Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І.І. _____

« » червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

за спеціальністю: 125 - Кібербезпека

на тему: «Узагальнення передумов виникнення доксінгу та дослідження основних складових, щодо протидії його проявам в ІТ-сфері»

оцінка « » Керівник Малахов С.В.
(прізвище та ініціали/підпис)

Голова ЕК Рецензент Гостев О.Л.
(прізвище та ініціали/підпис)

Лемешко О.В._____ Виконавець: студентка групи КБ-42

Чорна Т.Е.
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить: 63 сторінки, 6 рисунків, 8 таблиць, 26 використаних джерел, 1 додаток.

Мета роботи: – аналіз сучасного стану проблематики доксінгу та дослідження можливостей з комплексної протидії цій загрозі в IT-сфері.

Об’єкт дослідження: – технології і засоби комплексного захисту персоніфікованої та корпоративної інформації в сучасних інформаційних системах (ІС).

Предмет дослідження: – передумови і шляхи реалізації доксінгу в IT сфері та основні складові з протидії цій загрозі.

Основними методами досліджень є аналіз та порівняння.

В роботі досліджені основні особливості проблематики доксінгу та встановлено його зв’язок з внутрішніми загрозами ІБ. Проведено аналіз передумов і основних шляхи реалізації доксінгу. Досліджено юридичні аспекти питання захисту конфіденційної інформації. Проведено огляд субстантивної часті профільних документів GDPR та PDPO. Підкреслена необхідність реалізації комплексного підходу для ефективної протидії доксінгу. Встановлено тісний взаємозв'язок доксінгу та атак з використанням прийомів соціальної інженерії (SE-атак). Вивчено можливості запобігання передумовам здійснення доксінгу. Визначено основні шляхи з протидії SE-атакам та корпоративному інсайду. Розглянуті особливості впровадження систем захисту від витоку даних (DLP систем).

Результати роботи можуть бути використані в освітніх цілях та, як допоміжний (довідковий) матеріал для розширення рівня компетенцій в сфері забезпечення ІБ для персоналу сучасних IT-компаній.

Ключові слова: ДОКСІНГ, ІНФОРМАЦІЙНІ СИСТЕМИ, ЗАГРОЗА, ІНФОРМАЦІЙНА БЕЗПЕКА, DLP, GDPR, ІНСАЙД, СОЦІАЛЬНА ІНЖЕНЕРІЯ, ФІШИНГ.

ABSTRACT

The explanatory note contains: 63 pages, 6 figures, 8 tables, 26 used sources, 1 appendix.

The purpose of the work: - analysis of the current state of the issue of doxing and the study of opportunities for comprehensive countermeasures against this threat in the IT sphere.

The object of research: - technologies and means of comprehensive protection of personalized and corporate information in modern information systems (IS).

Subject of research: - prerequisites and ways of implementing doxing in the IT sphere and the main components of countering this threat.

The main research methods are analysis and comparison.

The work examines the main features of the doxing problem and establishes its connection with internal IS threats. An analysis of the prerequisites and main ways of implementing doxing was carried out. The legal aspects of the issue of protecting confidential information were studied. A review of the substantive part of the GDPR and PDPO profile documents was conducted. The need to implement a comprehensive approach to effectively combat doxing is emphasized. A close relationship between doxing and attacks using social engineering techniques (SE-attacks) was established. The possibility of preventing the prerequisites for doxing was studied. The main ways of countering SE-attacks and corporate insiders have been determined. The peculiarities of the implementation of data leakage protection systems (DLP systems) are considered.

The results of the work can be used for educational purposes and as auxiliary (reference) material for expanding the level of competencies in the field of IS provision for the personnel of modern IT companies.

Keywords: DOXING, INFORMATION SYSTEMS, THREAT, INFORMATION SECURITY, DLP, GDPR, INSIDE, SOCIAL ENGINEERING, PHISHING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

ІБ – інформаційна безпека;

ПЗ – програмне забезпечення;

API – прикладний програмний інтерфейс (Application Programming Interfaces);

DLP – технології запобігання витоку конфіденційної інформації (Data Leak Prevention);

FTP – протокол передачі файлів по мережі (File Transfer Protocol);

GDPR – Загальний регламент захисту даних (General Data Protection Regulation);

HTTP – протокол передачі даних (Hypertext Transfer Protocol);

HTTPS – захищений протокол передачі даних (Hypertext Transfer Protocol Secure);

IP – інтернет протокол (Internet Protocol);

IPS – система запобігання вторгненням (Intrusion Prevention System);

IRM – управління реагуванням на інциденти (Integrated Risk Management);

IS – інформаційна система (Information Systems);

ISP – провайдер послуг Інтернету (Internet Service Provider);

NIS – Директива про мережеву та інформаційну безпеку (Network and Information Security);

OSI – абстрактна мережева модель для комунікацій і розробки мережевих протоколів (Open Systems Interconnection);

OTP – пароль, дійсний тільки для одного сеансу автентифікації (One Time Password);

PAM – управління привілейованим доступом (Privileged Access Management);

PDPO – Постанова про персональні дані/конфіденційність (The Personal Data (Privacy) Ordinance);

SE – соціальна інженерія (Social Engineering);

SIEM – інформація про безпеку та управління подіями (Security information and event management);

SMS – сервіс для відправки коротких повідомлень (Short Message Service);

SMTP – простий протокол передачі електронної пошти (Simple Mail Transfer Protocol);

SSL – протокол безпечного шифрування даних (Secure Sockets Layer);

UAM – моніторинг активності користувачів (User Activity Monitoring Software);

UBA – технологія аналізу історії активності користувача на робочому місці (User Behavior Analytics);

URL – стандартизована адреса певного ресурсу в інтернеті (Uniform Resource Locator);

USB – послідовний інтерфейс для підключення периферійних пристроїв до обчислювальної техніки (Universal Serial Bus);

VPN – технології віртуальних захищених мереж (Virtual Private Network);

WHOIS – мережевий протокол, що використовується для отримання інформації про доменне ім'я.

ВСТУП

На сьогоднішній день дані є одним із найважливіших активів організацій, які в межах своєї діяльності здійснюють її зберігання, обробку і поширення. До таких даних належить інформація про потенційних клієнтів, їхні інтереси, події, спікерів, контент, соціальні медіа, пресу, персонал, бюджет, стратегічний план тощо. Оскільки організації відкривають свої двері для співробітників, партнерів, клієнтів, щоб забезпечити глибший доступ до конфіденційної інформації, ризики, пов’язані з бізнесом, зростають. Зараз, як ніколи, в умовах зростаючих загроз кібертероризму, проблем корпоративного управління, шахрайства та крадіжки особистих даних, потреба у захисті корпоративної інформації стала першочерговою. Крадіжка інформації стосується не лише зовнішніх хакерів і неавторизованих зовнішніх користувачів, які викрадають дані, це також стосується управління внутрішніми співробітниками. До проблеми захисту інформації додається зростаючий попит на корпоративне управління та дотримання законодавчих чи нормативних вимог. Недотримання вимог та забезпечення конфіденційності, аудиту і внутрішнього контролю може призвести не лише до потенційних наслідків для керівників, але й до можливих загроз життєздатності організації. Наявність інсайдерів також свідчить про потенційну небезпеку для захищеності даних. Завдання виявлення зловмисних інсайдерів є дуже складним, оскільки методи обману стають усе більш «вишуканими».

Аналіз відомостей, стосовно постійно зростаючої кількості інцидентів безпеки, пов'язаних із витоком інформації як на побутовому рівні так і на рівні організацій, вказує на виникнення та регулярний розвиток нових методів та інструментів незаконного збору даних.

Існують різні рішення, щоб уникнути витоку даних, такі як: використання брандмауєрів, віртуальної приватної мережі (VPN), звітність,

відеоспостереження, UAM, антишпигунське програмне забезпечення, тренінги з питань безпеки і тд.

Найбільш перспективною є технологія запобігання втраті даних (DLP), що стала невід'ємним компонентом набору безпеки організації. Рішення DLP відстежують конфіденційні дані, коли вони перебувають у стані спокою, у русі чи під час використання, і забезпечують дотримання політики захисту даних організації. Ці рішення зосереджені головним чином на даних та рівні їх конфіденційності, а також на запобіганні отримання до них доступу неавторизованими особами. Це дослідження зосереджено на вивченні засобів для виявлення та запобігання витоку даних.

Слід зауважити, що важливе значення у питанні захисту особистих даних відіграє нормативно-правова база. Відповідність всім нормам міжнародного законодавства підвищує рівень довіри до ресурсу, розширює сферу впливу організації на світовому ринку та суттєво впливає на її конкурентоспроможність.

Тому розгляд питань, стосовно безпеки персональних даних з метою підвищення ефективності роботи організацій, є безумовно актуальним, та потребує проведення ретельного аналізу і відповідних досліджень. Це мінімізує наслідки некоректних дій персоналу у системі, посприяє створенню культури інформаційної безпеки та протидії проявам доксування в ІТ-сфері.

1 АНАЛІЗ ІНЦИДЕНТІВ З ДОКСІНГУ ДАНИХ

1.1 Узагальнення випадків доксінгу

На тлі зростання популярності доксінгу у світі проводиться все більше і більше досліджень для вивчення його наслідків. Доксінг – це форма кіберзалякування, яка використовує конфіденційну або секретну інформацію, заяви чи записи для переслідування, викриття, нанесення фінансової шкоди чи іншої експлуатації цільових осіб [5]. Учасниками дослідження Нью-Йоркського університету 2017 року було виявлено та проаналізовано понад 5500 файлів, пов'язаних із доксуванням [1]. Результати показали, що понад 90% доксованих файлів містили адресу жертви, 61% - номер телефону та 53% - адресу електронної пошти. Сорок відсотків імен онлайн-користувачів жертв були оприлюднені, і такий самий відсоток розкрив IP-адресу жертви. У той час як менш поширена, конфіденційна інформація, така як номери кредитних карток (4,3%), номери соціального страхування (2,6%) або інша фінансова інформація (8,8%), також було розкрито (Рис. 1.1) [1, 2].

