, що мережева карта комп'ютера з IDS працює в режимі прослуховування (promiscuous mode). Захоплюючи й аналізуючи мережні пакети, IDS виявляє в них певні аномалії, що можуть свідчити про можливу атаку (різке збільшення мережевого трафіку, поява нового мережевого трафіку, спроби віддаленої авторизації, поява нових процесів, спроби авторизації з неіснуючим ім'ям користувача, підключення в неробочий час, підвищене використання системних ресурсів), або певні послідовності бітів, які відповідають сигнатурам відомих атак, що зберігаються в базі даних. Розгортання IDS рівня мережі не впливає сильно на продуктивність мережі (використовує копії пакетів), але при підвищеному навантаженні IDS може не встигати обробляти всі пакети і може пропустити атаку, не виявивши її. IDS рівня мережі не можуть аналізувати зашифровану інформацію і більшість з них не здатні зробити висновок про те, чи була атака успішною; вони можуть тільки визначити, що атака була розпочата і адміністратор повинен вручну досліджувати, чи відбулося реальне проникнення.

IDS рівня хоста (HIDS – host-based IDS) призначена для моніторингу, детектування і реагування на дії зловмисників на певному хості і може бути встановлена на окремі робочі станції і сервери для виявлення небажаних або аномальних дій. HIDS використовують в якості інформаційних джерел журнали реєстрації подій, що створюються ОС та прикладними програмами на конкретному вузлу мережі (поява нових файлів, поява нових директорій, зміни прав доступу, зміни файлів, зміни атрибутів...) і тому можуть виявити атаки, які не можуть виявити IDS рівня мережі, наприклад, коли трафік шифрований.

Аналізатори журналів подій за своєю природою є реактивними системами, тобто вони реагують на подію вже після того, як вона відбулась. Таким чином, журнал міститиме відомості про те, що проникнення в систему виконане.

IDS рівня вузла використовують обчислювальні ресурси хостів, за якими вони спостерігають, що впливає на ефективність роботи цих вузлів, тому системи HIDS встановлюються тільки на критичні сервери, а не на кожен комп'ютер в мереж. HIDS не розуміє і не відстежує мережевий трафік, а NIDS не контролює дії всередині системи. Кожен з цих засобів має свої завдання і виконує їх своїми способами.

Класифікація IDS по алгоритму дії. HIDS і NIDS можуть бути одного з наступних типів:

1. *IDS*, що відстежують шаблони (pattern matching), або сигнатурні *IDS*
2. IDS, що відстежують стан (stateful matching);
3. IDS, що відстежують аномалії (anomaly based).

IDS на основі сигнатур. Знання про окремі атаки накопичуються виробниками IDS і зберігаються у вигляді послідовності біт, характерної для атаки, яку називають сигнатурою атаки. Як тільки виявляється новий вид атаки, виробник сигнатурного IDS створює відповідну сигнатуру, яка в подальшому використовується при перевірці мережевого трафіку для виявлення такої ж атаки. Сигнатурні IDS є найбільш популярними в наш час і працюють подібно до антивірусного програмного забезпечення, тому і їх ефективність також залежить від регулярності оновлення баз сигнатур, як і в антивірусному програмному забезпеченні. Цей тип IDS практично не захищає від нових атак, так як він не може їх розпізнати до появи їх сигнатур.

IDS на основі стану. Кожна зміна в роботі системи (вхід користувача, запуск програми, взаємодія додатків, введення даних) призводить до зміни стану системи. При проведенні атак також відбуваються відповідні зміни станів (віддалений користувач підключається до системи, завантажуються данні, виконується код). IDS на основі стану відслідковує послідовність переходів стану і якщо ця послідовність буде не за встановленими правилами, то це свідчить про можливу атаку (наприклад багаторазова спроба ввести пароль до аккаунту, спроба отримання файлу по протоколу ftp, спроба підключення до закритого в даний момент порту...).

IDS на основі статистичних аномалій. Також називаються поведінковими або евристичними. Ці IDS на початку створюють профіль «нормальної» діяльності системи, коли відомо, що атак в мережі не спостерігалося і після цього весь наступний трафік і діяльність системи порівнюються з цим профілем. Наприклад, для кожного клієнта, сервера, протокола, дня тижня, часу доби вимірюється мінімальні, максимальні і середні значення параметрів PPS (пакетів в секунду). Цей тип IDS здійснює контроль шаблонів атак в контексті потоку дій, а не просто дивиться окремі пакети. Краще підходить для виявлення DDoS атак. Перевагою IDS на основі статистичних аномалій є їх можливість реагувати на нові типи атак. Недоліком – величезна кількість помилкових спрацювань, що пов’язано з постійними змінами в роботі мережі. Одним із нововведень для евристичних IDS є використання технології NetFlow.

Сигнатурна IDS повідомляє тип виявленої атаки, IDS на основі правил повідомляє, яке правило було порушено, а IDS на основі статистичних аномалій просто повідомляють про те, що сталося щось «ненормальне», що не відповідає профілю. Сучасні системи використовують кілька технологій одночасно.

Компоненти і архітектура IDS.

Хоча існують різні різновиди IDS, всі вони мають загальні компоненти: модуль стеження, аналізатор, сховище даних, систему реагування та керуючу консоль [3, 4].

У сучасних системах часто використовується множина сенсорів, розташованих у різних точках мережі, які збирають трафік або дані про дії користувачів і відправляють їх до аналізаторів, які шукають в них підозрілі дії. У разі виявлення аналізатором підозрілих дій, або підозрілої послідовності біт він відправляє відповідні повідомлення в підсистему реагування на подію. Керуюча консоль використовується для налаштування та управління системою загалом.

Модуль стеження забезпечує збір даних з журналу реєстрації або мережевого трафіку. Різні виробники дають цьому модулю наступні назви: сенсор (sensor), монітор (monitor), зонд (probe).

Сенсором може бути окремий комп'ютер, або це може бути програмний компонент маршрутизатора, головне, щоб його мережева карта працювала у не розбірливому режимі. В якому місці мережі краще розташувати сенсори. Якщо помістити пристрій перед брандмауером NIDS виявить найбільше нападів, але і число помилкових спрацьовувань буде велике, і адміністратор отримає масу непотрібних попереджень про небезпеку. Якщо розмістити після брандмауера, то можна пропустити атаку на маршрутизатор. Оптимальним є розмістити один сенсор перед МЕ для виявлення атак, а інший сенсор за фаєрволом для виявлення реальних вторгнень.

Сенсори слід також розміщувати в висококритичних областях і в DMZ. У середовищах з дуже великим обсягом трафіку слід розміщувати безліч сенсорів, щоб забезпечити впевненість, що всі пакети проаналізовані. Якщо внутрішня мережа побудована на комутаторах з VLAN, то сенсор повинен бути підключений до спеціального порту (span-port) на комунікаційному пристрої, на який автоматично копіюється весь трафік, що проходить через всі віртуальні канали, оскільки дані в комутованному середовищі передаються через незалежні віртуальні канали, а не транслюються, як в некомутованих середовищах.

SPAN (Switch Port Analyzer) або Mirror Port, Manage Port, Monitor Port, Analyzer Port - це порт, на який копіюється трафік з кількох портів комутатора.

Ааналізатор - основний модуль системи виявлення атак. Він здійснює аналіз інформації, одержуваної від сенсорів і працює на основі правил, складених адміністратором системи безпеки відповідно до політики безпеки. При виконанні умови одного з правил аналізатор виробляє повідомлення тривоги та передає його на керуючу консоль системи IDS. За результатами цього аналізу приймається рішення щодо варіантів реагування, збереження відомостей про атаку в сховище даних і інші операції, в залежності від передбачуваного функціоналу.

Сховище даних, в залежності від методів які використовуються в системі виявлення атак, може містити профілі користувачів і обчислювальної системи, сигнатури атак або шаблони, що характеризують несанкціоновану (підозрілу)

діяльність. Це сховище може поповнюватися виробником системи виявлення атак, користувачем системи або компанією, що здійснює підтримку цієї системи.

Підсистема реагування здійснює реагування на виявлені атаки та інші аномальні події. Атака не тільки повинна бути виявлена, але і необхідно правильно і своєчасно зреагувати на неї. В існуючих системах застосовується широкий спектр методів реагування, які можна розділити на три категорії:

• повідомлення;

• збереження;

• активне реагування.

Повідомлення. Найпростішим і широко поширеним методом повідомлення є відправлення адміністратору безпеки повідомлень про атаку на консоль управління. До категорії «повідомлення» відноситься також посилка керуючих послідовностей до інших систем, наприклад до систем мережевого управління або до МЕ.

До категорії «збереження» відносяться два варіанти реагування:

• реєстрація події в БД;

• відтворення атаки в реальному масштабі часу.

Перший варіант широко поширений і в інших системах захисту. Для реалізації другого варіанту буває необхідно «пропустити» атакуючого в мережу компанії і зафіксувати всі його дії. Це дозволяє адміністратору безпеки потім відтворювати в реальному масштабі часу (або із заданою швидкістю) всі дії, здійснені атакуючим, аналізувати «успішні» атаки і запобігати їх в подальшому, а також використовувати зібрані дані в процесі розгляду.

Активне реагування. До цієї категорії належать такі варіанти реагування:

• блокування роботи атакуючого;

• завершення сесії з атакуючим вузлом;

• управлінням мережевим обладнанням і засобами захисту.

Керуюча консоль призначена для управління різними компонентами системи виявлення атак.

Системи виявлення атак будуються на основі двох архітектур: «автономний агент» і «агент-менеджер». У першому випадку на кожен об'єкт захисту, встановлюються агенти системи, які не можуть обмінюватися інформацією між собою, а також не можуть управлятися централізовано з єдиної консолі. Цих недоліків позбавлена архітектура «агент-менеджер», або розподілена IDS. Для великих організацій, в яких філії рознесені по різних територіях і навіть містах, використання такої архітектури має принципове значення.

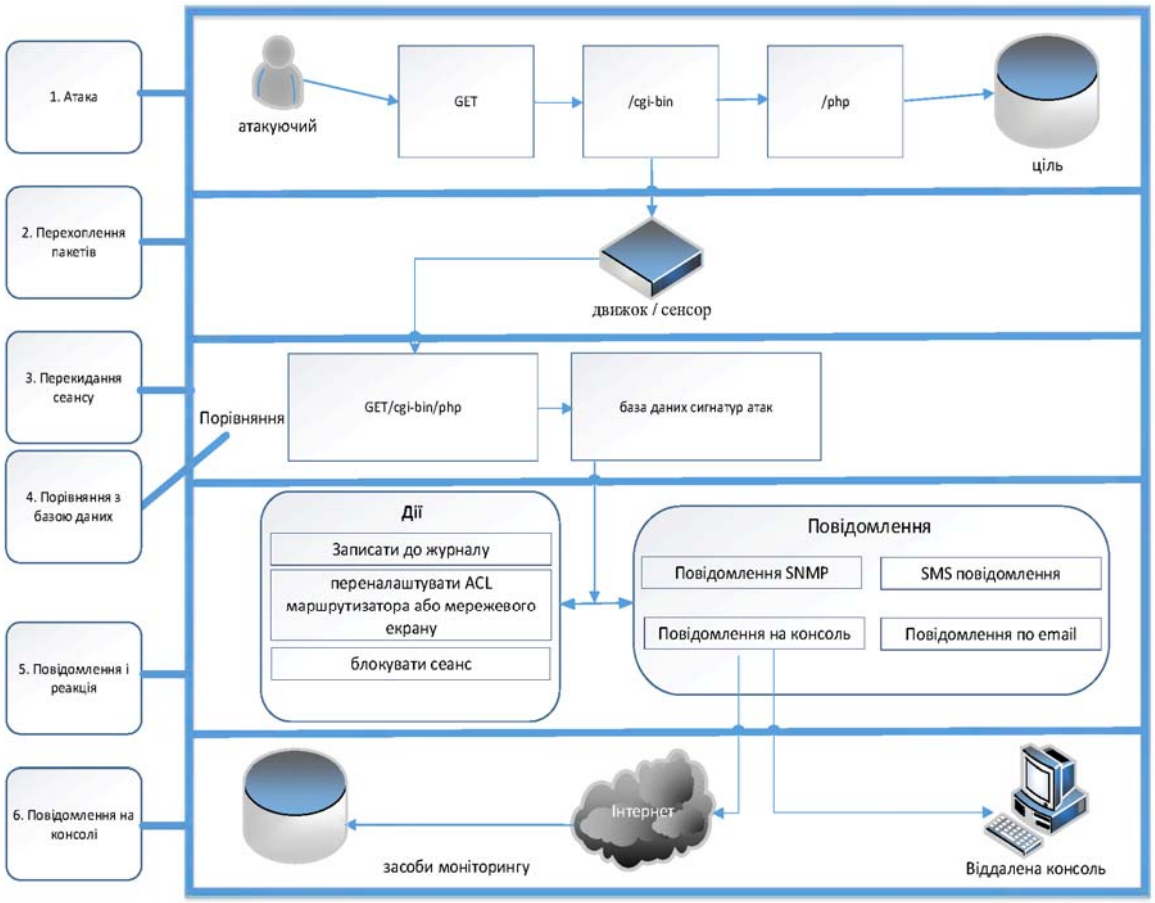


Рис. 1. Схема IDS.

Наведена на рисунку 1 схема IDS є функціональною, у реальній системі ці функції не обов'язково реалізуються в окремих блоках чи модулях системи. У мінімальному варіанті всі функції IDS можуть бути зосереджені в програмному забезпеченні єдиного комп'ютера, мережний адаптер якого виконує роль датчика за рахунок того, що приєднаний до *SPAN* порту комутатора або маршрутизатора.

Системи запобігання вторгнень.

Оскільки засоби IDS не здатні зупинити нелегальний доступ до активів компанії, а лише виявляють такі факти і відправляють повідомлення адміністратору, у компаній виникла потреба в нових продуктах і технологіях, що дозволяють вирішити цю проблему. В результаті з'явилися системи запобігання вторгнень (IPS – intrusion prevention system), метою яких є не тільки виявлення несанкціонованої діяльності, але і запобігання доступу зловмисника до ІТС. Системи IPS можна розглядати як розширення систем виявлення вторгнень, так як завдання відстеження атак залишається однаковим. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність у реальному часі й швидко реалізовувати дії по запобіганню атак. Можливі міри – блокування потоків трафіку в мережі, скидання з'єднань, видача сигналів операторові.

Таким чином, IPS є превентивною і проактивною технологією, зосередженою в першу чергу на запобігання атак, на відміну від IDS, що є детективною технологією, яка застосовується до вже здійснених фактів.

Як і в світі IDS, існують засоби IPS рівня хоста (HIPS) і рівня мережі (NIPS) (рисунок 2). Більшість мережевих IPS є лінійними (inline) пристроями, що включаються «в розрив» мережі і пропускають через себе і контролюють весь трафік.

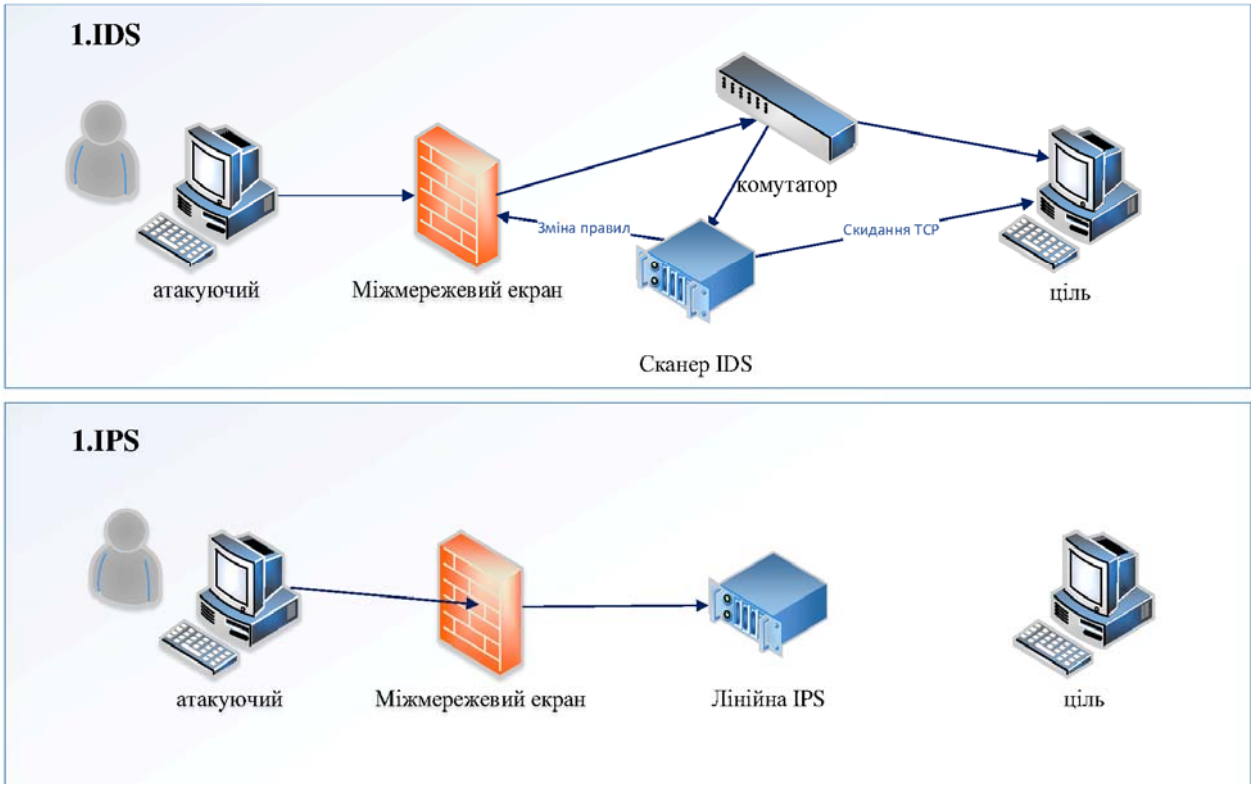


Рис. 2. Засоби IPS рівня хоста (HIPS) і рівня мережі (NIPS).

Як правило такі NIPS мають два мережевих інтерфейси – зовнішній і внутрішній. Трафік приходить на зовнішній інтерфейс, аналізується і, в разі визнання пакетів безпечними, вони направляються на внутрішній інтерфейс. Якщо пакети визнаються шкідливими, вони відбраковуються. Однак це може привести до появи «вузького місця» (пляшкового горлечка) і знизити продуктивність мережі. IPS для бездротових мереж (Wireless Intrusion Prevention Systems, WIPS): перевіряє активність у бездротових мережах. Зокрема, виявляє невірно зконфігуровані точки бездротового доступу до мережі, атаки людина посередині, спуфінг MAC-адреса.

Серед активних дій запобігання вторгнень слід виділити:

- *переривання з'єднань, сеансів або процесів*. Якщо процес використовує занадто багато системних ресурсів, найкраще завершити його. Якщо користувач намагається використовувати конкретну вразливість або здійснити нелегальний доступ до файлів, то рекомендується закрити сеанс цього користувача. Якщо зловмисник використовує мережеве з'єднання в спробах вивчення вразливостей системи, то варто закрити з'єднання;

- *переналаштування мережі*. Якщо відбувається кілька спроб доступу до комп'ютерів організації з конкретної IP-адреси, отже, є ймовірність того, що з цієї IP-адреси здійснена спроба атаки на інформаційну систему. У цьому випадку може знадобитися переналаштовування міжмережевого екрана або

маршрутизатора. Зміна налаштувань може бути тимчасовою або постійною, залежно від IP-адреси й запрограмованих логічних дій. Нові правила можуть заборонити установку будь-яких з'єднань із віддаленим вузлом або заборонити з'єднання лише по конкретних портах.

- *обманні дії.* Найбільш складним типом активної обробки подій є обманні дії. Відповідь обманом спрямована на введення зловмисника в оману за допомогою створення враження успішного й невиявленого проведення атаки. У той же час система-ціль захищається від атаки зловмисника або за допомогою його перенаправлення на іншу систему, або за допомогою переміщення життєво важливих компонентів системи в безпечне місце. Одним з типів обманних дій є Honeypot «горщик з медом». Під «горщиком з медом» мається на увазі об'єкт системи, які ззовні сприймаються як повноцінні машини з встановленими на них операційними системами, а відтак піддаються скануванню і виглядають для зловмисника настільки привабливим, що він не може їх пропустити (приманка). Такий комп'ютер повинен залучити зловмисника більше, ніж реальні системи в мережі. Хост-приманка не містить ніякої реальної інформації компанії, і немає ніяких ризиків в разі його успішного злому. Грамотно налаштований Honeypot практично неможливо розпізнати.

У той же час за атакуючим ведеться спостереження, і всі його дії фіксуються, з метою вивчення стратегії та методів сканування та визначення переліку засобів, необхідних для запобігання майбутнім атакам. Чим більше часу хакер залишається на цьому комп'ютері, тим більше інформації можна отримати про його методи.

Honeypot поставляються у вигляді програмних продуктів і окремих апаратних рішень (наприклад, Specter). Втім, Honeypot нескладно створити і самому, використавши для цього старий комп'ютер (або віртуальний комп'ютер). Зазвичай на нього поміщається максимальне число вразливих додатків і зовні привабливих ресурсів - і одночасно там же стоїть система виявлення вторгнень, яка фіксує всі дії хакерів. Для атакуючих з Інтернету зазвичай такі приманки поміщаються в DMZ, а у внутрішній мережі роль Honeypots зазвичай грають каталоги з привабливими назвами і налаштованим аудитом на файлових серверах.

При підготовці до атаки, хакери найчастіше насамперед визначають, чи становлений IDS в мережі, яку вони збираються атакувати. Якщо IDS встановлений, вони проводять DoS-атаку на нього, щоб порушити його роботу. Іншою тактикою є відправка IDS некоректних даних, які змусять IDS відправити повідомлення про початок атаки, хоча ніякої атаки насправді не буде. Це робиться для того, щоб домогтися відключення IDS фахівцями компанії через її «неправильну» роботу, або щоб відвернути увагу цих фахівців на аналіз некоректних пакетів, поки відбуватиметься реальна атака. Як протидія цьому може розглядатися використання хост-приманки (honeypot) (рисунки 3, 4).

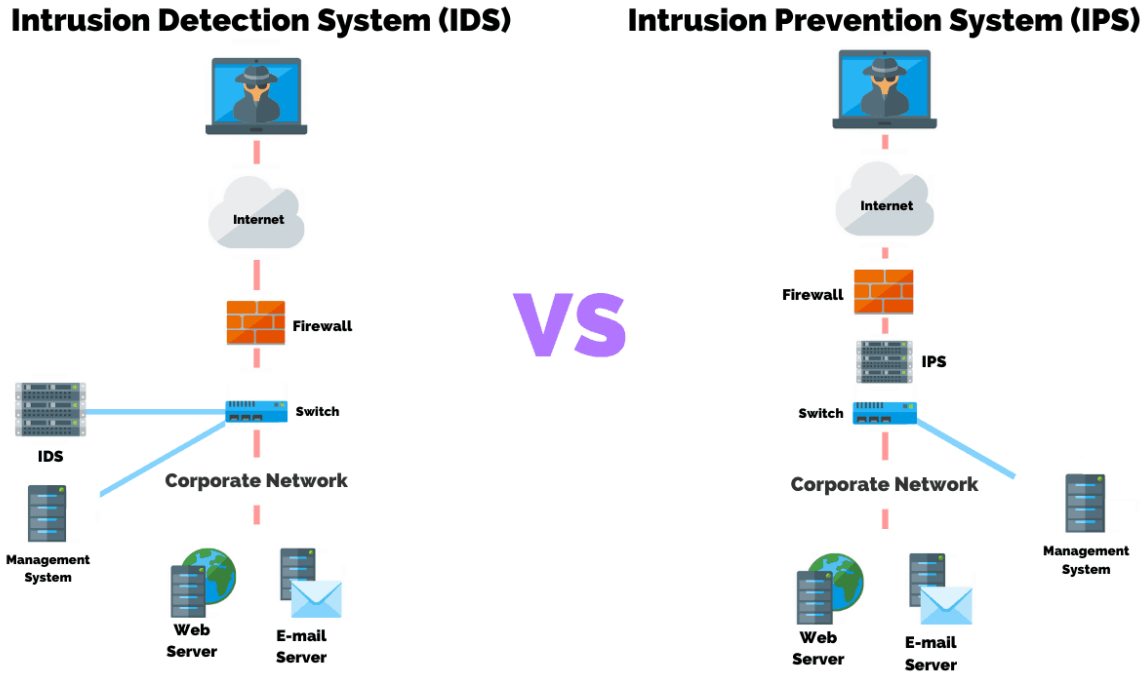


Рис. 3. Схема використання хост-приманки.

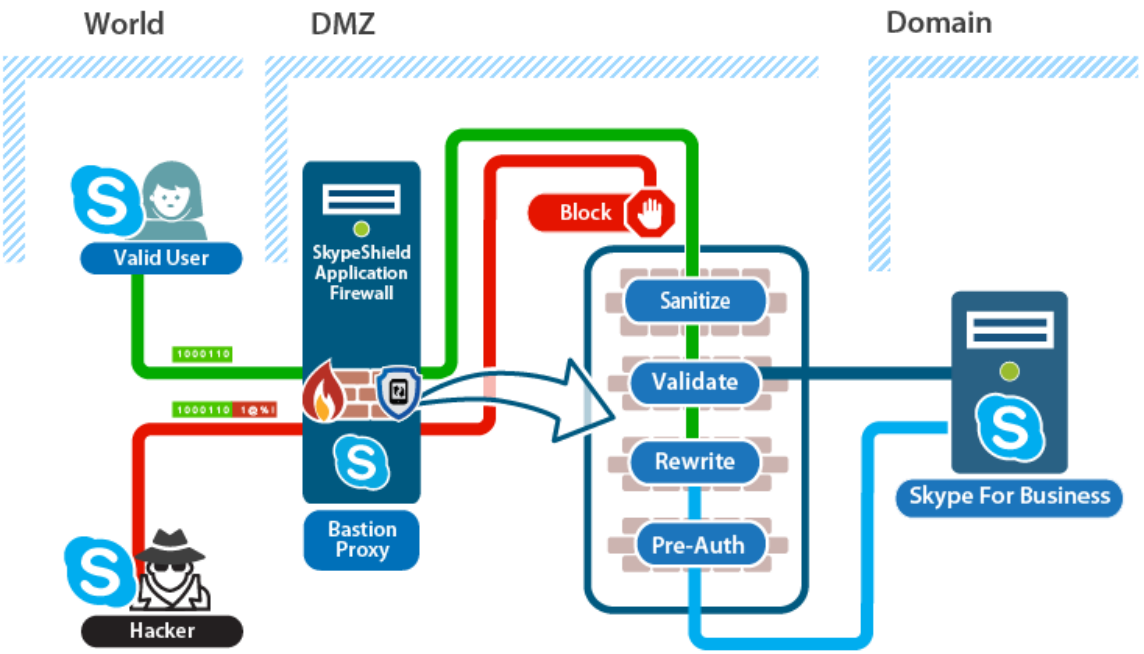


Рис. 4. Алгоритм використання хост-приманки.

Що стосується форм-фактора, IPS-системи можуть бути представлені як у вигляді окремого хардверного рішення, так і у вигляді віртуальної машини або софта.

Заміна реактивної природи IDS на превентивну створює деякі проблеми. Дійсно, після цієї зміни виникають два серйозні питання: потенційна можливість відмови в обслуговуванні і недостатній середній рівень доступності.

Відмова в обслуговуванні.

При запобіганні вторгненням головним механізмом обробки більше не являється повідомлення системи, мережі і системних адміністраторів. Тепер «ядром» системи є блокування спроби виконання дії. Коли IDS блокує атаку, вона запобігає виконанню дії, будь то системний виклик, операція додатка або мережеве з'єднання. Це блокування запобігає атаці. Очевидно, при цьому мається на увазі коректна ідентифікація системою IDS дії як атаки. Якщо дія, спроба якої була здійснена, насправді не була атакою, а IDS заблокувала його, то, можливо, IDS заблокувала законну дію, що виконується в інформаційному середовищі. Внаслідок цього IDS може викликати відмову в обслуговуванні. Якщо дія, що викликала проблему, була деякою аномалією (наприклад, пакет з помилками), то повторна передача пакету або повторна установка з'єднання, як правило, здійснюються успішно. Проте, якщо IDS некоректно ідентифікує легітимні дії або трафік, приймаючи їх за атаки, то, швидше за все, відмова в обслуговуванні відбуватиметься і надалі.

Висновки.

Сучасні виклики, пов'язані із зростанням зовнішніх втручань та збільшенням числа комп'ютерних інцидентів, спонукають до створення систем та пошуку оптимальних методів своєчасного виявлення атак та захисту комп'ютерних мереж. Постійно з'являються нові типи атак, що можуть проникнути через фаєрвол і досягти внутрішніх серверів мережі. Шляхом моніторингу мережевого трафіку і моніторингу подій, що відбуваються в комп'ютерній системі або мережі можна виявити сліди атак. Взагалі, реагування на підозрілу діяльність, спрямовану на обчислювальні або мережеві ресурси дає можливість виявлення атак. Моніторинг трафіку відбувається за допомогою програм-аналізаторів мережевих протоколів, а також маршрутизаторів, а моніторинг подій – за допомогою систем виявлення вторгнень IDS. Авторами розглянуті питання ефективності таких систем, яка, в першу чергу, залежить від застосовуваних ними методів аналізу отриманої інформації. Окрім статистичного аналізу проведено огляд нових методів, від експертних до використання нейронних мереж. Також надано класифікацію, проведено огляд компонент і архітектури систем IDS. У статті наведено різні типи і тактики хакерських атак та запропоновано відповідні технології протидії та захисту комп'ютерних систем і мереж. Оскільки засоби IDS лише виявляють, а не запобігають нелегальному доступу до активів компанії, виникла нагальна потреба в нових продуктах і технологіях. Авторами представлені не тільки методи і засоби виявлення несанкціонованої діяльності, але і запобігання доступу зловмисника до ІТС з використанням систем запобігання вторгненням (IPS). Проведене дослідження технологій виявлення комп'ютерних атак та методів їх аналізу із врахуванням архітектури систем IDS дозволило авторам запропонувати підходи до захисту комп'ютерної мережі на базі систем виявлення вторгнень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Горбенко І., Семенко Є., Замула О. Methods and means of synthesis and génération of signais - physical carriers of data in modern information and communication systems // Radiotekhnika, 3(202). 2020. С. 87-98. DOI: https://doi.org/10.30837/rt.2020.3.202.09.

2. Горбенко І. Д., Замула О. А., Хо Чі Ли Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп'ютерне моделювання. Серія: Технічні науки: зб. наук. праць / Інститут кібернетики імені В.М. Глушкова НАНУ. 2019. Вип. 19. 160 с.

3. Письмак Д. О., Клименко С. В., Малайко В.П. Перешкодостійке кодування повідомлення електронного підпису // Актуальні проблеми інформаційних технологій автоматизації. Дніпро: ДНУ. - Зб. наук.праць. Том 21. 2017. С. 123-131.

4. Петренко О. М., Клименко С. В., Поляков Г. О. Клієнт-серверна система для безпечного обміну приватними повідомленнями із застосуванням криптографії з відкритим ключем// Будівництво, матеріаловедення, машинобудівництво. Серія: Комп'ютерні системи та інформаційні технології в освіті, науці та управлінні. Зб. наук. пр. Вип. №101. Дніпро: ДВНЗ ПДАБА., 2017. С. 177-182.

УДК 004.056.53

АНАЛІЗ ПРОТОКОЛУ ДЛЯ ПОБУДОВИ ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ПРИКЛАДІ IPSEC

Ніколаєвський О.Ю.
к.т.н., доцент кафедри інформаційних систем,
програмування та кібербезпеки
ПВНЗ «Європейський університет»
alexander.nikolaievskyi@e-u.edu.ua

Левченко С.В.
старший викладач кафедри інформаційних систем,
програмування та кібербезпеки
ПВНЗ «Європейський університет»
sergiy.levchenko@e-u.edu.ua

Невзоров А.В.
к.т.н., доцент,
доцент кафедри математичних дисциплін
та інноваційного проектування
ПВНЗ «Європейський університет»
andrey.nevzorov@e-u.edu.ua

Скляренко О.А.
аспірант,
ПВНЗ «Європейський університет»
osklyarenko@e-u.edu.ua

Анотація. Формування захищених віртуальних каналів на мережевому рівні моделі OSI дає оптимальне співвідношення між прозорістю та якістю захисту. Для цього призначений IPsec (Internet Protocol Security) – набір протоколів для безпечної передачі даних IP мереж, який є доповненням до протоколу IP ver.4 та складовою IP ver.6. Стек протоколів IPSec використовується для автентифікації учасників обміну, тунелювання трафіку та шифрування IP-пакетів. У даній статті проведено огляд та аналіз протоколів, алгоритмів, стандартів, режимів і типів перетворень, які використовуються для організації IPSec. Результати проведеного дослідження можуть бути використані для побудови спеціалізованої захищеної комп'ютерної мережі на прикладі IPsec.

Вступ.

Постановка задачі. Провести аналіз протоколів, алгоритмів, стандартів, режимів і типів перетворень, які використовуються для організації IPSec з метою подальшого використання цієї інформації для успішної побудови спеціалізованої захищеної мережі.

Розглянемо детально набір протоколів для безпечної мережевої взаємодії на прикладі *IPsec (Internet Protocol Security)*.

Стек протоколів IPSec гарантує:

- цілісність даних, що передаються, тобто дані при передачі не спотворені, не втрачені і не продубльовані;
- автентичність відправника, тобто дані передані саме тим відправником, який довів, що він той, за кого себе видає;
- конфіденційність даних, що передаються, тобто дані передаються у формі, що запобігає їх несанкціонованому перегляду.

Для захисту трафіку в IPSec визначені наступні протоколи:

1. протокол аутентифікуючого заголовка – AH (Authentication Header), що забезпечує перевірку цілісності та аутентифікацію переданих даних;
2. протокол інкапсулюючого захисту даних – ESP (Encapsulating Security Payload) – забезпечує конфіденційність даних завдяки шифруванню алгоритмом DES, і додатково, може забезпечувати перевірку цілісності та аутентифікацію.
3. протокол обміну ключами IKE (Internet Key Exchange) – для передачі кінцевим точкам захищеного каналу ключів шифрування і узгодження параметрів віртуального каналу.

Кожен із цих протоколів може використовуватися як самостійно, так і одночасно з іншим, так що в тих випадках, коли шифрування через чинні обмеження застосовувати не можна, систему використовують тільки з протоколом AH.

Звичайно, подібний захист даних у багатьох випадках виявляється недостатнім. Сторона, що приймає, отримує лише можливість перевірити, що дані були надіслані саме тим вузлом, від якого вони очікуються, і дійшли в тому вигляді, в якому були відправлені. Однак від несанкціонованого перегляду даних на шляху їх проходження через мережу протокол AH захистити не може, тому що не шифрує їх. Для шифрування даних найбільш доцільно використовувати протокол ESP. У даній роботі наведено докази цього твердження на підставі аналізу ефективності використання наведених протоколів.

Протоколи AH і ESP.

Протокол AH використовується для автентифікації відправника інформації, для забезпечення цілісності даних і опціонально може використовуватися для захисту від повторної передачі даних. Цілісність та автентичність даних забезпечуються додаванням автентифікуючого заголовка *AH* в пакет даних між заголовком *IP* та заголовком транспортного рівня *TCP/UDP*. В цьому заголовку розміщується MAC-код (імітовставка, код перевірки цілісності IP-пакету даних ICV - Integrity Check Value), який обчислюється за алгоритмами HMAC-MD5 або HMAC-SHA-1. Значення MAC-коду шифрується симетричним алгоритмом. Ключ шифрування є таємним і погоджується між сторонами до обміну даними, що і забезпечує автентифікацію відправника (дані направив тільки той, хто знає ключ шифрування) [1, 2].

Одержувач, знаючи, яка одностороння функція шифрування була використана для складання хеш-коду, наново обчислює його, використовуючи дані з прийнятого пакету і той же секретний ключ шифрування, що і відправник. Якщо значення отриманого та обчисленого хеш-коду збігаються, це означає, що вміст пакета під час передачі не було змінено.

Якщо для отримання хеш-коду застосовується одностороння функція з параметром (якою є секретний ключ), відомим тільки відправнику та одержувачу, будь-яка модифікація повідомлення буде негайно виявлена. Протокол AH дозволяє приймальній стороні переконатися в наступному:

- пакет був відправлений саме тією стороною, з якою встановлено зв'язок;
- вміст пакета не зазнав спотворень у процесі передачі його по мережі;
- пакет не є дублікатом якогось пакета, отриманого раніше.

Однак протокол AH не забезпечує конфіденційності даних, що передаються, тобто він не призначений для їх шифрування. Дані можуть бути прочитані проміжними вузлами, але не можуть бути змінені.

Якщо протокол AH забезпечує захист від загроз цілісності даних, то протокол ESP також може забезпечувати і конфіденційність даних шляхом шифрування вмісту пакетів. Цілісність та автентичність даних забезпечуються так як і в протоколі AH на основі обчислення HMAC кодів. У протоколі ESP функції автентифікації та криптографічного закриття можуть бути задіяні або разом або окремо один від одного.