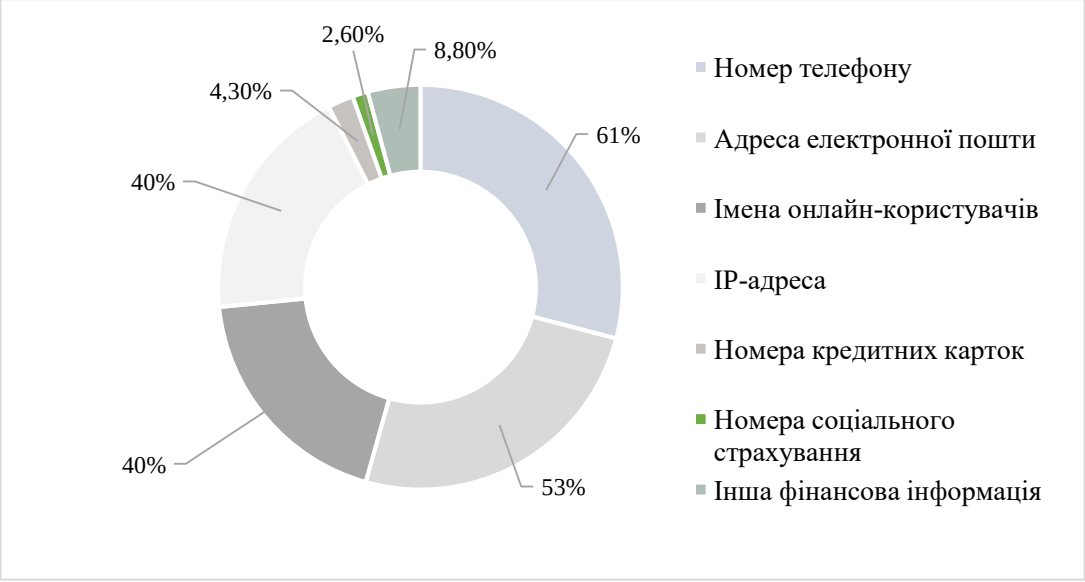

Рисунок. 1.1 – Найбільш поширені методи SE-атак

Здійснюючи спробу захисту інформації, опублікованої в соціальних мережах, 32% жертв докінгу закрили або змінили налаштування

конфіденційності у своєму обліковому записі Instagram, а 25% змінили налаштування облікового запису Facebook після атаки. Приблизно 10% жертв доксінгу змінили свій обліковий запис в Instagram, а 3% змінили свої налаштування у Facebook після того, як було вжито заходів щодо боротьби зі зловживаннями [1, 2].

У 2018 році в Гонконгу було проведено дослідження серед школярів [3], головною метою якого було отримання попереднього уявлення про доксування серед цієї вразливої групи населення, включаючи його поширеність, виконавців, наміри та зв'язок із розкриттям інформації. Цільовими респондентами були учні, вік яких переважно варіювався від 13 до 17 років. У цьому дослідженні вивчалася участь підлітків у доксуванні з використанням репрезентативної вибірки із 2120 учнів шкіл Гонконгу.

Понад 80% підлітків у США та Європейському Союзі мають свої особисті сторінки у соціальних мережах; приблизно 90% підлітків у Гонконгу мають хоча б один обліковий запис у соціальній мережі; та 90,9% підлітків у материковому Китаї використовують месенджери [3].

Поширення особистої інформації у соціальних мережах також є тенденцією, що росте, серед підлітків. Управління інформацією в мережі — складніший процес, ніж просто її розміщення. Багато підлітків діляться такою особистою інформацією, як своє повне ім'я, стать, день народження, школа, статус стосунків та адресу електронної пошти, а також особисті фотографії та відео. Таким чином, саморозкриття в Інтернеті є давньою проблемою для суспільства. Зростання неправомірного використання особистої інформації в Інтернеті (наприклад, кіберпереслідування) означає, що її обмін може бути дуже ризикованим. Відсутність у підлітків турботи про конфіденційність в Інтернеті може навіть призвести до насильства у реальному житті у формі залякування, приниження, фізичних нападів та викрадень [3].

Трохи більше одного з 10 займалися доксуванням, і доксування значно збільшувало можливість розкриття особистої інформації про інших (ставлення шансів коливалося від 2,705 до 5,181). Соціальне та вороже доксування були

двома найбільш поширеними формами доксування. Дівчата достовірно частіше проводили соціальний доксінг, метою якого було отримання соціальної інформації, тоді як хлопці частіше вдавалися до ворожого доксування, спрямованого на отримання особистої інформації та інформації про поточні життєві ситуації інших. Студенти, які вчинили акти доксінгу, з більшою ймовірністю зіткнулися з розкриттям інформації в якості жертв, злочинців або свідків [3].

Підлітки, які доксували, робили це з різними намірами. Як слідує з Табл. 1.1, 53,2% підлітків зізналися, що доксували людей, які їм подобалися, причому дівчатка (62%) частіше робили це, ніж хлопчики (41,2%). Підлітки цікавилися соціальними даними та намагалися з'ясувати статус відносин людини та отримати його чи її особисті фотографії чи відео [3].

Таблиця 1.1 – Платформи та цілі доксінгу

Інформація, добута шляхом доксінгу		Хлопці (n=110), %	Дівчата (n=149), %	Всі (n=259), %
Цілі доксінгу	Люди, які подобаються	*41.2*	*62*	*53.2*
	Люди, які не подобаються	*57*	*45.9*	*50.7*
Платформа доксінгу	Електронна пошта	*11.4*	*2.4*	*6.2*
	Чати	*9.9*	*11.4*	*10.7*
	Форуми	*29.4*	*9.5*	*18.0*
	Месенджери	*48.4*	*51.5*	*50.2*
	Пошукові системи	*43.0*	*23.8*	*31.9*
	Соціальні мережі	*66.8*	*86.7*	*78.2*
	Блоги	*7.2*	*3.2*	*4.9*
	Веб-сторінки	*9.6*	*11.3*	*10.6*
	Веб-сайти для обміну відео	*24.3*	*13.3*	*18.0*
	Інше	*0.8*	*0.4*	*0.6*

Крім того, більше дівчаток (86,7%), ніж хлопчиків (66,8%), обрали соціальні мережі як платформу для доксування. Помічено, що наміри підлітків займатися доксингом різняться залежно від статі [3].

Половина злочинців, які вчинили доксінг, обрали цілі, які їм не подобалися. Як показало дослідження [3] значно більше хлопчиків, ніж дівчаток, повідомили про те, що вони отримали особисту інформацію (*16,3%,*

наприклад, номери посвідчень особи, номери паспортів) та інформацію про поточну життєву ситуацію (*наприклад, 49,9% - домашня адресу, імена батьків*) своїх жертв через доксування.

Крім того, ті, хто націлювався лише на осіб, які їм не подобаються, більше цікавилися отриманням інформації, що дозволяє встановити особу (22,1 %), інформацію про поточну життєву ситуацію (58,1 %) та приватну інформацію (77,3 %) (Табл. 1.2).

Таблиця 1.2 – Особиста інформація про цілі, отримана шляхом доксінгу

Доксована інформація	СТАТЬ		МЕТА ДОКСІНГУ				
	Чоловіча (n=110),%	Жіноча (n=149), %	Тільки ті, хто подобаються (n=80), %	Тільки ті, хто не подобаються (n=70), %	Люди, які подобаються і не подобаються (n=59), %	Без спеціальних цілей та інше (n=50), %	ВСЬОГО
Ім’я	*92.7*	*95.6*	*96.3*	*90.6*	*95.8*	*95.1*	*94.4*
Соціальна інформація	*88.8*	*96.3*	*92.7*	*91.6*	*92.6*	*96.3*	*93.1*
Особиста інформація	*14.6*	*6.3*	*3.1*	*22.1*	*9.1*	*3.7*	*9.8*
Поточна життєва ситуація	*49.9*	*35.5*	*32.2*	*58.1*	*46.0*	*27*	*41.6*
Інформація про освіту	*25.2*	*24.1*	*22.6*	*24.9*	*32.1*	*18.2*	*24.6*
Приватна інформація	*65.1*	*64.3*	*50.5*	*77.3*	*68.9*	*63.4*	*64.6*
Чутлива інформація	*39.5*	*35.2*	*34.8*	*40.4*	*45.8*	*25.7*	*37.1*

Грунтуючись на результатах дослідження [3], можна стверджувати що цільова інформація підлітків про доксування різниться залежно від статі та цільових осіб щодо інформації, що дозволяє встановити особу, та інформації про поточну життєву ситуацію учнів. Оскільки особиста та конфіденційна інформація може використовуватися для приниження або нападу на людей як у кіберпросторі, так і в реальному світі, можна зробити висновок, що хлопчики схильні до ворожого доксування, ніж дівчатка. Крім того, хлопчики в цьому

досліджені були більш схильні використовувати пошукові системи, веб-сайти для обміну відео та форуми для доксінгу, що дозволяло їм отримувати більше інформації, ніж це було б можливо за допомогою соціальних мереж. Мається на увазі, що деякі хлопчики займаються доксуванням із сильними ворожими намірами [3].

1.2 Основні методи незаконного збору даних

На сьогодні відома ціла низка методів, які використовуються доксерами для збору даних про свої цілі, а саме [4]:

1) Відстеження імен користувачів. Користувачі різних онлайн сервісів часто використовують одне і те ж саме ім'я користувача, що дозволяє доксерам скласти уявлення про інтереси жертви;

2) Переслідування в соціальних мережах. В даному випадку зловмисники можуть дізнатися відомості, щодо розташування користувача, місце його роботи, друзів, фотографії, симпатії та антипатії, імена членів сім'ї тощо. Використовуючи цю інформацію, доксер може успішно атакувати інші облікові записи в Інтернеті [4];

3) Пошук WHOIS по доменному імені. Інформація будь-якого власника доменного імені зберігається в реєстрі, який часто є загальнодоступним через пошук у WHOIS. Якщо користувач не виконає дій, щодо приховання особистої інформації, то ці дані можуть бути доступні в мережі для третіх осіб [4, 5];

4) Фішинг. Атакуючий може виявити електронні листи жертви або людини, яка використовувала небезпечний обліковий запис електронної пошти, та опублікувати їх в широкий доступ [4];

5) Відстеження IP-адрес. Поєднання IP-адреси з фізичним розташуванням користувача може бути використане для видобутку інформації за допомогою деяких прийомів соціальної інженерії місцевого інтернет-провайдера (ISP) [5];

6) Зворотній пошук мобільного телефону. Експлуатує можливість пошуку за номером телефону, що дає змогу дізнатися додаткову особисту інформацію про жертву за номером його мобільного телефону [4, 5];

7) Аналіз пакетів (паркінг та/або сніфінг). Передбачає несанкціоноване перехоплення та аналіз мережевого трафіку жертви, з метою отримання чутливих відомостей *(паролі, номери кредитних карток, інформацію про банківські рахунки тощо)*;

8) Використання т.з. «брокерів даних». Брокери даних займаються протиправним збором чутливої інформації про людей з метою наступної реалізації цих відомостей [4].

Висновки за Розділом.

Доксінг є відносно новим явищем, причиною існування якого є виникнення та регулярний розвиток нових ІТ-технологій [4].

Існуючі концепції та механізми забезпечення ІБ не можуть гарантувати повного захисту чутливих даних, оскільки будь-які дані при їх відповідній обробці та багатопараметрічних узагальненнях *(наприклад, час, мова, геолокація, періодичність сеансів зв'язку, пошукові запити, час спілкування з учасниками мережевих груп тощо)*, можуть стати зброєю в руках доксерів, мотиви дій яких можуть варіюватися від особистої помсти до, навить, політичних цілей. При розміщенні особистої інформації на веб-сайтах і комунікаційних платформах, найкращою лінією поведінки є, залишатися інкогніто (за можливості) або мінімізувати обсяг доступної для широкого загалу, персоніфікованої інформації та чутливих даних [4].

2 ОСОБЛИВОСТІ НОРМ МІЖНАРОДНОГО ПРАВА ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Коли питання захисту конфіденційної інформації розглядається з юридичної точки зору, стає очевидною його складність. Зазвичай, в таких випадках, це порушення Закону про захист персональних даних, але коли мова йде про наслідки злочину, складно притягнути конкретну особу (виконавця або замовника атаки) до відповідальності. Тим не менш, у світі вже існує низка відповідних документів, спрямованих на запобігання та покарання доксерів. Наприклад, Загальний регламент ЄС про захист даних (General Data Protection Regulation, GDPR) та Постанова Гонконгу про конфіденційність персональних даних (The Personal Data (Privacy) Ordinance, PDPO) є правовими рамками для захисту даних і приватності [1].

Після технологічного розвитку та глобалізації, а також конституційного закріплення основного права на захист даних у ЄС, GDPR спрямований на взаємне узгодження елементів структури єдиного цифрового ринку, надання окремим особам контролю над своїми даними та формулювання сучасного управління захистом даних [6]. Враховуючи, що GDPR є показником значного розвитку закону про захист даних у порівнянні з Директивою ЄС [1, 6], нова нормативна база включає низку вимог, які не містяться в PDPO. Одним із ключових нововведень, внесених GDPR до галузі захисту даних за межами ЄС, є чітка вимога дотримання закону організаціями, створеними в юрисдикціях, що не входять до ЄС, за певних обставин. Враховуючи диверсифіковані моделі бізнесу або транзакцій (*наприклад, онлайн-транзакції*), для компаній у Гонконгу тим більш важливо переконатися, що GDPR застосовується до них, і не відстає від нових розробок [1] . Відмітимо основні відмінності GDPR ЄС та PDPO Гонконгу в Табл. 2.1 [7]:

Таблиця 2.1 – Порівняння GDPR і PDPO

Відмінність	GDPR	PDPO
1	*2*	*3*
Мета застосування	Обробники даних або контролери з установою в ЄС, або засновані за межами ЄС, які пропонують товари чи послуги особам у ЄС або контролюють їхню поведінку (Ст. 3, [8]).	Користувачі даних (контролери/обробники), які самостійно чи спільно з іншими особами контролюють збір, зберігання, обробку чи використання персональних даних у/з Гонконгу (Розд. 2(1), [9]).
Визначення поняття «Персональні дані»	Це будь-яка інформація, що стосується вже ідентифікованої фізичної особи або особи, що може бути ідентифікованою; приклади явно визначених особистих даних, які розширюються, щоб включати дані про місцезнаходження та онлайн-ідентифікатор. (Ст. 4(1), [8]).	• Це будь-які дані прямо чи опосередковано пов’язані з живою особою; • Дані, з яких можна прямо чи опосередковано встановити ідентичність особи; • Дані у формі, в якій доступ або обробка даних є практичними. (Розд. 2(1), [9]).
Підзвітність і управління	• Підхід, заснований на ризику; • контролери даних зобов'язані: здійснювати технічні та організаційні заходи для забезпечення відповідності (Ст. 24, [8]); • прийняти захист даних за проектом і за замовчуванням (Ст. 25, [8]); • проводити оцінку впливу на захист даних для обробки з високим ризиком (Ст. 35, [8]); і (для певних типів організацій) призначити посадових осіб із захисту даних. (Ст. 37, [8]).	• Принцип підзвітності та пов’язані з ним заходи управління конфіденційністю прямо не вказано. • Уповноважений з питань конфіденційності виступає за прийняття програми управління конфіденційністю, яка демонструє принцип підзвітності. Призначення відповідальних осіб із захисту даних і проведення оцінки впливу на конфіденційність є рекомендованими передовими практиками для досягнення підзвітності.
Конфіденційні особисті дані	• Розширено категорію конфіденційних персональних даних. • Обробка конфіденційних персональних даних дозволяється лише за певних обставин (Ст. 9, [8]).	Немає різниці між конфіденційними та неконфіденційними персональними даними для всіх цілей.

Продовження Таблиці 2.1

1	*2*	*3*
Дозвіл	Згода: • повинна бути вільно наданою, конкретною і свідомою; • однозначно вказувати на бажання суб'єкта даних шляхом заяви або чіткої позитивної дії на згоду (Ст. 4(1), [8]); • дається дитиною віком до 13-16 з дозволу батьків.	• Згода не є необхідною умовою для збору персональних даних, якщо вони не використовуються для нової мети. Для інших цілей, згода є чітко вираженою та добровільною. • Згода батьків не потрібна.
Повідомлення про порушення	• Контролери даних зобов'язані повідомляти органи влади про порушення даних без невиправданої затримки (застосовуються винятки). • Контролери даних зобов'язані повідомляти відповідних суб'єктів даних, якщо це може призвести до високого ризику для прав та інтересів суб'єктів даних, окрім винятків (Ст. 33-34, [8]).	• Немає обов'язкових вимог, але сповіщення Уповноваженого з конфіденційності (та суб'єктів даних, якщо це доречно) є рекомендованим в інтересах усіх зацікавлених сторін, включаючи користувачів/контролерів даних і суб'єктів.
Обробники даних	• Обробники даних додатково зобов'язані вести записи обробки, забезпечувати безпеку обробки, повідомляти про порушення даних, призначати посадових осіб із захисту даних тощо (Ст. 30, 32-33, 37, [8]).	• Обробники даних прямо не регулюються (Ст.2(12), [9]); • Користувачі даних зобов'язані прийняти договірні або інші засоби для забезпечення відповідності обробників даних.
Нові та розширені права для суб'єктів даних	• Право на повідомлення про обробку даних (Ст. 13-14, [8]); • Право на видалення персональних даних («право бути забутим») (Ст. 17, [8]); • Право на обмеження обробки та перенесення даних (Ст. 18, 20, [8]).	Менш розширені вимоги до сповіщень для користувачів даних/контролерів/обробників. Немає права: • На видалення, але дані не повинні зберігатися довше, ніж це необхідно (Ст.26, [9]); • На обмеження обробки та перенесення даних, але доступ до даних і запити на виправлення мають бути виконані.

Продовження Таблиці 2.1

1	*2*	*3*
Нові та розширені права для суб'єктів даних	Право на заперечення проти обробки (включаючи профілювання) (Ст. 21, [8]).	Заперечувати проти обробки (зокрема профілювання), але може відмовитися від прямої маркетингової діяльності, а PDPO містить положення, що регулюють процедуру зіставлення даних [9].
Сертифікація, печатки та кодекси поведінки	Механізми чітко визнаються та встановлюються для демонстрації дотримання контролерами та обробниками даних (Ст. 42, [8]).	Відсутність офіційного визнання сертифікації або механізмів конфіденційності для демонстрації відповідності. Уповноважений з питань конфіденційності може затвердити та видати кодекс практики після консультації [9].
Передача даних між юрисдикціями	Сертифікація та дотримання затверджених кодексів поведінки чітко визначено однією з правових підстав для передачі (Ст. 46, [8]).	Сертифікація та дотримання затвердженого кодексу практики не є прямою правовою основою.
Санкції	• Органи захисту даних мають право накладати адміністративні штрафи на контролерів та обробників даних (Ст. 58, [8]); • Залежно від характеру порушення штраф може становити до 20 мільйонів євро або 4% від загального світового річного обороту (Ст. 83, [8]);	• Уповноважений з питань конфіденційності не має повноважень накладати адміністративні штрафи чи пені. • Уповноважений із питань конфіденційності може надіслати користувачам даних Повідомлення про застосування, невиконання якого може призвести до штрафних санкцій після судового розгляду [9].

Законотворча діяльність Євросоюзу у сфері захисту приватності [1] не зупинилася на етапі розробки GDPR. Обробка персональних даних з метою кримінального правосуддя не входить до периметра дії регламенту, оскільки вимагає встановлення специфічного правового режиму. Тому в 2016 році одночасно з GDPR було прийнято директиву щодо захисту фізичних осіб при

автоматизованій обробці персональних даних державними органами з метою запобігання, розслідування, виявлення та переслідування кримінальних злочинів. Крім того, була прийнята Директива про мережеву та інформаційну безпеку (Network and Information Security, NIS) [10]. Основним завданням цього правового акту стає забезпечення високого рівня інформаційної безпеки для операторів критичних інфраструктур та провайдерів цифрових послуг. Метою є не лише захист персональних даних, а й забезпечення безпеки взагалі всіх даних [1].

Усі ці численні закони є результатом політики Європейського Союзу у сфері електронних комунікацій, кібербезпеки та приватності даних. Наступним кроком ЄС має стати ухвалення нового документу Regulation on Privacy and Electronic Communications (*«ePrivacy Regulation»*) [11], покликання якого полягає в заміні Директиви 2002 року. Ця реформа присвячена питанню використання метаданих (*Big Data*) та регулюванню використання файлів *cookie* [1].

Висновки за Розділом.

Таким чином, юридична сторона питання захисту конфіденційної інформації має безліч суб'єктивних сторін і умовностей, що є причиною наявності низки проблем у процедурі притягнення до відповідальності за порушення відповідних законодавчих норм. З метою запобігання, а також притягнення до відповідальності доксерів-зловмисників у світі існує низка документів, що сприяють забезпеченню високого рівеня захисту чутливої інформації. GDPR та інші закони у сфері приватності даних – не просто доповнення європейського законодавства. Регламент захисту персональних даних разом з усім пакетом реформ «Privacy» є результатом багаторічного розвитку юридичної думки, заснованої на необхідності захисту приватного життя будь-якого громадянина [1].

3 ДОСЛІДЖЕННЯ ВЗАЄМОЗВ'ЯЗКУ ДОКСІНГУ І АТАК З ВИКОРИСТАННЯМ ПРИЙОМІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

3.1 Визначення соціальної інженерії

Термін «соціальна інженерія» (SE) може бути визначений різними способами, що стосуються як фізичних, так і кібернетичних аспектів цієї діяльності. Автори літератури, присвяченої цьому питанню, надали цьому терміну такі визначення:

1) «Використання стороннім хакером психологічних трюків щодо законних користувачів комп’ютерної системи, щоб отримати інформацію, необхідну йому для отримання доступу до системи» [12];

2) «Практика обману когось особисто, по телефону чи за допомогою комп’ютера з явним наміром порушити певний рівень особистої чи професійної безпеки» [12];

3) «Соціальна інженерія — це нетехнічний вид втручання, який значною мірою залежить від взаємодії з людьми, що часто включає в себе обманом спонукання інших людей порушити нормальні процедури безпеки» зловмисник використовує соціальні навички та взаємодію з людьми, щоб отримати інформацію про організацію чи її комп’ютерні системи [12].