Протоколи ESP і AH мають схожу функціональність для забезпечення автентифікації даних, але є відмінність, яка полягає в тому, що протокол AH забезпечує автентифікацію всього пакета (і IP-заголовка, і самих даних), тоді як протокол ESP автентифікує лише дані з пакета.

У зв'язку з цим слід мати на увазі, що протокол AH не можна застосовувати в середовищі, де використовується механізм трансляції мережевих адрес NAT (Network Address Translation), так як заміна адреси призведе до розбіжності хешів під час перевірки цілісності пакетів. При використанні протоколу ESP з'являється можливість використання механізму трансляції мережевих адрес NAT, оскільки в цьому випадку адреси в заголовках IP-пакетів можна модифікувати.

Програмне забезпечення перелічених протоколів може функціонувати на виділених серверах, або комп'ютерах кінцевих користувачів. Однак найчастіше його встановлюють на маршрутизаторах або спеціальних пристроях, які в архітектурі IPSec називають шлюзами безпеки SG (Security Gateway).
Відповідно є три схеми застосування протоколу IPSec:

- хост-хост;
- шлюз-шлюз;
- хост-шлюз.

У схемі хост-хост захищений канал, встановлюється між двома кінцевими вузлами мережі. Тоді IPSec працює на кінцевих вузлах і захищає дані, що передаються від хоста 1 до хосту 2.

Відповідно до схеми шлюз-шлюз захищений канал встановлюється між двома проміжними вузлами, так званими шлюзами безпеки SG, на кожному з яких працює протокол IPSec. В такій схемі захищений обмін даними може відбуватися між будь-якими двома кінцевими вузлами, підключеними до мереж, що розташовані за шлюзами безпеки. Від кінцевих вузлів підтримка протоколу IPSec не потрібна, вони передають свій трафік у незахищеному вигляді через внутрішні мережі підприємств. Трафік, що направляється в загальнодоступну

мережу, проходить через шлюз безпеки, який і забезпечує його захист за допомогою протоколу IPSec.

Схема хост-шлюз часто застосовується при віддаленому доступі користувачів до локальних мереж підприємства. І тут захищений канал прокладається між віддаленим хостом, у якому працює протокол IPSec, та шлюзом, що захищає трафік для всіх хостів, що входять у внутрішню мережу підприємства [3, 4].

Режими роботи протоколів IPSec.

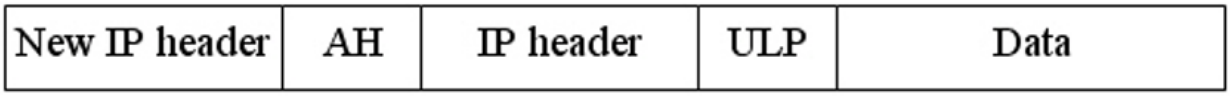
Обидва протоколи AH і ESP мають два режими роботи – *транспортний* та *тунельний*.

У *транспортному режимі* для протоколу AH заголовок вихідного IP-пакета залишається на своєму місці, але у ньому змінюється поле *Next Header* і з'являється заголовок протоколу AH, в якому і передається хеш-код для автентифікації даних.

Пакет протоколу ESP у транспортному режимі виглядає наступним чином:

Штрихуванням виділено фрагменти пакета, які захищаються за допомогою шифрування. Шифрується лише інформативна частина IP-пакета. Маршрутизація не зачіпається, тому що заголовок IP пакета не змінюється (не шифрується). Транспортний режим, як правило, використовується для встановлення з'єднання між хостами.

Тунельний режим використовується, якщо хоча б один із вузлів є шлюзом безпеки (маршрутизатор). Для протоколу AH пакет поміщається в інший пакет з новим IP-заголовком.



Протокол автентифікації AH створює своєрідний конверт із новим IP-заголовком. При цьому внутрішній (первинний) IP-заголовок містить цільову адресу пакета, а зовнішній IP-заголовок - адресу кінця тунелю. Для протоколу ESP пакет ще і шифрується цілком, утворюючи захищений IP-тунель.

Тунельний режим може використовуватися для безпечної передачі даних через відкриту мережу між різними сегментами приватної мережі, завдяки шлюзам безпеки.

Режим тунелюваня AH захищає весь вихідний IP-пакет за рахунок додаткового зовнішнього заголовка IP, який у режимі транспорту AH не використовується:

Розглянуті режими IPsec не є взаємовиключними. На одному й тому ж вузлі можна використовувати обидва режими.

Протокол Internet Key Exchange (IKE).

IPsec також містить у собі протокол Internet Key Exchange (IKE) для узгодження параметрів віртуального каналу та управління ключами. Протокол IKE вирішує три завдання:

- здійснює автентифікацію взаємодіючих сторін;
- погоджує алгоритми шифрування та характеристики ключів, які будуть використовуватись у захищеному сеансі обміну інформацією;
- забезпечує створення ключової інформації для з'єднання;
- керує параметрами з'єднання.

По протоколу IKE спочатку між двома точками встановлюється логічне з'єднання, яке в стандартах IPSec отримало назву безпечна асоціація SA (Security Association). Мета SA – забезпечити автентифікацію кожного кінцевого вузла (цей процес називається взаємною автентифікацією кінцевих вузлів), тому що заходи безпеки втрачають будь-який сенс, якщо дані передаються або приймаються невідомими користувачами [5].

Для виконання автентифікації сторін у IKE застосовуються або спосіб, заснований на використанні загального секрету, або спосіб, заснований на використанні цифрових сертифікатів стандарту X.509 і інфраструктури PKI.

Після проведення взаємної автентифікації сторони, що взаємодіють, можуть безпосередньо перейти до узгодження параметрів захищеного каналу. Параметри безпечної асоціації SA визначають тип протоколу, що використовується для забезпечення безпеки передачі даних; алгоритм автентифікації протоколу AH та його ключі; алгоритм шифрування, що використовується протоколом ESP, та його ключі; режим роботи протоколів; дані, необхідні кожному кінцевому вузлу, щоб локально генерувати спільні секретні ключі та ряд інших параметрів [6].

Параметри безпечної асоціації SA повинні влаштовувати обидві кінцеві точки захищеного каналу, тому при двосторонньому обміні даними необхідно встановити одну асоціацію SA для вхідних пакетів даних, а другу – для вихідних на кожному кінці тунелю.

Потім в рамках встановленої безпечної асоціації SA починає працювати протокол AH або ESP, за допомогою якого і виконується необхідний захист даних, що передаються з використанням вибраних параметрів. Для однієї асоціації SA може працювати лише один із протоколів захисту даних – або AH, або ESP, але не обидва разом.

Архітектура IPSec є відкритою, що дозволяє використовувати для захисту даних нові криптографічні алгоритми і протоколи, наприклад відповідні національним стандартам.

Висновки.

У даній статті розглянуті протоколи, алгоритми, стандарти, режими і типи перетворень, які використовуються для організації IPSec. Цією інформацією необхідно володіти для успішної побудови спеціалізованої захищеної мережі. Авторами статті на прикладі протоколу IPSec показано підхід до організації та побудови безпечної мережевої взаємодії. Налаштування шифрування може виявитися досить складним завданням. Його рішення повинне починатися з

визначення політики захисту IPSec, заснованого на вимогах загальної політики захисту організації.

Двома головними протоколами IPSec є AH, який забезпечує цілісність і автентифікацію даних (але не конфіденційність), і ESP, що забезпечує всі можливості AH, а також конфіденційність даних за допомогою шифрування.

Для автентифікації сторін IPSec і спрощення процесу створення секретних ключів, використовуваних алгоритмами шифрування IPSec, застосовується протокол IKE.

Параметри IPSec і секретні ключі, використовувані в сеансах IPSec, визначають асоціації захисту IPSec, які є однобічними. Параметри асоціацій захисту IPSec зберігаються в динамічній пам'яті в базі даних асоціацій захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лукацький А. Невідома VPN / Комп'ютер Пресс.-М.: № 10, 2016; http://abn.ru/inf/comdivss/network4.shtml

2. Норманн Р. Вибираємо протокол VPN / Windows IT Pro. - М.: № 7, 200; http://www.osp.ru/win2000/2011/07/010.htm

3. Петренко С. Захищена віртуальна приватна мережа: сучасний погляд на захист конфіденційних даних / Світ Internet. - М.: № 2, 2017.

4. Файльнер М. Віртуальні приватні мережі нового покоління LAN / Журнал мережевих рішень, - М.: № 11, 2015; http://www.osp.ru/lan/2015/11/030.htm

5. Фратто М. Секрети віртуальних приватних мереж. Мережі і системи зв'язку, № 3, 2008.

6. Штайнке С. VPN між локальними мережами. LAN / Журнал мережевих рішень, - К.: № 10,2018;

УДК 004.78

ДОКАЗ МОЖЛИВОСТІ ПОВНОЦІННОГО АУДИТУ СИСТЕМ ТАЄМНОГО ІНТЕРНЕТ ГОЛОСУВАННЯ

Хлапонін Ю.І.
завідуючий кафедрою кібербезпеки та
комп'ютерної інженерії
Київський національний університет
будівництва і архітектури
y.khlaponin@gmail.com

Вишняков В.М.
доцент кафедри кібербезпеки та
комп'ютерної інженерії
Київський національний університет
будівництва і архітектури
volodymyr.vyshniakov@gmail.com

Пригара М.П.
доцент кафедри технології машинобудування
ДВНЗ «Ужгородський національний університет»

Шпак О.І.
викладач кафедри програмного забезпечення систем
ДВНЗ «Ужгородський національний університет»

Анотація. Метою даного дослідження є довести можливість побудови системи таємного Інтернет голосування, в якій повноцінний аудит доступний для всіх виборців та їх довірених осіб. Під повноцінним слід розуміти такий аудит, при якому перевіряється все, що може викликати сумнів. На базі відкритого блоку серверів створено натурну модель системи для проведення експериментального голосування та розроблено детальну методику повноцінного аудиту. Експеримент може проводити будь-хто в будь-який момент за посиланням в Інтернеті. Таким чином, показано, що не лише при традиційних технологіях таємного голосування можливий повноцінний аудит, завдяки якому у виборців немає сумнівів щодо збереження таємниці свого голосування та чесності результатів. Для проведення повноцінного аудиту за описаною методикою не потрібно залучати висококваліфікованих спеціалістів, а цілком достатньо сучасної шкільної освіти, яка є обов’язковою у багатьох країнах.

1. Вступ.

Інтернет технології неухильно проникають і поглиблюються в процеси нашої діяльності. Проте на виборах представників влади, де вирішується доля багатьох громадян і цілих держав, впровадження нових технологій є

проблематичним. У країнах з розвиненою демократією, завдяки наявності аудиту, немає фальсифікацій на виборах, і вони не хочуть втрачати це досягнення при переході на нові технології. У рекомендаціях Ради ЄС щодо стандартів електронного голосування, прийнятих 14 червня 2017 року, у пункті 39 написано: «Система електронного голосування повинна підлягати аудиту. Система аудиту повинна бути відкритою та всеохоплюючою та активно повідомляти про потенційні проблеми та загрози». Якими б не були програмно-технічні засоби електронного голосування, але якщо для виборців вони являють собою «чорну скриньку», то усунути підозри у шахрайстві неможливо. Насправді, немає іншого способу забезпечити довіру виборців, як надати їм можливість провести повноцінний аудит. Під повноцінним аудитом слід розуміти такий, при якому перевіряється все, що може викликати сумніви. Мета дослідження – довести можливість побудови системи таємного Інтернет голосування, в якій повноцінний аудит доступний для всіх виборців та їх довірених осіб.

2. Постановка проблеми та задачі дослідження.

У роботі [1] висловлюється протест щодо он-лайн виборів представників влади через те, що аудит, який зазвичай проводять самі виборці, стає неможливим. Вказується, що в цьому випадку фахівці зможуть легко змінити результати голосування. У роботах з удосконалення систем Інтернет голосування можна виділити два напрями досліджень. Перший – це доробка естонської системи, яка не використовує технологію Blockchain, а другий – системи, що засновані на технології Blockchain. У роботі [2] були проаналізовані атаки на естонську систему, де було виявлено, що зловмисник може повторно голосувати за допомогою підробленого програмного забезпечення, і запропоновано більш безпечний протокол голосування. У роботі [3] для зміцнення довіри виборців пропонується проводити перевірку кіберризиків обізнаними користувачами. Однак питання аудиту апаратного та програмного забезпечення самими виборцями, для яких естонська система є «чорною скринькою», не зачіпаються. Для забезпечення довіри до систем голосування запропоновано та запатентовано використання технології Blockchain [4]. Дослідження в цьому напрямку тривають, що відображено в роботах [5–8], де вносяться пропозиції щодо покращення безпеки та анонімності виборців, а також протидії нечесності з боку кандидатів. Однак важко уявити собі широкодоступний аудит в системах за технологією Blockchain, оскільки ця технологія зрозуміла лише обмеженому колу фахівців. Таким чином, існує пробіл у дослідженнях Інтернет голосування з точки зору забезпечення широкодоступного аудиту виборцями. Зазначимо, що такий аудит є обов’язковим відповідно до пункту 39 рекомендацій Ради ЄС щодо стандартів електронного голосування [9]. Це дозволяє стверджувати, що доказ можливості побудови системи Інтернет голосування, в якій повноцінний аудит доступний

для всіх виборців, є доцільним. Для досягнення цієї мети необхідно було вирішити наступні завдання:

- визначити блоки та процедури в системі голосування, які можуть викликати недовіру виборців;
- обрати принципи побудови системи таємного Інтернет голосування, де було б передбачена можливість проведення аудиту виборцями;
– розробити методологію для повноцінного аудиту системи голосування;
– виконати натурне моделювання системи таємного Інтернет голосування з аудитом за розробленою методикою.

3. Методи та засоби дослідження.

Для вирішення поставлених завдань використано теорію комп'ютерних мереж та криптографію. Також методом дослідження було натурне моделювання систем електронного голосування за використанням інструментів аудиту. Важливу роль у порівняльній апробації різних варіантів моделей та виборі найбільш вдалих технічних рішень відіграли студенти та викладачі трьох вищих навчальних закладів Києва. Провідну роль зайняв Київський національний університет будівництва та архітектури. Активну участь у дослідженні взяли студенти та викладачі Національного авіаційного університету та Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», а також співробітники НДІ автоматизованих систем у будівництві, які надали технічне забезпечення для досліджень та доступ до Інтернету.

4. Результати дослідження.

4.1. Визначення блоків і процедур, які можуть викликати недовіру виборців.

Побоювання виборців щодо порушення їхніх законних прав можуть бути пов'язані лише з двома такими випадками:

- розкриття таємниці голосу;
- фальсифікація підрахунку голосів.

Передача інформації під час Інтернет голосування здійснюється через канали загального доступу, де слід не довіряти всім блокам, які беруть участь у процесі передачі. За відсутності засобів захисту каналів зв'язку зловмисники можуть як розкривати голоси, так і підробляти дані, утворюючи атаку посередника (*MITM – Man in the middle*). Може проявлятися недовіра до серверного блоку, який приймає та підраховує голоси виборців, оскільки існує загроза зловмисного втручання обслуговуючого персоналу в роботу цього блоку. Також недовіру може викликати процедура відображення результатів підрахунку голосів. Крім перерахованих об'єктів, недовіру може викликати реєстр виборців, куди можна внести зайвих людей, замість яких голосуватимуть порушники. Як зазначено в [10], це легко визначити, опублікувавши дані про кількість виборців для кожної вулиці в межах виборчої дільниці, для кожного

будинку в межах вулиці та для кожної квартири в будинку. Тоді самі виборці знайдуть зайвих мешканців у своїх квартирах, зайві квартири у своїх будинках і зайві будинки на своїх вулицях без використання технічних засобів. При відкритому оприлюдненні результатів по кожній виборчій дільниці неможливо сфальсифікувати загальні результати голосування, оскільки будь-яку неточність легко виявити. Таким чином, визначено повний перелік блоків і процедур, які можуть викликати недовіру виборців під час Інтернет голосування.

4.2. Вибір принципів побудови системи голосування з можливістю проведення аудиту самими виборцями.

Для того, щоб повноцінний аудит могли провести самі виборці, усі технічні рішення системи голосування мають бути зрозумілими. Апаратне та програмне забезпечення, яке отримує та реєструє голоси, має бути відкрите для перевірки. Необхідно надати можливість громадянам залучати до перевірок своїх довірених спеціалістів. Важлива роль для демонстрації бездоганної роботи сервера голосування належить серверу аудиту, який виявляє та документує перешкоди в роботі сервера голосування. Схема підключення засобів для повноцінного аудиту системи голосування в Інтернеті з роботи [10], наведена на рисунку 1.

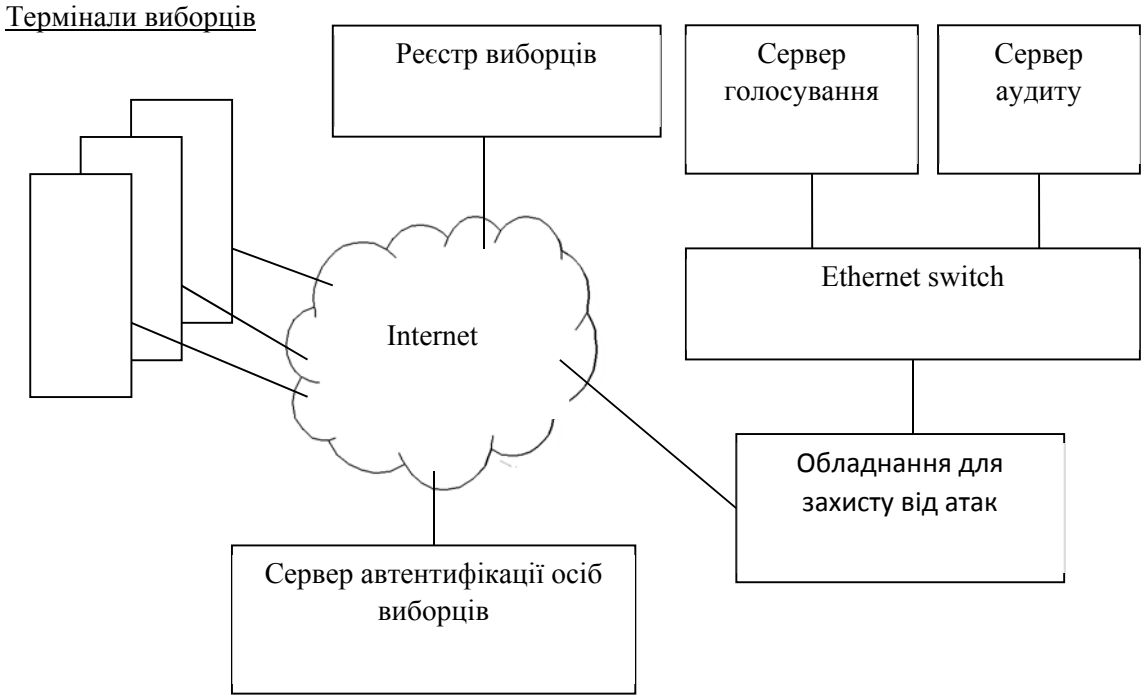


Рис. 1. Структурна схема системи Інтернет голосування.

У цій схемі сервери голосування та аудиту розміщено в одній мережі, що забезпечує надійність та швидкість проведення процедур аудиту. Виборці повинні переконатися, що їхні сеанси зв’язку з сервером голосування захищені від витоку та спотворення інформації. Для цієї мети можна використовувати технологію наскрізного шифрування, описану в [11]. Невелика кількість

інформації, яку виборець надсилає на сервер голосування (близько 60 байт), дозволяє використовувати шифр Вернама. Цей шифр надзвичайно простий для розуміння і для програмної реалізації, а його абсолютна безпечність математично доведена в роботі [12]. У таблиці 1 описані умови, які повинні бути виконані для абсолютного захисту переданих даних.

Таблиця 1.

Умови забезпечення абсолютного захисту даних під час передачі

Умова	Виконання умови
Отримання випадкових бітових послідовностей	Використовується метод отримання випадкових бітів, описаний у [13], який може бути застосовний на будь-якому комп’ютері.
Кожну випадкову послідовність можна використовувати один раз	Для кожного сеансу зв’язку їх випадкові бітові послідовності генеруються незалежно один від одного
Для передачі випадкових бітових послідовностей слід використовувати абсолютно безпечний канал зв'язку	Обмін випадковими бітовими послідовностями (ключами) відбувається за алгоритмом Діффі-Хеллмана [14] з такими параметрами, для яких у сучасних умовах немає можливості розкриття даних

Оскільки обмін ключами здійснюється за алгоритмом Діффі-Хеллмана, то при підключенні виборця до сервера слід переконатися, що немає атаки посередника. На прикладі сервера експериментальної виборчої дільниці далі розглянемо дії виборця щодо виявлення такої атаки. Через пристрій доступу до мережі Інтернет виборець завантажує веб-сторінку за посиланням http://91.198.50.8:29901/VD999901.html, вигляд якої наведено на рисунку 2. Верхній ряд кнопок потрібен виборцю як для голосування, так і для перевірки. Решта кнопок потрібні для перемикання режимів експерименту, що може відбуватися автоматично у встановлені моменти часу під час проведення голосування.

Рис. 2. Вигляд веб-сторінки виборчої дільниці.

Для проведення аудиту виборцю необхідно натиснути кнопку «Аудит сервера». При цьому веб-сторінка сервера аудиту відкриється в новому вікні, вигляд якого показано на рисунку 3.

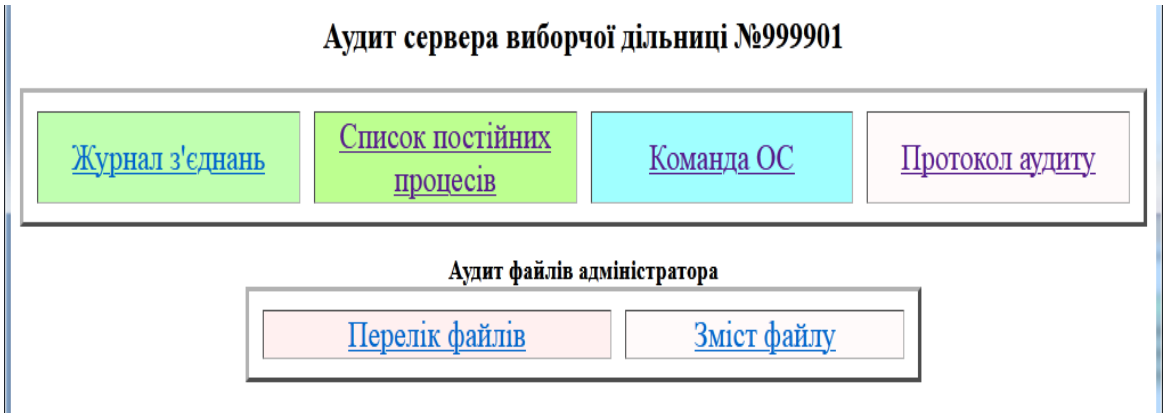


Рис. 3. Вигляд веб-сторінки сервера аудиту.

В одному вікні виборець може вести діалог із сервером голосування, а в іншому – контролювати роботу цього сервера. Коли виборець звертається до сервера, обмін кодовими словами відбувається за алгоритмом Діффі-Геллмана. Кожному такому з’єднанню присвоюється код, який є першими чотирма байтами кодового слова, надісланого виборцю сервером. Цей код (Код з'єднання) показано на рисунку 4 у діалоговому вікні виборця.

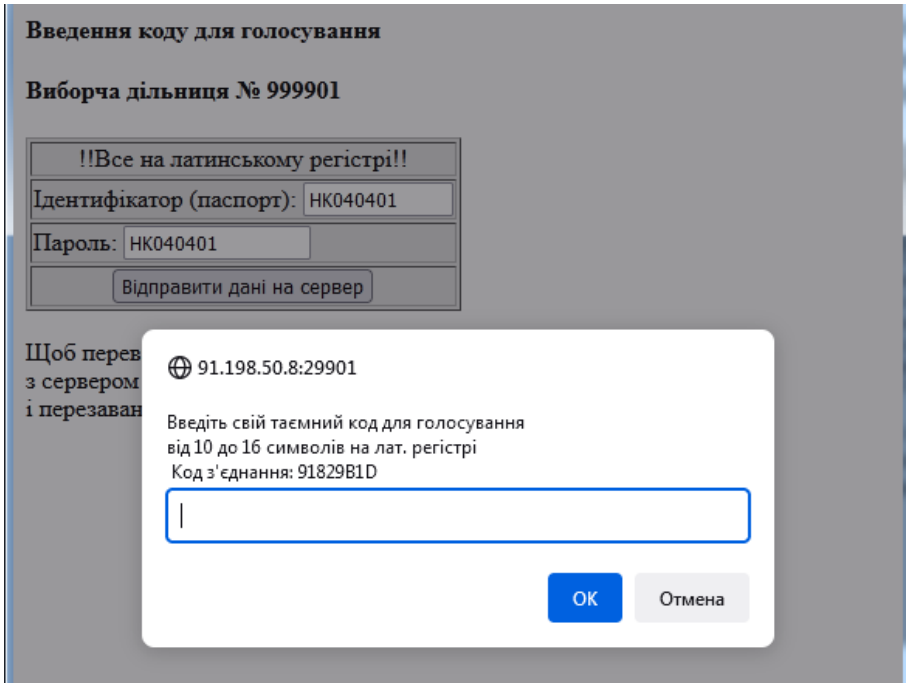


Рис. 4. Діалогове вікно з кодом з'єднання.

Для того, щоб переконатися у відсутності атаки посередника, виборцю достатньо у вікні аудиту, натиснувши клавішу «Журнал з'єднань», порівняти отриманий код (у цьому прикладі: 91829B1D) для порівняння з тим, що вказано в рядку журналу після дати та часу встановлення з'єднання з сервером. Фрагмент журналу з'єднань показано на рисунку 5.

```
 cat /home/admin/CC999901.TXT

23.02.2022  22:27:19  91829B1D

a66$ exit
```

Рис. 5. Фрагмент журналу з'єднань виборців з сервером (у вікні аудиту).

Якщо коди в обох вікнах збігаються, виборець переконується, що його конфіденційні дані дійсно передаються на штатний сервер і не можуть бути дешифровані під час передачі. Оскільки задачі шифрування та підрахунку голосів не є складним, то обидва модулі програми JavaScript (клієнтський і серверний) легко перевіряються на коректність. Виборець може порівняти текст програми, що використовується, з тим, що опубліковано на сайті. Таке порівняння за допомогою стандартних інструментів займає кілька хвилин. Далі слід переконатися, що обробка даних сервером голосування не зазнала жодного позаштатного втручання. Завдяки відкритому блоку серверів, що показаний на рисунку 6, і вибору відомих апаратних і програмних засобів, такі підозри легко усуваються.

Рис. 6. Зовнішній вигляд відкритого блоку серверів.

У роботі [15] в якості апаратного забезпечення сервера голосування пропонується використовувати відомий міні-комп'ютер, наприклад Raspberry Pi 3 Model B. Цей комп'ютер має високу надійність, малу вартість, низьке енергоспоживання та підходить для відкритого монтажу. Він має характерний зовнішній вигляд, що дозволяє візуально визначити всі його складові елементи. За продуктивністю він цілком підходить для сервера підрахунку голосів у масштабі виборчої дільниці. В якості операційної системи було обрано OpenBSD мінімальної конфігурації. Такий вибір обумовлений високими вимогами до захисту даних, що покладено за основу розробки цієї системи, а також вона є повністю відкритою для будь-яких перевірок. У таблиці 2 зведені всі можливі види підозр щодо обробки даних сервером та способи їх усунення.

Таблиця 2.

Усунення підозр щодо порушення нормальної роботи сервера

Можлива підозра	**Усунення підозри**
1	2
Заміна сервера	Відкритість сервера для перевірки виборцями та їх довіреними особами. У разі претензій допускається заміна сумнівного сервера. Виборцям надається право підключити свою консоль до сервера для виконання команд перевірки. Після завантаження OpenBSD неможливо потайки змінити сервер.

1	2
Зміна операційної системи (ОС)	Виборцям надається право брати участь у завантаженні операційної системи за відкритою інструкцією. Після цього можна перевірити ОС через звичайний або власний сервер аудиту, ввівши команди, наприклад, sysctl, ps -aux, аж до копіювання всіх файлів ОС для перевірки.
Зміна прикладної програми	Файл прикладної програми (текст node.js) попередньо публікується на сайті виборчої системи. Адміністратор сервера розміщує копію цього файлу у своєму каталозі /home/admin/, а виборець копіює його через сервер аудиту для порівняння з опублікованим. Після запуску програми адміністратор створює звіт про свої дії за допомогою команди history > [report file name]. Виборець перевіряє звіт і порівнює час його створення з моментом запуску програми (команда ps -aux на сервері аудиту). Якщо файл з програмою був вірним до його запуску, то заміни не було.
Позаштатне втручання персоналу	Сервер аудиту реєструє появу всіх активних процесів, включаючи дії адміністратора. Після запуску програми та створення звіту ніхто не повинен заважати роботі сервера. Аудитор за допомогою клавіші «Протокол аудиту» перевіряє, чи немає записів після запуску програми, що свідчить про відсутність втручання у роботу сервера.

Зазначимо, що допуск виборців до перевірки серверного блоку та участі в установці ОС може бути дозволений у період до голосування, коли на сервері немає критичних даних. Тривалість цього періоду становить приблизно один місяць. Цього достатньо, щоб виборці переконалися, що на наявному обладнанні неможливо створити імітатор, який створював би видимість чесних виборів, а насправді допускав би фальсифікації. Не обов’язково, щоб кожен виборець перевіряв серверне обладнання, але бажано, щоб хтось із них скористався цим правом, оскільки важливо записати результат команди ps -aux, що показано на рисунку 7. Ця команда відображає стан усіх активних процесів сервера.

```
ps -aux

USER       PID %CPU %MEM   VSZ   RSS TT  STAT   STARTED       TIME COMMAND
root     39820  1.8  0.4  1308  3432 ??  S       1:25PM    0:00.38 sshd: kontro
root         1  0.0  0.0   440   316 ??  S       8Jul21    9:53.69 /sbin/init
root     19788  0.0  0.1   724   532 ??  Ip      8Jul21    0:00.17 /sbin/slaacd
_slaacd  50298  0.0  0.1   724   572 ??  Ip      8Jul21    0:00.05 slaacd: engi
_slaacd  97395  0.0  0.1   728   600 ??  Ip      8Jul21    0:00.04 slaacd: fron
root     77435  0.0  0.2   812  1988 ??  IpU     8Jul21    0:00.43 syslogd: [pr
_syslogd 19541  0.0  0.1  1400  1308 ??  Sp      8Jul21   23:44.89 /usr/sbin/sy
root     89941  0.0  0.1   720   480 ??  IU      8Jul21    0:00.02 pflogd: [pri
_pflogd   1611  0.0  0.0   756   444 ??  Sp      8Jul21   23:32.26 pflogd: [run
_ntp     42631  0.0  0.3  1144  2392 ??  I<p     8Jul21    1:33.14 ntpd: ntp en
_ntp     50686  0.0  0.2  1060  2256 ??  Ip      8Jul21    0:00.46 ntpd: dns en
root     23582  0.0  0.1  1028  1328 ??  I<pU    8Jul21    0:01.11 /usr/sbin/nt
root     39753  0.0  0.1  1232  1320 ??  S       8Jul21  103:18.57 /usr/sbin/ss
root     42239  0.0  0.2  2000  1996 ??  Ip      8Jul21    0:02.26 /usr/sbin/sm
_smtpd   14505  0.0  0.4  1660  3432 ??  Ip      8Jul21    0:00.20 smtpd: klond
_smtpd   93816  0.0  0.4  1940  3736 ??  Ip      8Jul21    0:00.99 smtpd: contr
_smtpd   29763  0.0  0.4  1772  3676 ??  Ip      8Jul21    0:01.42 smtpd: looku
_smtpd   77896  0.0  0.4  2044  4128 ??  Ip      8Jul21    0:02.81 smtpd: pony
_smtpq   40229  0.0  0.4  1952  3728 ??  Ip      8Jul21    0:02.90 smtpd: queue
_smtpd   21890  0.0  0.4  1672  3532 ??  Ip      8Jul21    0:00.48 smtpd: sched
_sndiop  87793  0.0  0.1   560   784 ??  IpU     8Jul21    0:00.00 sndiod: help
_sndio   40541  0.0  0.1   588   684 ??  I<p     8Jul21    0:00.01 /usr/bin/snd
root     93843  0.0  0.1   736  1140 ??  Ip      8Jul21    1:50.46 /usr/sbin/cr
kontrol   9930  0.1  0.3  1232  2636 ??  S       1:25PM    0:00.03 sshd: kontro
admin    62604  0.0  5.6 220220 52632 p0- S      14Jul21   44:38.87 node --exper
kontrol  85491  0.0  0.1   800   660 p0  Sp      1:25PM    0:00.03 -ksh (ksh)
kontrol   4955  0.0  0.0   472   344 p0  R+pU/2  1:25PM    0:00.00 ps -aux
root     63197  0.0  0.1   464  1080 00  I+pU    8Jul21    0:00.04 /usr/libexec
b66$ exit
```

Рис. 7. Результат виконання команди ps -aux у вікні сервера аудиту.

Якщо значення PID (рисунок 7) для процесів операційної системи залишаються незмінними, це означає, що сервер працює безперервно з часу, зазначеного в стовпці STARTED. У цьому випадку з 8 липня 2021 року. Оскільки кожен раз, коли запускають OpenBSD, для усіх, крім першого, процесів генеруються випадкові PID. Неможливо перезапустити сервер з тими самими PID. Сервер аудиту безперервно відстежує активні процеси за допомогою команди ps -aux кожні кілька секунд і викликає тривогу, якщо з’являється новий невідомий процес.

Таким чином, в описаній системі голосування виборці можуть провести повноцінний аудит і переконатися, що їхній голос не може бути розкритий зловмисником при передачі по каналах зв’язку та не було стороннього втручання в роботу сервера голосування.

4.3. Методика проведення повноцінного аудиту системи Інтернет голосування.

Відповідно до цієї методики аудит представлено у вигляді двох етапів: підготовчого та дистанційного. Передбачається, що серед виборців є ті, хто самостійно або із залученням довірених осіб візьмуть участь у підготовчому етапі аудиту на території провайдера Інтернету. Кількість таких виборців не обов’язково обмежувати. Завданням підготовчого етапу є перевірка обладнання сервера голосування з операційною системою на відповідність номенклатурі, а також перевірка працездатності дистанційного аудиту. Перш за все треба переконатись, що сервер дійсно працює на міні-комп’ютері Raspberry Pi 3 Model B. Це можна перевірити за зовнішнім виглядом, а також за допомогою команди sysctl hw, результат якої показаний на рисунку 8, де тип комп’ютера вказано як hw.product.

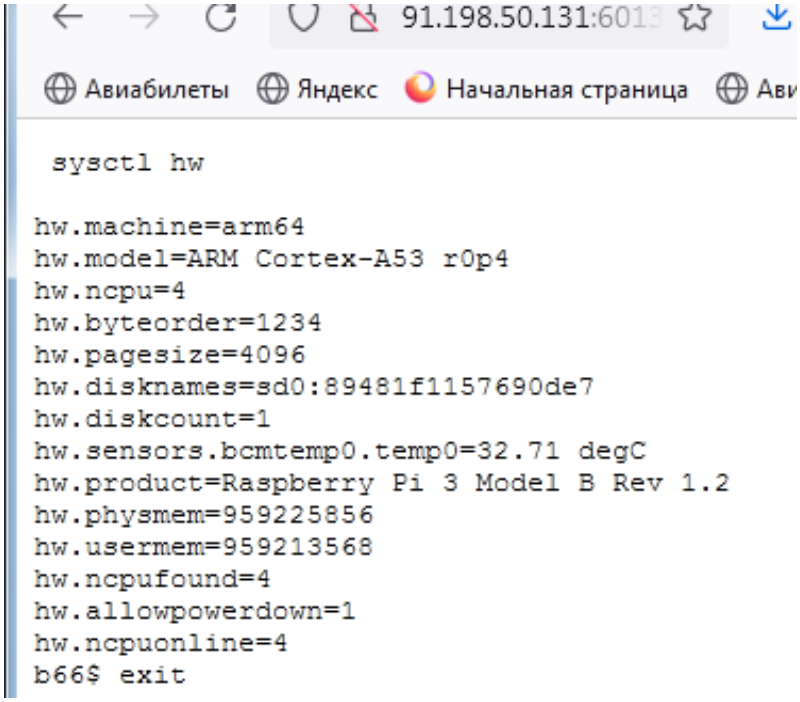


Рис. 8. Результат виконання команди sysctl hw.

Версію операційної системи можна визначити за допомогою команди uname -a. Для виконання команд необхідно підключити консоль, якою може бути будь-який комп'ютер з USB-портом. На рисунку 9 показано підключення консолі до Raspberry Pi 3 Model B.