Насправді соціальна інженерія може мати будь-яке з цих визначень залежно від обставин, які супроводжують атаку. Соціальна інженерія – це фактично маніпулювання хакером природною людською схильністю довіряти, щоб отримати конфіденційну інформацію, необхідну для отримання доступу до системи. Соціальна інженерія не вимагає високого рівня технічної експертизи, але вимагає від людини гідних соціальних навичок. Багато людей протягом кількох десятиліть використовували соціальну інженерію як метод дослідження та збору даних. Ці перші соціальні інженери використовували зібрану інформацію як форму шантажу проти інших організацій. Соціальну інженерію використовували для отримання несанкціонованого доступу до кількох великих

організацій. Хакер, який витрачає кілька годин на спроби зламати паролі, може заощадити багато часу, зателефонувавши співробітнику організації, видаючи себе за службу підтримки або працівника IT, і може просто попросити це.

3.2 Життєвий цикл соціальної інженерії

Кожна атака соціальної інженерії є унікальною, але, трохи розуміючи ситуації, що виникають, можемо скласти приблизний цикл усіх дій, через які проходить проект соціальної інженерії, що призводить до успішного результату. На Рис. 3.1 нижче показано загальне представлення життєвого циклу соціальної інженерії в чотирьох основних етапах [12]:

Рисунок. 3.1. – Життєвий цикл соціальної інженерії

Сліди (*Footprinting*). Це техніка накопичення інформації про ціль (цілі) та навколишнє середовище. Сліди можуть виявити осіб, пов'язаних із ціллю, з якою зловмисник має встановити стосунки, щоб підвищити шанси на успішну атаку. Збір інформації на етапі Footprinting включає (але не обмежується):

- Список імен і номерів телефонів співробітників;
- Організаційна схема;
- Інформація про відділ;
- Інформація про місцезнаходження.

Сліди зазвичай відносяться до однієї з фаз перед нападом; завдань, які виконуються перед фактичною атакою соціальної інженерії.

Встановлення довіри. Після переліку можливих цілей зловмисник починає розвивати стосунки з ціллю, яка зазвичай є співробітником або кимось, хто працює в бізнесі, щоб налагодити з ними хороші стосунки. Довіра, яку завойовує соціальний інженер, пізніше буде використана для розкриття конфіденційної інформації, яка може завдати серйозної шкоди бізнесу [12].

Психологічна маніпуляція. На цьому кроці соціальний інженер маніпулює довірою, яку він завоював на попередньому етапі, щоб витягти якомога більше конфіденційної інформації або отримати конфіденційні операції, пов’язані з цільовою системою, які виконує сам співробітник, щоб проникнути в систему з великою легкістю. Коли всю необхідну конфіденційну інформацію буде зібрано, соціальний інженер може перейти до наступної цілі або перейти до використання фактичної системи, що розглядається [12].

Вихід. Після того, як уся фактична інформація була витягнута, соціальний інженер повинен зробити чіткий вихід таким чином, щоб не звертати на себе увагу та відвести підозри. Він стежить за тим, щоб не залишити жодних доказів свого візиту, за якими могли б відстежити його справжню особу або пов’язати його з несанкціонованим проникненням у цільову систему в майбутньому [12].

3.3 «Зброя» соціального інженера

Старомодні технічні способи злому в комп’ютерній системі тепер замінено складними методами, які не тільки простіші, але й дають кращі та швидші результати на основі людської психології. Ці атаки можуть допомогти зловмиснику отримати доступ до будь-якої системи, незалежно від платформи, програмного чи апаратного забезпечення. На Рис. 3.2 показано деякі з найпопулярніших методів, які використовуються для здійснення атак соціальної інженерії [12].

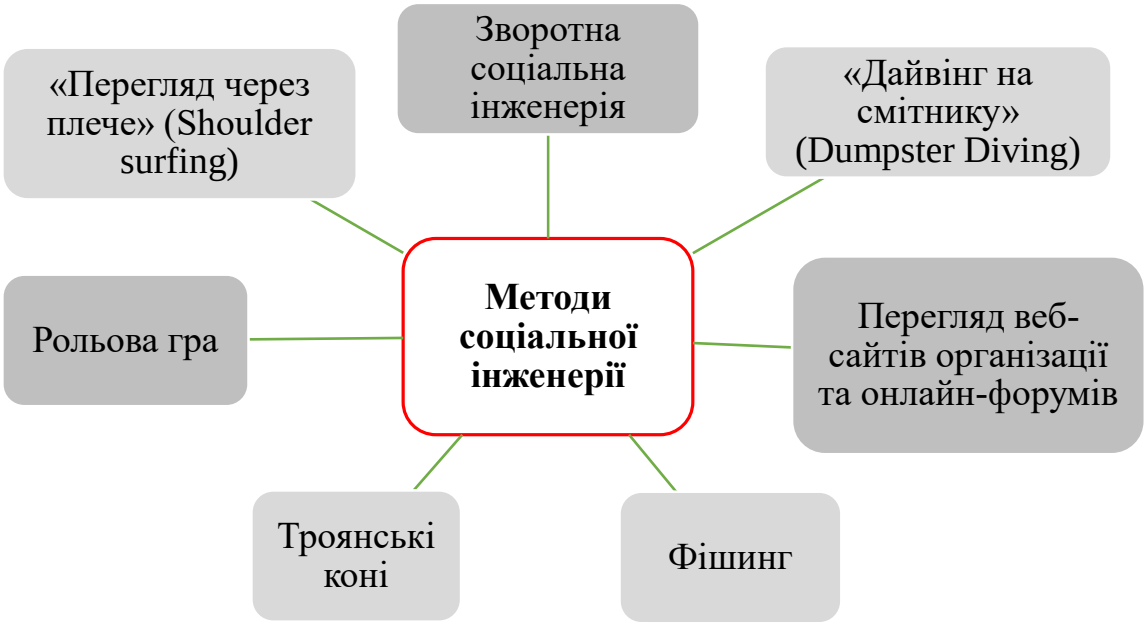

Рисунок 3.2 – Методи соціальної інженерії

- «Серфінг через плече»

«Перегляд через плече» (Shoulder surfing) – це атака на безпеку, у якій зловмисник використовує методи спостереження, як, наприклад, погляд через плече, щоб отримати інформацію під час виконання певної дії, що передбачає використання конфіденційної видимої інформації. Це можна зробити як на близькій, так і на великій відстані за допомогою бінокля чи інших пристроїв для покращення зору.

- «Дайвінг на смітнику»

Доволі часто великі організації недбало викидають такі елементи, як телефонні книги компанії, системні посібники, організаційні діаграми, управління з політики компанії, календарі зустрічей, подій і відпусток, роздруківки конфіденційних даних або імен для входу та паролів, роздруківок вихідного коду, дисків і стрічок, фірмові бланки та бланки службових записок, а також застаріле обладнання до смітників компанії. Зловмисник може використати ці елементи, щоб отримати величезну кількість інформації про організацію компанії та структуру мережі. Цей метод пошуку потенційно корисної інформації, викинутої працівниками компанії, відомий як «Dumpster Diving» [12].

- Рольова гра

Це одна з ключових зброй соціального інженера. Зловмисник прикидається службою підтримки, працівником, техніком, безпорадним або важливим користувачем, щоб розкрити конфіденційну інформацію. Дуже часто збір інформації виконується за допомогою сеансу онлайн-чату, електронної пошти, телефону або будь-якого іншого методу, який використовує компанія для взаємодії в Інтернеті з громадськістю [12].

- Троянські коні

Це один із найпоширеніших методів, який наразі використовують хакери, який полягає в тому, щоб обманним шляхом змусити жертв завантажити шкідливий файл у систему, що під час виконання створює бекдор на машині, який може бути використаний зловмисником у будь-який час у майбутньому, таким чином маючи повний доступ до машини жертви.

- Фішинг

Це акт створення та використання веб-сайтів і електронних листів, розроблених так, щоб вони виглядали як веб-сайти відомих законних підприємств, фінансових і державних установ, щоб ввести в оману користувачів Інтернету. Таким чином здійснюється спроба обманом змусити користувача надати особисту інформацію, яка у подальшому буде використана для крадіжки особистих даних [12].

- Перегляд веб-сайтів організації та онлайн-форумів

Величезна кількість інформації щодо організаційної структури, ідентифікаторів електронної пошти, номерів телефонів відкрито доступна на веб-сайті компанії та інших форумах. Ця інформація може бути використана зловмисником, щоб удосконалити свій підхід і створити план, на кого націлитися, і метод, який використовуватиметься.

- Зворотна соціальна інженерія

Зворотна атака соціальної інженерії – це атака, під час якої зловмисник переконує ціль, що у нього є або може виникнути певна проблема в

майбутньому, і що зловмисник готовий допомогти вирішити проблему. Зворотна соціальна інженерія складається з трьох частин:

1) Саботаж: після того, як зловмисник отримує простий доступ до системи, він пошкоджує систему або надає їй вигляду пошкодженої. Коли користувач бачить систему в пошкодженому стані, він починає шукати допомоги, щоб вирішити проблему;
2) Маркетинг: щоб переконатися, що користувач звернеться до зловмисника з проблемою, зловмисник рекламує себе як єдину людину, яка може вирішити проблему;
3) Підтримка: на цьому етапі він завойовує довіру цілі та отримує доступ до конфіденційної інформації [12].

3.4 Інсайдерські загрози

Внутрішня загроза – це можливість використання внутрішньою особою свого авторизованого доступу або особливого розуміння організації, щоб завдати їй шкоди. Ця шкода може включати зловмисні або ненавмисні дії, які негативно впливають на цілісність, конфіденційність і доступність організації, її даних, персоналу, засобів і пов’язаних ресурсів (Рис. 3.3) [13].

Рисунок 3.3 – Потенційні наслідки внутрішнього інциденту

3.4.1 Типи внутрішніх загроз

Загалом, внутрішні загрози походять від двох основних видів діяльності: ненавмисної та навмисної. Ненавмисні дії можна далі розбити на необережні та випадкові дії [13]:

1) Необережні. Інсайдери можуть наразити організацію на небезпеку своєю необережністю. Інсайдери цього типу зазвичай знайомі з політикою безпеки та/або IT, але вибирають ігнорувати їх, створюючи ризик для організації. Приклади включають дозвіл комусь «перейти» через захищену точку входу, неправильне розміщення або втрату портативного пристрою зберігання, що містить конфіденційну інформацію, та ігнорування повідомлень про встановлення нових оновлень і виправлень безпеки. Недбалі інсайдери зазвичай самовдоволені та демонструють навмисне нехтування правилами; вони демонструють поведінку, яку можна побачити та виправити;
2) Випадкові. Навіть найкращий працівник може бути неуважним або наївним і зробити помилку, спричинивши ненавмисний ризик для організації. Приклади включають неправильне введення адреси електронної пошти та випадкове надсилання конфіденційного ділового документа конкуренту, несвідоме чи ненавмисне натискання гіперпосилання або відкриття вкладення, яке містить вірус у фішинговій електронній пошті, або неналежна утилізація конфіденційних документів. Організації можуть успішно працювати над мінімізацією аварій, але вони траплятимуться; їх неможливо повністю запобігти, але ті, що виникають, можна пом'якшити.