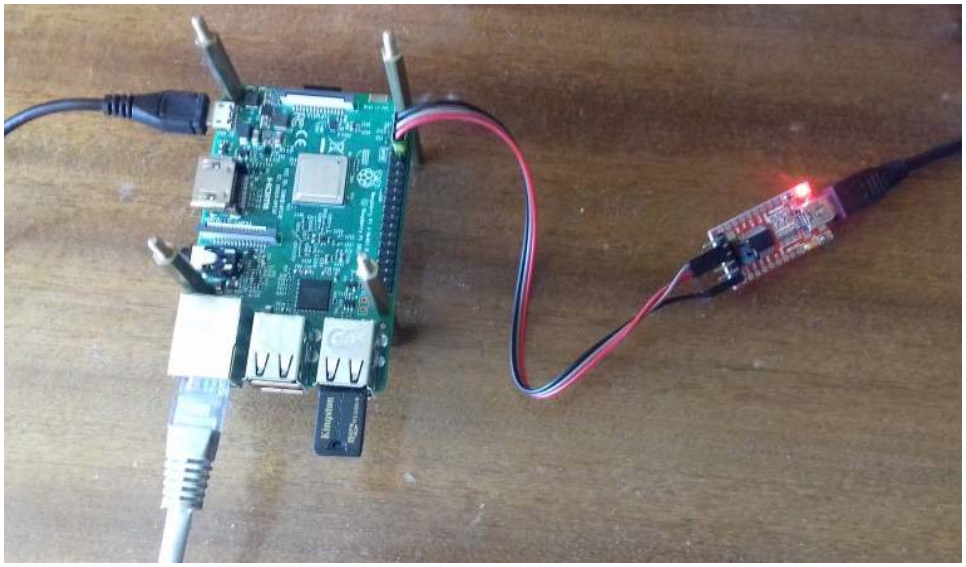


Рис. 9. Підключення консолі до міні-комп'ютера Raspberry Pi 3.

Кабель живлення показаний ліворуч, а кабель до комутатора Ethernet – нижче. Ці і тільки ці два шнури повинні бути завжди підключені. Праворуч показаний кабель для підключення консолі через адаптер типу UART-USB. Перевірка підключення до Інтернету здійснюється командою ifconfig, результат якої наведено на рисунку 10.

```
 ifconfig

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 32768
        index 2 priority 0 llprio 3
        groups: lo
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
        inet 127.0.0.1 netmask 0xff000000
enc0: flags=0<>
        index 1 priority 0 llprio 3
        groups: enc
        status: active
smsc0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        lladdr b8:27:eb:b8:5f:ca
        index 3 priority 0 llprio 3
        groups: egress
        media: Ethernet autoselect (100baseTX full-duplex)
        status: active
        inet 91.198.50.130 netmask 0xffffff00 broadcast 91.198.50.255
pflog0: flags=141<UP,RUNNING,PROMISC> mtu 33136
        index 4 priority 0 llprio 3
        groups: pflog
```

Рис. 10. Результат виконання команди ifconfig.

Ця команда показує статус використовуваних інтерфейсів, три з яких є сервісними (lo0, enc0, pflog0) і один (smsc0) для підключення до Інтернету. Ніякі інші інтерфейси з активним статусом не повинні бути виявлені. Якщо є сумніви в цілісності операційної системи, то потрібно скопіювати всі її файли для додаткової перевірки, яка детально описана в [15]. Ця перевірка полягає в завантаженні точно такої ж ОС за допомогою точно такого ж методу на іншому комп'ютері, а потім слід порівняти файли. Якщо результат порівняння позитивний, то в цілісності системи немає жодних сумнівів, оскільки змінити систему, залишивши всі її виконувані файли без змін, неможливо. Переконавшись, що ОС правильна, слід ввести через консоль команду ps -aux, результат якої було показано вище (рисунок 7). Усі результати виконання команд повинно зберігати для подальшого порівняння. Далі слід перевірити працездатність дистанційного аудиту. Для цього за допомогою будь-якого пристрою доступу до Інтернету за посиланням, опублікованим провайдером, необхідно відкрити веб-сторінку виборця. Потім, натиснувши клавішу аудиту, відкрити сторінку сервера аудиту, вигляд якої було показано вище (рисунок 3). Натиснувши клавішу введення команди ОС, слід ввести ті самі команди, які були введені через консоль, і перевірити результати. Для команди ifconfig результати повинні повністю збігатися, для команди sysctl hw може відрізнятися лише значення температури процесора, а для команди ps -aux значення PID всіх активних процесів ОС повинні збігатися. Ці результати мають бути опубліковані на сайті виборців. У разі недовіри до штатного сервера аудиту провайдер повинен допомогти виборцям встановити додатковий сервер аудиту. Принцип роботи сервера аудиту детально описано в [10]. Для доступу виборців до сервера аудиту рекомендовано використовувати протокол https, щоб нейтралізувати

атаку посередника. Наприкінці підготовчого етапу аудиту слід перевірити надходження запитів від виборців на сервер голосування за записами у файлі /home/admin/nohup.out. Для цього після запиту виборця на сервер голосування слід ввести через консоль команду cat /home/admin/nohup.out і перевірити адресу, яка буде відображатися в кінці файлу у вигляді: ADDR=217.66.97.56:63173. Ця адреса має відповідати реальній IP-адресі запиту виборця. Подальший аудит можна провести дистанційно. Для цього на веб-сторінці виборця слід натиснути клавішу аудиту, що відкриває голову веб-сторінку сервера аудиту. Далі, натиснувши клавішу «Команда ОС», слід виконати команди для порівняння, результати яких публікуються на сайті виборців. Крім того, виборці можуть перевірити вміст усіх файлів прикладного програмного забезпечення, що дає змогу порівняти тексти виконаних програм з опублікованими, а також звірити введені адміністратором команди у файлах звітів. Хоча ці перевірки дають змогу переконатися у відсутності маніпуляцій з апаратним та програмним забезпеченням сервера для голосування, їх недостатньо для повної переконливості у відсутності фальсифікацій. Найважливіші дві перевірки, які необхідно виконати в потрібний час, стосуються виявлення атаки посередника та маніпуляцій із сервером голосування. Першу з цих перевірок виборець має виконати під час діалогу з сервером голосування, оскільки атака посередника може бути здійснена в будь-який момент. Детальний опис цієї перевірки наведено вище (рисунки 4, 5). Другу з цих перевірок необхідно провести після отримання результатів голосування. Вона полягає у перегляді протоколу аудиту за допомогою клавіші «Протокол аудиту» (рисунок 3). Результати натискання цієї клавіші показані на рисунках 11, 12.

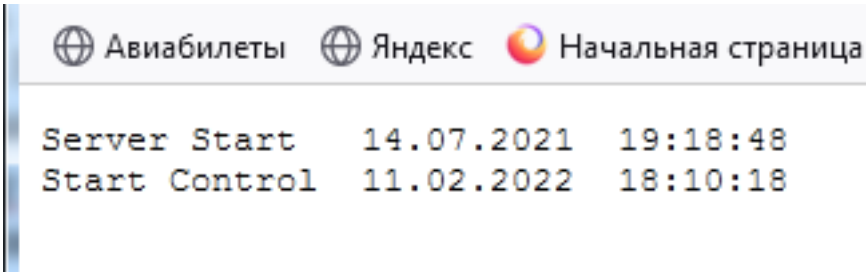


Рис. 11. Протокол аудиту, коли не було втручання у роботі сервера.

```
Server Start   14.07.2021  19:18:48
Start Control  11.02.2022  16:32:09
admin    62604 11.02.2022  16:32:29 !!!!!!!!!!
admin    62604  0.0  5.6 220220 52428 p0- S
admin    74413 11.02.2022  16:32:29 !!!!!!!!!!
admin    74413  0.0  0.1   800   664 p0  I+p

admin    62604 11.02.2022  16:32:59 !!!!!!!!!!
admin    62604  0.0  5.6 220220 52428 p0- S
admin    74413 11.02.2022  16:32:59 !!!!!!!!!!
admin    74413  0.0  0.1   800   664 p0  I+p

admin    62604 11.02.2022  16:33:29 !!!!!!!!!!
admin    62604  0.0  5.6 220220 52432 p0- S
admin    74413 11.02.2022  16:33:29 !!!!!!!!!!
admin    74413  0.0  0.1   800   664 p0  I+p

admin    62604 11.02.2022  16:33:59 !!!!!!!!!!
admin    62604  0.0  5.6 220220 52436 p0- S
admin    74413 11.02.2022  16:33:59 !!!!!!!!!!
admin    74413  0.0  0.1   800   664 p0  I+p

admin    62604 11.02.2022  16:34:29 !!!!!!!!!!
admin    62604  0.0  5.6 220220 52436 p0- S
admin    74413 11.02.2022  16:34:29 !!!!!!!!!!
admin    74413  0.0  0.1   800   664 p0  I+p

Stop Control   11.02.2022  16:34:32
Start Control  11.02.2022  16:53:08
```

Рис. 12. Вигляд протоколу аудиту у разі втручання в роботу сервера на підготовчому етапі аудиту.

Під час перевірки протоколу аудиту важливо звернути увагу на момент початку останнього контролю, після якого записів бути не повинно. Якщо увімкнути контроль на підготовчому етапі аудиту, то непотрібні записи потраплять у протокол (рисунок 12). Це може бути корисно для перевірки працездатності системи автоматичного аудиту.

Таким чином, шляхом проведення аудиту за представленою методикою можна виявити всі загрози, які викликають занепокоєння з боку виборців. Під час підготовчого етапу аудиту було підтверджено, що сервер голосування фактично реалізований на міні-комп’ютері Raspberry Pi 3 Model B під управлінням OpenBSD. Приховано замінити ці засоби неможливо, оскільки будь-яка спроба входу на сервер з правами адміністратора відразу реєструється сервером аудиту. Завдяки підготовчому етапу аудиту в умовах відкритого серверного блоку виборці можуть продовжити повноцінний аудит дистанційно до повного завершення роботи сервера для голосування. Завдяки етапу дистанційно аудиту виборці можуть переконатись, що програмне забезпечення не було підроблено і що не було стороннього втручання в роботу сервера. Це свідчить про те, що результати підрахунку голосів, опубліковані на сервері, не можуть бути сфальсифікованими.

4.4. Моделювання системи таємного Інтернет голосування.

Метою даного моделювання було підтвердження можливості практичної реалізації повноцінного аудиту за розробленою методикою та визначення якісних характеристик такої системи голосування. Перш за все зазначимо, що моделювання стосувалося лише тієї частини системи, яка потребувала аудиту для забезпечення таємності волевиявлення та відсутності шахрайства при визначенні результату. Основні принципи цього моделювання з точки зору вибору апаратного забезпечення полягали в тому, що було обрано засоби виключно масового виробництва, широко доступні, високої надійності та такі, що легко ідентифікувати за зовнішнім виглядом. Крім того, вони повинні бути недорогими, щоб, якщо виникли сумніви в автентичності, не було проблем із їх заміною. Що стосується програмного забезпечення, то основною вимогою була його повна відкритість і можливість перевірити відсутність шкідливих закладок. Для програм, які використовуються в готовому вигляді, головне – їх безпека, а для створеного прикладного програмного забезпечення – максимальна доступність і популярність мовних засобів. Особливою вимогою був вибір найбільш простих і зрозумілих програмних рішень, а також мінімізація обсягу програм для полегшення їх детальної перевірки. Усі ці вимоги були враховані під час вибору принципів побудови цієї системи голосування, про яку йдеться вище (п. 4.2). У моделі відкритого блоку серверів, показаній на рисунку 13, передбачено підключення консолі до кожного з серверів для контролю аудиторами.

Рис. 13. Робота аудитора через консоль з відкритим блоком серверів.

Важливою частиною моделювання була підготовка виборців, які могли б не тільки голосувати, а й проводити аудит програмного забезпечення. Оскільки це моделювання відбувалось за участі студентів, які вже оволоділи комп'ютерними мовами в школі, робота з цією моделлю сприяла їх творчому розвитку. Найскладнішою для розуміння частини моделі були криптографічні перетворення, які засновані на обчисленні ступеню великих чисел за правилами операцій над полем Галуа $GF(2^{503})$. Для спрощення аудиту цей розрахунок реалізовано у вигляді блоку, розміщеного у файлі CRIPTO.js, що містить не більше 100 операторів JavaScript. Цей блок неодноразово перевірявся і не потребує перевірки. Дії, запрограмовані в цьому блоці, виконуються над символьними рядками з нулів і одиниць по 503 символи кожен. Криптографічні перетворення на стороні клієнта і сервера є симетричними і виконуються ідентичними програмами на JavaScript. Реалізація алгоритму Діффі-Хеллмана виглядає так:

$$C_C(C_S(q, X),Y) = C_S(C_C(q, Y),X), \quad (1)$$

де C_C та C_S – перетворення, які виконує блок CRIPTO.js на стороні клієнта та сервера відповідно; q – рядок символів 010000... , що представляє собою примітивний елемент поля Галуа; X і Y – рядки випадкових символів (0, 1), які генеруються на стороні сервера та клієнта відповідно.

Оскільки перетворення C_C та C_S однакові, і вираз (1) в арифметичному еквіваленті має вигляд:

$$(q^X)^Y = (q^Y)^X, \quad (2)$$

то справедливість рівності (1) не викликає сумніву. Це означає, що на стороні сервера і клієнта утворюються однакові послідовності з 503 випадкових символів 0 і 1. Дані для шифрування перетворюються в рядки символів 0 і 1, а потім до кожного символу за модулем 2 додається поточний символ із випадкової послідовності. Для розшифрування на стороні одержувача виконується точно таке ж перетворення, оскільки шифр Вернама симетричний.

Таким чином, моделювання показало, що аудит системи, включаючи найскладнішу для розуміння частину програмного забезпечення, доступний для осіб лише зі шкільною освітою. Саме для цього покоління створюються нові системи голосування, в яких завдяки широко доступному повноцінному аудиту, усуваються необґрунтовані підозри щодо можливого шахрайства.

5. Обговорення результатів створення відкритого блоку серверів.

При традиційній технології голосування, як зазначено в [1], завдяки повноцінному аудиту у виборців не виникає підозр у шахрайстві. Однак при таких же технологічних можливостях в інших країнах вибори можуть закінчитися скандалами. Це свідчить про те, що якщо в суспільстві не визріла потреба в чесному голосуванні, то умови для повноцінного аудиту не будуть створені або його результати будуть проігноровані. У цій роботі показано, що у

разі Інтернет голосування, завдяки відкритому блоку серверів, стає можливим проведення повноцінного аудиту. Для цього достатньо, щоб виборці дотримувалися методики, що представлена в цій роботі, але це не означає, що результати перевірки не можна буде ігнорувати. Іншими словами, ці дослідження доводять, що запровадження Інтернет голосування можна здійснити, не втрачаючи можливості в повноцінному аудиті, у чому до проведення цих досліджень могли виникнути сумніви.

6. Висновки.

1. Виходячи з того, що побоювання виборців пов'язані лише з розкриттям таємниці їх голосів та можливою фальсифікацією підрахунку, визначено блоки та процедури в системі Інтернет голосування, які можуть викликати недовіру виборців.

2. Вибрано принципи побудови системи таємного голосування в Інтернеті на основі використання відкритого серверного блоку, що забезпечує можливість проведення повноцінного аудиту не лише самими виборцями, а й будь-якими їх довіреними особами.

3. Розроблено методику проведення повноцінного аудиту системи Інтернет голосування. Завдяки цій методиці такий аудит не вимагає залучення фахівців високого рівня, а для цього цілком достатньо сучасної шкільної освіти.

4. Створено модель системи таємного Інтернет голосування, що включає засоби проведення аудиту за розробленою методикою. Завдяки цій моделі показано, що немає проблем з вибором апаратного та програмного забезпечення для здійснення повноцінного аудиту в системах таємного Інтернет голосування. Для експериментального голосування модель доступна в Інтернеті за адресою http://91.198.50.8:29901/VD999901.html.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lombardi, E. (2022) Electronic Vote & Democracy. Retrieved from http://www.electronic-vote.org.

2. Ajish, S., Anil Kumar, K. S. (2020) Secure I-Voting System with Modified Voting and Verification Protocol. Advances in Electrical and Computer Technologies. https://www.springerprofessional.de/en/secure-i-voting-system-with-modified-voting-and-verification-pro/18356152?searchResult=7.Ajish&searchBackButton=true.

3. Solvak, M. (2020) Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. 5th International Joint Conference, E-Vote-ID 2020, Bregenz, Austria, October 6–9, 2020, pp 213-228. https://link.springer.com/chapter/10.1007/978-3-030-60347-2_14.

4. Patent US 2017/0109955 A1 Blockchain Electronic Voting System And Method Apr. 20, 2017.

5. Ibrahim, M., Ravindran, K., Lee, H., Farooqui, O., Mahmoud, Q.H. (2021) An Electronic Voting System using Blockchain and Fingerprint Authentication. 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C). https://www.computer.org/csdl/proceedings-article/icsa-c/2021/391000a123/1tuzQj20SwE.

6. Alvi, S.T., Uddin, M.N., Islam, L., Ahamed, S. (2020) From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms. 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020 vol. 1, pp. 1-6. https://www.computer.org/csdl/proceedings-article/sti/2020/09350399/1rgGtTphP3i.

7. Fernandes, A., Garg, K., Agrawal, A., Bhatia, A. (2021) Decentralized Online Voting using Blockchain and Secret Contracts. International Conference on Information Networking (ICOIN), 2021, vol. 1, pp. 582-587. https://www.computer.org/csdl/proceedings-article/icoin/2021/09333966/1qTrSPKAJ7W.

8. Schneier, B. (2020) Voatz Internet Voting App Is Insecure. March 15. Retrieved from https://www.schneier.com/crypto-gram/archives/2020/0315.html.

9. Recommendation CM/Rec(2017) of the Committee of Ministers to member States on standards for e-voting.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f

10. Khlaponin, Y., Vyshniakov, V., Ternavska, V., Selyukov, O., Komarnytsyi, O. (2021) Development of audit and data protection principles in electronic voting systems. Eastern-European Journal of Enterprise Technologies, 2021, № 4/2 (112). 47–57. http://journals.uran.ua/eejet/article/view/238259/237901 DOI: 10.15587/1729-4061.2021.238259.

11. Вишняков, В.М., Пригара, М.П., Воронін О.В. (2014) Відкрита система таємного голосування, Управління розвитком складних систем, 2014, №20, С. 110 – 115. http://urss.knuba.edu.ua/files/zbirnyk-20/22.pdf.

12. *Shannon C. (1949) Communication Theory of Secrecy Systems.* Bell System Technical Journal. 1949. 28 (4). Pp. 656–715.

13. Chupryn, V., Vyshniakov, V., Prygara, M. (2016) Generation of random numbers by regular means of Internet hosts. Ukrainian Information Security Research Journal V. 18, №4. – 323-335.

14. Diffie, W., Hellman, M.E. (1976) New Direction in Cryptography. *IEEE Transactions on Information Theory.* 1976. v.IT-22, n.6. Pp. 644-654.

15. Вишняков, В.М., Комарницький, О.А. (2019) Транспарентні системи електронної демократії. Accent Graphics Communications & Publishing , Ottawa, Canada.

УДК 004.056.53

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ (ML) ДЛЯ ВИЗНАЧЕННЯ ЗАГРОЗ З КІБЕРБЕЗПЕКИ

Венгерський П.С.
факультет прикладної математики та інформатики
Львівський національний університет імені Івана Франка
Львів, Україна
petro.vengersky@gmail.com

Карпюк Р.
CSOC спеціаліст
SoftServe Inc.
Львів, Україна
simmppllee@gmail.com

Анотація. Розглянуто процес аналізу подій з кібербезпеки, а саме аспект зменшення кількісті хибних спрацювань. Розглянуто шляхи зниження фінансових витрат на кібербезпеку та збільшення швидкості протидії зловмисникам.

Кожного дня, центри з протидії кіберзагрозам (CSOC) стикаються з тим, що потрібно знайти баланс між кількістю фахівців, котрі можуть займатися аналізом подій з кібербезпеки до самої кількості цих подій. В нашому дослідженні ми сконцентруємо свою увагу саме на тому, як зменшити навантаження на аналітиків, а саме як зменшити кількість хибних спрацювань.

Що є основним джерелом вхідних даних для аналітика, в розрізі кібербезпеки? Вірно, кореляційні правила або різні автоматизовані системи виявлення різноманітних загроз, наприклад:

- системи захисту кінцевих користувачів (EDR)
- системи виявлення\запобігання мережевих вторгнень
- системи запобігання витоку інформації
- інші.

З чим спершу зустрічається інженер з виявлення загроз (threat detection engineer) коли хоче покращити час реакції (time to triage, TTT) і час опрацювання (time to closure, TTC) подій з кібербезпеки – із зменшенням кількості хибних спрацювань котрі генеруються кореляційними правилами. Що для цього можна зробити?

Тут потрібно зрозуміти, як будується виявлення якоїсь аномалії. Отже, найперший і найлегший спосіб – це збудувати кореляційне правило, котре міститиме чітко визначене верхнє порогове значення при перевищені котрого буде відбуватися сповіщення аналітику, що потрібно здійснити дослідження конкретного випадку. Такий підхід має багато недоліків, але найбільшими є:

1. Як коректно визначити «порогове значення»?

2. Таке правило, за замовчуванням, буде створювати велику кількість спрацювань, котрі потребують додаткового дослідження аналітиком, оскільки інформаційна система є досить динамічною та гранулярною одиницею і не можливо обмежитись, для всіх випадків виключно, визначенням «жорстко» прив'язаного порогового значення.

Коли перший спосіб себе вичерпує повністю, а аналітики «тонуть» в величезній кількості подій, котрі потребують додаткового дослідження і, як наслідок, ефективність CSOC суттєво падає, оскільки TTT\TTC стрімко зростає, на допомого приходить статистика. Тобто, threat detection engineer змінює чітко визначену межу для спрацювання в своїх кореляційних правилах на обрахунок, до прикладу, середнього квадратичного відхилення (standard deviation, stdev). Це перший, найпростіший, крок до пошуку аномалій. Дані нововведення покращають ситуацію для аналітиків, але кількість хибних спрацювань однаково залишається значною. Оскільки, як вище було сказано, інформаційна дуже динамічна одиниця і за годину, чи добу може змінитися дуже багато. Наступним кроком до покращення є використання статистики в поєднані із часовими проміжками. Тобто здійснюємо всі ті ж розрахунки, що і кроком вище, але порівнюємо не грубо з stdev, а з стандартною девіацією за вчора, або, наприклад, сьогоднішній обідній час із вчорашнім аналогічним часовим відрізком. Насправді, на цьому більшість і зупиняється і цього, для когось може бути достатньо, але не для нас. Ми хочемо досягнути найкращого TTT\TTC, а для цього потрібно зробити виявлення аномалій найбільш прицільним.

Отже, всі покращення і побудову взаємодію з ML будемо здійснювати на основі SIEM «Splunk».

SIEM (security information and event management) — це комбінація двох термінів, які вказують на сферу застосування прикладного програмного забезпечення: SIM (Security information management) – управління інформаційною безпекою та SEM (Security event management) – керування подіями безпеки. Технологія SIEM забезпечує аналіз в режимі реального часу подій кібербезпеки, що надходять від мережевих пристроїв і програм. SIEM представлений додатками, пристроями або службами, а також використовується для реєстрації даних і створення звітів для сумісності з іншими бізнес-даними. Сам термін був винайдений Gartner в 2005 році, але з тих пір сама концепція і все, що до неї належить, зазнало багато змін.

Машинне навчання (ML) – це вивчення комп'ютерних алгоритмів, які можуть автоматично покращуватися завдяки досвіду та використанню даних. ML розглядається як частина штучного інтелекту. Алгоритми машинного навчання будують модель на основі вибіркових даних, відомих як «навчальні дані», щоб робити прогнози або рішення, не будучи явно запрограмованими для цього.

Підмножина машинного навчання тісно пов'язана з обчислювальною статистикою, яка зосереджена на прогнозуванні за допомогою комп'ютерів; але не все машинне навчання є статистичним навчанням. Вивчення математичної

оптимізації надає методи, теорію та прикладні області у сфері машинного навчання.

Для чого саме можна використати ML в сфері кібербезпеки (рисунок 1)?

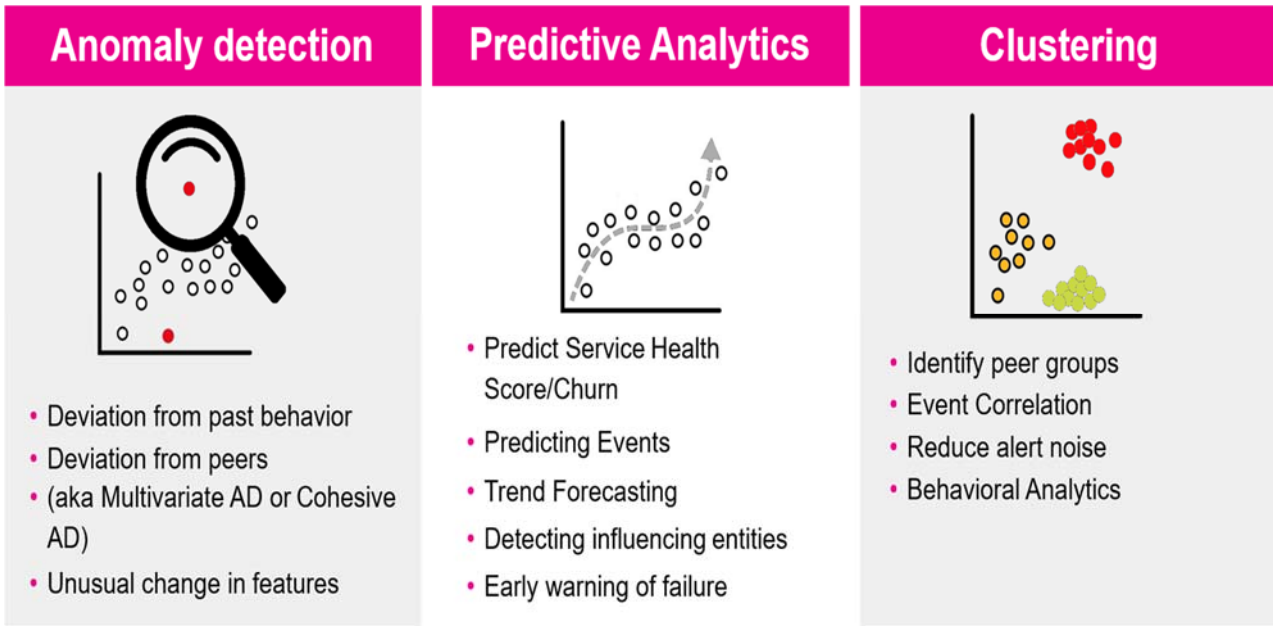


Рис.1. Можливості Splunk ML.

Ми розглянемо першу частину – Anomaly Detection, адже саме вона допоможе нам в побудові кореляціних правил для виявлення різного роду аномалій.

Splunk, за замовчуванням, надає можливість оперувати різними алгоритмами машинного навчання (рисунок 2), а саме:

ACF	ElasticNet	KernelPCA	OneClassSVM	SpectralClustering
ARIMA	ExampleAlgo	KernelRidge	OrthogonalMatchingPursuit	StandardScaler
AgglomerativeClustering	ExtraTreesClassifier	Lasso	PACF	StateSpaceForecast
AutoPrediction	FieldSelector	LatentDirichletAllocation	PCA	SystemIdentification
BernoulliNB	GMeans	LinearRegression	RandomForestClassifier	TFBinary
Birch	GaussianNB	LinearSVC	RandomForestRegressor	TFIDF
CollaborativeFilter	GradientBoostingClassifier	LocalOutlierFactor	Ridge	TSNE
CorrelationMatrix	GradientBoostingRegressor	LogisticRegression	RobustScaler	TruncatedSVD
CustomDecisionTreeClassifier	HashingVectorizer	MDS	SGDClassifier	XMeans
DBSCAN	ICA	MLPClassifier	SGDRegressor	
DecisionTreeClassifier	Imputer	MinMaxScaler	SVM	
DecisionTreeRegressor	IsolationForest	NMF	SVR	
DensityFunction	KMeans	NPR	SavgolFilter	

Рис.2. Алгоритми Splunk ML.

Всі ці алгоритми будуть корисними і функціональними під різні сценарії створення кореляційних правил.

Нам вдалося класифікувати алгоритми за їх способом застосування і кожному в залежності від їх властивостей призначити ранг (Range), який відповідає їх затребуваності (рисунок 3).

Algorithm	Prepare Data	Regression	Clustering	Classification	Dimension reduction	Unsupervised	Supervised	Massively	Range
ACF	+								1d
ARIMA		+						2	3
AgglomerativeClustering			+			+			2
AutoPrediction				+			+		2
BernoulliNB				+			+	2	4
Birch			+			+		2	4
CollaborativeFilter	+								1d
CorrelationMatrix	+								1d
CustomDecisionTreeClassifier				+			+		2
DBSCAN			+			+		2	4
DecisionTreeClassifier				+			+	3	5
DecisionTreeRegressor		+					+	2	4
DensityFunction						+		4	5
ElasticNet		+					+	2	4
ExampleAlgo									
ExtraTreesClassifier				+			+		2
FieldSelector	+							1	2d
GMeans			+			+		1	3
GaussianNB				+			+	2	4

Рис.3. Ранг алгоритмів Splunk ML.

Одним із найефективніших, на нашу думку, алгоритмів виявлення аномалій є DensityFunction. Реалізація цього алгоритму дозволяє задавати різні параметри, від яких може залежати навчання і, його кінцевий результат (рисунок 4). Наприклад, співвідношення між навчальними даними та різними часовими інтервалами (частина дня, вихідні, конкретні години), назвами кінцевих користувачів, іншими об’єктними характеристиками, поєднуючи їх разом або розділяючи, тощо. Алгоритм також передбачає оцінку різного розподілу подій у вибірці для навчання (рисунок 5).

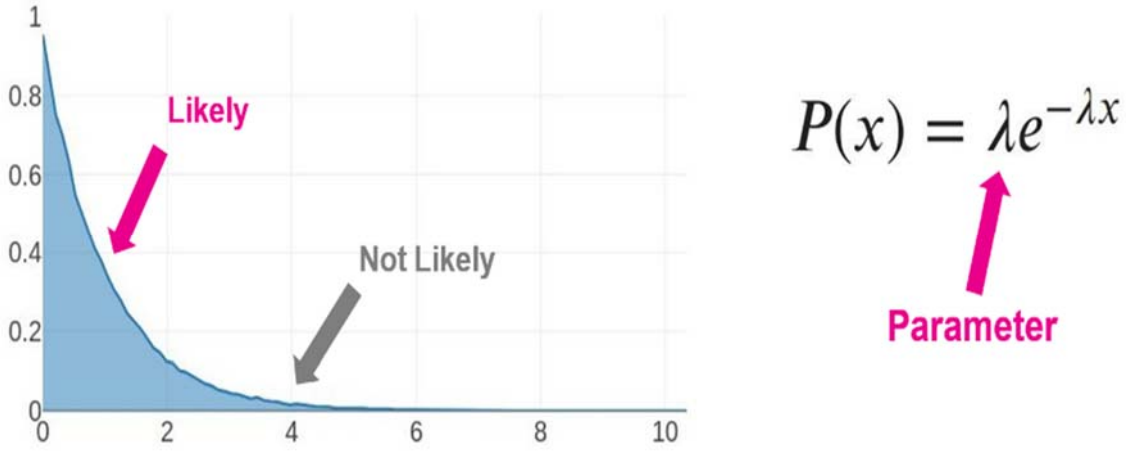


Рис.4. Параметр, що відповідає за вхідні дані від яких залежатиме навчання.

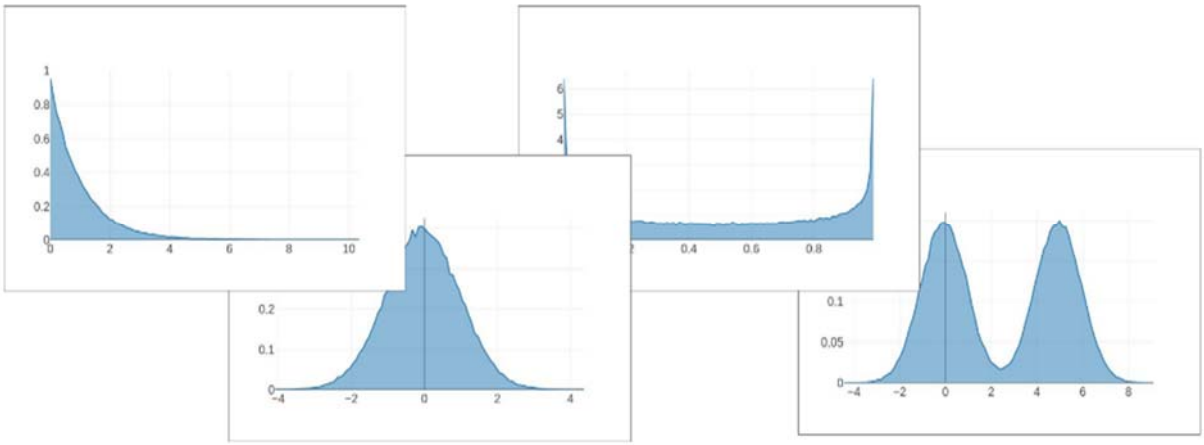


Рис.5. Типи розподілу: Exponential, Normal, Beta, Gaussian Kernel Density Estimation (Gaussian KDE) distribution.

Отже, давайте напишемо правила кореляції для різних випадків використання.

Перше правило допоможе нам виявити аномальну кількість заражених кінцевих користувачів одним типом зловмисного програмного забезпечення. Для реалізації такого випадку нам потрібні вхідні дані, у нашому випадку це будуть дані з системи EDR. Щоб навчити DensityFunction, ми створимо навчальну вибірку за 180 днів, не враховуючи сьогодні (рисунок 6). Ми будемо використовувати навчений алгоритм щогодини для аналізу подій за попередню годину і таким чином будемо виявляти аномалії (рисунок 7).

Title Threat - ML Calculate & Fit Substantial increase in Malware Infections - Model Gen

Description optional

Search

```
| tstats summariesonly=true `els` values(Malware_Attacks.command_line) as
    command_line values(Malware_Attacks.file_path) as file_path count
    allow_old_summaries=true from datamodel=Malware.Malware_Attacks where
    Malware_Attacks.action=blocked  by "Malware_Attacks.signature",
    "Malware_Attacks.dest", "Malware_Attacks.action", "Malware_Attacks.file_name"
    , "Malware_Attacks.process" _time span=1h
| rename "Malware_Attacks.*" as "*"
| search NOT `exclude_malware_signatures`
| eval DayOfWeek=strftime(_time, "%A")
| eval HourOfDay=strftime(_time, "%H")
| eval IsWeekend=if(DayOfWeek="Sunday" OR DayOfWeek="Suturday","Yes","No")
| eval PartOfDay=if(HourOfDay>20 OR HourOfDay<7,"Night","Day")
| eval process=if(process="","-",process)
| stats sum(count) as malware_infections values(dest) as system_list values
    (command_line) as command_line by signature action process DayOfWeek
    HourOfDay PartOfDay IsWeekend _time
| `ele`
| fit DensityFunction malware_infections by signature into
    count_malware_infections_by_signature_1h_with_features
```

Earliest time -180d

Time specifiers: y, mon, d, h, m, s Learn More

Latest time -1d

Time specifiers: y, mon, d, h, m, s Learn More

Рис. 6. Навчання DensityFunction на EDR даних для побудови ML моделі для виявлення аномального поширення шкідливого програмного забезпечення.

Alert Threat - ML Anomaly Detection of Malware Infection by Signature - Rule

Description Optional

Search

```
| tstats summariesonly=true `els` values(Malware_Attacks.command_line) as
    command_line values(Malware_Attacks.file_path) as file_path count
    allow_old_summaries=true from datamodel=Malware.Malware_Attacks  where
    Malware_Attacks.action=blocked by "Malware_Attacks.signature",
    "Malware_Attacks.dest", "Malware_Attacks.action", "Malware_Attacks.process"
    , "Malware_Attacks.file_name" _time span=1h
| rename "Malware_Attacks.*" as "*"
| search NOT `exclude_malware_signatures`
| eval DayOfWeek=strftime(_time, "%A")
| eval HourOfDay=strftime(_time, "%H")
| eval IsWeekend=if(DayOfWeek="Sunday" OR DayOfWeek="Suturday","Yes","No")
| eval PartOfDay=if(HourOfDay>20 OR HourOfDay<7,"Night","Day")
| eval process=if(process="","-",process)
| stats sum(count) as malware_infections values(dest) as system_list values
    (command_line) as command_line by signature action process DayOfWeek
    HourOfDay PartOfDay IsWeekend _time
| `ele`
| eval LH=if(now()-_time<3600,"1","0")
| apply count_malware_infections_by_signature_1h_with_features threshold=0.01
| search "IsOutlier(malware_infections)"=1
| rex field=dest (?<dest>(\w+)(?=\.softservecom\.com))
| `notable_event_severity_malware_signatures`
| eval urgency=mvdedup(urgency)
| lookup asset_lookup_by_str asset as dest OUTPUT service_importance priority
    as host_priority
| fillnull value="-"
| `risk_score_calculation(dest,system)`
```

Рис.7. Навчена модель ML виявляє поширення шкідливих програм.

Правило реалізовано і працює в реальних умовах. Результатом роботи є 8 сповіщень за останні 7 днів, що є відмінним результатом, оскільки компанія має понад 15 000 різних типів кінцевих користувачів (сервери, ноутбуки, ПК), де встановлено EDR.

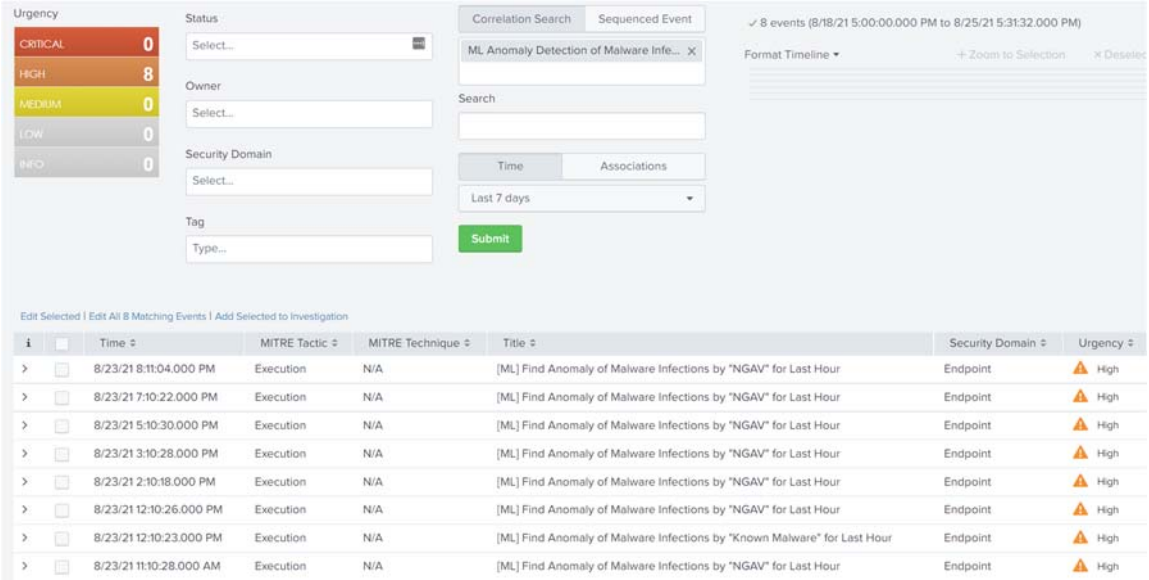


Рис.8. Результати.

Але постає питання, як поступати стосовно виявлення аномалій, пов’язаних із поведінкою зловмисника в межах однієї машини, з використанням різних тактик, технік та процедур (TTPs)? Ми будемо використовувати, як і в попередньому випадку, дані з EDR, але змінимо розрахунок статистики на узагальнення всіх подій в межах однієї машини. Також цей сценарій можна розділити на кілька, враховуючи те, що зловмисники можуть здійснювати свою діяльність акуратно, а саме розтягувати останню в часі. Тобто тут наступним, основним параметром буде час. Ви також можете ввести побічні параметри у вигляді того, чи відбувається активність вночі чи вдень, у вихідні чи в будні.

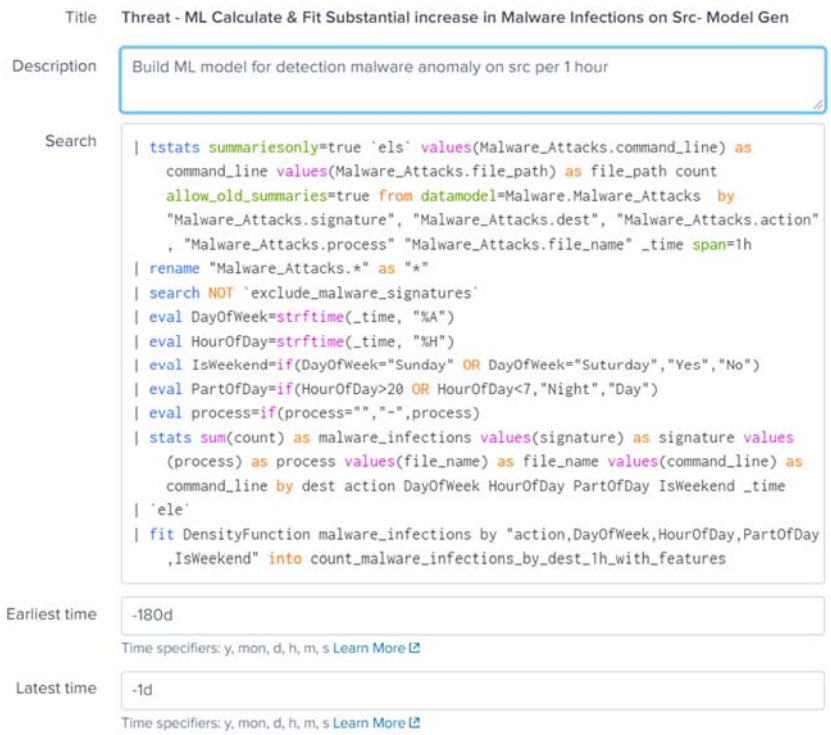


Рис. 9. Навчання DensityFunction на EDR даних для побудови ML моделі для виявлення шкідливої активності в кінцевого користувача.

Alert Threat - ML Anomaly Detection of Malware Infection on Src - Rule

Description Optional

Search

```
| tstats summariesonly=true `els` values(Malware_Attacks.command_line) as
    command_line values(Malware_Attacks.file_path) as file_path count
    allow_old_summaries=true from datamodel=Malware.Malware_Attacks  where
    Malware_Attacks.action=blocked by "Malware_Attacks.signature",
    "Malware_Attacks.dest", "Malware_Attacks.action", "Malware_Attacks.process"
    "Malware_Attacks.file_name" _time span=1h
| rename "Malware_Attacks.*" as "*"
| search NOT `exclude_malware_signatures`
| eval DayOfWeek=strftime(_time, "%A")
| eval HourOfDay=strftime(_time, "%H")
| eval IsWeekend=if(DayOfWeek="Sunday" OR DayOfWeek="Suturday","Yes","No")
| eval PartOfDay=if(HourOfDay>20 OR HourOfDay<7,"Night","Day")
| eval process=if(process="","-",process)
| stats sum(count) as malware_infections values(signature) as signature values
    (process) as process values(file_name) as file_name values(command_line) as
    command_line by dest action  DayOfWeek HourOfDay PartOfDay IsWeekend _time
| `ele`
| eval LH=if(now()-_time<3600,"1","0")
| apply count_malware_infections_by_dest_1h_with_features threshold=0.01
| search "IsOutlier(malware_infections)"=1
| rex field=dest (?<dest>(\w+)(?=\.softservecom\.com))
| `notable_event_severity_malware_signatures`
| eval urgency=mvdedup(urgency)
| lookup asset_lookup_by_str asset as dest OUTPUT service_importance priority
    as host_priority
| fillnull value="-"
| `notable_asset_object(dest)`
```

Рис.10 Навчена ML модель виявляє шкідливу активність.

Інший варіант використання цікавий для пошуку шкідливої аутентифікації за допомогою Kerberos або LDAP протоколів. Ця активність може говорити про використання деяких інструментів для проникнення в інфраструктуру, таких як BloodHound, SharpHound або Kerberoasting. Для цього виявлення ми можемо використовувати дані з AD, Azure AD, MS CAS. Це виявлення ми можемо зкорелювати з певною іншою мережевою активністю та певними артефактами AD\Azure AD, щоб підвищити точність майже до 100%.

Title Access - ML Calculate & Fit MS CAS Kerberos Activity - Model Gen

Description optional

Search

```
index=softserve_it_mcas sourcetype="ms:cas:activities" app="Active Directory"
    body="Failed log on*"
| bin _time span=30m
| eval DayOfWeek=strftime(_time, "%A")
| eval HourOfDay=strftime(_time, "%H")
| eval IsWeekend=if(DayOfWeek="Sunday" OR DayOfWeek="Saturday","Yes","No")
| stats count values(DayOfWeek) as DayOfWeek values(HourOfDay) as HourOfDay
    values(IsWeekend) as IsWeekend dc(targetObjects) as object_count by src_ip
    _time
| fillnull value="-"
| fit DensityFunction dist=norm object_count by "src_ip,DayOfWeek,HourOfDay
    ,IsWeekend" into ml_anomaly_kerberos_object_casb_test as
    ML_kerberous_cas_object
| fit DensityFunction dist=norm count by "src_ip,DayOfWeek,HourOfDay,IsWeekend"
    into ml_anomaly_kerberos_count_casb_test as ML_kerberous_cas_count
```

Earliest time -31d@d

Time specifiers: y, mon, d, h, m, s Learn More

Latest time -1d@d

Time specifiers: y, mon, d, h, m, s Learn More

Рис. 11. Навчання DensityFunction на MS CAS даних для побудови ML моделі для виявлення активності пов’язаної з Kerberoasting.

Alert Access - ML Microsft CAS Kerberos Activity Anomaly (over 30 Minutes) - Rule

Description Using Microsft Cloud App Security Data

Search

```
index=softserve_it_mcas sourcetype="ms:cas:activities" app="Active Directory"
    body="Failed log on*"
| eval DayOfWeek=strftime(_time, "%A")
| eval HourOfDay=strftime(_time, "%H")
| eval IsWeekend=if(DayOfWeek="Sunday" OR DayOfWeek="Saturday","Yes","No")
| stats count values(DayOfWeek) as DayOfWeek values(HourOfDay) as HourOfDay
    values(IsWeekend) as IsWeekend dc(targetObjects) as object_count by src_ip
| fillnull value="-"
| lookup cmdb_assets_expanded host_key as src_ip OUTPUT nt_host
| apply ml_anomaly_kerberos_object_casb_test threshold=0.0001
| apply ml_anomaly_kerberos_count_casb_test threshold=0.0001
| eval RiskScore=0
| fillnull value="-"
| eval ML_kerberous_cas_object=if(ML_kerberous_cas_object="-","0.0"
    ,ML_kerberous_cas_object)
| eval ML_kerberous_cas_count=if( ML_kerberous_cas_count="-","0.0",
    ML_kerberous_cas_count)
| foreach ML_kerberous_cas* [ eval RiskScore=RiskScore + '<<FIELD>>']
| where (RiskScore>0 AND (count>100 OR object_count>100)) OR count>500 OR
    object_count>500
| eval urgency=if(RiskScore=2,"high",if(RiskScore=1,"medium",if(count>1000 OR
    object_count>1000,"high","medium")))
| `notable_asset_object(src_ip)`
```

Рис. 12. Навчена ML модель виявляє активність, пов'язану з Kerberoasting.

ML може допомогти при виявлені багатьох інших аномалій або зменшення хибних спрацювань, наприклад:

- зменшити кількість тригерів, пов'язаних з IDS;
- підозріла активність, пов'язана з відправкою\отриманням пошти;
- виявлення підбору паролів\користувачів (brute-force);
- невдалі спроби входу;
- збої http;
- аномалії мисливської мережі;
- тощо.

Ми впровадили понад 50 кореляційних правил, які використовують ML для виявлення різних аномалій, пов’язаних із кібербезпекою. Всі ці правила діють в реальному часі в існуючій компанії.

Вплив на внутрішній CSOC компанії:

- менше хибних спрацювань до 60%;
- зменшення TTT\TTC до середнього значення в 15\30 хвилин на подію;
- виявлення унікальної шкідливої активності (частина процесу “Threat Hunting”).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Soma Haider, Sinan Ozdemir, Hands-On Machine Learning for Cybersecurity // Packt Publishing Ltd- 2018. - 601 p.
2. https://www.splunk.com- the Splunk Platform. A data platform built for expansive data access, powerful analytics and automation.
3. https://towardsdatascience.com/machine-learning-for-cybersecurity-101-7822b802790b - machine learning for cybersecurity.
4. https://www.recordedfuture.com/machine-learning-cybersecurity-applications/ - machine learning: practical application for cybersecurity.

УДК 004.457

ЗАСТОСУНОК ДЛЯ АНАЛІЗУ ФАЙЛІВ МЕРЕЖЕВОГО ТРАФІКУ НА МОВІ PYTHON

Герей Т.М.
Ужгородський національний університет
gerey37ng@gmail.com

Буковецький В.І.
Ужгородський національний університет
bukovetsky@outlook.com

Матьовка Т.В.
к.е.н.,
старший викладач кафедри фінансів і банківської справи
Ужгородський національний університет
rtanyusha17@gmail.com

Різак В.М.
д.ф-м.н., проф.,
зав. каф. твердотільної електроніки та інформаційної безпеки
Ужгородський національний університет
vrizak@uzhnu.edu.ua

Анотація. Досліджено криптографічні алгоритми захисту інформації та програмне забезпечення, яке їх використовує; розроблено програмне забезпечення у вигляді прихованої програми для заміток «Нотатки» із безпечним зберіганням даних для вирішення проблеми конфіденційності інформації користувачів; зазначено що дане програмне забезпечення складається з 3 компонентів і написане на мові програмування Python, програма «Нотатки» є основним компонентом, її основні функції: створювати, зберігати, видаляти та редагувати текстові замітки; зазначено що використовуючи криптографічний алгоритм на основі RSA, програма для заміток зашифровує та розшифровує інформацію, що міститься в базі даних; описано що для приховування існування програми для заміток, вона впроваджена в програмний додаток «Калькулятор»; вказано що даний додаток містить в собі повноцінний математичний функціонал, з якого відбувається запуск програми «Нотатки», при певних діях та правильній авторизації.

Мережевий трафік відображає всю активність як легітимних так і нелегітимних користувачів певної комп'ютерної мережі, локальної чи глобальної. Фахівці з кібербезпеки, аналізуючи мережевий трафік, можуть реконструювати події, які відбувалися в мережі, знайти і вилучити докази незаконних дій, запобігти проведенню сканування чи атаки на мережу. Для цього

використовується спеціальне програмне забезпечення для перехоплення та аналізу трафіку — так звані аналізатори трафіку. Зараз можна спостерігати велику кількість складних, багатофункціональних аналізаторів. Проте такі програми часто орієнтовані на фахівців із значним досвідом роботи у сфері кібербезпеки та комп'ютерних мереж, яким доводиться досліджувати величезний обсяг мережевого трафіку. Програм із простим функціоналом, які могли б дати початківцям загальне уявлення про основні етапи аналізу трафіку, не так уже і багато.

Відповідно, метою даної роботи є створення додатку для аналізу мережевого трафіку. Створений додаток повинен бути зрозумілий у користуванні для новачків у галузі кібербезпеки і водночас мати достатній функціонал для проведення ґрунтовного аналізу трафіку.

Для написання аналізатору трафіку була вибрана мова програмування Python (застосовується версія 3.7), так як вона досить широко використовується серед фахівців з кібербезпеки та має багато допоміжних бібліотек. Бібліотека Scapy призначена для роботи з мережевими пакетами і вона також використовується.

В результаті виконаної роботи створено додаток для аналізу файлів мережевого трафіку з інтерфейсом командного рядка. Структура додатку — це три файли: «analyzer.py», містить клас Analyzer, у якому прописані статичні методи для обробки заданого файлу мережевого трафіку; «pcap.py», тут прописана власне взаємодія користувача і програми; «ip_mal.py» містить список шкідливих IP-адрес для порівняння. Запускати потрібно файл pcap.py, передавши йому файл мережевого трафіку для обробки: **python pcap.py traffic_file.pcap** (приклад запуску у командному рядку Windows). Після запуску виводяться короткі відомості про трафік у файлі та основні функції програми:

1. Відобразити приватні та публічні IP-адреси з файлу;
2. Відобразити таблицю MAC-адрес із файлу якщо наявні ARP-пакети;
3. Відобразити всі унікальні з'єднання, які стосуються заданої користувачем однієї IP-адреси — вхідні та вихідні;
4. Відобразити весь обмін пакетами між двома заданими користувачем IP-адресами;
5. Перевірити на наявність шкідливих IP-адрес у файлі;
6. Отримати список сервісів, до яких відбувалося звернення різних хостів;
7. Відобразити всі пакети за заданий користувачем період часу (дата початку і дата кінця).

Кожен з отриманих результатів можна зберегти у txt файлі, для функцій 4 та 7, де відображаються всі пакети, є можливість зберегти дані у окремий файл мережевого трафіку pcap, для подальшого аналізу іншими програмами. Додаток було протестовано у ОС Windows 7, Windows 10, Ubuntu Linux, тестування показує, що програма працює коректно.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вілсон Е. Моніторинг і аналіз мережі: підхід до усунення несправностей. Цинциннаті, 1998-2009 рр. 350 с. 2.

2. Чіу Д. М., Садама Р. Моніторинг мережі: Розробка та застосування. Мічиган: Мічиганський університет, 1992. 207 с. 3.

3. Хунг-Чанг Д., Пек-Янг Ч., і Чжі-Лі Ч. Масштабований моніторинг мережі у високошвидкісних мережах. 2011. 148 с. 4.

4. Бежтліч Р. Дао моніторингу безпеки мережі. 2004. 832 с. 5.

5. Бежтліч Р. Практика моніторингу мережної безпеки: розуміння інциденту. 2013. 376 с

РОЗДІЛ 3.
КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.53

ПРИХОВАНА ПРОГРАМА ДЛЯ ЗАМІТОК ІЗ БЕЗПЕЧНИМ ЗБЕРІГАННЯМ ДАНИХ

Боценюк Л.Р.,
магістр,
кафедра твердотільної електроніки та інформаційної безпеки,
wulfik1999@gmail.com

Матьовка Т.В.,
кандидат економічних наук, старший викладач
кафедра фінансів і банківської справи
rtanyusha17@gmail.com

Буковецький В.І.,
аспірант,
кафедра твердотільної електроніки та інформаційної безпеки,
bukovetsky@outlook.com

Різак В.М.,
доктор фізико-математичних наук, професор,
кафедра твердотільної електроніки та інформаційної безпеки,
vrizak@uzhnu.edu.ua

Державний вищий навчальний заклад
«Ужгородський національний університет»

Анотація. Наведена робота досліджує криптографічні алгоритми захисту інформації та програмне забезпечення, яке їх використовує. Розроблено програмне забезпечення у вигляді прихованої програми для заміток «Нотатки» із безпечним зберіганням даних для вирішення проблеми конфіденційності інформації користувачів. Дане програмне забезпечення складається з 3 компонентів і написане на мові програмування Python. Програма «Нотатки» є основним компонентом. Її основні функції: створювати, зберігати, видаляти та редагувати текстові замітки. Використовуючи криптографічний алгоритм на основі RSA, програма для заміток зашифровує та розшифровує інформацію, що міститься в базі даних. Для приховування існування програми для заміток, вона впроваджена в програмний додаток «Калькулятор». Даний додаток містить в собі повноцінний математичний функціонал, з якого відбувається запуск програми «Нотатки», при певних діях та правильній авторизації.

Користувачі персональних комп’ютерів дедалі більше інформації зберігають у пам'яті своїх пристроїв. Часто користувачі пишуть замітки, зберігаючи їх чи у текстових файлах чи використовуючи певні програми. Огляд різноманітних програмних продуктів для створення заміток показує, що не всі вони захищають інформацію користувача належним чином.

Питання захисту інформації користувачів завжди буде актуальним і його вирішення потребуватиме більш ніж одного рівня захисту. Саме багаторівневий захист і забезпечує розроблене програмне забезпечення:

– перший рівень – використання надійного криптоалгоритму для шифрування інформації;

– другий рівень – приховування самого факту наявності програми для нотаток на комп’ютері користувача, і відповідно зменшення шансів зловмисника на виявлення приватної інформації.

Розроблена програма для нотаток буде корисна для будь-яких користувачів персональних комп’ютерів для зберігання інформації.

1. Вступ.

В наш час актуальність захисту інформації набуває дуже великого значення і стає невід’ємною частиною будь-якої сфери людської діяльності. Відомості, які мають певну цінність для свого власника, потребують захисту.

Захист інформації набуває величезної потреби внаслідок великого розповсюдження і використання інформаційних систем, які обробляють інформацію. Особливо захист інформації актуальний у воєнний час, адже багато що залежить від того, чи отримає ворог цінні відомості та інформацію і чи зможе ними скористатися на свою користь. Також інформаційні технології дедалі тісніше впроваджуються у найрізноманітніші сфери людської діяльності, що в свою чергу означає дедалі більше інформації, яка потребує захисту. Стрімко зростає використання пластикових карток, особистих електронних документів людини і все більше державних установ переходять на систему електронного документообігу. Розповсюдження таких технологій також вимагає надійного захисту інформації.

Відповідно, розробка різноманітного програмного забезпечення для захисту інформації як ніколи є актуальною. Основною перевагою розробленої програми є те, що вона може використовуватися звичайними користувачами у повсякденному житті. Тобто, можливість захистити свою приватну інформацію стає доступною і для пересічних користувачів.

Метою написання статті є розгляд характеристик і надійності програми «Нотатки». У статті розглянуто існуючі напрацювання з проблематики захисту інформації та розробки захищеного програмного забезпечення. Визначено основні переваги використання криптографічного методу захисту текстової інформації.

2. Аналіз літературних джерел та постановка проблеми.

Вислів Н. Ротшильда «Хто володіє інформацією – той володіє світом» досить точно описує, яку важливу роль відіграє інформація в житті людей. Однією з властивостей інформації є її конфіденційність, іншими словами –

секретність. Будь то персональні дані, державна, військова чи комерційна таємниці, інформація повинна бути надійно захищена від несанкціонованого доступу зловмисників. Досить значного поширення отримують різноманітні програми для створення записів, нотаток користувачів. Через неуважність чи непрофесійність, у таких нотатках можуть зберігатися приватні дані, чи навіть якісь таємниці. Тому важливо організовувати захист інформації на рівні програмного забезпечення, не лише довіряти користувачам.

Одним з найпоширеніших засобів захисту інформації є криптографічний захист – шифрування даних. У міжнародному стандарті NIST визначається, що шифрування – це процес зміни відкритого тексту на зашифрований за допомогою криптографічного алгоритму з метою забезпечення конфіденційності інформації[1].

Головною метою будь-якого криптографічного алгоритму є збереження інформації та відомостей, які є цінними для свого власника, шляхом захисту їх від можливості ознайомитися з ними стороннім особам. Стійкість криптографічного алгоритму залежить від декількох факторів. До них включаються:

– складність математичного алгоритму, який використовується;

– довжина ключів шифрування та дешифрування.

Відповідно, стійким алгоритмом можна назвати той, який може вистояти проти криптоаналізу в необхідний і достатній час.

У роботах [2, 3] досить детально описано сучасний стан розвитку криптографічних технології, розглянуті симетричні та асиметричні алгоритми шифрування, їх використання у технологіях цифрового підпису, інфраструктурі відкритих ключів. Зокрема, значна увага приділяється алгоритму RSA, який використовується у розробленій програмі. Проте у більшості випадків розглядається застосування криптографії у масштабах міжнародних організацій чи компаній, чи для захисту трафіку глобальної мережі Інтернет.

Криптографічні методи захисту інформації можна проваджувати в різні системи захисту. Це можуть бути як фізичні засоби захисту, які здійснюють шифрування інформації на рівні обладнання системи, так і програмні продукти, у функціонал яких включена можливість захистити дані криптографічним шляхом. Програмні методи шифрування є дуже гнучкими, вони легко впроваджуються в програмні продукти, піддаються зміні і оновленню. Для зміни чогось у програмному продукті, достатньо просто змінити код програми і певні алгоритми роботи. При цьому, вартість оновлення програми доволі таки незначна, адже необхідно просто встановити новішу версію програми на комп’ютерах користувачів. Однак, при використанні цього методу, дуже важливим аспектом є безпечне передання ключів шифрування та дешифрування по мережі.

У роботах [4, 5] розглянуто переваги і недоліки впровадження криптографічних методів захисту інформації на рівні фізичного обладнання та на рівні програмного захисту. Автори робіт запевняють, що фізичні методи захисту вважаються більш надійнішими та швидшими, ніж програмні. Проте їх доцільно використовувати, коли необхідно зашифрувати величезну кількість

даних (гігабайти чи навіть терабайти). За своєю собівартістю вони є дорогими і не дуже практичними, адже щоразу при їх оновленні необхідно витрачати кошти на купівлю та встановлення обладнання. У свою чергу, для шифрування невеликого обсягу інформації, такої як нотатки користувача, цілком достатньо захисту на рівні програмного забезпечення.

Один з оптимальних варіантів для зберігання даних певної програми це використання баз даних. У роботі [6] розглянуто основні моделі загроз для баз даних та запропоновано криптографічні засоби захисту інформації. Проте зазначається, що шифрування даних не вирішує всіх проблем, так як контроль доступу до даних є теж одним із рівнів захисту інформації. Тобто, при використанні баз даних у різноманітних програмних застосунках, потрібно також подбати про авторизацію користувачів.

У статті [7] проведено порівнянна двох досить популярних систем керування базами даних – MySQL та SQLite. Використання тієї чи іншої СКБД завжди залежить від функціоналу та застосування кінцевого програмного продукту. Опираючись на статтю [7], можна зробити висновок, що SQLite підходить для локального зберігання даних програми.

Зараз на ринку можна знайти велику кількість різних програмних рішень для керування та зберігання нотаток користувачів. Програма Evernote, розроблена у 2008 році, зараз є однією з найбільш популярних програм для нотаток. Це пояснюється тим, що вона кросплатформна, працює у середовищах операційних систем Windows, Linux, Android, iOS та у звичайному браузері. Користувач може зберігати свої нотатки офлайн, у базі даних локально на своєму пристрої, а також може створити аккаунт Evernote, і тоді інформація буде зберігатися на серверах компанії. Це одразу сприяє появі серйозних вразливостей безпеки. На серверах Evernote спочатку інформація зберігалася у незашифрованому вигляді. Навіть тепер користувач сам повинен у налаштуваннях вибрати опцію шифрування своїх даних, по замовчуванню програма цього не робить. Автор статті [8] описує інцидент 2016 року, коли компанія Evernote заявила, що їх працівники зможуть переглядати нотатки користувачів для перевірки правильності роботи їхнього алгоритму машинного навчання. Звичайно, користувачам таке не сподобалося. Тому у статті [8] розглядаються деякі альтернативи для Evernote.

Безкоштовна програма Turtl є одним з безпечних застосунків для зберігання заміток користувача. Як і Evernote, вона дозволяє зберігати текст, зображення, файли. Проте вся інформація є зашифрованою, навіть на серверах. Ключ генерується на основі електронної пошти та паролю користувача, у основі – симетричний алгоритм шифрування. Все шифрування в Turtl відбувається до того, як будь-які дані залишають програму (відправляються на сервер). Це означає, що навіть якщо трафік користувача буде перехоплено, інформацію зловмисник не отримає.

Ще одна безкоштовна програма, Laverna, взагалі не використовує централізовані сервера для зберігання інформації. Якщо використовується браузерна версія, то дані зберігаються локально у базі даних веб-переглядача. Також є можливість синхронізувати свої дані із аккаунтом DropBox чи RemoteStorage. Шифрування відбувається за алгоритмом AES, при першому використанні програми користувач повинен ввести пароль, на основі якого потім буде генеруватися ключ. Графічний інтерфейс програми простенький, без прикрас. Немає мобільної версії.

Враховуючи постійний розвиток технологій, впровадження їх у всі сфери людської діяльності зростає необхідність захисту інформаційних систем та інформації що обробляється в них. А отже, захист інформації є невирішеною проблемою, яка буде актуальною завжди. Це дозволяє стверджувати, що доцільним є проведення дослідження, присвяченого розробки програмного забезпечення, що буде надійно зберігати інформацію в інформаційно-комп'ютерних системах. Розроблена програма здійснює шифрування даних у стані спокою («data at rest») [9]. Тобто, дані зберігаються у базі даних програмного забезпечення, змінюються лише тоді, коли з ними працює користувач.

3. Мета та завдання дослідження.

Метою даної статті є розробка і створення програми для безпечного зберігання текстової інформації на базі мови програмування Python. Дана програма є захищеною та непомітною шляхом приховання її існування в алгоритмі роботи іншої непримітної програми.

Для досягнення поставленої мети необхідно виконати наступні завдання:

– проаналізувати переваги та недоліки наявного програмного забезпечення, яке вирішує проблеми захисту конфіденційної інформації користувача за допомогою криптографії та розробити алгоритм, який буде усувати недоліки;

– розробити програму згідно запропонованого алгоритму;

– провести тестування розробленої програми, швидкодії алгоритму шифрування.

4. Матеріали та методи дослідження.

Головним і базовим компонентом для створення програмного продукту і його подальшого дослідження виступає високорівнева мова програмування Python, розроблена Гвідо ван Россумом.

До переваг даної мови програмування можна віднести дуже величезну кількість пунктів. Перш за все, це чистий синтаксис написання програмного коду і поширення самої мови програмування під ліцензією "відкритого коду". Це надає можливість редагувати і покращувати середовище Python іншим користувачам, які зацікавлені в допомозі розвитку даної мови програмування. Можна використовувати її в інтерактивному режимі через командний рядок, що дає змогу вирішувати прості завдання та проводити експерименти. Python – мова програмування сценаріїв (скриптів). Це дозволяє об'єднувати кілька файлів сценаріїв у один робочий і повноцінний проект [10].

Найголовнішим плюсом Python є те, що мова програмування також містить в собі дуже потужні додаткові модулі, які допомагають в розв'язанні складних математичних задач, навіть з комплексними числами. Це дозволяє використовувати Python як потужний калькулятор.

Розробники та користувачі мови Python весь час працюють над написанням різноманітних сторонніх модулів (або бібліотек) для виконання різних задач. Завдяки цьому Python є дуже гнучкою і використовується для написання застосунків практично для всіх сфер діяльності людини. Дану мову програмування можна використовувати для створення як локальних програмних продуктів, так і для роботи із веб-застосунками та хмарними середовищами [10].

При розробці програми «Нотатки» використовувалося середовище Python 3.8 та різноманітні допоміжні бібліотеки.

Графічний інтерфейс програми – це компонент, із яким взаємодіє напряму користувач програми. Графічний інтерфейс спрощує використання користувачем функцій програми та зазвичай є інтуїтивно зрозумілим. Він містить різні текстові написи, кнопки, при натисканні на які, буде виконуватися певна функція, записана в коді програми та інші елементи, наприклад для відображення інформації. Під час розробки програми для заміток використовувалася стандартна бібліотека Tkinter. Вона була написана Стіном Лумгольтом і Гвідо ван Россумом, потім була перероблена Фредріком Лундом. До переваг бібліотеки можна віднести:

– кросплатформність, тобто написаний код інтерфейсу буде працювати як на Windows, так і Linux-подібних операційних системах;

– візуальні елементи відображаються з використанням нативних елементів операційної системи, тому програми виглядають так, ніби вони належать платформі, на якій вони запускаються;

– споживає мало ресурсів комп'ютера.

До недоліків часто відносять власне зовнішній вигляд елементів графічного інтерфейсу, який вважають трохи застарілим. Проте на функціонал програми це ніяк не впливає [11].

Текстова інформація, яку обробляє програма для нотаток буде зберігатися у базі даних. Для роботи з базою даних використовується бібліотека sqlite3, написана Герхардом Гарінгом. Дана бібліотека також входить в стандартний пакет бібліотек мови програмування Python. Головне її призначення – це взаємодія з базою даних. До функціональних особливостей даної бібліотеки можна виділити:

– створення і встановлення з'єднання із базою даних;

– створення таблиці з різними полями, вибираючи при цьому тип даних, які будуть зберігатися в кожному окремому полі таблиці;

– можливість редагування даних, які зберігаються у базі.

Криптографічний алгоритм RSA є одним із найпопулярніших базових асиметричних криптоалгоритмів, який базується на відкритому ключі. Даний алгоритм був створений у 1978 році. В основі даного методу лежить складність факторизації величезних чисел, тобто обчислювальна важкість виконання такої операції. Даний алгоритм може бути використаний не тільки для шифрування та

розшифрування тексту, а і для цифрового підпису, який використовується для підтвердження отриманих даних і перевірки, чи не були вони видозмінені або спотворені під час передачі по мережі [12].

5. Результати дослідження та розробки програмного забезпечення.

5.1. Результати аналізу наявних програмних продуктів та опис запропонованого алгоритму захисту інформації.

Аналіз наявного різноманітного програмного забезпечення показує, що пріоритетним є захист інформації користувачів, для чого використовуються криптографічні засоби захисту. Невирішеною залишається проблема захисту самої програми для нотаток. Сам факт наявності такої програми на пристрої користувача дає зловмиснику додаткові вектори атаки:

– він може пошукати базу даних програми для нотаток;

– можливо користувач десь записав на видному місці свій пароль до програми, і тоді потрібно лише знайти її на пристрої і відкрити;

– програми-шпигуни можуть вмикатися при певних діях користувача, наприклад відкритті програми Evernote, і записувати зображення екрану.

Саме тому пропонується наступний алгоритм побудови програми для нотаток:

1. Дані зберігатимуться у локальній базі даних;
2. Дані будуть шифруватися до їх відправки у базу даних;
3. Для шифрування використовуватиметься криптоалгоритм на основі RSA для більшої надійності;
4. Програма для нотаток буде схована під виглядом якоїсь іншої програми, яка б не викликала підозр.

5.2. Результати розробки програми для нотаток.

Використовуючи визначені методи та засоби дослідження (мову програмування Python, її бібліотеки та криптографічний алгоритм RSA), розроблено програмне забезпечення «Нотатки» із безпечним зберіганням даних. Воно являє собою кінцевий програмний продукт. Дана програма складається з декількох складових програмних компонентів. Вона поділяється на:

– програмний компонент для приховання функціоналу основної програми;

– безпосередньо програму для зберігання зашифрованих даних;

– алгоритм, за допомогою якого шифрується текстова інформація.

Всі програмні компоненти розроблені на мові програмування Python, з використанням бібліотеки Tkinter для графічного інтерфейсу та бібліотеки sqlite3 для взаємодії з базою даних.

В ролі програми, що слугує для приховання основного функціоналу, виступає програмний компонент «Калькулятор». Графічний інтерфейс програми «Калькулятор» зображено на рисунку 1. Його опис міститься у класі Interface() файлу Interface.py. У цьому класі визначені поле для введення даних та виведення результату обрахунків та кнопки, при натисканні на які вводяться дані та виконуються математичні операції.

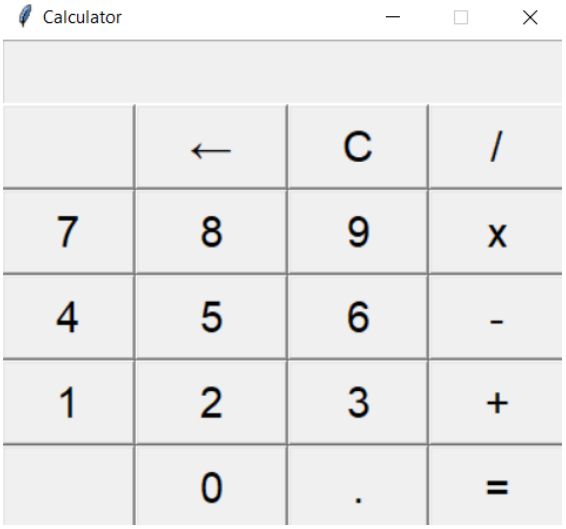
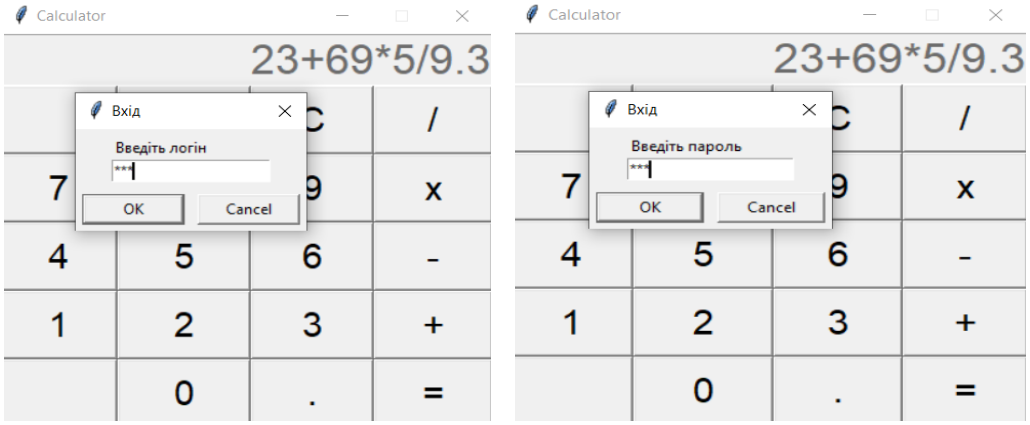


Рис. 1. Графічний інтерфейс програми «Калькулятор».

Головний функціонал програми «Калькулятор» розташований у файлі function.py. В ньому створюється і запускається екземпляр класу Interface(), який відповідає за відображення графічного вікна. Інші функції файлу function.py відповідають за правильність виконання основних математичних дій: додавання, віднімання, ділення та множення. Функція equal() видає кінцевий результат обрахунку. Програма «Калькулятор» є цілком самостійною і тому для звичайного користувача або зловмисника вона не виглядатиме підозрілою. Однак, дана програма є першим рівнем захисту основного програмного компонента.