Інсайдери можуть навмисно вживати дій, які завдають шкоди організації, для особистої вигоди або для вирішення особистих скарг. Деякими навмисними інсайдерами спонукає невдоволення, пов’язане з передбачуваною образою, амбіціями чи фінансовим тиском. Інші можуть мати бажання отримати визнання та шукати уваги, створюючи небезпеку або розголошуючи

конфіденційну інформацію. Вони можуть думати, що діють на благо суспільства. Наприклад, невиправдані очікування через відсутність певної форми визнання (наприклад, підвищення по службі) або навіть звільнення спонукали багатьох інсайдерів «відплатитися» шляхом витоку конфіденційної інформації, переслідування партнерів, саботування обладнання або вчинення насильства. Інші викрали конфіденційні дані або інтелектуальну власність, щоб просувати свою кар'єру [13].

Інші загрози:

1) Крім загроз, які стосуються лише інсайдерів організації, інсайдерські загрози також можуть стосуватися осіб, які не належать до організації. Ці змовні погрози та погрози третіх сторін можуть бути як ненавмисними, так і навмисними;
2) Загрози за змовою: цей підтип загрози проявляється, коли один або кілька інсайдерів співпрацюють із зовнішнім учасником загрози для компрометації організації. У цих інцидентах часто кіберзлочинці вербують інсайдера або кількох інсайдерів для шахрайства, крадіжки інтелектуальної власності, шпигунства або комбінації цих трьох. Цей тип внутрішньої загрози складно виявити, оскільки зовнішні учасники, як правило, добре розбираються в методах безпеки та стратегіях уникнення виявлення;
3) Загрози третіх сторін: загрози третіх сторін пов'язані з особами, які офіційно не є членами організації, але яким надано певний рівень доступу до об'єктів, систем, мереж або людей для виконання їх роботи. Цей підтип загроз також може включати численні сторонні загрози, що змовляються. Загрози від третьої сторони можуть бути прямими, коли конкретні особи діють таким чином, що скомпрометують цільову організацію, або непрямими, коли в системах можуть бути недоліки, які відкривають ресурси для ненавмисних або зловмисних загроз [13].

3.5 Типи атак Keylogger

Кейлоггер — це інструмент або технологія, яка відстежує та записує послідовні натискання клавіш на клавіатурі. Зазвичай це працює приховано, щоб потенційні жертви не підозрювали, що за їхньою діяльністю стежать. Хакери використовують цей інструмент, щоб фіксувати онлайн-активність своєї цілі та отримувати її особисту інформацію, яку потім вони можуть використовувати для власної фінансової вигоди або шантажувати мішень, знімати кошти з її банківського рахунку або продавати інформацію кіберзлочинцям у темній мережі [14].

Хоча вони найчастіше використовуються зі зловмисною метою, кейлоггери також можуть використовуватися з кількох законних причин. Наприклад, керівники підприємств і менеджери можуть використовувати їх, щоб забезпечити оптимальну продуктивність своїх співробітників і переконатися, що їхні співробітники не розголошують внутрішні секрети.

Кейлоггери, які часто помилково називають зловмисним програмним забезпеченням, не завжди є програмними. Вони також можуть працювати з самого обладнання, коли вони або інтегровані в нього, або доступні як автономні пристрої. Що стосується програмних клавіатурних шпигунів, якщо вони не є легітимними, вони зазвичай пов’язані зі шкідливим програмним забезпеченням, шпигунським програмним забезпеченням або вірусами. Хакери зазвичай поширюють ці зловмисні кейлоггери через фішингові електронні листи, які містять скомпрометовані вкладення та/або посилання на заражені веб-сайти [14].

3.5.1 Програмні кейлоггери

Що стосується програмного забезпечення, кейлоггери працюють через фонові процеси, часто ненав’язливі, які копіюють натискання клавіш. Деякі кейлоггери також можуть робити скріншоти введеного тексту. Потім ці дані зазвичай передаються онлайн або зберігаються у файлі на жорсткому диску жертви. В останньому випадку доступ до жорсткого диска здійснюється без

авторизації. Ці типи кейлоггерів є найвідомішими, і з ними можна ефективно боротися за допомогою брандмауера або антивірусної програми (Табл.3.1).

ПЗ Keylogger доступне в багатьох різних версіях [14].

Таблиця 3.1 – Короткий опис програмних кейлоггерів

Програмний кейлоггер	Функціональність
1	*2*
Простий програмний кейлоггер	Комп'ютерна програма, яка читає команди клавіатури з фонового процесу.
Кейлоггер на основі гіпервізора	Кейлоггер використовує зловмисну програму гіпервізора, щоб вбудувати себе в операційну систему, залишаючи саму операційну систему недоторканою. Таким чином, кейлоггер функціонує як віртуальна машина і працює незалежно від операційної системи.
Кейлоггер на основі ядра	Шкідлива програма вбудовується безпосередньо в операційну систему та отримує доступ до облікового запису root. Там записуються натискання клавіш. Ці кейлоггери також можуть маскуватися під драйвери, і їх відносно важко виявити. Антивірусне програмне забезпечення, наприклад, потребує root-доступу, щоб знайти цей тип зловмисного програмного забезпечення.
Кейлоггер на основі API	Ці кейлоггери підключаються до API клавіатури *(інтерфейсів прикладного програмування)* і реагують на кожне натискання клавіші.
Кейлоггер на основі введення форми	Цей тип кейлоггера записує онлайн-форми та копіює відповідні дані для входу. Програмне забезпечення також може отримати доступ до історії браузера, щоб визначити, які сторінки були відвідані.
Людина в браузері *("Man in the Browser", MITB)*/ ін'єкція пам'яті	Ці кейлоггери вбудовуються у веб-браузер і записують непомічені натискання клавіш. Наприклад, ці реєстратори натискань клавіш збирають інформацію, надіслану через поля введення, і зберігають її у внутрішніх журналах браузера. Тоді журнали доступні зовні.
Віддалений доступ	Ці віддалені реєстратори натискань клавіш забезпечують зовнішній доступ до зловмисного програмного забезпечення. Записані натискання клавіш "набираються" електронною поштою або завантажуються. Ці кейлоггери часто працюють у поєднанні з відповідним обладнанням.

3.5.2 Апаратні кейлоггери

Багато користувачів Інтернету навіть не знають, що існують апаратні кейлоггери, які шпигують не тільки за програмними паролями. Цей тип кейлоггера можна використовувати, наприклад, у вигляді невеликого USB-роз’єму, який підключається між клавіатурою та комп’ютером. Такий штекер має внутрішню пам'ять, в якій зберігаються протоколи введення з клавіатури. Апаратні кейлоггери також доступні в дуже оригінальних і дивовижних варіантах (Табл. 3.2). Приватні користувачі, однак, рідко вступають з ними в контакт [14].

Таблиця 3.2 – Характеристика апаратних кейлоггерів

Апаратний кейлоггер /Принцип/Технологія	Функціональність
1	*2*
Клавіатура/зовнішнє обладнання	Обладнання встановлюється між клавіатурою та ПК, зазвичай безпосередньо на з’єднувальному кабелі клавіатури. Ці кейлоггери зазвичай розроблені як невеликі роз’єми з внутрішньою пам’яттю. Натискання клавіш зберігаються в цій пам'яті. Клавіатури доступні для підключення USB і PS2. Пристрої підключаються безпосередньо до порту ПК і не привертають увагу користувача.
Сніфер клавіатури та миші	Ці пристрої зчитують дані, передані бездротовою клавіатурою або мишею до кінцевої системи. Оскільки бездротовий зв'язок часто шифрується, сніфер також повинен розшифрувати код.
Клавіатурні аксесуари/ комплектуючі	Зловмисники часто використовують такий спосіб фіксації натискань клавіш у банкоматах. Вони встановлюють пристрій на поле введення машини. Його часто важко розпізнати, і користувач сприймає його як частину машини. Коли клієнти вводять свій PIN-код та інші конфіденційні дані, вони мимоволі передають їх до кейлоггера.
Акустичні реєстратори натискання клавіш	Аналізують звуки, які користувач створює за допомогою клавіатури ПК. Натискання кожної клавіши має різний звук, який люди не можуть розрізнити. Акустичні кейлоггери працюють зі статистичними даними про особливості поведінки людини за роботою на ПК. Як правило, ці пристрої вимагають достатнього розміру вибірки щонайменше 1000 натискань клавіш.

Продовження Таблиці 3.2

1	*2*
Перехоплення електромагнітних хвиль	Усі клавіатури генерують електромагнітні хвилі, які можуть поширюватися до 20 метрів. Спеціальні пристрої можуть записувати і зчитувати ці хвилі.
Відеоспостереження	Випадок, коли введення з клавіатури спостерігається за допомогою камери та записується зовні.
Фізичний аналіз слідів	Технологія використовується більше для полів введення чисел, аніж для традиційних клавіатур ПК. Якщо одні клавіші натискати частіше за інші, це залишає фізичні сліди, які можна використовувати, наприклад, для відновлення пароля.
Датчики для смартфонів	Смартфони оснащені акселерометрами, які можна перепрограмувати на спеціальні реєстратори натискань клавіш. Якщо смартфон знаходиться близько до цільової клавіатури, він може зчитувати вібрацію від набору тексту.

Висновки за розділом.

Станом на сьогоднішній день, кіберзлочинці винайшли багато методів здійснення зловмисних дій у скомпрометованої системі чи мережі користувачів з метою викрадення конфіденційної інформації чи особистих даних. При цьому людський фактор є найслабшою ланкою безпеки, яку не можна виправити одноразовим навчанням, а лише впровадженням неперервого процесу підвищення особистий компетенцій з питань ІБ та вдосконалення існуючих механізмів захисту [13].

Сучасним організаціям та приватним користувачам важливо мати розуміння різноманітності внутрішніх загроз безпеки, до яких вони повинні підготуватися. Цілістне розуміння багатовекторності сучасного міру кіберзагроз є запорукою усвідомлення необхідності впровадження комплексної програми захисту від внутрішніх загроз. Класифікація та характеристика існуючого спектру внутрішніх загроз, допоможе краще структурувати програми безпеки та підходи щодо захисту від внутрішніх та зовнішніх загроз, в тому числі для безпеки конфіденційних даних.