У функції equal() також записаний виклик програми «Нотатки». Для того, щоб її відкрити, необхідно ввести певну послідовність символів. Вона у свою чергу відкриває вікно авторизації для введення логіну та паролю (рисунок 2а та рисунок 2б). Воно створено для того, щоб підтвердити легітимність особи користувача, так як послідовність символів можна підгледіти – це ще один рівень захисту. Користувач спочатку вводить логін, а потім у ще одному окремому вікні – пароль.



а) б)

Рис. 2. Вікна авторизації програми: а – вікно для вводу логіна;
б – вікно для вводу пароля.

Коли мова йде про захист конфіденційної (приватної) інформації користувача, не варто нехтувати тим, що комбінація символів, яка відкриває вікно авторизації, може бути випадково набрана будь-яким іншим користувачем. Тому варто використовувати складну та довгу комбінацію, також бажано, щоб числа і дії над ними не були якимось очевидним стандартним вибором. Рекомендується використовувати дробові числа та як мінімум дві різні математичні операції. Так само рекомендується, щоб пароль користувача був довжиною як мінімум 8 символів, містив літери верхнього та нижнього регістрів, цифри і можливо спецсимволи.

Визначена послідовність для відкриття діалогових вікон для авторизації, значення логіну та паролю записані саме у коді функції equal(). Якщо користувач правильно ввів всі три значення, вікно програми «Калькулятор» закривається. Відбувається виклик функція start_program(), імпортованої з файлу Nfunction.py, яка запускає програму для заміток (рисунок 3).

Графічний інтерфейс програми описаний у файлі Main_Window.py. Тут описаний клас Main_Window, який містить в собі елементи графічного вікна. Задаються відповідні параметри для інтерфейсу, а саме розмір вікна, назва і відключається можливість змінювати розміри вікна. Також створюються елементи, які будуть відображатися у вікні програми:

– кнопки, при натисканні на які будуть виконуватися певні функції;

– списки з можливістю вибору із переліку теми користувача та відповідні їм замітки;

– а також поле для вводу і виводу тексту, який буде зберігатися в базі даних.

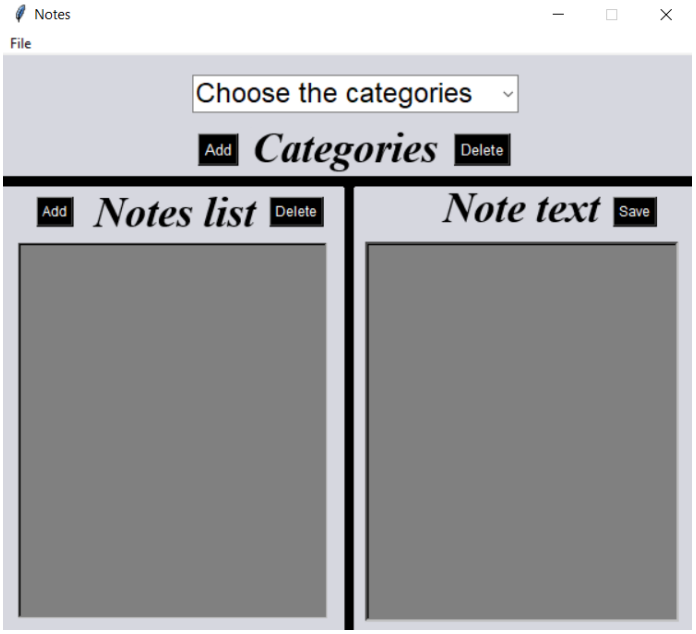


Рис. 3. Графічний інтерфейс програми «Нотатки».

Програмний компонент «Нотатки» виконує функцію створення, редагування, видалення текстових заміток на різноманітні теми (“Categories”), теж створені користувачем. Програма взаємодіє із базою даних для збереження, оновлення або витягнення інформації з неї, в залежності від бажаної функції.

Клас Categories містить в собі функції, які відповідають за взаємодію з базою даних за допомогою бібліотеки sqlite3. Запити до бази даних передаються на мові SQL (Structured Query Language), інформація, що повертається, відображається у вікні програми. Типи запитів, які використовуються:

– створення та видалення таблиць (CREATE і DROP);

– створення, оновлення та видалення полів у таблицях (INSERT, UPDATE, DELETE);

– вибірка інформації із таблиць для відображення (SELECT);

Для кожної теми (“category”) створюється окрема таблиця. Таблиця має наступні поля: id (автоматично додано), notes_name (заголовок нотатки), notes_text (текст нотатки). Схема таблиці зображена на рисунку 4.

Category 1		
id	notes_name	notes_text
1	Note 1	My first note
2	Note 2	My second note
…	…	…

Рис. 4. Схема таблиці у базі даних програми.

В процесі передачі даних від користувача у базу, відбувається шифрування текстової інформації. Зберігається інформація у зашифрованому вигляді. Відповідно, при відкритті певної замітки із бази даних витягується зашифрована інформація, дешифрується і відображається користувачу в звичайному текстовому вигляді.

Алгоритм передачі і отримання даних із бази даних програми включає в себе також і процес шифрування та дешифрування цих даних. Алгоритм шифрування даних реалізовано згідно математичного опису криптографічного алгоритму RSA. У файлі Algorithms.py заданий клас Algorithms(), функції якого відповідають за шифрування та дешифрування інформації.

Важливою складовою кожного алгоритму і процесу шифрування та розшифрування є ключі. Для стійкості шифру варто використовувати ключі довжиною як мінімум 1024 біт, щоб виключити можливість їх взлому.

Основним файлом програми є Nfunction.py. У нього імпортуються файли Main_Window.py, Categories.py та Algorithms.py для відображення вікна програми, шифрування інформації та взаємодії із базою даних. У цьому файлі функція start_program() запускає програму. Решта визначених функцій віповідають за додавання чи видалення тем, додавання, зміну та видалення нотаток. Робоче вікно програми «Нотатки» вже із деякими створеними нотатками зображено на рисунку 5.

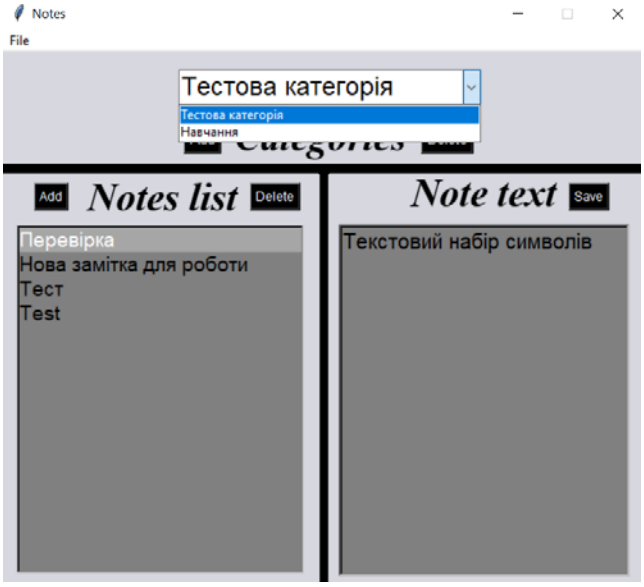


Рис. 5. Функціональна робота програми «Нотатки».

5.3. Результати тестування розробленої програми, швидкодії алгоритму шифрування.

Обидва програмні компоненти, як «Калькулятор» так і «Нотатки», містять багато перевірок на помилки вводу від користувачів.

Розглядаються ситуації, коли користувач під час введення назви теми для групи заміток, чи назви або тексту самої замітки залишає поле для тексту порожнім. У такому випадку з'являється вікно помилки, а хибний запис не створюється (рисунок 6). Також не можна створювати нотатки з ідентичними назвами. При успішному створенні теми чи нотатки, користувач отримує відповідне сповіщення. Якщо користувач натискає кнопку видалення нотатки, то програма додатково запитує про підтвердження дії, щоб уникнути випадкового видалення (рисунок 7).

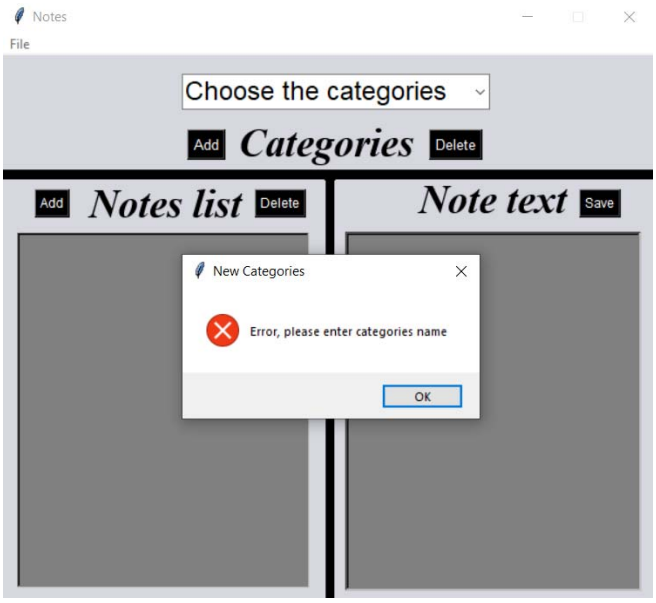


Рис. 6. Вікно помилки при введені порожнього значення.

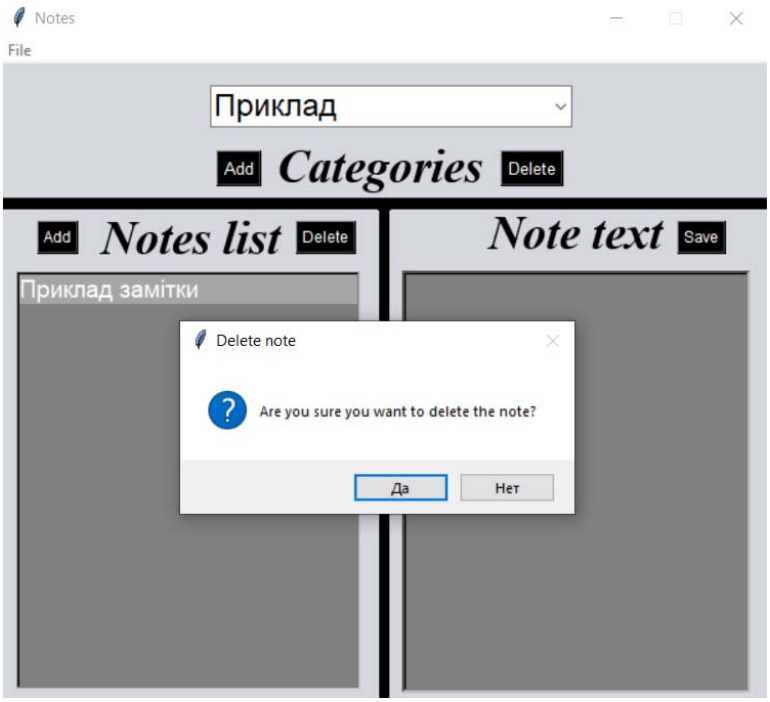


Рис. 7. Запит на підтвердження видалення нотатки.

У випадку програми «Калькулятор» відбуваються перевірки на коректність математичного виразу, введеного користувачем – якщо він все-таки вирішить щось порахувати. Не можна ввести «.», якщо попередній символ не цифра. Також не можна почати математичний вираз із знаку математичної дії, а саме «+», «-«, «*», «/». Також при натисканні на знак математичної дії програма перевіряє попередній введений користувачем символ. Якщо попередній символ був знаком дії, то він замінюється на щойно натиснений користувачем.

Однією із головних характеристик процесу шифрування є швидкодія алгоритму. У таблиці 1 наведений виміряний час, який витрачається на шифрування відкритого повідомлення та його розшифровування. Використовуються ключі довжиною 1024 біт. Очікувано, що із збільшенням кількості символів повідомлення, зростає і час роботи програми.

Таблиця 1.

Час, який витрачається на шифрування та розшифрування повідомлення різної довжини

Кількість вхідних символів	Час шифрування	Час розшифрування
10	0,01 с	0,03 с
100	0,02 с	0,51 с
500	0,05 с	2,51 с
1000	0,08 с	5,01 с
2000	0,18 с	10,5 с

Розробка і тестування програми відбувалися у середовищі ОС (операційної системи) Windows 10. Перемикання між компонентами «Калькулятор» і «Нотатки» відбувається згідно визначеного алгоритму послідовність символів – логін – пароль. Самі програмні компоненти працюють коректно в межах заданих функцій. Взаємодія із базою даних також відбуваються правильно, вибирається тільки та інформація, яку користувач запитав. Час роботи алгоритму шифрування нотаток є прийнятним. Також обидва програмні компоненти коректно реагують на помилки користувача.

6. Обговорення результатів розробки програми для заміток «Нотатки».

Після проведення аналізу різноманітного програмного забезпечення для створення та зберігання нотаток були отримані такі результати:

– інформація користувачів захищається за допомогою криптографічних засобів захисту на віддалених серверах чи у локальних базах даних;

– такого захисту не завжди достатньо, так як зловмисник може використати вразливості самої програми або помилки користувача для атаки;

Ці отримані результати пояснюються тим, що навіть попри те, що дуже велика кількість приватної інформації зберігається у електронному вигляді, розробники ПЗ більше уваги приділяють інтерфейсу і функціоналу програм. Безпеці даних користувача не приділяється достатньої уваги, на відміну від зручності використання ПЗ та його красивого оформлення.

Розроблена прихована програма для заміток «Нотатки» із безпечним зберіганням даних (рисунки 3, 5). Для захисту інформації використовується шифрування на основі алгоритму RSA. Програма має багато рівнів захисту. Окрім шифрування, налаштований також парольний захист. Проте суттєвою відмінністю розробленого програмного забезпечення є те, що приховується сам факт існування програми для нотаток на комп’ютері користувача. Програма для нотаток може бути запущена тільки після введення певної послідовності символів у поле програми-калькулятора, яка також є складовою розробленого програмного забезпечення (рисунки 1, 2). Це додає ще один рівень захисту даних користувача.

Тестування програми за позитивним сценарієм показало, що її функції виконуються як очікувано. За негативним сценарієм виводяться повідомлення про помилки. Вимірювання часу роботи алгоритму шифрування заміток користувача показує, що він цілком прийнятний (таблиця 1).

Автор статті [13] описує найкращі практики при розробці програмного забезпечення із захищеним зберіганням даних. Деякі з цих практик були дотримані, а саме розробка із врахуванням можливих дій користувача та ретельне тестування програми. Проте, на відміну від статті [13], був розроблений не веб-застосунок, а повноцінна програма для нотаток із локальним зберіганням даних у зашифрованому вигляді.

Розроблене під час дослідження програмне забезпечення цілком виконує свої визначені завдання: надійно захищає приватну інформацію користувача і при цьому є схованим від зловмисника. Це пояснюється використанням

алгоритму шифрування на основі RSA та існування додаткового програмного компоненту «Калькулятор» для приховування існування програми «Нотатки».

Як видно із таблиці 1, час дешифрування повідомлення більший, ніж час шифрування. Відповідно, розмір заміток все-таки має значення, так як дешифрування досить великої замітки користувача займе багато часу. В першу чергу, дане обмеження пов'язане з концепцією розробки і використання програми. Однак, навіть при розшифруванні великого розміру замітки, хоча час і буде дещо завеликим, але при цьому можна знехтувати швидкодією програми на користь стійкості та захисту.

Основним недоліком є те, що розроблена програма працює лише на операційних системах, що використовуються на персональних або портативних комп'ютерах. Тобто, використання її на мобільних пристроях неможливе, адже не існує версії для операційних систем Android чи iOS.

Розвиток даного дослідження полягатиме у покращенні швидкодії алгоритму шифрування. Також варто зробити графічний інтерфейс більш привабливим для користувача.

7. Висновки.

1. Аналіз популярних програм для нотаток показав, що недостатня увага приділяється захисту даних користувача. Тому встановлено необхідність розробки захищеного програмного забезпечення із безпечним зберіганням інформації. Запропоновано наступний алгоритм:

– використання криптографічного захисту на основі шифрування RSA;

– захист самої програми шляхом приховання її присутності на пристрої користувача.

2. Згідно запропонованого алгоритму, розроблено програмний застосунок для безпечного зберігання даних користувача. Компонент «Калькулятор» приховує існування компоненту «Нотатки». Для доступу до програми «Нотатки» потрібно пройти парольну автентифікацію (рисунки 2а, 2б). Сама програма «Нотатки» реалізує безпечне зберігання приватної інформації користувача у своїй базі даних за допомогою криптографічного методу захисту (рисунки 3, 5).

3. Тестування показує, що програма «Нотатки» цілком коректно виконує визначені функції, зберігаючи та захищаючи інформацію користувача. Перехід від програми «Калькулятор» до програми «Нотатки» відбувається тільки із введенням правильних символьної послідовності, логіну та паролю. Також обидва програмні компоненти правильно реагують на помилки користувачів (рисунки 6, 7). Час виконання процесу шифрування та розшифрування повідомлення зростає із збільшенням довжини повідомлення, але є цілком прийнятним (таблиця 1).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NIST SP 800-175B Rev. 1 https://doi.org/10.6028/NIST.SP.800-175Br1.

2. Martin, K. (2017). Everyday Cryptography: Fundamental Principles and Applications (2nd ed.). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199695591.001.0001.

3. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781351133036.

4. Application Level Encryption for Software Architects. Retrieved May 23, 2022 from InfoQ website: https://www.infoq.com/articles/ale-software-architects/.

5. Cryptography In Software Or Hardware - It Depends On The Need. Retrieved May 23, 2022 from Maxim Integrated website: https://www.maximintegrated.com/en/design/technical-documents/tutorials/5/5421.html.

6. Nigm, El Sayed & El-Rabaie, El-Sayed & Faragallah, Osama & Mousa, Ayman. (2010). Cryptography and Database Security: Concepts, Compliance Risks and Technical Challenges Retrieved June 14, 2022 from ResearchGate website: https://www.researchgate.net/publication/263754046_Cryptography_and_Database_Security_Concepts_Compliance_Risks_and_Technical_Challenges.

7. Wolfe M. (2010) MySQL vs. SQLite Exploring the differences between two popular databases. Retrieved June 15, 2022 from Towards Data Science website: https://towardsdatascience.com/mysql-vs-sqlite-ba40997d88c5.

8. The 5 Best Secure Encrypted Notes Apps for Truly Private Notes. Retrieved May 31, 2022 from MUO – Technology, Simplified website: https://www.makeuseof.com/tag/encrypted-alternatives-evernote/.

9. Data At Rest Encryption. Retrieved May 23, 2022 from IBM website: https://www.ibm.com/docs/en/strategicsm/10.1.3?topic=security-data-rest-encryption.

10. Анісімов А. В., Дорошенко А. Ю., Погорілий С. Д., Дорогий Я. Ю. (2014) Програмування числових методів мовою Python. Видавничо-поліграфічний центр "Київський університет".

11. Python GUI Programming With Tkinter. Retrieved May 23, 2022 from Real Python website: https://realpython.com/python-gui-tkinter/.

12. Burnett, S., Paine, S. (2001). RSA Security's Official Guide to Cryptography. Osborne/McGraw-Hill.

13. Best practices for secure application development. Retrieved June 06, 2022 from Synopsys website: https://www.synopsys.com/blogs/software-security/secure-application-development-best-practices/.

УДК 004.056.55:519.876.5

ОГЛЯД ОСНОВНИХ ЗАДАЧ, ЯКІ МОЖНА ВИРІШУВАТИ ЗА ДОПОМОГОЮ СТЕГАНОГРАФІЇ

Мартинюк Г.В.
к.т.н., доцент, доцент
кафедра засобів захисту інформації
Національний авіаційний університет
ganna.martyniuk@gmail.com

Мелешко Т.В.
старший викладач
кафедра засобів захисту інформації
Національний авіаційний університет
sorokunnet@ukr.net

Бичков В.В.
старший викладач
кафедра засобів захисту інформації
Національний авіаційний університет
volodymyr.bychkov@npp.nau.edu.ua

Анотація. У роботі наводяться особливості поширених методів стеганографії. Розглядаються вимоги до стеганосистем. Особлива увага приділяється основним задачам та областям застосування методів відкритої стеганографії.

Стеганографія – це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі [1]. На відміну від криптографії, що приховує вміст секретного повідомлення, стеганографія приховує факт його існування. Як правило, повідомлення буде виглядати як щось інше, наприклад, як зображення, стаття, список покупок, аудіо- або відеофайл. Перевагою стеганографічних методів є те, що тільки цільові одержувачі стегоконтейнера можуть отримати приховане повідомлення [2]. Третя сторона не буде знати про наявність прихованих даних у повідомленні. Стеганографію зазвичай використовують разом із методами криптографії, в такий спосіб, доповнюючи її.

Перевага стеганографії над чистою криптографією у тому, що повідомлення не привертають до себе уваги. Криптографія захищає зміст повідомлення, а стеганографія захищає сам факт наявності будь-яких прихованих посилань.

Можливості стеганографії вражають. Так, наприклад, зміна у 1% оцифрованого звуку (частота дискретизації 44100 Гц, 8-бітний рівень відліку, стерео-режим) дозволяє приховати повідомлення у 10 Кбайт [1]. Причому, людина нічого не помітить при прослуховуванні.

Інтерес до стеганографії відродився в останнє десятиліття і був викликаний широким поширенням технологій мультимедіа, що цілком закономірно, беручи

до уваги проблеми, пов'язані із захистом інформації. Не менш важливим стала поява нових типів каналів передачі інформації, що в сукупності з першим фактором дало новий імпульс розвитку та удосконаленню стеганографії, сприяло виникненню нових стеганографічних методів, в основу яких були покладені особливості подання інформації в комп'ютерних файлах, обчислювальних мережах і т. д. Це, у свою чергу, дає можливість говорити про становлення нового напряму у сфері захисту інформації – комп'ютерної стеганографії.

Нижче наведено основні терміни стеганографії.

Стеганографія – це сукупність методів, з допомогою яких додаткова інформація вбудовується в основний, приховуючий об'єкт – контейнер, зі збереженням його належної якості [1].

Контейнер – це деяка інформація, або файл, в який можна вбудувати додаткову інформацію, що не призначена для використання сторонніми користувачами.

Належна якість контейнера після вбудовування – це збереження тих його основних характеристик, до зміни котрих чутливі органи відчуттів людини.

Типовими варіантами контейнерів є: нерухоме зображення, відеозаписи, потокове відео, аудіозаписи, змістовний друкований текст, Інтернет-протоколи, програмне забезпечення.

У більшості стеганосистем для вбудовування та витягнення повідомлень використовується ключ, що визначає секретний алгоритм, який визначає порядок внесення повідомлення в контейнер. За аналогією із криптографією, тип ключа спричиняє існування двох типів стеганосистем:

- з секретним ключем – використовується один ключ, що визначається до початку обміну стеганограмою або передається захищеним каналом;
- з відкритим ключем – для пакування та розпакування повідомлення використовуються різні ключі, які відрізняються таким чином, що за допомогою обчислень неможливо одержати один ключ із іншого, тому один із ключів (відкритий) може вільно передаватися по незахищеному каналу.

Ще одним розповсюдженим методом стеганографії є метод використання цифрових водяних знаків (ЦВДЗн). Цифрові водяні знаки забезпечують захист авторських прав на цифровий ІР, який включає програмування, зображення, звукозаписи та відео. Цифрові водяні знаки не можна виявити неозброєним оком, але служать сигналами під час завантаження чи відтворення матеріалів, захищених авторським правом.

Найбільш надійні цифрові водяні знаки випадковим чином поширюють бітові дані в захищеному захищеним авторським правом матеріалі. Для досягнення оптимального ефекту цифрові водяні знаки повинні бути неперетворюваними та підтримувати зміни, включаючи скорочення алгоритму або переформатування файлів.

Процес вбудовування ЦВДЗн проілюстровано на рисунку 1.

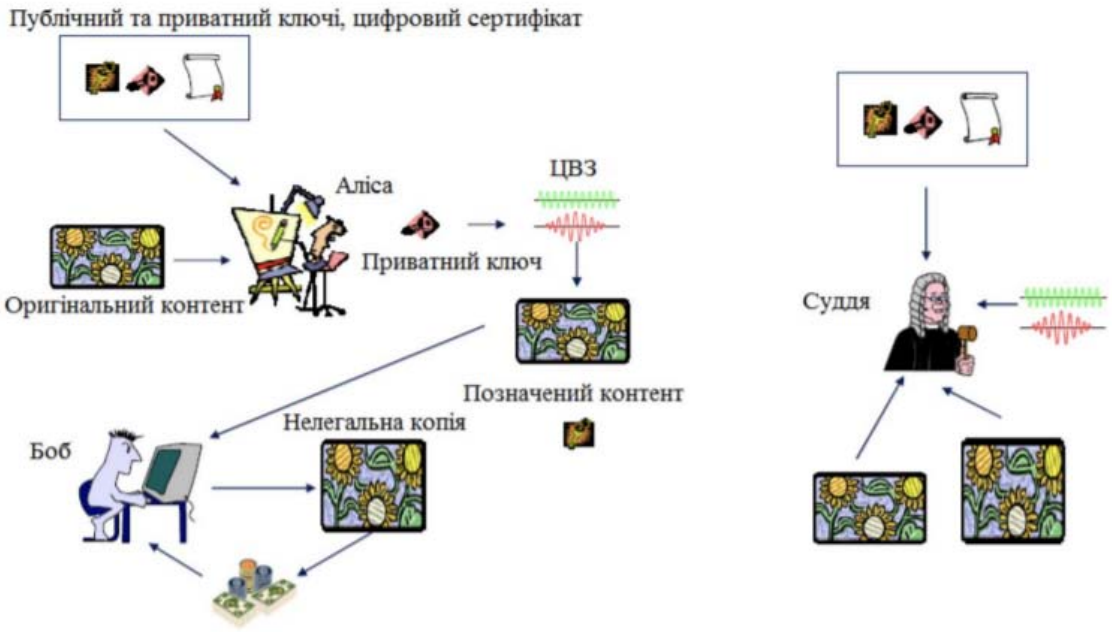


Рис. 1. Блок-схема процесу вбудовування ЦВДЗн
з метою захисту авторських прав.

Яким б різними не були напрями стеганографії, пропоновані ними вимоги багато в чому збігаються. Найбільш істотна відмінність постановки завдання прихованої передачі даних від постановки завдання вбудовування цифрового водяного знаку (ЦВДЗн) полягає в тому, що в першому випадку зловмисник повинен виявити приховане повідомлення, тоді як у другому випадку про його існування всі знають. Більше того, у зловмисника на законних підставах може бути пристрій виявлення ЦВДЗн.

Отже, у стеганосистемі відбувається об’єднання двох типів інформації таким чином, щоб вони по-різному сприймалися принципово різними детекторами. У якості одного з детекторів виступає система виділення прихованого повідомлення, у якості іншого – людина.

Алгоритм вбудовування повідомлення в найпростішому випадку складається із двох основних етапів:

- Вбудовування в стегакодері секретного повідомлення в контейнероригінал.
- Виявлення (виділення) у стеганодетекторі (декодері) прихованого зашифрованого повідомлення з контейнера-результату.

Виходячи із цього, слід розглянути математичну модель стеганосистеми. Процес тривіального стеганографічного перетворення описується залежностями:

$$E : C \times M \qquad (1)$$

$$D : S \rightarrow M, \qquad (1)$$

де $S = \{(c_1, m_1), (c_2, m_2), ..., (c_n, m_n), ..., (c_q, m_q)\} = \{s_1, s_2, ..., s_q\}$ – множина контейнерів-результатів (стеганограм).

Залежність (1) описує процес приховання інформації, залежність (1) – витягнення прихованої інформації. Необхідною умовою при цьому є відсутність "перетинання", тобто, якщо $m_a \neq m_b$, причому $m_a, m_b \in M$, а $(c_a, m_a), (c_b, m_b) \in S$, то $E(c_a, m_a) \cap E(c_b, m_b) = \varnothing$.

Крім того, необхідно, щоб потужність множини $|C| \geq |M|$. При цьому обидва адресати (відправник і одержувач) повинні знати алгоритм прямого (E) і зворотного (D) стеганографічних перетворень.

Отже, у загальному випадку стеганосистема – це сукупність $\Sigma = (C,M,S,E,D)$ контейнерів (оригіналів і результатів), повідомлень і перетворень, які їх пов'язують.

Для більшості стеганосистем множина контейнерів C вибирається таким чином, щоб у результаті стеганографічного перетворення (1) заповнений контейнер і контейнер-оригінал були подібні.

На сьогоднішній день існує велика кількість стеганографічних методів [1-5], проте, необхідно відмітити, що майже всі такі методи реалізовані тільки при використанні двох контейнерів: зображення та аудіосигналу.

Зображення чи аудіофайли вибирають в якості контейнера по ряду причин:

- великий обсяг цифрового представлення контейнера, що дозволяє приховувати повідомлення великого обсягу або підвищувати стійкість впровадження;
- наперед відомий розмір контейнера, відсутність обмежень, що накладаються вимогами реального часу;
- наявність у більшості реальних зображень текстурних областей, що мають шумову структуру і добре підходять для вбудовування інформації;
- слабка чутливість людського ока до незначних змін кольорів зображення чи незначних змін в аудіосигналі.

Нижче буде надано більш детальну інформацію про використання такого виду контейнерів.

Аудіосигнали. Для впровадження інформації в аудіосигнали, необхідно визначити вимоги, які можуть бути пред'явлені до стеганосистем, які застосовуються для вбудовування інформації в аудіосигнали:

- інформація, що приховується, повинна бути стійкою до наявності різних пофарбованих шумів, стиснення з втратами, фільтрування, аналоговоцифрового та цифро-аналогового перетворень;
- інформація, що приховується, не повинна вносити в сигнал спотворення, що сприймаються системою слуху людини;
- спроба видалення інформації, що приховується, повинна призводити до помітного пошкодження контейнера (для ЦВДЗ);
- інформація, що приховується, не повинна вносити помітних змін до статистики контейнера.

Для впровадження інформації в аудіосигнали можна використовувати методи, що застосовуються в інших видах стеганографії.

Наприклад, можна впроваджувати інформацію, заміняючи найменш значні біти (всі або деякі). Або можна будувати стеганосистеми, ґрунтуючись на особливостях аудіосигналів та системи слуху людини.

Систему слуху людини можна уявити, як аналізатор частотного спектра, який може виявляти і розпізнавати сигнали діапазоні 10 – 20000 Гц. Систему слуху людини можна змоделювати, як 26 фільтрів, що пропускають, смуга пропускання, яких збільшується зі збільшенням частоти.

Система слуху людини розрізняє зміни фази сигналу слабше, ніж зміни амплітуди чи частоти.

Аудіосигнали можна розділити на три класи:

- розмова телефонної якості, діапазон 300 – 3400 Гц;
- широкосмугове мовлення 50 - 7000 Гц;
- широкосмугові аудіосигнали 20 – 20 000 Гц.

Зображення. Ефект маскування в просторовій множині може бути пояснений шляхом побудови стохастичних моделей зображення. При цьому зображення представляється у вигляді марківського випадкового поля.

Таким чином, можна запропонувати таку узагальнену схему впровадження даних у зображення:

1. Виконати фільтрацію зображення за допомогою орієнтованих смугових фільтрів. При цьому одержимо розподіл енергії по частотнопросторових компонентах.

2. Обчислити поріг маскування на основі знання локальної величини енергії.

3. Масштабувати значення енергії впроваджуваного ЦВДЗ у кожному компоненті так, щоб воно було менше порога маскування.

Високорівневі властивості зорової системи людини (ЗСЛ) поки рідко враховуються при побудові стеганоалгоритмів. Їх відмінністю від низькорівневих є те, що ці властивості проявляються «удруге», обробивши первинну інформацію від ЗСЛ, мозок видає команди на її «підстроювання» під зображення.

З огляду на це, нижче наведено основні властивості зорової системи людини:

1. Чутливість до контрасту. Висококонтрастні ділянки зображення, перепади яскравості привертаються до себе значну увагу.

2. Чутливість до розміру. Більші ділянки зображення «помітніші» менших за розміром. Причому, існує поріг насичення, коли подальше збільшення розміру не істотне.

3. Чутливість до форми. Довгі й тонкі об’єкти привертають більшу увагу, ніж круглі однорідні.

4. Чутливість до кольору. Деякі кольори (наприклад, червоний) «помітніші» інших. Цей ефект підсилюється, якщо тло заднього плану відрізняється від кольору фігур на ньому.

5. Чутливість до місця розташування. Людина схильна в першу чергу розглядати центр зображення.

6. Люди звичайно уважніше до зображень переднього плану, ніж заднього.

7. Якщо на зображенні є люди, в першу чергу людина зверне свою увагу на них. На фотографії людина звертає першочергову увагу на особу, очі, рот, руки.

8. Чутливість до зовнішніх подразників. Рух очей спостерігача залежить від конкретної обстановки, від отриманих їм перед переглядом або під час його інструкцій, додаткової інформації.

Для передачі прихованих повідомлень методами стеганографії використовуються спеціальні стеганографічні системи, так звані стегосистеми. Проте, для адекватної їх роботи висувається низка вимог [3]:

1. Безпека системи має повністю визначатися секретністю ключа. Це означає, що порушник може повністю знати всі алгоритми роботи стегосистеми та статистичні характеристики множин повідомлень та контейнерів, і це не дасть йому жодної додаткової інформації про наявність або відсутність повідомлення у цьому контейнері.

2. Знання порушником факту наявності повідомлення у будь-якому контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах.

3. Заповнений контейнер повинен візуально не відрізнятися від незаповненого. Біти повідомлення, яке необхідно приховати, повинні вбудовуватися у візуально значущі області, а відносна непомітність може бути досягнута за рахунок використання спеціальних методів, наприклад, модуляції з розширенням спектра.

4. Стегосистема повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не містить.

5. Повинна забезпечуватися потрібна пропускна спроможність (ця вимога є актуальною, в основному, для стегосистем прихованої передачі інформації).

6. Стегосистема повинна мати прийнятну обчислювальну складність реалізації. При цьому можлива асиметрична за складністю реалізації система, тобто складний стегокодер і простий стегодекодер.

Приклад вбудовування секретної інформації в контейнер реалізовано на рисунку 2.

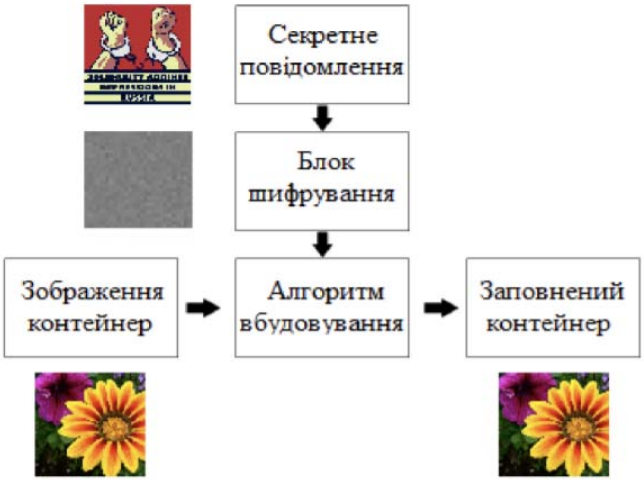


Рис. 2. Ілюстрація алгоритму вбудовування інформації в контейнер.

Для того щоб перейти до обговорення питань впровадження інформації в контейнери, необхідно визначити вимоги, які можуть бути пред'явлені до стеганосистем, які застосовуються для вбудовування інформації:

- інформація, що приховується, повинна бути стійкою до наявності різних пофарбованих шумів, стиснення з втратами, фільтрування, аналогово-цифрового та цифро-аналогового перетворень;
- інформація, що приховується, не повинна вносити в сигнал спотворення, що сприймаються системою слуху або органами зору людини;
- спроба видалення інформації, що приховується, повинна призводити до помітного пошкодження контейнера;
- інформація, що приховується, не повинна вносити помітних змін до статистики контейнера.

Керуючись даними вимогами, можна використовувати різні методи стеганографії для різних контейнерів. Це допоможе приховати інформацію і вирішити основні задачі.

На сьогоднішній день стеганографія використовується для захисту авторських прав, приховання зв'язку, автентифікації, для відстеження порушників (відбитків пальців), додавання додаткової інформації (наприклад, субтитрів до відео), додавання підписів до зображень, захист цілісності зображення (виявлення шахрайства), контроль копіювання при DVD-записі та в інтелектуальних браузерах, для автоматичного надання інформації в доступі та авторських правах, тощо (рисунок 3).

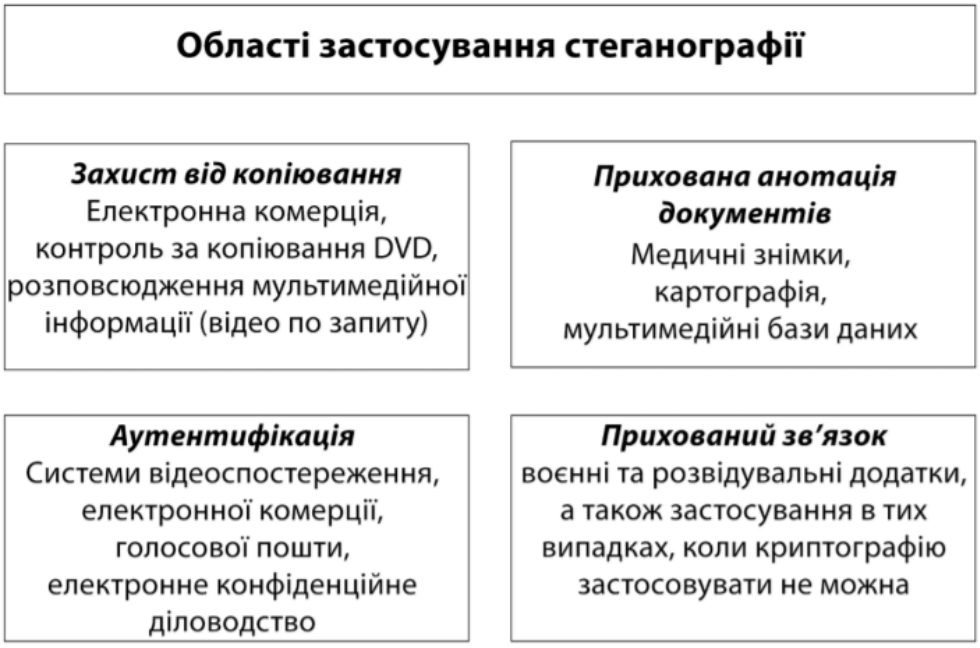


Рис. 2. Основні області застосування стеганографії.

Крім того, авторами було прийнято рішення більш детально описати основні задачі, а також технології та шляхи їх вирішення, які на сьогоднішній день використовують методи стагенографії. Така інформація наведена у таблиці 1.

Таблиця 1.

Основні задачі та області застосування стеганографії

Задача	Технології та шляхи вирішення	Приклад реалізації	Область застосування
1	2	3	4
Захист конфіденційної інформації від несанкціонованого доступу	Вбудовування прихованої інформації у загальнодоступну мультимедійну інформацію	1 секунда оцифрованого звуку (44100 Гц, 8 біт, стерео) дозволяє приховати 5 сторінок текстової інформації, зміна значень відліків становить 1%	Військові та інші додатки, а також застосування у випадках, коли не можна використовувати криптографію
Подолання систем моніторингу та управління мережевими ресурсами	Стегометоди, спрямовані на протидію промисловому шпигунству, дозволяють протистояти контролю над інформацією в комп'ютерних мережах	Група Hacktivismo випустила утиліту Camera/Shy, яка працює не залишаючи в браузері історії діяльності, використовуючи стеганографічну техніку LSB та алгоритм шифрування AES з 256-розрядним ключем, функціонує дуже швидко та дозволяє приховувати повідомлення у gif-файлах. Крім того, ця програма здатна автоматично сканувати HTML-сторінки на наявність графічних зображень з прихованою інформацією	За заявою авторів, ця програма була створена для обходу національних міжмережевих екранів, що дає можливість безпечно обмінюватися будь-яким цифровим контентом через Інтернет.

1	2	3	4
Камуфлювання програмного забезпечення (ПЗ)	У випадках, коли використання ПЗ обмежено, воно може бути закамуфльовано під стандартні програми або приховано у файлах мультимедіа	Використовуються офіційні редактори, звуковий супровід, реклама тощо.	Забезпечується багаторівневий санкціонований доступ до ПЗ
Захист авторського права на інтелектуальну власність від копіювання та автентифікація	Використовуються технології цифрових водяних знаків (ЦВЗ) та ідентифікаційних номерів (ІН)	ЦВЗ вбудовуються в об'єкт, що захищається і можуть бути як видимими, так і невидимими. Вони містять автентичний код, інформацію про власника та керуючу інформацію. Відмінністю ІН від ЦВЗ є те, що будь-яка копія має свій ІН (технологія відбитків пальців)	Використовується для збереження авторського права
Прихована анотація документів та оптимізація банків даних (інформації)	Використовуються технології ЦВЗ та ІН	Інформація в електронних медичних документах, доступна тільки лікарю	Використовується для прихованої анотації документів у медицині, картографії, мультимедійних банках даних, а також для пошуку потрібної інформації

У таблиці 1 також наведено поширені приклади застосування методів стеганографії в залежності від задачі, яку необхідно вирішити.

У роботі наведено основні вимоги, які необхідно виконувати при приховуванні інформації. Автори також структурували використання стеганографічних методів за областю їх застосування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. R. Din. Review on Steganography Methods in Multi-Media Domain / R. Din, M. Mahmuddin, A. J. Qasim // International Journal of Engineering & Technology, 2019 – № 8 (1.7). – p. 288-292.
2. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика [Монографія] / Г.Ф. Конахович, А.Ю. Пузиренко. – К.: "МК-Пресс", 2006. – 288 с.
3. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 232 с.
4. Мартинюк Г.В. Доцільність використання стеганографічного LSB-методу для аудіосигналу / Г.В. Мартинюк, Т.В. Мелешко, А.Д. Сорокун // Актуальні питання забезпечення кібербезпеки та захисту інформації: Матеріали VII міжнарод. наук.-практ. конф., 24–27 лютого 2021 р.: тези доп. – К., 2021. – С. 53-56.
5. Основи комп'ютерної стеганографії: навч. посібн. для студентів і аспірантів / В. О. Хорошко, О. Д. Азаров, М. В. Шелест та ін. – Вінниця : ВДТУ, 2003. – 143 с.
6. A secure, robust watermark for multimedia / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoon // Information hiding: first international workshop. Lecture Notes in Comp. Science. – 1996. – Vol. 1174. – P. 183–206.

УДК 004.056; 004.415.24

МАШИННЕ НАВЧАННЯ ЯК СУЧАСНА ОСНОВА СТЕГАНОАНАЛІЗУ

Кошкіна Н.В.
д.т.н., с.н.с.
провідний науковий співробітник
Інститут кібернетики ім. В.М. Глушкова НАНУ
nata.koshkina@gmail.com

Анотація. У роботі здійснено класифікацію стеганоаналітичних методів за різними критеріями, окреслено місце та особливості методів стеганоаналізу на базі машинного навчання. Описано способи формування тестових наборів контейнерів, переваги та недоліки кожного. Продемонстровано широкий спектр наявних статистичних моделей характеристичних векторів, що концентрують зміни, внесені стеганографічним перетворенням. Виділено та проаналізовано класифікатори, які застосовуються для вирішення задач стеганоаналізу. Здійснено чисельні експерименти, що підтверджують перевагу ансамблевого класифікатора на базі лінійного дискримінанту Фішера над методом опорних векторів з лінійним ядром при роботі з великорозмірними моделями. Описано як наявні класифікатори розширюються на багатокласовий стеганоаналіз.

Вступ.

Основною умовою, яку повинні задовольняти стеганографічні системи, що створені для прихованої передачі даних, є унеможливлення виявлення факту їх експлуатації та доведення цього третім особам. У сучасному світі, де велику роль грає цифрове представлення інформації та можливі різноманітні комбінації методів роботи з даними на цифрових носіях, у стеганографії з'явилося багато нових можливостей і областей застосування. Сучасні стеганографічні системи пропонують різні варіанти організації таємної комунікації під час обміну через публічні канали даними, що не привертають уваги сторонніх спостерігачів. Але така форма комунікації може бути використана для реалізації протиправних дій та стати загрозою інформаційній безпеці як державних, так і комерційних структур. Тому поряд з розвитком стеганографії актуальним та важливим є розвиток протилежного їй напрямку – стеганоаналізу.

Стеганоаналіз розвивається з деяким запізненням відносно стеганографії, про що зокрема свідчить порівняння кількості публікацій, присвячених тим чи іншим проблемам даних дисциплін. Як правило, стеганоаналітик не змінює вміст атакованих сигналів чи зображень, але виявляє наявність в них прихованих повідомлень та в деяких випадках їх об'єм чи зміст. Тобто стеганоаналіз можна розглядати як здійснення пасивних атак на стеганографічні системи. Стеганоаналітичні здобутки можуть бути використаними як для контролю

протиправного використання стеганографічних методів та програмних продуктів, так і для виявлення їх слабкостей, отримання якісних і кількісних оцінок стійкості та подальшого вдосконалення.

Кількість робіт, у яких пропонуються різні стеганоаналітичні методи, останнім часом стрімко збільшується, особливо на зарубіжних теренах. Такий стрибок у розвитку вимагає систематизації виконаних досліджень, здійснення класифікації, аналізу та порівняння наявних методів, виявлення їх переваг і недоліків. Вивчення публікацій останніх років показало, що в левовій частці досліджень стеганоаналіз розглядається як задача класифікації потенційних носіїв прихованих даних (контейнерів). Вона може бути бінарною: 1 клас – пусті контейнери (тобто ті, які не містять прихованих повідомлень); 2 – заповнені контейнери (з прихованими повідомленнями) або стеганограми. І може бути багатокласовою, коли крім факту наявності прихованого повідомлення, визначається задіяний стеганографічний метод і/або довжина повідомлення. Щоб автоматизувати процес класифікації залучаються методи штучного інтелекту, а саме така його підобласть, як машинне навчання.

Машинне навчання було започатковане ще в 50-х роках XX століття, коли з’явився термін «штучний інтелект» – ідея машини, що здатна вирішувати абстрактні задачі без допомоги людини. Першу програму на основі алгоритмів, здатних самонавчатися, розробив А. Самуель в 1959 році, призначена вона була для гри в шашки. А. Самуель дав і перше визначення терміну «машинне навчання»: це «область досліджень розроблення машин, які не є заздалегідь запрограмованими» [1]. Більш точне визначення терміну «навчання» дав набагато пізніше Т.М. Мітчелл: кажуть, що комп'ютерна програма навчається на основі досвіду E по відношенню до деякого класу задач T і міри якості P, якщо якість вирішення завдань з T, виміряна на основі P, поліпшується з набуттям досвіду E [2]. В 1990-х роках XX століття машинне навчання почало бурхливо розвиватися та змінило основний фокус з досягання штучного інтелекту на розв'язання задач практичного характеру. Символьні підходи були відтіснені методами та моделями, запозиченими зі статистики та теорії ймовірності. Потужним поштовхом у розвитку стало збільшення доступності оцифрованих даних та можливість їх розповсюдження через локальні та глобальні комп’ютерні мережі.

Інтерес стеганоаналітиків до методів машинного навчання викликаний можливістю побудови універсальних систем, які придатні для виявлення стеганограм, створених не одним, а багатьма наявними методами комп’ютерної стеганографії. Такі системи не використовують особливості («слабкі місця») того чи іншого алгоритму приховування, а базуються за зборі та порівнянні різних статистичних показників природніх контейнерів та стеганограм. Ключовими для ефективного стеганоаналізу на базі машинного навчання є:

1) множина тестових контейнерів; 2) модель простору ознак контейнера (або його характеристичних векторів); 3) метод класифікації (класифікатор).

Метою даної роботи є огляд, аналіз та систематизація ключових елементів для здійснення стеганоаналізу на базі машинного навчання. Зауважимо, що основна увага приділена проблемі стеганоаналізу зображень, як найбільш поширених контейнерів. Слід зважати, що для інших типів контейнерів будуються свої моделі характеристичних векторів, а от класифікатор може бути використаний один і той же, як для зображень, так і для аудіо- чи відеосигналів, текстових файлів тощо.

Класифікація стеганоаналітичних методів за різними критеріями.

Якість стеганоаналітичного методу в цілому може бути оцінена за наступними показниками: *ефективність*, *придатність*, *практичність* та *складність*. Ефективність відображає точність розрізнення пустих та заповнених контейнерів. При розрізненні можливе виникнення помилок двох типів: прийняття пустого контейнера за заповнений – *хибно позитивна тривога*, та прийняття заповненого контейнера за пустий – *хибно негативна тривога*. Вірогідність виникнення обох типів помилок повинна бути мінімізована. Придатність вимірюється кількістю стеганографічних перетворень, які здатен виявити даний метод стеганоаналізу. Практичність оцінюється широтою сфери практичного застосування методу, можливостями його автоматизації та роботи в реальному режимі часу. Складність є показником необхідних для реалізації програмно-апаратних ресурсів та їх вартості.

В процесі дослідження було виділено декілька базових критеріїв за якими всі існуючі методи стеганоаналізу можна розділити на групи (рисунок 1).

Так, за критерієм мети атаки стеганоаналіз можна класифікувати на три групи:

1) *статичний стеганоаналіз*, тобто такий, що ставить на меті розрізнення пустих та заповнених контейнерів та визначення програми чи методу, за допомогою яких стеганоконтейнери створювалися;

2) *динамічний стеганоаналіз*, тобто такий, що ставить на меті визначення довжини прихованого повідомлення та його місцеположення у стеганоконтейнері, отримання оцінки таємного ключа, певних параметрів алгоритму вкраплення, а також вилучення прихованого повідомлення з контейнера;

3) *допоміжний стеганоаналіз*, тобто розроблення активних та зловмисних атак з метою спровокувати повторну передачу повідомлення.

Рис. 1. Класифікація стеганоаналітичних методів.

Для успішного здійснення стеганоаналізу необхідно, але не достатньо:

- мати для аналізу програмний продукт, за допомогою якого виконувалося приховання інформації;
- мати можливість відновлювати криптографічні та стеганографічні алгоритми, закладені у програмний продукт, виконувати їх експертний аналіз та розробляти методи визначення чи оцінювання ключів;
- мати необхідні для проведення стеганоаналізу обчислювальні ресурси;
- підтримувати на належному рівні теоретичні та практичні знання в області стеганографії.

В залежності від кількості інформації, якою володіє аналітик, виділяють два класи стеганоаналітичних методів: *направлений* стеганоаналіз конкретного програмного забезпечення та *універсальні* методи. При розробленні направлених методів передбачається, що аналітик володіє інформацією про всі деталі приховання, крім використаного стеганографічного ключа. При створенні універсальних методів використання алгоритму вкраплення можливе тільки у режимі «чорного ящику». В таких випадках аналітик намагається відшукати певні особливості пустих контейнерів, що задовольняли б умовам репрезентативності та контекстної незалежності, та одночасно змінювалися при вкрапленні у контейнери додаткової інформації. Універсальні методи, як правило, є менш точними у порівнянні з направленими, але мають значно більшу область застосування.

В залежності від об'єкта пошуку в підозрілих контейнерах стеганоаналітичні методи можна поділити на три класи: *візуальні*, *сигнатурні* та *статистичні*.

Візуальні методи базуються на здатності аналізу зорових образів системою людського зору. Під час візуального стеганоаналізу вивчається графічне представлення бітових зрізів контейнерів-зображень з метою пошуку видимих порушень кореляції всередині пікселя та між пікселями. В окремих випадках інформативним є візуальний контроль однорідних фрагментів зображення,

аналіз артефактів стиснення у збільшеному масштабі чи візуальний аналіз гістограм зображень в просторовій та частотній областях.

Сигнатурні методи направлені на пошук «відбитків пальців», що залишають у заповнених контейнерах деякі стеганографічні програми. Це можуть бути нетипові значення в службових полях або полях даних файлів, невідповідності формату, специфічні для певних стеганографічних програм бітові послідовності та інше.

Порівняно з двома попередніми статистичні методи стеганоаналізу характеризуються значно більшою гнучкістю та широтою області застосування. Вони, як правило, базуються на аналізі розбіжностей у статистичних характеристиках природніх контейнерів та тих, що підлягали стеганоперетворенню і є носіями прихованої інформації.

Першим статистичним методом є «*Хі-квадрат атака*», запропонована в 1999 році в роботі [3] для виявлення стеганографії на базі методу найменшого значущого біту (НЗБ). У цьому методі застосовується критерій згоди Пірсона, на підставі якого відбувається порівняння близькості розподілу досліджуваної послідовності елементів контейнера до розподілу, характерному для стеганограм. «Хі-квадрат атака» дає чудові результати у випадках, коли аналітику відомо, в яких елементах контейнера здійснювалося приховування. Якщо ж стеганосистема передбачає залежні від ключа місця розташування вкраплених бітів, то зі зниженням довжини приховуваного повідомлення ефективність даного методу швидко падає.

Один з перших методів статистичного стеганоаналізу, що враховує можливість залежності місць розташування приховуваних даних від секретного ключа, – це *RS-аналіз* (Regular-Singular), запропонований в роботі [4]. Даний метод спрямований на виявлення прихованих залежностей між елементами контейнера. В розгляд уводяться функції гладкості і перевороту, з використанням яких групи пікселів зображення діляться на три класи: регулярні, сингулярні і невикористовувані. Природні зображення характеризуються великою кількістю регулярних груп у порівнянні з сингулярними. При розрізненні пустих і заповнених контейнерів використовується переворот з накладеною на групу маскою, що складається зі значень -1, 0 і 1. Для природних зображень кількість регулярних груп, отриманих з деякою маскою M приблизно така ж, як і кількість регулярних груп, отриманих з інверсною маскою $-M$. Те ж саме спостереження справедливо і для сингулярних груп. Вкраплення повідомлення в молодші біти контейнера тягне за собою зближення кількості регулярних і сингулярних груп, отриманих з маскою M. Зі збільшенням довжини приховуваного повідомлення різниця між кількістю цих груп наближується до нуля. У той же час різниця між кількістю регулярних і сингулярних груп, отриманих з маскою $-M$ зі збільшенням довжини приховуваного повідомлення збільшується.

Узагальненням RS-аналізу та його формулюванням у дещо інших термінах є метод SPA (Sample Pair Analysis), запропонований в роботі [5].

Методи на базі машинного навчання – це найбільш багаточисленна група статистичних методів. На відміну від «Хі-квадрат атаки», RS-аналізу та SPA такі методи, як правило, є універсальними. Схема стеганоаналізу, за якою визначається ефективність методів цієї групи, містить наступні кроки:

1. *Визначення тестових наборів контейнерів.* Вибір тих чи інших тестових наборів може суттєво вплинути на оцінки точності. Важливими є кількість контейнерів, їх природній вміст, розміри, коефіцієнт стиснення, відсутність чи наявність попередньої обробки (фільтрації, обрізування, обертання тощо) [6]. Щоб отримати достовірні оцінки потрібно мати досить велику кількість контейнерів з відомими мітками класу. Мінімальна кількість складає приблизно 1000 пустих контейнерів, які аналізуються в парах із створеними на їх основі стеганограмами.

2. *Визначення характеристичних векторів контейнерів.* Характеристичний вектор повинен бути чутливим до змін, що вносяться стеганографічними програмами, але при цьому не залежати від вмісту контейнерів. Елементи характеристичних векторів пустих і заповнених контейнерів повинні помітно відрізнятися. Чим більша різниця між ними спостерігається, тим краще такий елемент підходить для цілей стеганоаналізу.

3. *Вибір та навчання класифікатора*. Вибір класифікатора залежить від наявних обчислювальних ресурсів, розмірності характеристичних векторів, кількості контейнерів навчальної вибірки та інших показників. Для цілей стеганоаналізу можуть бути використані як класичні методи машинного навчання з учителем, так і ансамблевий підхід чи найновіші методи глибокого навчання. Якщо не зважати на доступну обчислювальну потужність, то, як правило, чим складніші дані для аналізу, тим складніший метод для них обирається. Також зауважимо, що контейнери навчальної вибірки повинні мати максимально схожі параметри до параметрів контейнерів, класифікація яких є метою стеганоаналізу. Невраховування цього правила зокрема тягне за собою проблему зниження точності стеганоаналізу при переході з лабораторії до реального світу (так звана проблема неспівпадіння джерела контейнерів [6]).

4. *Класифікація контейнерів*, які підлягають перевірці (контрольного набору). Це заключний етап визначення ефективності. Контрольний набір, як і навчальний, зазвичай складається з пар пустий/заповнений контейнер. Крім загальної точності, на цьому етапі можуть бути прораховані відсотки хибно-позитивних та хибно-негативних тривог. Існує також практика випадкового розбиття тестового набору на навчальну і контрольну частину та повторення експериментів декілька десятків або сотень разів, кожного разу з новим випадковим розбиттям. Цей крок дає уявлення про ступінь залежності чисельних

оцінок точності від вихідних даних. Для подальшого коректного стеганоаналізу повинна прослідковуватися дуже незначна залежність.

Розглянемо ключові елементи методів на базі машинного навчання більш детально.

Способи формування тестових наборів зображень.

У науковій літературі в основному використовується три варіанти отримання тестових зображень: 1) загальні («еталонні») набори даних; 2) завантаження зображень із різних інтернет джерел; 3) формування наборів зображень із власних архівів. Кожен із варіантів має свої переваги та недоліки.

Загальні набори даних фігурують у різних областях, зокрема цифровій обробці зображень, проблемах штучного інтелекту, кібербезпеці. Вони дають можливість перевіряти, порівнювати, відтворювати різні методи та алгоритми, що сприяє прозорості та цілісності академічних досліджень. Вивчення наукових публікацій дозволило виділити ряд загальних наборів зображень, що застосовуються при дослідженні ефективності тих чи інших методів стеганоаналізу.

1. Фотогалерея NRCS (Natural Resources Conservation Service) Міністерства сільського господарства США (Режим доступу: https://photogallery.sc.egov.usda.gov/). Містить *.tif та *.jpeg кольорові зображення порівняно великих розмірів (2100×1500 пікселів, 2700×1800, 4288×2848 та інші). Наприклад, у роботі [7] використано 3000 зображень з цієї галереї, вони були приведені до розмірів 640×418 та конвертовані у відтінки сірого. В [8], як частина тестового набору з 5000 графічних контейнерів, застосовано 1543 зображення, що були обрізані від центру до розмірів 512×512 пікселів. У [9] використано 1576 зображень з NRCS (конвертованих у відтінки сірого) розмірами 2100×1500 пікселів, вони склали один із чотирьох тестових наборів, на яких досліджувалася точність запропонованого методу. В [10] використано 3161 зображення розмірами 2100×1500 пікселів, кожне з них було поділене на 4 окремі контейнери, тобто загальний тестовий набір містив 12644 зображення розмірами 525×375 пікселів.

2. ImageNet (Режим доступу: http://image-net.org/) – база даних зображень, що створювалася для дослідження алгоритмів пошуку, індексації, анотації та організації даних. Вона містить понад 14 мільйонів *.jpeg зображень, розділених за більш ніж 20-ти тисячами категорій. Зображення різних (порівняно невеликих) розмірів та стиснуті з різними коефіцієнтами якості. У роботі [11] використовувалося три набори, сформованих на основі ImageNet – набір на 50 тисяч, 500 тисяч та 5 мільйонів контейнерів. Зображення обиралися таким чином, щоб їх розміри перевищували 256×256 пікселів, а потім обрізалися до згаданих розмірів, конвертувалися у відтінки сірого та повторно стискалися з коефіцієнтом якості 75. Для формування однієї з контрольних вибірок у [12] використовувалося сто тисяч випадково обраних з ImageNet зображень, конвертованих у відтінки сірого та обрізаних до розмірів 256×256. У [13] використовувалася версія ImageNet CLS-LOC, що містить 1281167 зображень, відсортованих за тисячею категорій. Кожне зображення, сторони якого більші за

256 пікселів, обрізалося до розмірів 256×256 та перестискалося з коефіцієнтом 75.

3. BOSSbase 1.01 (Режим доступу: http://agents.fel.cvut.cz/boss/), Break Our Steganography System – база, яка розроблялася саме для досліджень ефективності методів стеганоаналізу та містить 1000 *.pgm зображень. Зображення були відзняті у форматі RAW сімома різними камерами, перетворені у сірі напівтонові, зменшені з використанням алгоритму Ланшоца з виключеним згладжуванням таким чином, щоб менша сторона складала 512 пікселів, а потім обрізані до розмірів 512×512. Ця база та її похідні застосовується чи не найчастіше. Наприклад, у роботах [14-15] використовувалася версія BOSSbase 0.92, що містить 9074 зображення, а в [16] безпосередньо BOSSbase 1.01. У дослідженні [17] фігурують зображення з BOSSbase 1.01, стиснуті з коефіцієнтами якості 75 та 95. В роботі [18] – зображення з BOSSbase, перетворені у формат JPEG з 50, 75 та 95 коефіцієнтами якості, для деяких експериментів розмір зображень було зменшено до 256×256 пікселів.

4. MIRFickr (Режим доступу: http://press.liacs.nl/mirflickr/). Існує дві бази даних зображень MIRFlickr: MIRFlickr 1M, що містить 1 мільйон *.jpeg зображень, та більш ранній варіант MIRFlickr 25k, що містить 25 тисяч. Зображення з врахуванням індексу цікавості були завантажені з сайту соціальних фото Flickr, куди їх додавали різні користувачі. Зображення в цій базі в основному стиснуті з коефіцієнтом якості 96, але є деяка кількість з іншими коефіцієнтами (наприклад, 92 та 95 в MIRFlickr 25k). Розміри різні, але не перевищують 500×500 пікселів (для MIRFlickr 25k 399×462 пікселі в середньому). Наприклад, у роботі [19] використовувалося 9000 випадково обраних зображень з бази MIRFlickr 25k, а в [20] – 1300 випадково обраних зображень з MIRFlickr 1M.

Та все ж такі набори містять зображення з фіксованими параметрами та/або зображення з обмеженої кількості джерел, тому оцінки точності стеганоаналізу, отримані з їх використанням відображають тільки частину можливих випадків. Не завжди наявної кількості зображень достатньо для запланованих експериментів. Та, як правило, «еталонні» зображення мають малі розміри і не зрозуміло як буде співвідноситися отримана точність з точністю стеганоаналізу більших за розміром зображень, особливо в частотній області.

Більш наближеними до практики є оцінки, отримані шляхом завантаження великої кількості зображень з усіх куточків мережі Інтернет, тобто потенційно реальних контейнерів. Так, наприклад, в роботі [21] використовувалося 49678 зображень з мережі Інтернет. В [20] окрім MIRFlickr 1M використовувалися також 5000 зображень товарів з сайту https://www.amazon.cn і 2,4 мільйони зображень, завантажених з веб-сайту Flickr та за допомогою пошукової системи Google Images.

Щоб виявити існуючі закономірності в [22] із різних інтернет ресурсів було зібрано базу з 1,1 мільйону унікальних зображень. За допомогою них автори досліджували ефективність наявних на той час універсальних методів стеганоаналізу. Так як робота виконувалася у 2006 році, то атаки здійснювалися на стеганографічні методи, які на сьогодні вважаються нестійкими до пасивного

стеганоаналізу, зокрема на Outguess та F5. У [22] показано, що точність стеганоаналізу різна для зображень, що безпосередньо створені у форматах без втрат даних (*.bmp, *.pgm тощо), та тих, що створені у форматі *.jpeg, а потім конвертовані до одного з форматів без втрат. Та багато питань із цього дослідження його автори залишили для майбутнього, зокрема це залежність точності стеганоаналізу від розмірів контейнера.

Недоліком варіанту завантаження зображень із різних інтернет джерел є в першу чергу неконтрольована обробка, тобто невідомо яким процедурам, що змінюють природню статистику, вони підлягали, перед тим як потрапити в мережу. Не можна також відкидати імовірність, що деякі з них вже містять приховані стеганографічними методами таємні повідомлення або цифрові водяні знаки для захисту авторських прав. Саме щоб запобігти вказаним недолікам науковці звертаються до самостійного формування тестових наборів зображень згідно з потребами дослідження.

Обравши вихідний тестовий набір зображень, дослідники створюють на його основі один, а частіше цілий ряд, наборів стеганоконтейнерів. Крім вихідного набору перед початком експериментів визначається також програмний засіб або алгоритм (один чи декілька), які будуть атакуватися, та ступінь наповненості вихідних контейнерів, тобто відсоток реально приховуваних бітів інформації від максимально можливої кількості, яку здатна забезпечити атакована стеганографічна програма. Для повноти картини часто формують ряд стеганонаборів з наповненістю від деякої мінімальної (1-5%) до максимальної (100%) з кроком 5, 10 чи 20%. Оскільки діє правило, чим вища наповненість, тим вища точність стеганоаналізу, часто обмежуються аналізом тільки малозаповнених контейнерів (до 50%).

Наступний крок після формування всіх потрібних наборів – це вибір моделі характеристичних векторів, яка немов мікроскоп, буде наближати різницю між пустими та заповненими контейнерами. Розглянемо існуючі варіанти обчислення характеристичних векторів для контейнерів-зображень, збережених у різних форматах.

Моделі характеристичних векторів для зображень у форматах без втрат.

1. SPAM (Subtractive Pixel Adjacency Matrix) – статистична модель характеристичних векторів для стеганоаналізу зображень у форматах без втрат, що була запропонована Томасом Певні у роботі [9]. Стегоаналіз з використанням моделі SPAM проводиться на основі оцінок кореляції між різницями яскравості суміжних пікселів, що розраховані із застосуванням марківських ланцюгів (МЛ) першого та другого порядку. Для оцінки параметрів МЛ для напівтонового зображення $\boldsymbol{I}_{x,y}$, розмірами $M \times N$ пікселів використовуються матриці суміжності (co-occurrence matrix) різниць значень яскравості суміжних пікселів $\boldsymbol{C}_{\Delta x,\Delta y}$:

$$C_{\Delta x,\Delta y}(i,j) = \sum_{m=1}^{M}\sum_{n=1}^{N}([I_{m,n} - I_{m+\Delta x,n+\Delta y} = i]_I \times [I_{m+\Delta x,n+\Delta y} - I_{m+2\Delta x,n+2\Delta y} = j]_I),$$

де $[a]_I = \begin{cases} 1, & a = True \\ 0, & a = False \end{cases}$ – нотація (дужка) Айверсона; $(i, j) \in \{[1; Z_I] \times [1; Z_I]\}$ − поточна позиція елемента матриці суміжності $\boldsymbol{C}_{\Delta x,\Delta y}$; Δx, Δy − просторовий зсув між пікселями зображення; $Z_I = (2^k - 1)$ − діапазон значень яскравості пікселів; k (біт) − глибина кольору зображення $\boldsymbol{I}_{x,y}$.

Розрахунок матриці $\boldsymbol{M}_{\Delta x,\Delta y}$ імовірностей переходу між елементами МЛ (різниць значень яскравості суміжних пікселів) проводиться шляхом нормалізації отриманої матриці суміжності $\boldsymbol{C}_{\Delta x,\Delta y}$: $M_{\Delta x,\Delta y}(i,j) = \dfrac{C_{\Delta x,\Delta y}(i,j)}{\sum_{i=1}^{Z_I}\sum_{j=1}^{Z_I} C_{\Delta x,\Delta y}(i,j)}$.

Для усереднення параметрів моделі SPAM використовуються матриці $\boldsymbol{M}\Delta x,\Delta y$ для горизонтального ($\Delta x \neq 0$, $\Delta y = 0$), вертикального ($\Delta x = 0$, $\Delta y \neq 0$) та діагонального ($\Delta x \neq 0$, $\Delta y \neq 0$) напрямків, в яких розраховуються значення кореляції різниць яскравості суміжних пікселів. Кількість елементів характеристичного вектора (розмірність простору ознак) моделі SPAM складає 686.

2. PSRM (Projection Spatial Rich Model) – модель, яка була запропонована у 2013 році у роботі [16]. Вона передбачає проектування сусідніх вибірок залишків на набір випадкових векторів та формування характеристичних векторів зображень як статистик першого порядку (гістограм) проекцій. В результаті застосування проекцій отримуються більш «заселені» (статистично значимі) характеристичні вектори. З огляду на це автори представляють дану модель як таку, що має переваги над моделями на базі матриці суміжності, тобто, наприклад, над моделлю SPAM. Проте досліджувана модель характеризується високою обчислювальною складністю. Так, для обчислення елементів моделі PSRM потрібно близько 65000 згорток та гістограм. При цьому PSRM застосовує той же набір залишків, що і модель SRM (Projection Spatial Rich Model), представлена у роботі [15]. Розмірність результуючого характеристичного вектора для PSRM складає 12780 елементів. Розроблялася модель в першу чергу для атаки на найбільш сучасні методи приховування, такі як S-UNIWARD, WOW, HUGO. Автори відмічають, що проекційний підхід можна застосувати не тільки в просторовій, а й в частотній області зображення. Що дає можливість протидіяти таким алгоритмам як, наприклад, nsF5 та J-UNIWARD.

3. Зважаючи на високу обчислювальну складність PSRM дослідники частіше використовують дві спрощені багаті моделі – SRM та SRMQ1 (Spatial Rich Model with the fixed quantization q=1c). Вони обидві не містять етапу проектування та разом з тим використовують той же набір залишків, що й PSRM. Всі три моделі складаються з ряду субмоделей, які формуються з залишків шуму $\mathbf{R} = (R_{ij}) \in R^{n1 \times n2}$, що в свою чергу розраховуються з використанням високочастотних фільтрів наступної форми: $R_{ij} = \hat{X}_{ij}(N_{ij}) - cX_{ij}$, де $c \in N$ – порядок залишків, N_{ij} – локальний окіл пікселя X_{ij}, $X_{ij} \notin N_{ij}$ і $\hat{X}_{ij}(\square)$ є предиктором cX_{ij}, визначеним на N_{ij}.

Кожна субмодель формується як квантована та урізана версія залишку: $R_{ij} \leftarrow trunc_T\left(round\left(\frac{R_{ij}}{q}\right)\right)$.

SRMQ1 по суті є частиною моделі SRM, в якій використовується тільки один крок квантування для складових субмоделей q=1. В той час як повна модель передбачає побудову субмоделей з наступними кроками квантування: $q \in \begin{cases} \{c, 1.5c, 2c\}, c > 1 \\ \{1, 2\}, \quad c = 1. \end{cases}$

Модель SRM складається з 106 субмоделей та містить 34671 елементи. Модель SRMQ1, як і PSRM, складається з 39 субмоделей. SRMQ1 містить 12753 елементів.

4. CSR (Content-Selective Residuals) – статистична модель характеристичних векторів для зображень у форматах без втрат, запропонована у 2014 році у роботі [23]. Автори розробляли її для протидії методу S-UNIWARD, взявши за основу таку особливість цього методу як наявність смуг з низькою та високою вірогідністю вкраплення, що чергуються у високотекстурованих та шумних областях зображення. Для атаки на S-UNIWARD було введено концепцію селективних за вмістом залишків, що й дало назву моделі CSR.

Модель CSR передбачає поділ пікселів зображення на два класи, що не перетинаються: пікселі, що будуть з високою вірогідністю змінені, та ті, які маловірогідно зміняться після вкраплення. Потім для кожного класу обчислюються залишки шуму: $R_{ij}^{(1)} = X_{i,j+1} - X_{i,j}$, $R_{ij}^{(2)} = X_{i,j+1} - 2X_{i,j} + X_{i,j-1}$, $R_{ij}^{(3)} = -X_{i,j+2} + 3X_{i,j+1} - 3X_{i,j} + X_{i,j-1}$.

Характеристичний вектор формується з елементів статистик першого та другого порядків цих залишків. Розмірність вектору – 1183 елементи.

Експерименти, проведені авторами моделі, показали, що ефективність CSR для протидії S-UNIWARD, залежить від того, наскільки влучно підібраний параметр σ при розрахунку спотворень, спричинених вкрапленням: $D(\boldsymbol{X}, \boldsymbol{Y}) = \sum_{k=1}^{3} \sum_{u=1}^{M} \sum_{v=1}^{N} \frac{\left| W_{uv}^{(k)}(\boldsymbol{X}) - W_{uv}^{(k)}(\boldsymbol{Y}) \right|}{\left| \sigma + W_{uv}^{(k)}(\boldsymbol{X}) \right|}$, де σ – це так звана стабілізаційна константа, уведена з метою запобігання ділення на нуль.

Більш глибокі дослідження цієї моделі показали, що вона є направленою (атака на S-UNIWARD) та не може бути застосовна для виявлення, наприклад, НЗБ-стеганографії чи інших методів приховування. Крім того, при виявленні S-UNIWARD даній моделі можна з успіхом протидіяти, ретельно підібравши значення стабілізаційної константи. Тобто в цілому модель показала недолік S-UNIWARD, з виправленням якого CSR стає неефективною. Тому реалізація в стеганоаналітичних системах інших статистичних моделей для зображень у форматах без втрат, зокрема SPAM, SRM, SRMQ1 та PSRM, є більш пріоритетною.

Моделі характеристичних векторів для JPEG-зображень.