4 МОЖЛИВОСТІ ЩОДО ЗАПОБІГАННЯ ПЕРЕДУМОВ ЗДІЙСНЕННЯ ДОКСІНГУ ТА СПОСОБИ ПРОТИДІЇ SE-АТАКАМ

4.1 Методи боротьби з інсайдерськими загрозами

Персонал сучасних організацій є водночас найсильнішими елементами їх внутрішніх програм безпеки та її найбільшою вразливістю. Руйнівні наслідки інцидентів, котрі пов’язані із інсайдерами, ставить під загрозу безпеку чутливих даних, має негативні репутаційні наслідки та погіршує атмосферу довіри в компанії. В спробах вирішення цього питання організації розробляють програми «пом’якшення» (зменьшення) внутрішніх загроз [13].

Успішні релізи цих програм використовують практики та системи, які обмежують або контролюють доступ до організаційних функцій. Ці практики та системи, у свою чергу, обмежують масштаб шкоди, яку може завдати потенційний інсайдер, незалежно від того, чи є його дія навмисною або ненавмисною. Вдала реалізація програми зменшення внутрішніх загроз (або ризикив), дозволяє вирішувати наступні питання [13]:

1) Визначає та зосереджує увагу на тих критичних активах, даних і послугах, які організація визначає як цінні;
2) Відстежує поведінку, щоб виявити та ідентифікувати довірених інсайдерів, які порушують довіру організації;
3) Оцінює загрози для визначення індивідуального рівня ризику виявлених осіб, які викликають занепокоєння;
4) Управляє всім спектром інсайдерських загроз, включаючи впровадження стратегій, зосереджених на особі, потенційних жертвах та/або частинах організації, вразливих або націлених на інсайдерську загрозу;
5) Залучає окремих інсайдерів, які потенційно знаходяться на шляху до ворожих, недбалих або шкідливих дій, щоб запобігти, виявити та пом’якшити їх.

Цілісна програма пом’якшення внутрішніх ризикив поєднує фізичну безпеку, гарантію персоналу та принципи, орієнтовані на інформацію. ЇЇ цілі полягають у тому, щоб зрозуміти взаємодію інсайдерів в організації, відстежувати цю взаємодію, якщо це доречно, і втручатися, щоб управляти цією взаємодією, коли вона становить загрозу для організації [13].

Успішні програми пом’якшення внутрішніх загроз досягають цих цілей, дотримуючись трьох основних принципів, які застосовуються до організацій будь-якого розміру та рівня зрілості.

1) Сприяння культурі захисту та підтримки в усій організації. Культура захисту дає людям впевненість у тому, що програма пом’якшення внутрішньої загрози підтримує за своєю природою. Як показано на Рис. 4.1, успішні програми зосереджені на допомозі членам організації, щоб запобігти інсайдерському інциденту, а не на дисциплінарних покараннях за недбалий або навмисний вчинок [13].

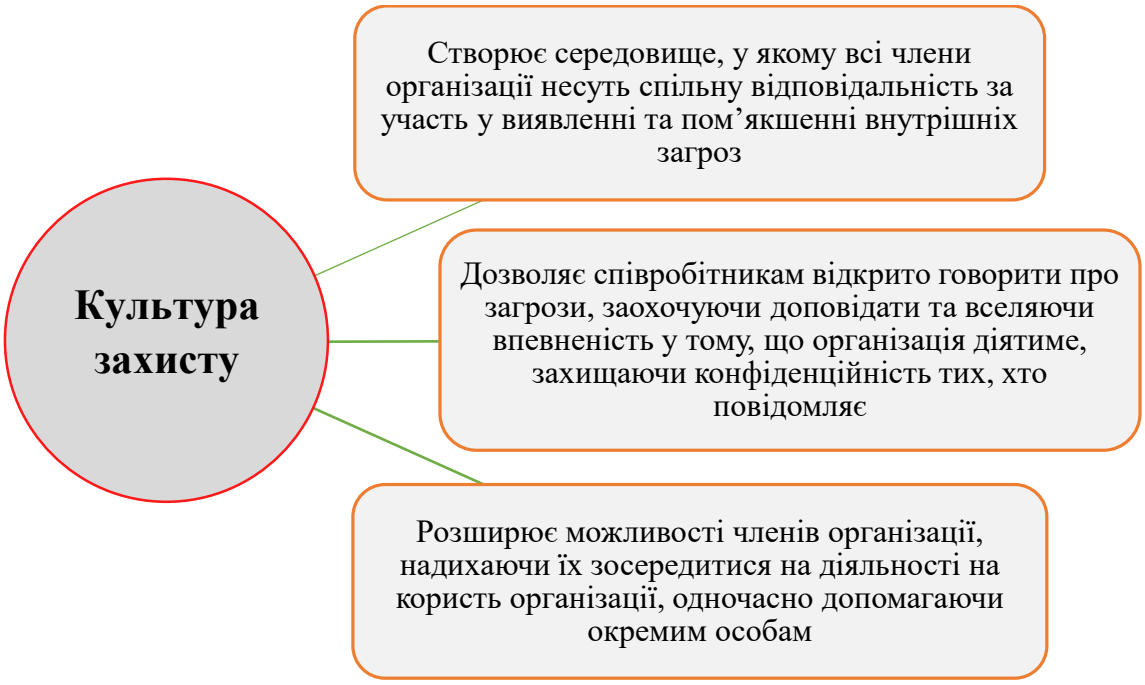

Рисунок 4.1 – Зміст заходів захисту від внутрішніх загроз

Тим не менш, вільне від звинувачень середовище не означає, що люди не відповідають за свої дії. Надання людям можливості визнати свою відповідальність за інцидент, одночасно залучаючи їх до усунення наслідків, може зменшити можливість повторення.

2) Захист організаційних цінностей, захищаючи конфіденційність, права та свободи

Програми «пом’якшення» наслідків внутрішніх загроз мають уявлення про конфіденційну інформацію, персонал та їх поведінку. Організації повинні знайти баланс між необхідністю захисту активів і потребою в прозорості політики моніторингу та очікувань конфіденційності [13].

3) Адаптація у міру розвитку організації та змін її толерантності до ризику

Інсайдерська загроза вимагає адаптивних і стійких практик для вирішення проблем захисту динамічного середовища. Це передбачає швидку зміну технологій та організаційних пріоритетів. Різні ступені доступу та розуміння, нові можливості, що постійно розвиваються, і безперервний розвиток у більшості організацій роблять очевидними вимоги до динамічної та адаптивної програми. Передові методи включають:

- Адаптація програм пом’якшення внутрішніх загроз у міру розвитку та адаптації організації;
- Постійне вдосконалення на основі найкращих практик і уроків, отриманих від ширшої спільноти управління внутрішніми загрозами;
- Динамічний реєстр ризиків внутрішньої загрози з регулярними оцінками ризиків і рейтингами ризиків, що дає змогу отримати більш актуальну та точну картину ризиків, яка дає змогу застосовувати проактивні рішення для запобігання та пом’якшення наслідків у масштабах усієї організації, а не просто вносити зміни після інцидентів ІБ;
- Використання обміну інформацією, отриманих уроків і найкращих практик від авторитетних установ і неурядових організацій.

На додаток до основоположних концепцій і основних принципів, описаних вище, є кілька ключів до успіху програми [13]:

1) Щоб досягти ефективного рівня забезпечення персоналу, організація повинна знати та залучати своїх людей. Відповідно, вона повинна

перевірити їх перед прийомом на роботу та включити процеси постійної підзвітності як частину культури захисту. І це має залучати їх до регулярного та постійного інформування та навчання;

2) Визначення активів організації та пріоритетності ризиків. Розуміння того, що цінує організація та що може пошкодити або порушити ці активи, є важливим для ефективної програми пом'якшення внутрішньої загрози. Повне розуміння активів організації дозволить належним чином управляти потенційним ризиком для цих активів;
3) Встановлення перевіреного операційного підходу виявлення та ідентифікації–оцінки–управління. Найкращі методи пом'якшення внутрішніх ризиків безпеки використовують оперативний підхід, який узгоджується з існуючими програмами безпеки, щоб дозволити виявлення та ідентифікацію потенційної загрози, оцінку цієї загрози, а потім як активні, так і пасивні методи управління цією загрозою. Цей підхід збирає та досліджує інформацію про інциденти та загрози, оцінює та класифікує ці ризики та впроваджує стратегії управління для пом'якшення загроз [13].

Інформація, технології, люди, шляхи звітування та кваліфіковані аналітики чи дослідники є основними елементами для оперативної програми пом'якшення внутрішньої загрози. Хоча кожен елемент окремо може виявляти аномалію поведінки, саме злиття елементів виявляє аномальну поведінку, що вказує на діяльність внутрішньої загрози.

«Група управління» повинна створити та підтримувати центр для збору, інтеграції, перегляду, аналізу та оцінки елементів для ефективного адміністрування програми внутрішніх загроз. Хаб повинен використовувати автоматизовані та цифрові імпульси для отримання даних і прагнути отримати регулярний електронний доступ до сховищ даних.

Є кілька організаційних аспектів, які можна вдало інтегрувати [13]:

- Кадрові справи та кадрові записи;
- Записи доступу до закладу;

- Подорожні записи;
- Звіти про іноземні контакти;
- Подання фінансової інформації;
- Доступ до мережі та друк журналів;
- Аудити IT підприємства;
- Публічні записи та фінансові дані;
- Журнали UAM;
- Відеоспостереження.

Доступ до інтегрованих активів дозволяє «групі управління загрозами» виявляти, збирати, аналізувати, досліджувати та реагувати на аномальну поведінку чи несанкціоновану діяльність, потенційно запобігаючи внутрішній атаці. На додаток до використання «групи управління загрозами», можна встановити технологічні механізми, які забезпечать додатковий шлях для виявлення проблемної поведінки та повідомлення про них організації. UAM, програмне забезпечення для аналізу поведінки користувачів (UBA) і системи контролю доступу можуть надати контекст поведінки користувачів. Ці системи можуть контролювати активи, відстежувати переміщення, а також надсилати сповіщення та звіти групі внутрішніх загроз.

Загалом програмне забезпечення UAM відстежує весь спектр кібер-поведінки користувача. Він може реєструвати натискання клавіш, робити знімки екрана, робити відеозаписи сеансів, перевіряти мережеві пакети, контролювати ядра, відстежувати веб-перегляд і пошук, записувати завантаження та завантаження файлів і контролювати системні журнали для повної картини активності в мережі. UBA подібні до UAM, за винятком того, що вони використовують машинне навчання для перегляду кінцевих точок, мереж, хостів і хмарних середовищ, до яких користувачі мають доступ, щоб знайти викиди. Крім того, системи контролю доступу використовують технологію для відстеження, контролю та моніторингу доступу до об’єктів і фізичних переміщень людей. Інструменти, які можуть покращити здатність

організації захищати свої мережі, системи, обладнання та учасників від внутрішніх загроз, представлені у Табл. 4.1 [13].