5. CHEN – модель, заснована на процесах Маркова, яка використовує внутрішньоблокові та міжблокові кореляції між коефіцієнтами дискретного косинусного перетворення (ДКП) природних зображень. Запропонована у 2008 році в роботі [24]. Для визначення внутрішньоблокових кореляцій в моделі генеруються чотири різницеві матриці: горизонтальна $F_h = F(u,v) - F(u+1,v)$, вертикальна $F_\varpi = F(u,v) - F(u+1,v)$, головна діагональна $F_d = F(u,v) - F(u+1,v+1)$ та побічна діагональна $F_m = F(u+1,v) - F(u,v+1)$, де $F(u,v)$ – абсолютні значення ДКП коефіцієнтів зображення. Потім для кожної різницевої обчислюється матриця ймовірностей переходу. Наприклад, для горизонтальної різницевої матриці вона буде мати вигляд $M_h(i,j) = \frac{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v}\lambda(F_h(u,v)=i, F_h(u+1,v)=j}{\sum_{u=1}^{S_u-1}\sum_{v=1}^{S_v}\lambda(F_h(u,v)=i}$, де $\lambda=1$, якщо його аргументи виконуються і $\lambda=0$ в протилежному випадку, S_u та S_v – розміри зображення. Міжблокові кореляції відображають залежності між коефіцієнтами ДКП, які розташовані в одній і тій же позиції в сусідніх блоках. Для аналізу міжблокових порушень для відповідних горизонтальної і вертикальної різницевих матриць обчислюються також матриці ймовірностей переходу. Діагональні матриці автори ігнорують, бо вони суттєво не впливають на результат. Щоб зменшити розмірність результуючого вектору для всіх матриць ймовірностей переходу використовується усікання до діапазону [-4, +4], що з кожної різницевої матриці дає по 81 елементу для характеристичного вектора. Таким чином, 81×4 елементи фіксують внутрішньоблокові порушення після стеганоперетворення, 81×2 – міжблокові.

6. CC-CHEN – модель CHEN, покращена декартовим калібруванням. Взагалі ідея калібрування JPEG-зображення полягає в десинхронізації блоків 8×8, всередину яких відбувається приховання даних. Як правило, для калібрування застосовують обрізування на 4 пікселі в горизонтальному та вертикальному напрямках від початку, але з цією ж метою може бути використане і масштабування або обертання на невеликий кут. Результатом калібрування деякого зображення F є опорне зображення F_r. Так як калібрування руйнує приховані дані, опорне зображення можна розглядати як наближення пустого контейнера. Тому спершу в стеганоаналізі виникла ідея розглядати калібровані характеристичні вектори, як такі, що отримані за значеннями різниці між вихідним та каліброваним зображенням $F_{cal} = F_r - F$. Але в роботі [25] показано, що статистика опорного зображення не завжди близька до статистики оригінального і аналіз різниць відповідно не завжди приводить до покращення точності детектування. Крім того в деяких випадках може бути погіршення у порівнянні з некаліброваним варіантом, бо при калібруванні відніманням може втрачатися корисна інформація. Як більш ефективну альтернативу в [25] запропоновано використовувати декартове калібрування, коли $F_{cal} = [F_r, F]$. Таким чином, CC-CHEN – це модель, в якій аналізується шість матриць ймовірностей переходу для досліджуваного зображення і таких же шість матриць – для його каліброваної (шляхом обрізування) версії. Розмірність цієї моделі – 972 елементи.

7. LIU – модель, яка запропонована у роботі [26] та базується на тому, що стеганографічні приховання змінюють спільну щільність сусідніх елементів. Як і попередні, дана модель аналізує внутрішньоблокову та міжблокову статистику значень квантованих ДКП коефіцієнтів зображення. Матриці щільності сусідніх внутрішньоблокових з'єднань в горизонтальному та вертикальному напрямках визначаються як: $absNJ_{1h}(x,y)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{n=1}^{7}\lambda\left(\left|c_{ijmn}\right|=x,\left|c_{ijm(n+1)}\right|=y\right)}{56MN}$, $absNJ_{1v}(x,y)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{n=1}^{8}\lambda\left(\left|c_{ijmn}\right|=x,\left|c_{ij(m+1)n}\right|=y\right)}{56MN}$, де c_{ijmn} – коефіцієнт, розташований у m рядку та n стовпчику блоку $M\times N$ ДКП коефіцієнтів. Для оптимізації обчислень в подальшому аналізується усереднена матриця з двох даних. Аналогічні міжблокові матриці мають вигляд $absNJ_{2h}(x,y)=\frac{\sum_{m=1}^{8}\sum_{n=1}^{8}\sum_{i=1}^{M}\sum_{j=1}^{N-1}\lambda\left(\left|c_{ijmn}\right|=x,\left|c_{i(j+1)mn}\right|=y\right)}{64M(N-1)}$ та $absNJ_{2v}(x,y)=\frac{\sum_{m=1}^{8}\sum_{n=1}^{8}\sum_{i=1}^{M-1}\sum_{j=1}^{N}\lambda\left(\left|c_{ijmn}\right|=x,\left|c_{(i+1)jmn}\right|=y\right)}{64(M-1)N}$ і також усереднюються. Так як спільна щільність варіюється для різних зображень, щоб відобразити її зміну, спричинену стеганоперетворенням, застосовується калібрування зображення. Потім обчислюються середні значення матриць щільності каліброваної версії та розраховуються диференціальні характеристики між отриманими статистиками. Автори обмежили розгляд цілочисельних параметрів x та y діапазоном [0, 5], що на виході дало 144 елементи для значень різниць матриць щільності вихідного та каліброваного зображення *ref-diff-absNJ* та 72 елементи для значень часток *diff-absNJ-ratio*.

8. CC-PEV – модель PEV, покращена декартовим калібруванням, запропонованим в [25]. Вихідна модель PEV представлена у роботі [27]. Характеристичний вектор в цій моделі має 274 елементи, 193 з них сформовані на базі ДКП, а 81 – елемент, отримано на основі процесів Маркова. Набір статистичних даних на базі ДКП в свою чергу включає 11 елементів глобальної гістограми H розподілу коефіцієнтів ДКП; по 11 елементів для п'яти локальних гістограм h_l^{ij} розподілу значень перших п'яти AC-коефіцієнтів; по 9 елементів для 11-ти дуальних гістограм g_{ij}^{d}; 1 елемент усередненої варіації V значень коефіцієнтів ДКП у суміжних блоках розбиття зображення; 2 елементи блочності (скаляри, обчислені з декомпресованого зображення, що представляють інтегральну міру міжблокової залежності); 25 елементів матриці спільної появи значень коефіцієнтів ДКП, квантованих у діапазоні [-2, +2] в блоках розбиття зображення. 81 елемент на основі процесів Маркова – це усереднені значення чотирьох внутрішньоблокових матриць ймовірності переходу, розрахованих за алгоритмом моделі CHEN. Для підвищення точності детектування в моделі CC-PEV розраховуються всі вищезгадані елементи як для вихідного зображення, так і для його каліброваної версії.

9. CC-C300 – модель, що грунтується на використанні високорозмірних векторів, з метою охопити найбільше залежностей між коефіцієнтами ДКП. Запропонована в [14]. Характеристичні вектори складають елементи матриць спільної появи пар коефіцієнтів ДКП, де пара визначається згідно формулі $P(\Delta i,\Delta j,k_1,l_1,k_2,l_2)=\left\{\left[D_{k_1l_1}^{(i,j)},D_{k_2l_2}^{(i+\Delta i,j+\Delta j)}\right]\,|\,i=1,\ldots N^{(i)},j=1,\ldots N^{(j)}\right\}$. Тут $D_{kl}^{(i,j)}$ – (k, l)-тий коефіцієнт в (i, j)-тому блоці ДКП; $k_1,l_1,k_2,l_2\in\{0,\ldots 7\}$; $\Delta i,\Delta j$ – натуральні числа; $N^{(i)}=8\lceil M/8\rceil-\Delta i$, $N^{(j)}=8\lceil N/8\rceil-\Delta j$; $M\times N$ – розміри зображення. При чому вихідні

коефіцієнти ДКП усікаються до діапазону [-T, T] та повинна справджуватися нерівність $|\Delta i|+|\Delta j|+|k_1-k_2|+|l_1-l_2|>0$. Матриці спільної появи мають вигляд: $C_{st}=\frac{1}{N^{(i)}N^{(j)}}\sum_{i=1}^{N^{(i)}}\sum_{j=1}^{N^{(j)}}\{[a,b]\in P(\Delta i,\Delta j,k_1,l_1,k_2,l_2)\mid a=s,b=t\}$. Автори фіксують $T=4$, що дає 81-елементну матрицю C_{st} для кожної шестірки значень $(\Delta i,\Delta j,k_1,l_1,k_2,l_2)$. Для того щоб зробити побудову окремих матриць більш системною всі можливі пари коефіцієнтів ДКП сортуються за ступенем важливості і матриці потім обчислюються у порядку від найважливіших до найменш важливих пар. Як міра важливості використовується взаємна інформація, обчислена на досить великому наборі випадково вибраних пар коефіцієнтів. Таким чином, результуючий набір елементів характеристичного вектора об'єднує в собі Ω найважливіших матриць спільної появи, маючи розмірність $\Omega\times 81$. Після декартового калібрування розмірність, яку автори позначають через CC-CΩ, подвоюється до $2\times\Omega\times 81$. В роботі [14] використовувався набір CC-C300, тобто такий що об'єднує 300 матриць спільної появи.

10. GFR – модель характеристичних векторів, побудованих як гістограми квантованих залишків, отриманих з використанням двовимірних фільтрів Габора (Gabor Filter Residual). 2D-фільтри Габора описують особливості текстури зображення з позицій різних масштабів та орієнтацій. Модель представлена в [28]. На відміну від попередніх будується в просторовій області. Спочатку зображення декомпресується без заокруглення значень. Генерується двовимірний банк фільтрів Габора, що включає фільтри з двофазним зміщенням $(\phi=0,\pi)$, чотирма масштабами ($\sigma=0.5$, 0.75, 1, 1.25) та 32-ма орієнтаціями ($\theta=0,\pi/32,\ldots 31\pi/32$). Далі розпаковане зображення згортається з 8×8 2D-фільтром Габора $G^{\phi,\sigma,\theta}$, щоб отримати відповідне залишкове зображення $U^{\phi,\sigma,\theta}$. Відповідно до фази (a,b), $0\le a,b\le 7$ залишки поділяються на 64 підмножини $U_{a,b}^{\phi,\sigma,\theta}$, для кожної з яких обчислюються гістограми $h_{a,b}^{\phi,\sigma,\theta}(r)=\frac{1}{|U_{a,b}^{\phi,\sigma,\theta}|}\sum_{u\in U_{a,b}^{\phi,\sigma,\theta}}[Q_T(|u|/q)=r]$, де Q_T – квантувач з цілочисельними центроїдами $\{0,1,\ldots T\}$, q – крок квантування, [P] – дужка Айверсона. Завдяки симетрії отримані 64 гістограми $h_{a,b}^{\phi,\sigma,\theta}$ зливаються до 25-ти: разом складаються гістограми, індекси яких, $(a,b),(a,8-b),(8-a,b),(8-a,8-b)$ за умови що ці показники залишаються в межах $\{0,1,\ldots 7\}\times\{0,1,\ldots 7\}$. Потім ці 25 гістограм з'єднуються в гістограму $h^{\phi,\sigma,\theta}$ залишку $U^{\phi,\sigma,\theta}$. Гістограми $h^{\phi,\sigma,\pi-\theta}$ та $h^{\phi,\sigma,\theta}$ об'єднуються згідно симетричним орієнтаціям. Наостанок результуючі гістограми стають елементами характеристичного вектора. Розмірність GFR – 17000 елементів.

11. DCTR – модель характеристичних векторів із ДКП залишків (Discrete Cosine Transform Residual), що враховує фази. Була запропонована в 2015 році у роботі [29], як і GFR будується в просторовій області. Елементи характеристичних векторів в даній моделі будуються як гістограми залишків, отримані з використанням базових шаблонів ДКП, що мають вигляд $B_{mn}^{(k,l)}=\frac{w_k w_l}{4}\cos\frac{\pi k(2m+1)}{16}\cos\frac{\pi l(2n+1)}{16}$, $w_0=\frac{1}{\sqrt{2}}$, $w_k=1(k>0)$, $0\le m,n\le 7$. Для створення

характеристичних векторів потрібно обчислити 64 згортки розпакованого в просторову область без заокруглення до цілих чисел JPEG зображення з 64 ядрами 8×8 та сформувати нормалізовані гістограми, аналогічні тим, що описані для попередньої моделі. Для подальшої компактизації векторів використовується симетрія шаблонів – гістограми об'єднуються за тим же принципом, що й в моделі GFR. Загальна розмірність симетризованого характеристичного вектора становить $64\times(36/4+24/2+4)\times(T+1)=1600\times(T+1)$. Як компроміс між швидкодією та точністю автори пропонують використовувати $T=4$.

Огляд класифікаторів.

Наступний важливий етап – це вибір класифікатора. Зазвичай в наукових публікаціях деякий метод на базі машинного навчання представляють та досліджують як комбінацію певної моделі характеристичних векторів та бінарного класифікатора. На вхід той чи інший бінарний класифікатор приймає характеристичні вектори контейнерів, виходом є одна з двох міток класу «пустий» чи «заповнений». Які ж класифікатори дослідники застосовують для задач стеганоаналізу?

У роботах [30–31] для класифікації застосовується метод k найближчих сусідів (k nearest neighbor). Це простий метричний класифікатор, що базується на оцінюванні подібності об'єктів. Поточний об'єкт класифікації відноситься до того класу, якому належить більшість з k його сусідів, тобто найближчих до нього об'єктів навчальної вибірки. Метод k найближчих сусідів неявно спирається на одне важливе припущення, яке має назву гіпотеза компактності: якщо міра подібності об'єктів введена досить вдало, то схожі об'єкти набагато частіше лежать в одному класі, ніж в різних. У цьому випадку межа між класами має досить просту форму, а класи утворюють компактно локалізовані області в просторі об'єктів. Відзначимо, що для оцінки подібності об'єктів в даному методі зазвичай використовується міра відстані Евкліда.

Наступний можливий варіант – використання наївного байєсівського класифікатора. Це простий імовірнісний класифікатор, заснований на теоремі Байєса зі строгими припущеннями про незалежність. Теорема Байєса дозволяє переставити місцями причину і наслідок. Знаючи з якою ймовірністю причина призводить до якоїсь події, ця теорема дозволяє розрахувати ймовірність того що саме ця причина призвела до події, що спостерігається. Наївний байєсівський класифікатор зручний у випадках, коли розмірність характеристичного вектору велика і є відносно невелика навчальна вибірка. Його застосування у цілях стеганоаналізу описано, наприклад, в роботах [32–33].

У роботах [34–35] для класифікації пустих і заповнених контейнерів використано ще один з класичних методів інтелектуального аналізу даних – дерева рішень. Дерева рішень є послідовними ієрархічними структурами, що складаються з вузлів, які містять правила, тобто логічні конструкції виду "якщо... то...". Кінцевими вузлами дерева є "листя", які відповідають знайденим рішенням і об'єднують деяку кількість об'єктів вибірки, що розглядається. Кожному об'єкту відповідає єдиний вузол, що дає рішення. Щоб класифікувати новий об'єкт, потрібно спуститися по дереву до листа і видати відповідне значення. На

сьогоднішній день існує значна кількість алгоритмів, що реалізують дерева рішень: CART, C4.5, NewId, ITrule, CHAID, CN2.

Нейронні мережі також можуть бути використані як класифікатори контейнерів. Основу нейронних мереж складають нейрони – елементи, які імітують роботу нейронів головного мозку і характеризуються своїм станом. У нейронів є входи (синапси), що з'єднані з виходами інших нейронів, і є вихід (аксон), сигнал з якого надходить на синапси інших нейронів. Кожен синапс характеризується величиною синаптичного зв'язку, яку ще називають вагою. Стан нейрона визначається як сума станів його входів. Значення на виході нейрона – це функція від його стану. Ця функція називається активаційною і може мати різний вигляд, найчастіше використовується логістична функція або функція S-подібного вигляду (сигмоїд). На нейрони самого нижнього шару подаються значення вхідних параметрів (у даному випадку це значення елементів характеристичного вектору). Ці значення сприймаються мережею як сигнали, що передаються у наступний шар, ослабляючись або посилюючись в залежності від ваги зв'язків. У результаті на виході нейрона верхнього шару виробляється деяке значення, яке розглядається як відповідь – відгук мережі на вхідні параметри. Для того, щоб мережа працювала потрібно здійснити її навчання, яке полягає у підборі ваг міжнейронних зв'язків, що забезпечують найбільшу близькість одержуваних відповідей до відомих правильних. Найпоширеніший тип нейромережі – багатошаровий перцептрон. Він складається з наступних шарів: вхідний (сенсорний), один або декілька прихованих і вихідний. Завдання класифікації при наявності двох класів може бути вирішеним на мережі з одним нейроном у вихідному шарі, який може приймати одне з двох значень 0 або 1, залежно від того, до якого класу належить зразок. Крім перцептрона, можуть бути використані і інші архітектури, наприклад, згорткова нейронна мережа (CNN), рекурентна нейронна мережа (RNN) тощо. Нейронні мережі використовують для класифікації контейнерів, наприклад, в роботах [36–37].

Найбільш популярним і, як правило, найточнішим для задач стеганоаналізу серед класичних класифікаторів є метод опорних векторів (SVM – support vector machine). SVM – це бінарний класифікатор, що відноситься до граничних методів. Він дозволяє отримати функцію класифікації з мінімальною оцінкою помилки класифікації, а також використовувати лінійних класифікатор для роботи з лінійно нероздільними даними. Основною проблемою методу є вибір оптимальної гіперплощини, яка дозволяє розділити класи з максимальною точністю. Для цього поділяюча гіперплощина вибирається таким чином, щоб відстань між найближчими об'єктами, розташованими по різні сторони від неї, була максимальною. Для лінійно нероздільних даних вводяться ослабляють коефіцієнти (soft-margin SVM). Так само для лінійно нероздільних даних в SVM реалізована ідея переходу до простору більш високої розмірності, в якому раніше нероздільні дані можуть стати лінійно роздільними.

Нехай маємо навчальну вибірку $(E, X) = \{\vec{\delta}_n, \chi_n\}_{n=1}^{N}$, де $\vec{\delta}_n$ – деякий об’єкт в просторі R^n, $\chi_n \in \{-1,+1\}$ – його мітка класу. Задача полягає в тому, щоб на основі

навчальної вибірки спрогнозувати мітку класу $\hat{\chi}$ для нового об'єкту $\vec{\delta}$. В застосуванні до стеганоаналізу $\vec{\delta}_n$ – характеристичний вектор. Якщо $\vec{\delta}_n$ вилучено з пустого контейнера, то $\chi_n = -1$, якщо з заповненого, то $\chi_n = +1$.

Функція прийняття рішень для лінійної SVM має вигляд $p(\vec{\delta}) = sign(\vec{w} \cdot \vec{\delta} - b)$ З погляду геометрії лінійний класифікатор відповідає деякій поділяючій гіперплощині, де об'єкт відноситься до першого класу, якщо він лежить з додатної сторони від гіперплощини, та до другого в протилежному випадку. Вектор $\vec{w}$ є перпендикуляром до поділяючої гіперплощини, а параметр b визначає її зсув відносно початку координат. Провести поділяючу гіперплощину можна по-різному, разом з тим оптимальною є така гіперплощина, яка максимізує відстань між нею та найближчим об'єктом класу. Метод опорних векторів зводить навчання класифікатора до задачі квадратичної оптимізації, яка розв'язується евристичними алгоритмами. Розв'язок – $\vec{w} = \sum_{i=1}^{N} \alpha_i \chi_i \vec{\delta}_i$. Для більшості векторів $\alpha_i = 0$. Всі вектори, для яких $\alpha_i > 0$ називають опорними. Для будь-якого опорного вектора $b = \vec{w} \cdot \vec{\delta}_i - \chi_i$, тобто він належить опорній гіперплощині (всі об'єкти певного класу лежать по одну сторону від даної гіперплощини).

Об'єкти, що класифікуються, не завжди можуть бути розділені гіперплощиною. У реальних системах наявні похибки даних, внаслідок яких гіперплощина не виконає розподіл абсолютно точно. Тому для роботи методу SVM вводять допустиму похибку класифікації, що називається м'якою межею. Крім того, існує ще один шлях до вирішення проблеми лінійної нероздільності: вихідний простір можна відобразити в простір більш високого розміру, де навчальна вибірка стане лінійно роздільною: $\Phi : \vec{\delta} \to \varphi(\vec{\delta})$ (спрямляючий простір). Об'єкти навчальної вибірки входять в лінійну функцію прийняття рішень тільки у вигляді попарних скалярних добутків $\vec{\delta}_i \cdot \vec{\delta}_j$. Отже для того, щоб побудувати оптимальну поділяючу гіперплощину в новому просторі, необхідно знати лише $\varphi(\vec{\delta}_i) \cdot \varphi(\vec{\delta}_j)$. Припустимо, що існує деяка функція $K : R^n \to R$, така що $K(\vec{\delta}_i, \vec{\delta}_j) = \phi(\vec{\delta}_i) \cdot \phi(\vec{\delta}_j)$. Тоді для побудови оптимальної поділяючої гіперплощини не обов'язково задавати перетворення Φ в явному вигляді, достатньо лише знати K. При цьому функцію прийняття рішень можна переписати як $p(\vec{\delta}) = sign(\sum_{i=1}^{N} \alpha_i \chi_i K(\vec{\delta}_i, \vec{\delta}) - b)$. Такий підхід називають переходом до ядра (kernel trick). Два найбільш вживані для задач стеганоаналізу ядра SVM – це лінійне $K(\vec{\delta}_i, \vec{\delta}_j) = \vec{\delta}_i \cdot \vec{\delta}_j + \theta, \theta \geq 0$ та гаусівське $K(\vec{\delta}_i, \vec{\delta}_j) = \exp\left(-\frac{\left\| \vec{\delta}_i - \vec{\delta}_j \right\|}{2\sigma^2} \right), \sigma > 0$.

SVM комбінується з різними моделями характеристичних векторів у багатьох публікаціях, наприклад в [10, 38–43]. Проте розвиток комп'ютерної стеганографії, її ускладнення та поява контент-адаптивних методів приховування, є природніми причинами створення все більш складних і багаторозмірних моделей. Моделі, в яких фіксуються велика кількість різних статистичних показників (так звані «багаті»), сильно сповільнюють швидкість стеганоаналітичних систем з SVM.

Щоб вирішити проблему швидкодії в роботі [44] було запропоновано використання ансамблевого класифікатора, як альтернативи методу опорних векторів, що добре масштабується за розмірністю моделі характеристичних векторів та кількістю контейнерів у навчальній вибірці. Ансамблевий класифікатор, а саме такий його вид як Bootstrap aggregating (bagging) [45], працює за наступною схемою:

- взяти d елементів (ознак) статистичної моделі характеристичних векторів;
- отримати L випадково обраних підмножин із множини всіх елементів, кожна з яких складається з dsub<d ознак;
- навчити L елементів ансамблевого класифікатора на навчальній вибірці розрізняти оригінальні зображення та стеганоконтейнери.

Нехай далі Nv(X) – кількість елементів ансамблю, що голосують за належність зображення X до класу пустих. Рішення про мітку класу цього зображення приймається згідно правилу більшості голосів:

$$Rule(L, N_v) = \begin{cases} -1, & \text{при } N_v > L/2, \\ +1, & \text{при } N_v < L/2, \\ random\{-1, +1\} & \text{інакше.} \end{cases}$$

Існують різні варіанти вибору елементів ансамблю, це можуть бути SVM, наївні байесівські класифікатори, дерева рішень (ансамбль з дерев рішень отримав назву метод випадкових лісів), тощо. У статті [44] як базовий елемент запропоновано використовувати лінійний дискримінант Фішера (ЛДФ) з огляду на його швидке навчання та гарні результати отримані при вирішенні задач стеганоаналізу. При використанні ЛДФ віднесення зображення до класу пустих чи заповнених відбувається згідно наступній функції прийняття рішень $p(\vec{\delta}) = \arg\max_{\chi \in \{\chi_1, \chi_2\}} \left[\ln(\rho_\chi P_\chi) - \frac{1}{2}(\vec{\delta} - \mu_\chi)^T \Sigma_\chi^{-1} (\vec{\delta} - \mu_\chi) - \frac{1}{2} \ln\left(\left| \Sigma_\chi^{-1} \right| - \frac{d_{sub}}{2} \ln(2\pi) \right) \right]$, де $\vec{\delta}$ – характеристичний вектор досліджуваного зображення, χ_1, χ_2 – мітки класів пустих та заповнених контейнерів, ρ_χ – ваговий коефіцієнт (величина штрафу за хибку класифікацію), P_χ – апріорна ймовірність появи контейнерів класу χ (частка пустих або заповнених контейнерів у тестовому наборі), μ_χ – середні значення характеристичних векторів класу χ, Σ – оцінка матриці коваріації характеристичних векторів пустих чи заповнених контейнерів.

Як приклад доцільності використання ансамблевого класифікатора таблицях 1 та 2 наведено результати чисельних експериментів для програмних

модулів, що комбінують моделі SPAM, SRM та SRMQ1 з лінійним SVM та з ансамблевим класифікатором на базі ЛДФ. Стеганоаналітична атака виконувалася на 100% заповнені bmp-контейнери, створені програмою Hide4PGP. Кількість пустих та стеганозображень – по 1330 (половина використовувалася для навчання, друга половина – для контролю). Оцінки точності та швидкодії узагальнювалися за 10 експериментами (в таблиці 2 наведено середнє значення точності стеганоаналізу та середньоквадратичне відхилення).

Таблиця 1.

Порівняння швидкості навчання (в сек).

Модель	Розмірність моделі	Linear SVM	Ensemble classifier
SPAM	686	2.5	6.4
SRM	34671	129.4	9.7
SRMQ1	12753	43.3	10.4

Таблиця 2.

Порівняння точності класифікації (в %).

Модель	Розмірність моделі	Linear SVM	Ensemble classifier
SPAM	686	89.7143±0.9725	99.2932±0.3194
SRM	34671	91±0.7934	99.3759±0.2482
SRMQ1	12753	91.8571±0.6068	99.3308±0.2867

Як бачимо, ансамблевий класифікатор дійсно кращий у швидкодії для «багатих» моделей. І чим більша розмірність моделі, тим відчутніша перевага. Крім того, доповнений процедурами визначення оптимальних параметрів, він і точніше виявляє використані у дослідженні стеганоконтейнери, ніж лінійний SVM. Проте для повної картини потрібно побудувати також SVM з гаусівським ядром та дослідити його можливості при різних умовах стеганоаналізу.

Побудова багатокласових стеганоаналітичних систем.

В загальному випадку стегоаналітична система повинна мати можливість працювати в режимі мультикласифікації. Це потрібно як і для того, щоб визначити за допомогою якого стеганографічного методу створено заповнений контейнер (класи – це методи), так і, наприклад, для того, щоб визначитися з довжиною прихованого повідомлення (класи – це орієнтовна довжина). Деякі з розглянутих методів класифікації за своєю побудовою можуть бути використані або легко розширені для багатокласових задач. Це, зокрема, метод k найближчих сусідів, наївний байєсівський класифікатор, дерева рішень, нейронні мережі, лінійний дискримінант Фішера. Проте й алгоритми, що розроблені для бінарної класифікації (в даному огляді це SVM), можуть бути адаптовані для багатокласових задач.

Зазначимо, що проблема ефективного розширення бінарного SVM класифікатора для вирішення задач із багатокласовим розпізнаванням все ще залишається предметом досліджень. На сьогодні існує два підходи до її вирішення: 1) зведення задачі багатокласової класифікації до бінарної (основні стратегії: OVA – «Один проти всіх», OVO – «Один проти одного», DAGSVM – направлений ациклічних граф SVM, ECOC – аналіз з використанням кодів корекції помилок); 2) побудова багатокласових SVM за один крок (це так звані стратегії «Всі разом»).

Дослідження та порівняльний аналіз всіх стратегій виходить за рамки даної роботи. Зважаючи на високу обчислювальну складність реалізації порівняльний аналіз різних стратегій, як правило, виконується на невеликих вибірках даних [46]. В загальному випадку обчислювально складніше вирішити задачу багатокласової класифікації за один крок, тобто безпосередньо розглядати всі вихідні дані в одній оптимізаційній формулі. З огляду на сказане опишемо тільки дві найперші стратегії зведення до бінарної класифікації, які можуть бути застосовані для побудови стеганоаналітичних систем.

Нехай потрібно навчити класифікатор $p: Q \to Z$, де $Z = \{1, 2 ... k\}$, а k – кількість класів. Стратегія «Один проти всіх» (або «Один проти решти») передбачає навчання k бінарних класифікаторів, кожний з яких відділяє один клас від всіх інших. З вихідної навчальної вибірки $(Q, Z) = \{\vec{q}_n, z_n\}_{n=1}^{N}$ формується k бінарних вибірок $(Q_1, Z_1), (Q_2, Z_2), ... (Q_k, Z_k)$, де в вибірці (Q_i, Z_i), контейнер помічається міткою +1, якщо в вихідній вибірці він був помічений міткою *i*. В усіх інших випадках контейнер помічається міткою -1. Таким чином, для кожного i=1,2...k на базі вибірки (Q_i, Z_i), навчаємо бінарний класифікатор $p_i : Q \to \{\pm 1\}$. Далі, маючи набір k бінарних класифікаторів, будуємо багатокласовий класифікатор за правилом $p(Q) = \arg\max_{i \in Z} \left(p_i \left(Q \right) \right)$.

Для уникнення неоднозначності (коли одному зразку призначається декілька класів) ця стратегія потребує, щоб класифікатори p_i на виході продукували не просто мітку класу, а мітку з оцінкою її достовірності (впевненості в передбаченні). При чому при обчисленні оцінок достовірності потрібно зважати на те, що шкала їх значень для базових бінарних класифікаторів може відрізнятися. Крім того, навіть якщо розподіл зразків класу в вихідній навчальній вибірці збалансований (кількість представників кожного класу відрізняється менше, ніж на порядок),), в більшості випадків у бінарних вибірках (Q_i, Z_i) зразків з міткою -1 буде значно більше, ніж з +1.

Альтернативною стратегією є «Один проти одного» (або «Всі пари»). Ця стратегія передбачає попарне навчання $k(k-1)/2$ бінарних класифікаторів. В даному випадку для будь яких $1 \le i < j \le k$ з вихідної навчальної вибірки $(Q, Z) = \{\vec{q}_n, z_n\}_{n=1}^{N}$ формується бінарна вибірка (Q_{ij}, Z_{ij}), що містить тільки ті зразки (характеристичні вектори), мітка яких рівна *i* або *j*. Зразкам, які у вихідній вибірці мали мітку *i*, ставиться у відповідність бінарна мітка +1, а тим, що мали мітку *j*, – ставиться -1. На базі отриманого набору виконується навчання

бінарного класифікатора $p_{ij} : Q \to \{\pm 1\}$. Багатокласовий класифікатор як результат видає мітку класу, що отримала найбільшу кількість +1: $p(Q) = \arg\max_{i \in Z} \sum_{j=1..k, j \neq i} p_{ij}(Q)$.

Зауважимо, що при формуванні вихідної навчальної вибірки потрібно контролювати, щоб кількість представників всіх класів була достатньо великою та репрезентативною, щоб запобігти виникненню проблеми перенавчання [46]. Дана стратегія як і попередня страждає від неоднозначності в тих випадках, коли зразок отримує рівну кількість голосів за декілька класів. Разом з тим її застосування до методу опорних векторів є кращим вибором у порівнянні з «Один проти всіх», бо має меншу обчислювальну складність процесу навчання та потребує менше ресурсів пам'яті [47].

З прикладами багатокласового стеганоаналізу на базі SVM можна познайомитися у роботах [48–49]. Приклад розширення ансамблевого класифікатора на багатокласові задачі, який передбачає заміну правила більшості голосів узагальненим критерієм відношення правдоподібності (Generalized Likelihood Ratio Test), описано у публікації [50].

Висновки.

Проведене дослідження показало, що в сучасному стеганоаналізі широко використовуються здобутки з області штучного інтелекту, а саме методи машинного навчання: SVM, метод k найближчих сусідів, наївний байєсівський класифікатор, дерева рішень, нейронні мережі. В останні роки розвиток та ускладнення методів комп'ютерної стеганографії змусили дослідників будувати моделі характеристичних векторів великої розмірності, щоб охопити максимум змін, привнесених стеганоперетвореннями у звукові або графічні контейнери. Для забезпечення прийнятної швидкодії стеганосистем зі складними моделями характеристичних векторів потрібно підключати класифікатори, які добре масштабуються за розмірністю і передбачають ансамблеву архітектуру або глибоке навчання (deep learning). Використання надбань теорії машинного навчання дозволяє автоматизувати процес стеганоаналізу та досягти високих показників якості стеганоаналітичних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Samuel A.L. «Some Studies in Machine Learning Using the Game of Checkers», IBM Journal of Research and Development, V. 3, № 3, P. 210–229, 1959.
2. Mitchell T.M. «Machine Learning», New York: McGraw-Hill, 432 p., 1997.
3. Westfeld A., Pfitzmann A. «Attacks on steganographic systems», Information Hiding: 3rd International Workshop, P. 61–76, 1999.
4. Fridrich J., Goljan M., Du R. «Reliable detection of LSB steganography in grayscale and color images», Proc. of the ACM Workshop on Multimedia and Security, P. 27–30, 2001.
5. Dumitrescu S., Wu X., Wang Z. «Detection of LSB steganography via sample pair analysis», Information Hiding, 5th Intern. Workshop, V. 2578, P. 355–372, 2003.
6. Кошкіна Н.В. «Про вплив параметрів зображень у форматі JPEG на точність їх стеганоаналізу», Cybernetics and Computer Technologies, № 1, С. 74–85, 2021.

7. Ker A.D. «Steganalysis of LSB matching in grayscale images», IEEE Signal Processing Letters. V. 6, №12, P. 441–444, 2005.

8. Huang F., Shi Y.Q., Huang J. «New JPEG steganographic scheme with high security performance», International Workshop on Digital Watermarking", V. 6526, P. 189–201, 2010.

9. Pevny T., Bas P., Fridrich J. «Steganalysis by subtractive pixel adjacency matrix», IEEE Transactions on information Forensics and Security, V. 2, № 5, P. 215–224, 2010.

10. Xia Z., Wang X., Sun X., Wang B. «Steganalysis of least significant bit matching using multi-order differences», Security and Communication Networks, V. 8, № 7, P.1283–1291, 2014.

11. Zeng J., Tan S., Li B., Huang J. «Large-Scale JPEG Image Steganalysis Using Hybrid Deep-Learning Framework», IEEE Transactions on Information Forensics and Security, V. 13, № 5, P. 1200–1214, 2018.

12. Mustafa E.M., Elshafey M.A., Fouad M.M. «Enhancing CNN-based Image Steganalysis», GPUs. Journal of Information Hiding and Multimedia Signal Processing, V. 11, № 3, P. 138–150, 2020.

13. Boroumand M., Chen M., Fridrich J. «Deep Residual Network for Steganalysis of Digital Images», IEEE Transactions on Information Forensics and Security, V. 14, № 3, P. 1181–1193, 2019.

14. Kodovsky J., Fridrich J. «Steganalysis in high dimensions: fusing classifiers built on random subspaces», Proc. SPIE, Electronic Imaging, Media, Watermarking, Security and Forensics XIII, V. 7880 (78800L), 2011.

15. Fridrich J., Kodovsky J. «Rich Models for Steganalysis of Digital Images», IEEE Transactions on Information Forensics and Security, V.7, № 3, P. 868–882, 2012.

16. Holub V., Fridrich J. «Random Projections of Residuals for Digital Image Steganalysis», IEEE Transactions on Information Forensics and Security, V. 8, № 12, P. 1996–2006, 2013.

17. Holub V., Fridrich J. «Phase-Aware Projection Model for Steganalysis of JPEG Images», Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XVII, 9409, 2015.

18. Li W., Zhou W., Zhang W., Qin C., Hu H., Yu N. «Shortening the Cover for Fast JPEG Steganography», IEEE Transactions on Circuits and Systems for Video Technology, V. 30, № 6, P. 1745–1757, 2020.

19. Progonov D. «Statistical Steganalysis of Multistage Embedding Methods», International Journal Information Models & Analyses, V. 5, № 1, P. 23–36, 2016.

20. Yang Y., Kong X., Wang B., Ren K., Guo Y. «Steganalysis on Internet images via domain adaptive classifier», Neurocomputing, V. 351 (2), P. 205–216, 2019.

21. Корольов В.Ю., Поліновський В.В., Герасименко В.А., Горинштейн М.Л. «Дослідження кольорових цифрових фотографій методами RS-стегоаналізу та статистики», Інформація і право, Т. 3, № 3, С. 102–110, 2011.

22. Kharrazi M., Sencar H.T., Memon N.D. «Performance study of common image steganography and steganalysis techniques», Journal of Electronic Imaging, V. 15, № 4, P. 041104-1–16, 2006.

23. Denemark T., Fridrich J., Holub V. «Further study on security of S–UNIWARD», SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics, V. 9028, P. 1–13, 2014.

24. Chen C., Shi Y.Q. «JPEG image steganalysis utilizing both intrablock and interblock correlations», IEEE ISCAS, International Symposium on Circuits and Systems, P. 3029–3032, 2008.

25. Kodovsky J., Fridrich J. «Calibration revisited», In J. Dittmann,S. Craver, and J. Fridrich, editors, Proceedings of the 11th ACM Multimedia and Security Workshop, P. 63–74, 2009.

26. Liu Q. «Steganalysis of DCT–embedding based adaptive steganography and YASS», Proceedings of the 13th ACM Multimedia & Security Workshop, P. 77–86, 2011.