Таблиця 4.1 – Інструменти для покращення захисту ресурсів організації

Інструменти	Функція
Моніторинг бази даних	Відстеження транзакції бази даних і блокує виконання несанкціонованих транзакцій.
Системи контролю доступу	Відстеження, контроль та спостерігання за доступом і переміщенням усередині та навколо об'єктів. Для цього використовують безконтактні картки, біометричні системи, розпізнавання відбитків пальців/облич. Ці системи можуть бути веб-орієнтованими, щоб вони могли повністю інтегруватися в IT-архітектуру організації.
Системи безпеки та керування подіями	Збір, аналіз та звітування про дані журналів і подій у режимі реального часу, щоб забезпечити моніторинг загроз, кореляцію подій та реагування на інциденти.
Білий список	Блокування будь-якої неавторизованої програми від розміщення в мережі інформації без дозволу.
Технології керування привілейованим доступом	Запобігання доступу інсайдерів до певних систем, програм або засобів без відповідних дозволів. Ці системи використовують паролі, управління сеансами та доступом.
Запобігання втраті даних	Захист зв'язку між електронною поштою, кінцевими точками, Інтернетом, мережами та хмарою, перш ніж він покине мережу хоста, щоб уникнути витоку інформації. Деякі інструменти також можуть блокувати, контролювати або сповіщати, коли USB або зовнішній пристрій підключено до комп'ютера. Крім того, інші інструменти запобігання втраті даних можуть ініціювати електронні листи або повідомлення співробітникам і керівникам, коли співробітники намагаються надіслати вкладення.
Аналіз мережевого потоку	Відстежує пакети даних, щоб визначити, чи зв'язок, що виходить із хост-мережі, здійснюється між зловмисним програмним забезпеченням та іншим сервером керування.

Організації повинні використовувати численні технологічні інструменти, особливо в міру того, як організація росте. Але технологія лише покращує здатність організації виявляти та ідентифікувати, оцінювати та управляти внутрішніми загрозами. Існування внутрішніх загроз вимагають кваліфікованого аналітика ІБ для інтерпретації та розуміння даних.

Глобальний звіт Інституту Ponemon про інсайдерські загрози за 2020 рік [15] містить цінний перелік найбільш часто використовуваних інструментів і заходів для зменшення кіберзагрози від довіреного інсайдера (Рис. 4.2).

Рисунок 4.2 – Застосовувані компаніями інструменти та дії

4.2 Впровадження DLP-систем у контур безпеки організацій

Лише політика та навчання персоналу не вирішать проблему витоку даних, тому потрібна технологія, яка допоможе управляти та захищати інтелектуальну власність протягом усього її життєвого циклу, а також з’ясувати, де вона знаходиться та куди переміщується. Для цього існує технологія запобігання втраті даних (DLP) [16].

Запобігання витоку даних (DLP) — це рішення, призначене для своєчасного виявлення потенційних інцидентів порушення даних і запобігання їм шляхом моніторингу даних під час використання (дії кінцевої точки), у русі (мережевий трафік) або в стані спокою (зберігання даних). Рішення DLP використовуються для вирішення бізнес-проблеми захисту конфіденційних даних.

Розглянемо алгоритм роботи DLP:

1) Класифікація даних. DLP використовується для сортування та маркування кожної частини даних в інфраструктурі організації

певним рівнем класифікації, наприклад публічний, конфіденційний або внутрішній. Процес класифікації вимагає розробки політики класифікації даних. Це може бути ручним або автоматизованим, залежно від наявного рішення DLP.

2) Визначення рівнів конфіденційності. На основі результатів класифікації співробітники служби безпеки призначають конкретні фрази, що вказують на рівень конфіденційності для різних типів даних: *приватні*, *конфіденційні*, *цілком таємні* тощо. Кількість маркерів конфіденційності залежить від організайії.
3) Розробка правил безпеки. Після обробки всіх даних організації команда кібербезпеки налаштовує поведінку системи DLP, створюючи правила. Ці правила визначають, як система реагує на спрацьовування певного маркера конфіденційності (надсилання сповіщення, припинення передачі конфіденційних даних або скасування прав доступу користувача).
4) Моніторинг і розслідування. Система починає моніторинг конфіденційних даних після встановлення правил безпеки. Під час спрацьовування сповіщення, система реагує на подію в залежності від попередніх налаштувань, і повідомляє команду кібербезпеки. Потім працівники служби безпеки аналізують подію, щоб визначити, чи це інцидент чи помилковий результат.
5) Класифікація нових даних. Коли нові дані надходять в інфраструктуру організації, процес DLP починається заново, починаючи з етапу класифікації [17].

Рішення DLP розрізняють три фази даних протягом життєвого циклу: «дані в стані спокою», «дані в русі» та «дані у використанні» [16].

Дані в пам’яті (Data-At-Rest, DAR) визначаються як усі дані в пам’яті комп’ютера. Щоб захистити дані від доступу, викрадення чи зміни неавторизованими особами, зазвичай використовуються такі заходи безпеки, як шифрування даних і контроль доступу. Необхідною умовою для цих заходів

безпеки є виявлення вмісту, яке служить для визначення місця зберігання всіх даних. Одним із способів досягти цього є використання функцій виявлення вмісту продуктів DLP.

Використовувані дані (Data-In-Use, DIU) – це будь-які дані, з якими взаємодіє користувач. Системи, пов'язані з кінцевими точками, слугують для захисту даних, що використовуються, і для моніторингу даних під час взаємодії користувача з ними. Зазвичай агент застосовується для моніторингу даних під час їх використання або транспортування від пристрою кінцевої точки або клієнта через різні вихідні канали до периферійних пристроїв.

Основна ідея полягає в тому, що якщо буде зроблена спроба надіслати конфіденційні дані, то потенційний витік буде негайно виявлено та усунено (заблоковано) до того, як ці дані будуть надіслані. Інструменти використання даних можуть контролювати наступні дії [16]:

- Операції копіювання та вставки, знімки екрана з конфіденційними даними;
- Передача конфіденційного вмісту з одного місця в інше за допомогою портативних пристроїв зберігання, таких як USB-накопичувачі, CD/DVD, смартфони тощо;
- Друк або надсилання (факсом, E-mail та ін.) конфіденційного вмісту.

Data-In-Motion (DIM) – це дані, які надсилаються через мережу. Ці дані можуть надсилатися у внутрішню мережу організації або передаватись у зовнішню мережу. Рішення DLP використовуються для виявлення та перевірки даних, які надсилаються через канали зв'язку через мережу за допомогою відомих протоколів, включаючи електронну пошту, HTTP, миттєві повідомлення та навіть невідомі протоколи (просто перевіряючи вміст пакетів). Якщо дозволено шифрування або зашифровані з'єднання без можливості розшифровки даних, рішення DLP не зможе виявити витік зашифрованих конфіденційних даних у русі [16].

Хоча існують різні способи, за допомогою яких системи DLP аналізують свої дані, цей аналіз можна згрупувати у дві великі групи. Це контекстний

аналіз і контент-аналіз. Контекст зосереджується на оточенні даних, тоді як вміст зосереджується на фактичних даних [18].

Аналіз контексту. Цей метод аналізу фактично аналізує властивості метаданих із конфіденційними даними. Це робиться шляхом вивчення інформації про дані та відстеження даних за допомогою різних атрибутів даних, таких як розмір документа, джерело, призначення, час створення або зміни документа та інші властивості. За допомогою цих атрибутів метаданих конфіденційних даних можна використовувати шаблон і підпис для формування процесу визначення того, як можна створити політики для виявлення втрати даних [18].

Аналіз вмісту. У цьому методі аналіз зосереджується на вмісті конфіденційних даних, якими може бути текст або будь-який мультимедійний матеріал. Він робить це шляхом порівняння переданих даних з оригінальними конфіденційними даними та виявляє порушення, якщо є високий відсоток подібності. Цей процес можна здійснити в основному за допомогою трьох методів: відбитків даних (ідентифікує шаблони з точним або частковим збігом), регулярного виразу (ідентифікує його шаблони на основі слів або тексту) і статистичного аналізу (з використанням попередньо записаної інформації). Системи DLP можуть бути або профілактичними, або детективними, залежно від типу методів, які використовуються організацією. Запобіжні методи включають: політику та права доступу, віртуалізацію та ізоляцію, криптографічні підходи, кількісну оцінку та обмеження; тоді як детективні методи включають: ідентифікацію даних, соціальні та поведінкові, інтелектуальний аналіз даних/кластеризацію тексту, кількісну оцінку та обмеження [18].

Системи DLP можуть бути або профілактичними, або детективними, залежно від типу методів, які використовуються організацією. Запобіжні методи включають:

- політику та права доступу;
- віртуалізацію та ізоляцію;

- криптографічні підходи;
- кількісну оцінку та обмеження.

У той же час детективні методи включають:

- ідентифікацію даних;
- соціальні та поведінкові методи;
- інтелектуальний аналіз даних/кластеризацію тексту;
- кількісну оцінку та обмеження.

Системи DLP, як і інші механізми безпеки, під час захисту конфіденційних даних від втрати стикаються з багатьма проблемами, які можуть зробити систему неефективною. Під час огляду, проведеного дослідниками в галузі як промислових, так і академічних систем DPL, було виявлено, що було визначено сім загальних проблем[18]. Щоб запровадити ефективну систему DLP, необхідно вирішити ці різні проблеми. Далі обговоримо ці виклики і спробуємо запропонувати можливі рішення для кожного з них у Табл. 4.2.

Виходячи з наведених у таблиці даних, система DLP є найбільш вразливою до модифікайії данних та до використання шифрування та стеганографії.

З точки зору безпеки, на ринку існує багато систем безпеки та постачальників безпеки. Ці системи унікальні та відрізняються своєю функціональністю. У Табл. 4.3 узагальнено характеристики DLP у порівнянні з системою запобігання вторгненням (IPS) і системою брандмауера [18].