27. Pevny T., Fridrich J. «Merging Markov and DCT features for multiclass JPEG steganalysis», Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, V. 6505, P. 301–314, 2007.

28. Song X., Liu F., Yang C., Luo X., Zhang Y. «Steganalysis of Adaptive JPEG Steganography Using 2D Gabor Filters», Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. ACM, P.15–23, 2015.

29. Holub V., Fridrich J. «Low Complexity Features for JPEG Steganalysis Using Undecimated DCT», IEEE Transactions on Information Forensics and Security, V. 10, № 2, P. 219–228, 2015.

30. Yamini B., Sabitha R. «Blind steganalytic attack as pattern recognition using k-nearest neighbour classification technique», Fifth international conf. on advan-ced computing, P. 677–682, 2013.

31. Dautrich, J. «Multi-class steganalysis», Machine learning course research project distinguishing images embedded using reversible steganographic schemes, P. 1–6, 2009.

32. Kaipa B., Robila S.A. «Statistical steganalyis of images using open source software», Applications and technology conference (LISAT), P. 1–5, 2010.

33. Zeng W., Ai H., Hu R., Gao S. «An algorithm of echo steganalysis based on bayes classifier», Proc. of the 2008 IEEE Int. Conf. on Information and Automation, Zhangjiajie, P. 1667–1670, 2008.

34. Geetha S., Ishwarya N., Kamaraj N. «Audio steganalysis with Hausdorff distance higher order statistics using a rule based decision tree paradigm», Expert system with applications journal, V. 37, № 12, P. 7469–7482, 2010.

35. Benton R., Chu H. «Soft computing approach to steganalysis of LSB embedding in digital ima-ges», 3rd Int. Conf. on Information Technology: Research and Education, P. 105–109, 2005.

36. Nissar A., Mir A. H. «Texture based steganalysis of grayscale images using neural network», Signal processing research, V. 2, № 1, P. 17–24, 2013.

37. Ghanbari S., Keshtegary M., Ghanbari N. «New steganalysis method using glcm and neural network», International journal of computer applications, V. 42, № 7, P. 45–50, 2012.

38. Ru X., Zhuang Y., Wu F. «Audio steganalysis based on “negative resonance phenomenon” caused by steganographic tools», Journal of Zhejiang University SCIENCE A, V. 7, № 4, P. 577–583, 2006.

39. Johnson M., Lyu S., Farid H. «Steganalysis of Recorded Speech», Proc. SPIE, V. 5681, P. 664–672, 2005.

40. Bhattacharyya S., Sanyal G. «Feature Based Audio Steganalysis», Computer Network and Information Security, V. 11, P. 62–73, 2012.

41. Lyu S., Farid H. «Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines», Proc. Information Hiding, 5th International Workshop, ser. Lecture Notes in Computer Science, V. 2578, P. 340–354, 2002.

42. Rodriguez B.M., Peterson G.L., Agaian S.S. «Steganography anomaly detection using simple one-class classification», Proc. SPIE 6579, Mobile Multimedia/Image Processing for Military and Security Applications, V. 6579, P.1–9, 2007.

43. Sajedi H., Jamzad M. «CBS: Contourlet-Based Steganalysis Method», Journal of Signal Processing Systems, V. 61, P. 367–373, 2010.

44. Kodovský J., Fridrich J., Holub V. «Ensemble Classifiers for Steganalysis of Digital Media», IEEE Transactions on Information Forensics and Security, V. 7, № 2, P. 432–444, 2012.

45. Breiman L. «Bagging predictors», Machine Learning, V. 24, P. 123–140, 1996.

46. Hsu C.W., Lin C.J. «A comparison of methods for multiclass support vector machines», IEEE Transactions on Neural Networks, V. 13, № 2, P. 415–425, 2002.

47. R. Rifkin Multiclass Classification [Електронний ресурс]. – Режим доступу: https://www.mit.edu/~9.520/ spring09/ Classes /multiclass.pdf

48. Rodriguez B., Peterson G. «Detecting Steganography Using Multi-Class Classification», IFIP International Federation for Information Processing, V. 242, P. 193–204, 2007.

49. Koshkina N.V. «Comparison of Efficiency of Statistical Models Used for Formation of Feature Vectors by JPEG Images Steganalysis», Theoretical and Applied Cybersecurity, V. 2, № 1, P. 22–28, 2020.

50. Cogranne R., Fridrich J. «Modeling and Extending the Ensemble Classifier for Steganalysis of Digital Images Using Hypothesis Testing Theory», IEEE Transactions on Information Forensics and Security, V. 10, №. 12, P. 2627–2642, 2015.

УДК 004.056

АНАЛІЗ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРИКЛАДІ ПІДПРИЄМСТВА «РАЕС»

Фесенко А.О.
к.т.н.
доцент кафедри кібербезпеки та захисту інформації
КНУ імені Тараса Шевченка
aafesenko88@gmail.com

Мирутенко Л.В.
к.т.н. доцент
доцент кафедри кібербезпеки та захисту інформації
КНУ імені Тараса Шевченка
myrutenko.lara@gmail.com

Куроєдов А.С.
студент кафедри кібербезпеки та захисту інформації
КНУ імені Тараса Шевченка
askuroyedov@gmail.com

Анотація. Атомна енергетика відіграє дуже важливу роль в сучасному енерговиробництві. Безперервна робота АЕС є головною метою підприємства «НАЕК Енергоатом». Описано криптографічні системи захисту інформації для об'єкту критичної інфраструктури Рівненської АЕС, що стандартизовані в Україні, та які запропановано використовувати для захисту інформації, наприклад, ГОСТ 28147-89, FIPS-197, «Стрибог» тощо. За допомогою криптографічних алгоритмів підприємство може захиститись від вторгнення, викрадення чи пошкодження спеціального обладнання та інформації, що може призвести до призупинення роботи АЕС, фінансових та матеріальних втрат для компанії. Описано важливість впровадження криптографічної системи захисту інформації на АЕС.

Рівненська АЕС – це одне з найбільших підприємств України, яке є відокремленим підрозділом державного підприємства «НАЕК «Енергоатом» [1].

Щорічно, АЕС виробляє близько 19 млрд кВт год електроенергії, що становить 23% від виробництва атомними електростанціями або 12% від загального виробництва електроенергії в Україні [1]. Таким чином, правильне та безупинне функціонування Рівненської АЕС надзвичайно важливе для енергозабезпечення підприємства та держави [2].

Для безпечного функціонування підприємства на етапі його будівництва та в подальшому, створюється комплексна система захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю, яка передбачається постановою Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [3].

Захист інформації на такому підприємстві як АЕС являється дуже важливим завданням, так як АЕС являється об'єктом критичної інфраструктури і відіграє стратегічну роль для України [2]. Для захисту інформації прийнято використовувати різні криптографічні системи. Криптографічні системи захисту інформації – це сукупність різних криптографічних алгоритмів, протоколів і процедур формування, розподілу, передачі й використання криптографічних ключів [3].

Криптографічні системи, у загальному випадку, класифікуються на основі наступних трьох незалежних характеристик [4]:

1) тип операцій з перетворення відкритого тексту в шифрований;

2) число ключів, що використовуються;

3) метод обробки відкритого тексту.

До шифрів, які використовуються для криптографічного захисту інформації, висувають низку вимог: статистична безпека алгоритмів; надійність математичної бази алгоритмів; простота процедур шифрування й розшифрування; незначна надмірність інформації за рахунок шифрування; простота реалізації алгоритмів на різній апаратній базі [4].

В Україні на даний час стандартизовані різні криптографічні алгоритми захисту інформації. Наприклад, алгоритм «Калина», який описано в ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення; алгоритм криптографічного перетворення ГОСТ 28147-89; FIPS-197; ітеративна криптографічна геш-функція ДСТУ 7564:2014; «Стрибог», що описаний в ГОСТ 34.11-2018 [5]. Всі ці алгоритми захисту інформації рекомендовано використовувати саме на об'єктах критичної інфраструктури держави, яким є Рівненська АЕС.

За допомогою криптографічних методів захисту інформації, підприємство може захиститись від вторгнення, викрадення чи пошкодження спеціального обладнання, що може призвести до збою чи відключення цього обладнання, до збору конфіденційної інформації, за допомогою якої можна виявити слабкі місця для подальшого вторгнення або продати інформацію в Даркнеті [6]. Підприємство, що є об'єктом критичної інфраструктури, в даному випадку АЕС, має постійно вдосконалювати системи захисту інформації та використовувати новітні розробки. Отже проблема захисту інформації на об'єкті критичної інфраструктури є актуальною.

Таким чином, АЕС є важливим стратегічним об'єктом держави, одним з головних завдань якого є забезпечення безпеки інформації, що обробляється на даному підприємстві. Використовуючи різноманітні криптографічні системи захисту, корпорація може забезпечити протидію зловмисним діям та захистити себе від кібератаки, що призведе до успішної та ефективної роботи АЕС і як наслідок процвітання держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рівненська АЕС. Офіційна статистика [Електронний ресурс] Режим доступу – https://sprut2.rnpp.rv.ua/about-info

2. Рівненська АЕС. Місія та бачення [Електронний ресурс] Режим доступу – https://sprut2.rnpp.rv.ua/about-mission

3. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс] Режим доступу – https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

4. Криптографія. Шифрування та дешифрування інформації [Електронний ресурс] Режим доступу – https://www.znanius.com/3851.html

5. ТЕХНІЧНІ СПЕЦИФІКАЦІЇ до RFC 5652 [Електронний ресурс] Режим доступу – https://zakon.rada.gov.ua/laws/show/z1273-20#Text

6. Комп’ютерна безпека інформаційних та управляючих систем АЕС [Електронний ресурс] Режим доступу – http://dspace.nbuv.gov.ua/bitstream/handle/123456789/104983/12-Klevtsov.pdf?sequence=1

УДК 004.056.55:519.876.5

АНАЛІЗ МЕТОДИКИ ОЦІНЮВАННЯ КОЕФІЦІЄНТУ ЯКОСТІ ШУМУ ДЛЯ ГЕНЕРАТОРІВ РОЖЕВОГО ШУМУ

Мартинюк Г.В.
к.т.н., доцент, доцент кафедри
засобів захисту інформації
Національний авіаційний університет
ganna.martyniuk@gmail.com

Мартинайтус Є.О.
заступник начальника центру –
начальник 1 відділу 4 центру ТЗІ
ДержНДІ технологій кібербезпеки
Martin00@ukr.net

Анотація. У роботі наводяться методики оцінювання коефіцієнту якості шуму, які зустрічаються на сьогодні для оцінки генераторів. Проводиться аналіз відомих методик на доцільність їх використання для сучасних генераторів рожевого шуму.

Проблема захисту та обробки мовної інформації є однією з проблем інформаційної безпеки. У сучасному світі з наростаючими обсягами оброблюваних даних зростає і кількість мовної інформації у державних установах і на підприємствах, у процесі проведення різноманітних нарад, конференцій, зборів, засідань тощо. На рисунку 1 наглядно наведено шляхи витоку мовної інформації з приміщення.

Відповідно до загальних методів захисту інформації для захисту від прослуховування використовуються такі методи [1]:

- структурний камуфляж
- приховування енергії.

Структурний камуфляж може бути реалізований такими методами:

- шифрування смислової мовної інформації у функціональних каналах зв'язку;
- технічне закриття електричних та радіосигналів у каналах телефонного зв'язку;
- дезінформація.

Енергетичне приховування може бути реалізовано:

- звукоізоляцією акустичного сигналу;
- звукопоглинанням акустичних хвиль;
- зашумленням приміщення іншими звуками (шум, перешкоди), що забезпечує маскування акустичних сигналів;
- виявленням, локалізацією та вилученням вбудованих пристроїв.

У цій роботі автори вирішили вивчити саме генератори шуму, які встановлюються в приміщенні для запобігання виявлення мовної інформації.

Для запобігання витоку інформації під час таких нарад, необхідно забезпечувати гарантований захист відомостей, який можна організувати з використанням активних засобів, наприклад, за допомогою генераторів маскуючого шуму. Розробці та дослідженню різних методів обробки та захисту мовної інформації, а також визначенню розбірливості мовних повідомлень як основного показника їхньої захищеності присвячено велику кількість робіт, наприклад [1,2]. Проте необхідно пам’ятати, що зашумлений інформативний сигнал може бути підданий фільтрації і у разі неякісного маскування зловмисник отримає доступ до відомостей, що захищаються. Тому виникає завдання, пов'язане з оцінкою якості шумового сигналу, що породжується засобами активного захисту.

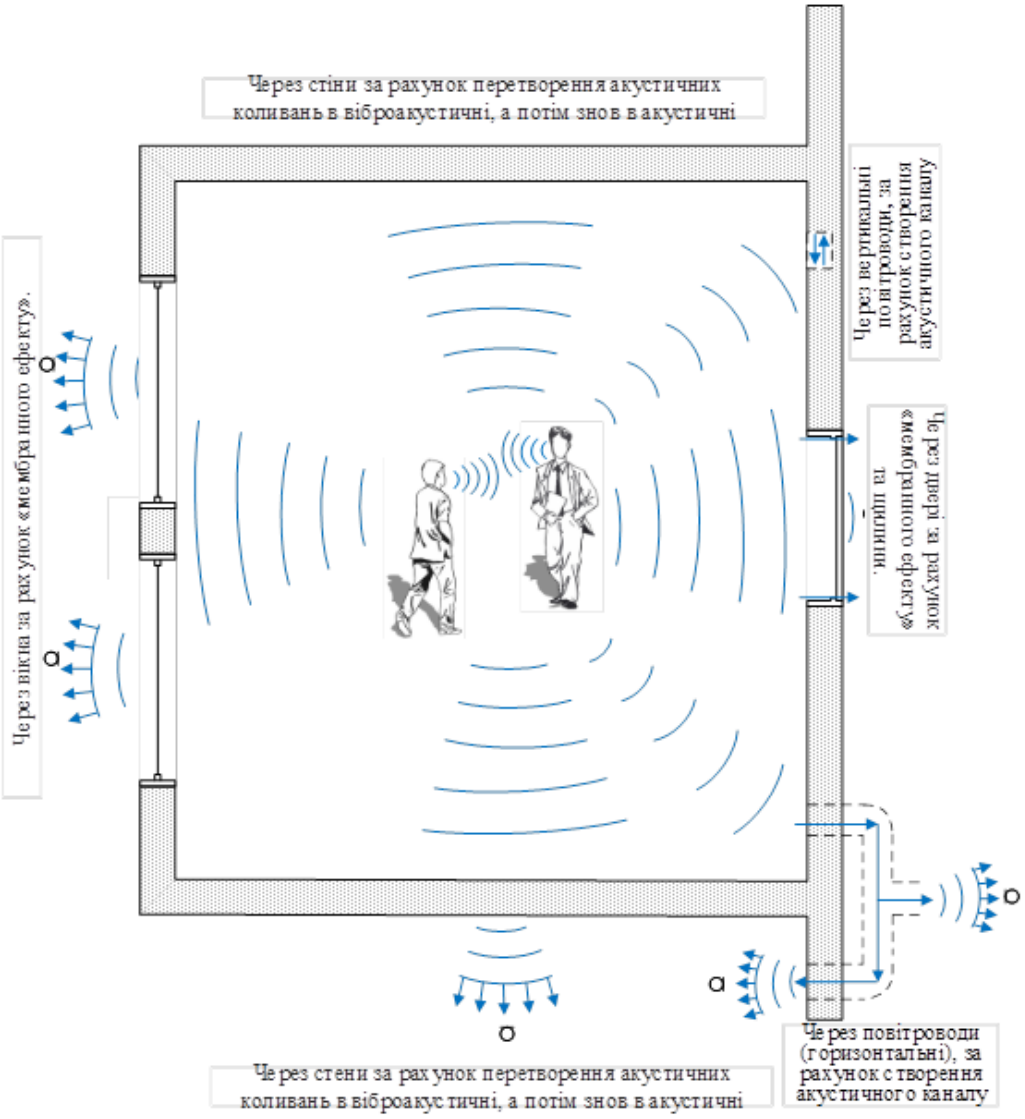


Рис. 1. Ілюстрація можливих шляхів витоку мовної інформації з приміщення.

Існує три загальні тенденції розробки таких генераторів. Перша тенденція – використання зворотного зв’язку для регулювання спектру шумового сигналу та

його рівня залежно від рівня акустичного сигналу, який треба маскувати. Друга тенденція – створення закритого ланцюга зв'язку для розмов між учасниками переговорів. Вона реалізується або за рахунок шифрування розмов, що передаються в ізольованому від навколишнього акустичного середовища колі, або шляхом використання поза цього кола спеціальної завади, що не дозволяє зняття розбірливої акустичної інформації за межами цього кола.

Третя тенденція – використання змішаної завади, яка складається з тихої музики, шуму та голосових сигналів декількох учасників розмови, які зсунуті у часі та інвертовані по спектру. Така суміш сигналів не дозволяє зняти розбірливі сигнали розмови. Навіть якщо записати розмову, що замасковано таким чином, та очистити її відомими нині методами, неможливо отримати розбірливих сигналів. При цьому методі маскування рівень завади, що випромінюється у повітря приміщення, значно нижчий від рівня шуму, який випромінюється при застосуванні звичайного генератору.

Ефективний захист конфіденційної мовної інформації генераторами маскуючого шуму є досить важливим завданням для більшості державних та комерційних установ. Тим не менш, в даний час немає єдиного підходу до оцінки якості маскуючих шумів для зашумлення мовної інформації, а існуючі методики потребують серйозного доопрацювання.

Для визначення оціночних характеристик маскуючого шуму використовуються інформаційні та енергетичні критерії. Перша група критеріїв розглядає статистичні параметри шумових сигналів у часовій області та дозволяє безпосередньо визначити числовий коефіцієнт якості шуму. На основі розрахунку математичного сподівання, дисперсії та ентропії миттєвих значень вибірки та їхньої обвідної обчислюється ступінь наближення до деяких еталонних розподілів. Такі методи спрямовані на знаходження ступеня невизначеності миттєвих значень шумових сигналів, що виражаються, наприклад через ентропійний коефіцієнт якості маскуючого шуму.

Критерії з другої групи для гарантованого захисту інформації використовують постулат про необхідність перевищення енергетики шуму над сигналом, що маскується. Тому для перевірки якості шуму використовуються інтегральні показники, які враховують перевищення рівня шуму над рівнем інформативного сигналу. Наприклад, весь частотний діапазон шуму, що маскує, може розбиватися на кілька октавних смуг, на середніх частотах кожної з яких вимірюється рівень шуму.

З погляду енергетичної ефективності генерації маскуючих шумів, а також для безпосереднього визначення їх ймовірнісних властивостей найбільший інтерес становлять інформаційні критерії.

Перед тим, як навести методики визначення коефіцієнтів якості шуму, необхідно навести загальну інформацію про рожевий шум, який використовується в генераторах для маскування інформації.

Рожевий шум (флікер-шум) – шум, спектральна густина якого змінюється з частотою f за законом 1/f. Цим забезпечується однакова енергія сигналу перешкоди на кожну октаву. Іноді рожевим шумом називають будь-який шум, спектральна щільність якого зменшується зі зменшенням частоти (рисунок 2).

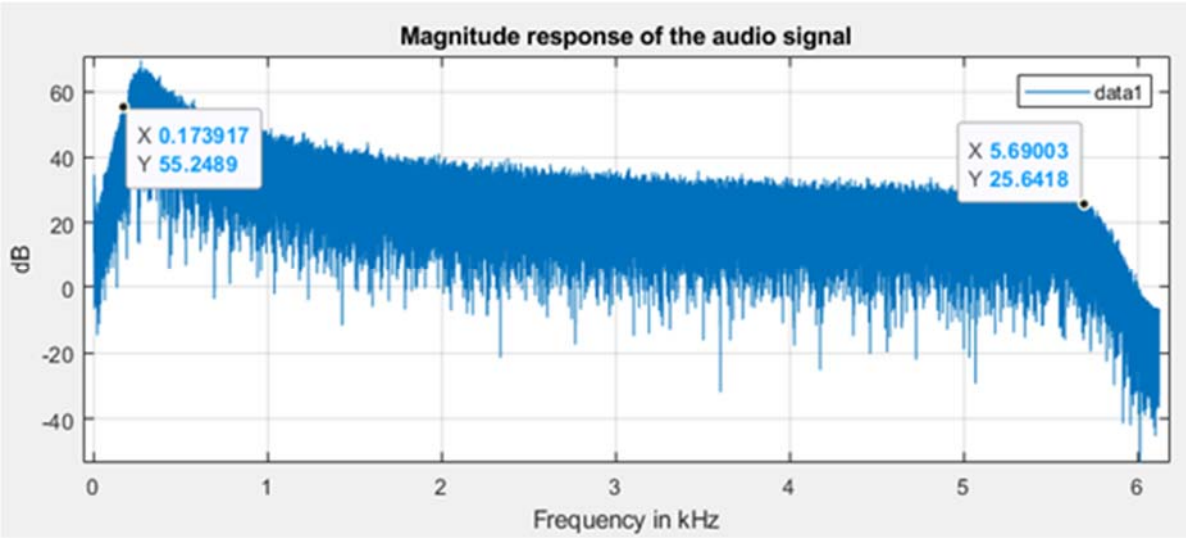


Рис. 2. Графік спектральної щільності шумового сигналу
в діапазоні 180 -5600 Гц.

Отже, для рожевого шуму характерною є постійність енергії у межах кожної октави зміни частоти. Це означає, що спектральна щільність зменшується при збільшенні частоти за логарифмічним законом. Такий шум широко розповсюджений у природі і багато випадкових процесів підпорядковується саме йому.

Далі наведено різні методики, які описані в літературі для визначення характеристик якості акустичного шуму, випромінюваного генераторами.

Методика визначення коефіцієнта якості шуму з використанням коефіцієнтів асиметрії та ексцесу.

Дана методика була розроблена для оцінки якості електромагнітного поля шуму, проте авторами була проведена спроба використання її для генераторів рожевого шуму, які використовуються для активного маскування мовного сигналу. Методика заключається в наступному:

1. Отримання вибірки шумового сигналу у дискретній формі.
2. Визначення математичного сподівання m_1 отриманої вибірки.
3. Розрахунок другого m_2, третього m_3 та четвертого m_4 центральних моментів.
4. Визначення розрахункових значень коефіцієнту асиметрії $\gamma_a = \frac{m_3}{\sqrt{m_2^3}}$ та коефіцієнту ексцесу $\gamma_e = \frac{m_4}{m_2^2} - 3$ досліджуваної вибірки.
5. Визначення коефіцієнта якості шуму за формулою

$$\Theta = 1.06987 + 3\gamma_e - 1.56\ln\left(e^{2\gamma_e} + 0.037e^{0.23e^{3.43|\gamma_a|}}\right)$$

Згідно з даною методикою, коефіцієнт якості шуму повинен бути в межах від 0,8 до 1,0. Авторами були проведені експериментальні дослідження з генераторами рожевого шуму різних торгових марок, а також проводився експеримент над генераторами, побудованими за допомогою псевдовипадкової

послідовності чисел, реалізованої у програмному середовищі Python. Результати для всіх вибірок розміром 10 с (441000 відліків) дали результати по коефіцієнту якості шуму, показані в таблиці 1.

Таблиця 1.

Розрахункові показники коефіцієнта якості шуму з використанням коефіцієнтів асиметрії та ексцесу

Генератор шуму	Коефіцієнт асиметрії	Коефіцієнт ексцесу	Коефіцієнт якості шуму
Фірмовий генератор	0,0119	-0,1219	0,9936
Створений з псевдовипадкової послідовності	-0,0089	-0,6998	0,8823

Як видно з таблиці 1, дана методика показала, що можна використовувати на практиці як фірмові генератори різних торгових марок, так і шумовий сигнал, утровений з пседовипадкової послідовності чисел.

Наступні методики зводяться до низки обчислювальних операцій, вироблених з квантованими виміряними значеннями електричного сигналу, в який перетворюється маскуючий шум. Основу даних методів становить розрахунок міри невизначеності (ентропії) закону розподілу миттєвих значень маскуючого шуму, а також ентропії закону розподілу значень огинаючої шумового сигналу.

У роботах Козлачкова С.Б., Тупоти В.І., Купріянова О. І., Сахарова О. В.та ін. запроваджується поняття ентропійного коефіцієнта якості шуму. Зазначені коефіцієнти розраховуються щодо деяких еталонних законів розподілу. Для миттєвих значень маскуючого шуму в умовах обмежень, що накладаються на середню потужність, еталонним є нормальний закон розподілу, а для обвідної нормально розподілених миттєвих значень маскуючого шуму - закон розподілу Релея.

Методика визначення ентропійного коефіцієнту якості.

У ряді робіт замість знаходження коефіцієнту якості шуму, описаного вище, пропонується знаходити ентропійний коефіцієнт якості шуму. Ентропія дозволяє оцінити маскуючі властивості сигналів завади безвідносно до конкретних способів їх прийому і обробки. Завдання вибору максимально ефективної завади зводиться до визначення такого розподілу завади, при якому при заданих статистичних властивостях сигналу відтворена інформація засобами технічної розвідки була б мінімальною.

Обчислення ентропії зводиться до побудови гістограми розподілу щільності ймовірностей $p(x_i)$, після чого необхідно використати формулу

$$H(x) = -\sum_{i=1}^{n} p(x_i)\log(p(x_i)), \quad (1)$$

де $p(x_i)$ – ймовірність потрапляння елементу вибірки до i-го діапазону гістограми, n – кількість діапазонів гістограми.

Ентропійний коефіцієнт якості шуму знаходиться за формулою

$$\gamma = \frac{e^{2H(x)}}{2\pi e}. \quad (2)$$

Ентропійний коефіцієнт якості шуму повинен не перевищувати 1, проте, в ході проведення досліджень з різними генераторами рожевого шуму, автори пересвідчилися, що використовуючи формулу (1) для знаходження ентропії, ентропійний коефіцієнт якості перевищує одиницю в сотні разів, що унеможливлює використання даної формули. Тому було прийнято рішення використати іншу формулу для знаходження ентропії.

Враховуючи те, що в рамках дослідження використовувалися генератори рожевого шуму, то необхідно відзначити, що рожевий шум підпорядкований нормальному закону розподілу. Це було доведено в результаті знаходження гістограми для генераторів шуму (рисунок 3). Варто також зазначити, що отримані результати гістограми однакові для всіх використовуваних в експериментів генераторів.

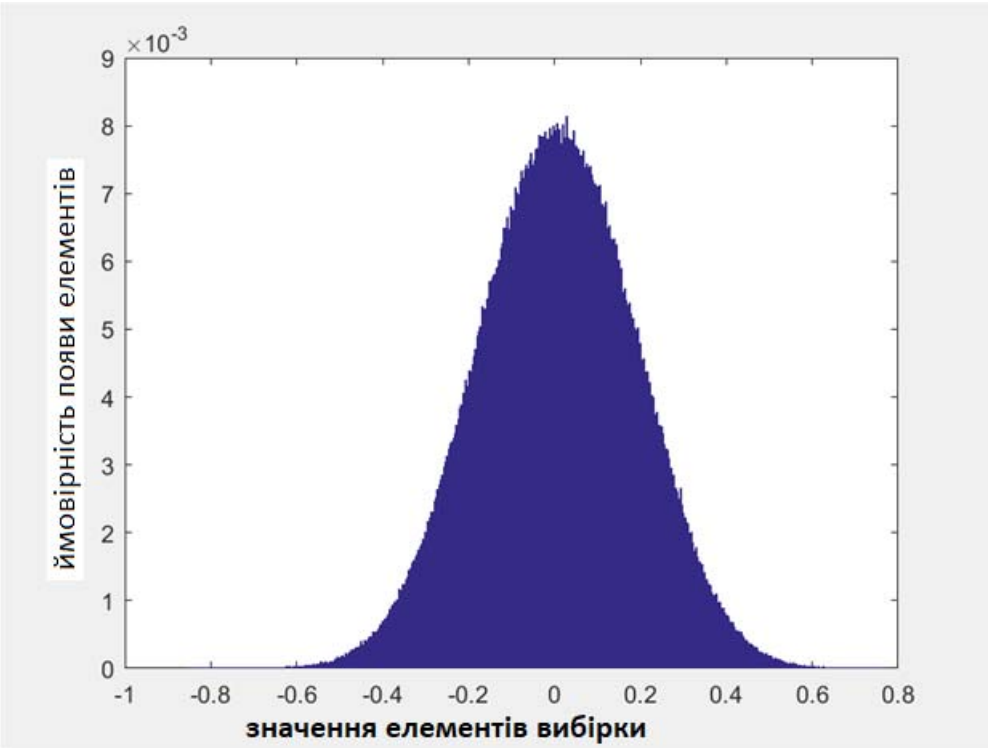


Рис. 3. Гістограма генератора шуму.

У зв’язку з цим було прийнято рішення ентропію за формулою (1) можна замінити на знаходження ентропії для нормального гаусового розподілу, що має вигляд

$$H(x) = \ln\left(\sqrt{2\pi e\sigma^2}\right), \quad (3)$$

де σ^2 – дисперсія вибірки.

Використовуючи для знаходження ентропійного коефіцієнту якості шуму формулу (3), автори отримали результати, наведені у таблиці 2.

Таблиця 2.

Результати визначення ентропійного коефіцієнту якості шуму

Генератори	**Ентропійний коефіцієнт**	**Середня потужність сигналу**	**Коефіцієнт якості сигналу**
Фірмовий генератор	0,0534	0,0533	1,0
Створений з псевдовипадкової послідовності	0,2118	0,2118	1,0

Як видно з таблиці 2, ентропійний коефіцієнт дорівнює 1 для всіх видів генераторів, які використовувалися в експерименті. Необхідно зазначити, що автори також змінювали довжину вибірки (тривалість сигналу), змінювали рівні шуму та рівні квантування, але результати знаходження ентропійного коефіцієнту якості сигналу завжди знаходилися в межах 0,99-1,0.

Таким чином, можна зробити висновок про неефективність використання методики визначення ентропійного коефіцієнту якості шуму на практиці.

Методика визначення ентропійного коефіцієнту якості розподілу обвідної шумового сигналу.

Дана методика подібна до попередньої, але ентропія знаходиться не для вибірки генератора шуму, а для вибірки огинаючої генератора шуму, яка повинна бути підпорядкована розподілу Релея. Алгоритм визначення коефіцієнту якості наступний:

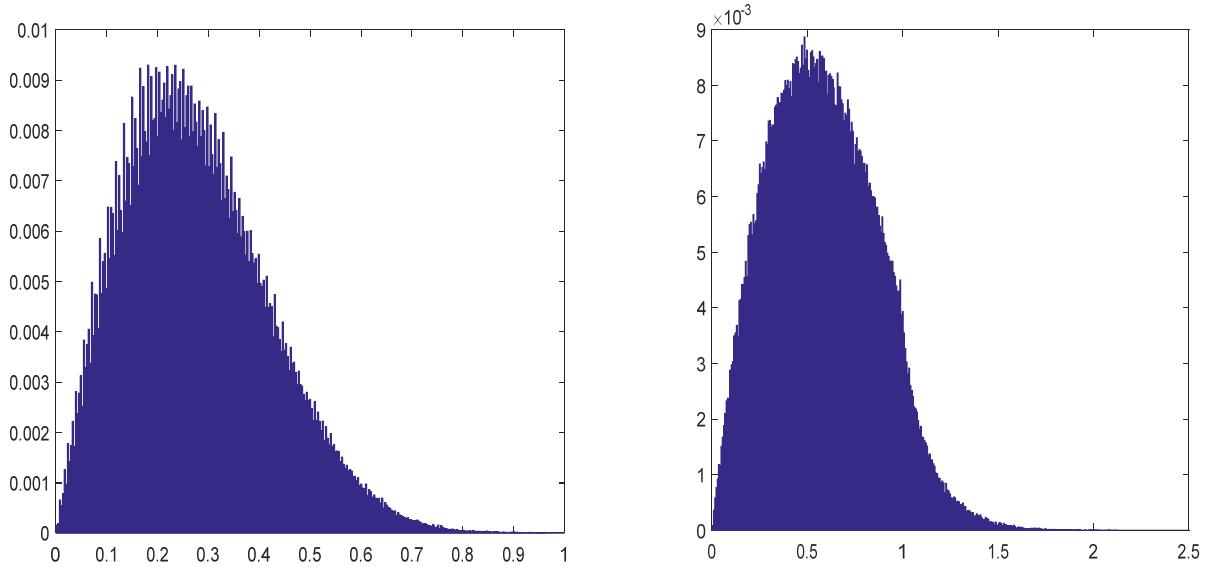
1. Знаходження обвідної шумового сигналу за формулою
2.

$$A(t) = \sqrt{s(\mathrm{t})^2 + s_{\perp}(t)^2}\ ,$$

де $s_{\perp}(t)$ - пов'язана (за Гільбертом) функція, яка визначається як уявна частина аналітичного сигналу

$$\dot{s}_a(t) = s(t) + is_{\perp}(t)\ .$$

3. Побудова гістограми закону розподілу огинаючої шумового сигналу. Результати отриманих гістограм наведено на рисунку 4.



а) б)

Рис. 4. Гістограми обвідної генераторів шуму:
а) гістограма, отримана для фірмового генератора;
б) гістограма, отримана для генератора з псевдовипадкової послідовності.

4. Знаходження ентропії H_0 закону розподілу огинаючої за формулою (1).

5. Знаходження параметру еталонного розподілу Релея r за формулою $\frac{\mu_2^0}{2r^2} + \ln r = M\left[\ln x\right] + 1 + \frac{\gamma}{2} - \ln\sqrt{2}$, де μ_2^0 – другий момент закону розподілу огинаючої шумового сигналу; $M\left[\ln x\right]$ – математичне сподівання натурального логарифму значень огинаючої шумового сигналу, γ – константа Ейлера.

6. Знаходження ентропії еталонного розподілу Релея за формулою $\hat{H} = 1 + \frac{\gamma}{2} + \ln\left(\frac{r}{\sqrt{2}}\right)$.

7. Знаходження ентропійного коефіцієнта якості розподілу огинаючої шумового сигналу за формулою $\eta = e^{H_0 - \hat{H}}$.

Необхідно зазначити, що при використанні формули (1) для знаходження ентропійного коефіцієнту за даною методикою, ентропійний коефіцієнт був в межах 0,01-0,02. Проте такі результати не відповідають дійсності.

Через це авторами було прийнято рішення замість використання формули (1) використати формулу для знаходження ентропії розподілу Релея:

$$H = 1 + \ln\left(\frac{\sigma}{\sqrt{2}}\right) + \frac{\gamma}{2},$$

де σ – середньоквадратичне відхилення, $\gamma \approx 0{,}57721566490153286060$ – контсанта Ейлера.

Провівши ряд експериментів за даною методикою, автори отримали результати, наведені у таблиці 3.

Таблиця 3.

Результати знаходження ентропійного коефіцієнту якості розподілу обвідної генератору шуму

Генератор	Ентропія обвідної	Ентропія еталонного розподілу Релея	Ентропійний коефіцієнт якості
Фірмовий генератор	1,0059	0,8661	1,15
Створений з псевдовипадкової послідовності	0,3124	0,8661	0,5748

Як видно з отриманих результатів, методика оцінки ентропійного коефіцієнту якості розподілу обвідної шумового сигналу – єдина методика, яка дає різні результати для різного виду генераторів шуму і потребує подальшого статистичного напрацювання для визначення інтервалу, який буде відповідати за адекватну роботу генераторів шуму.

Проаналізувавши існуючи на сьогодні методики оцінки коефіцієнту якості шуму, автори дійшли висновку, що вони потребують доопрацювання. Крім того, автори вважають, що для більш детальної оцінки маскувальних ознак генераторів рожевого шуму недостатньо знаходити тільки коефіцієнт якості шуму, необхідно вводити також й інші оцінки для більш детального обгрунтування доцільності використання того чи іншого генератора рожевого шуму на практиці.

Висновки. Згідно з отриманими результатами, наведеними у роботі, можна зробити наступні висновки.

- Розглянуто різні методики визначення коефіцієнтів якості шуму для генераторів рожевого шуму.
- Для кожної розглянутої методики наведено практичні результати.
- Зроблено висновки про доцільність використання кожного з методів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації. НД ТЗІ Р-001-2000.

2. Прокофьєв М. Оцінювання коефіцієнта якості шумової завади в системах активного захисту інформації / М. Прокофьєв, В. Куліш, М. Ващенко, В. Дворський, В. Стеченко, А. Тодоренко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. – Вип. 1 (29). – С. 15-20.

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Колективна монографія

Відповідальні за випуск О.В. Скляренко, А.М. Давиденко

Видається в авторській редакції

Відповідальність за достовірність фактів, цитат, власних імен та інших даних несуть автори статей. Думки, положення і висновки, висловлені авторами, не обов'язково відображають позицію редакційної колегії.

Українською та англійською мовами

Комп'ютерна верстка – Піддубенко Т. А.

Підписано до друку 16.03.2023 р.
Зам. 10. Формат 60х84/16.
Гарнітура Times New Roman.
Ум. друк. арк. 11,85.

Поліграфкомбінат ПВНЗ «Європейський університет»
03115, Україна, Київ -115, вул. Депутатська 15/17.

Реєстраційне свідоцтво ДК №3833 від 14.07.2010 р.