Таблиця 4.2 – Варіанти вирішення загальних проблем систем DLP

Проблема	Опис	Рішення
Канали витоку	Проміжні канали можуть стати причиною витоку конфіденційних даних, але ці канали не можна повністю заблокувати, оскільки це важливий аспект у обміні даними, який вимагає, щоб деякі або навіть усі ці канали були відкритими.	• Використання хостових DLP для приводів CD/DVD і каналів USB-портів, але цього недостатньо для інших каналів (миттєві повідомлення (IM) і електронні листи); • В каналах обміну файлами та веб-сервісах, пов'язаних з даними «в дорозі», необхідно проводити інтенсивну фільтрацію трафіку.
Людський фактор	Обмеження, накладені системою DLP, можна легко обійти шляхом спільного використання права доступу користувачами навмисно або ненавмисно.	Людський фактор завжди буде серйозною проблемою при розгортанні систем DLP, доки людина взаємодіє з системою.
Права доступу	Системи DLP не зможуть запобігти нелегітимним користувачам отримати доступ до конфіденційної інформації, якщо немає належної категоризації та оновлення прав доступу.	• Права доступу слід завжди регулярно оновлювати; • Для ефективності система DLP повинна підтримувати та контролювати права доступу організації.
Шифрування та стеганографія	Через складне шифрування даних DLP системі важко аналізувати вміст даних. Після стиску або перетворення даних в інший формат DLP не зможе якісно аналізувати ці документи.	Система DLP не може зчитувати зашифровані дані та дані, приховані в зображеннях, аудіо та відео.
Модифікація даних	Користувач може повністю змінити структуру або формат документа, тим самим зробивши документи невидимими для систем DLP.	Ця система не є ефективною, коли конфіденційні документи значно змінюються.
Масштабованість та інтеграція	Обсяг оброблених даних може вплинути на продуктивність системи DLP.	Обчислювальну складність методів аналізу слід враховувати при розгортанні систем. Слід виключати повторення функцій, оскільки це призведе до зниження пропускної здатності системи.
Класифікація даних	Проблема у визначенні рівня конфіденційності даних. Процес класифікації довіряють людям, які не володіють потрібною інформацією.	• Заборона персоналу, який не має дозволу на перегляд певної інформації, мати доступ до даних такого типу.

Таблиця 4.3 – Порівняння системи DLP з IPS/Firewall

Вразливості в безпеці	Системи IPS/Firewall	Системи DLP
Розділення мережі на розділи мережевої безпеки	Ні	Так
Інтеграція балансувальника навантаження	Ні	Обмежено
Прискорене виконання програми	Ні	Так
Пул з'єднань TCP	Ні	Так
Розвантаження SSL	Ні	Так
Вбудований механізм автентифікації	Ні	Так
Перевірка зашифрованих сеансів	Ні	Так
Єдиний вхід у кілька програм	Ні	Так
Захист від ін'єкційних атак (XSS, SQL)	Обмежено	Так
Нормалізація закодованого трафіку	Ні	Так
Перевірка трафіку HTTPS	Ні	Так
Протидія підробці, перехопленню сеансу	Ні	Так
Примусове запобігання перегляду веб-сторінок	Ні	Так
Захист від викрадення даних, клоакінгу	Ні	Так
Захист від Brute-force атак	Ні	Так
Захист від завантажень троянів, черв’яків (Warms), вірусів, шкідливого ПЗ	Так (виявлення атак Back Door)	Так (блокування та повідомлення про дії користувачів)
Захист контролю швидкості	Ні	Так
Зміна запиту/відповіді	Ні	Так
Реєстрація доступу до додатків та відстеження аудиту користувачів	Ні	Так (залежить від правил політики)

Системи DLP мають більшу перевагу над іншими систем безпеки, оскільки вони мають можливість виконувати різні функції. Це знижує витрати на придбання багатьох систем безпеки при моніторингу різних прогалин у безпеці.

Щоб забезпечити належне впровадження будь-яких систем DLP, наведемо перелік кроків, дотримання яких допоможе організації належним

чином запровадити системи DLP для захисту своїх конфіденційних даних. До цих кроків входять:

1) Впровадження універсальної методики та ціннісної пропозиції для DLP, зосередженої на оцінці ризику;
2) Залучення людей за допомогою правильної моделі організації;
3) Визначення конфіденційних даних та методу їх обробки;
4) Забезпечення поетапного впровадження на основі прогресу;
5) Зменшення впливу на продуктивність системи та бізнес-операції;
6) Створення значущих політик DLP і процесів керування політиками;
7) Запровадження ефективних механізмів перевірки і розслідування подій;
8) Надання аналізу і змістовного звіту;
9) Впровадження заходів безпеки та відповідності;
10) Впровадження організаційного потоку даних і механізму нагляду.

Отже для ефективного функціонування системи DLP необхідно адекватно розуміти, які конфіденційні дані хоче зберігати організація, де конфіденційні дані мають зберігатися з точки зору місць та призначення і канали, через які ця інформація буде проходити [18].

4.3 Вектори протидії фішингу та кейлогерам

Для здійснення атаки фішингу на основі шкідливих програм на пристрій жертви таємно встановлюються шкідливі програми, щоб надати зловмиснику доступ до комп'ютера користувача та його конфіденційних даних [19]. Доволі часто для цих цілей використовують кейлогери.

Заходи з виявлення клавіатурних шпигунів є важливими для захисту особистих або організаційних інформаційних активів. Наявність кейлогерів, встановлених на комп’ютерах користувачів, можливо виявити за допомогою деяких загальних показників, наведених у наступному переліку [19]:

- Сповіщення від брандмауеру, антишпигунського програмного забезпечення, клавіатурних шпигунів і антивірусних програм;
- Деякі клавіші не працюють належним чином;

- Для появи символу на екрані після натискання клавіші потрібен час;
- Натискання мишею не завжди спрацьовує;
- Операції подвійного натискання та перетягування спрацьовують некоректно;

Якщо будь-яка із цих ознак з’являється навіть після перезавантаження системи, імовірно, у комп’ютерній системі існує кейлогер. Користувачі повинні завжди пам’ятати про загрози клавіатурних шпигунів під час введення важливої інформації за допомогою клавіатури. Навіть якщо програми пропонують віртуальні клавіатури для введення особистої інформації, вони не повністю захищають особисту інформацію користувачів. Не слід забувати, що деякі передові клавіатурні шпигуни можуть робити знімки екрану на основі натискання миші з метою відкриття критично важливої інформації [19].

Використання брандмауеру захищає систему від шкідливого коду або підозрілих пакетів, які надходять із зовнішньої мережі. Брандмауер вирішує, які пакети слід пропускати, а які блокувати, та здатен фільтрувати трафік даних, який намагається вийти з «внутрішьої» мережі назовні [20], таким чином запобігаючи, серед іншого, різним типам шкідливого коду, вірусам і хробакам. Також існують зворотні брандмауери (мережеві екрани), які можна використовувати для сповіщення користувача, коли кейлогер використовує мережеве з’єднання. Це дає користувачеві можливість заборонити кейлогеру надсилати отриману інформацію третім особам [14].

Вкрай важливо встановити антикейлогери. Це тип програмного забезпечення, розробленого спеціально для виявлення кейлогерів; часто таке програмне забезпечення також містить можливість видаляти або принаймні знешкоджувати зловмисне програмне забезпечення кейлогера. Порівняно з більшістю антивірусних або антишпигунських програм основна відмінність полягає в тому, що анти-клавіатурний шпигун не розрізняє законну програму-клавіатурний шпигун і нелегітимну програму (наприклад, зловмисне програмне забезпечення); усі клавіатурні шпигуни будуть позначені та (за бажанням) видалені [14].

Програмне забезпечення для захисту від кейлогерів використовує методи моніторингу інтерфейсу прикладного програмування (Application Programming Interface, API), такі як проксі-бібліотека DLL (Dynamic Link Library) і виправлення таблиці адрес імпорту (Import Address Table, IAT).

Сучасне програмне забезпечення (ПЗ) виявлення Keylogger переважно намагається сканувати систему клавіатурних перехоплень і кейлогерів на рівні ядра. Дуже мало методів виявлення зосереджені на порушенні зв'язку між хост-системою та хакером. Як згадувалося раніше, більшість клавіатурних шпигунів працюють однаково. Хоча існують різні способи підключення до клавіатури або перехоплення натискання клавіш і їх реєстрації, більшість клавіатурних шпигунів все ще покладаються на підключення до певного типу SMTP *(«Simple Mail Transfer Protocol»)* або FTP-сервера для передачі файлу журналу.

Нижче наведемо узагальнений перелік запобіжних заходів, наведених в [19], [21], [22], [23], для протидії витоку даних, спричиненому кейлогерами:

- Виконання без наявності сторонніх осіб періодичної перевірки журналів комп'ютера;
- Постійний моніторинг будь-якої активності на комп'ютері;
- Використання таких методів запобігання, як брандмауери, засоби захисту від вірусів, шпигунського програмного забезпечення та спаму;
- Відсутність доступу сторонніх осіб до комп'ютера;
- Уважна перевірка наявності ознак роботи кейлогерів і систем моніторингу активності;
- Використання екранних клавіатур;
- Підтримка оновлення системи безпеки в актуальному стані;
- Завантаження програм лише з перевірених веб-сайтів;
- Уважне ознайомлення із спливаючими вікнами попереджень безпеки, ліцензійних угод і заяв про конфіденційність;

- Використання комплексу засобів захисту від шпигунського програмного забезпечення для виявлення та видалення зловмисного програмного забезпечення та вірусів;
- Використання лише ліцензійного програмного забезпечення;
- Періодичний моніторинг інформації про появу нових загроз;
- Явне обмеження привілей операційної системи;
- Наявність політики надійних паролів;
- Заборона підключення до Інтернету або до внутрішньої мережі, використовуючи права адміністратора;
- Перевірка порту клавіатури комп'ютера на наявність підключення апаратного кейлогеру;
- Контроль біт тайм-ауту порту PS/2;
- Використання альтернативних розкладок клавіатури, які підтримуються програмою для створення розкладок клавіатури;
- Використання смарт-карти;
- Використання одноразових паролів (OTP) та їх отримання через SMS (Short Message Service) [14];
- Використання програми автоматичного заповнення форм;
- Контроль правового статусу шпигунського програмного забезпечення.

Інші заходи, які пропонуються для захисту користувачів від деяких уразливостей кейлогерів, включають використання бездротових, інфрачервоних, Bluetooth або лазерних клавіатур, віртуальних клавіатур і моніторів із сенсорним екраном. Однак ці заходи можуть нести свої ризики.

Користувачі комп'ютерів також повинні розглянути можливість використання таких технологій, як BlueGem Security [19]. Ця технологія використовує шифрування LocalSSL (Secure Socket Layer), щоб запобігти використанню хакерами інструментів кейлогера для перехоплення та перегляду натискань клавіш користувача. LocalSSL захищає передачу за допомогою 128-ключового шифрування в обхід операційної системи. Також було представлено

іншу пропозицію про те, що програма віртуальної клавіатури може обходити системну чергу повідомлень і надсилати повідомлення клавіатури безпосередньо в чергу повідомлень конкретної програми за допомогою перехоплення на рівні програми. Після отримання цих повідомлень клавіатури програма виконує відповідні дії так, ніби вона отримала фактичне апаратне забезпечення через чергу системних повідомлень. Таким чином черга повідомлень системного рівня обходиться, і програмний кейлогер не може захопити конфіденційні дані [19].

4.4 Способи запобігання SE атакам

Незалежно від того, які засоби контролю реалізовано, завжди є «людський фактор», який впливає на поведінку людини (персоналу), тому не можна стверджувати про наявність 100% ефективних способів захисту від атак соціальної інженерії так як цей процес завжди перебуває в русі та напряму залежить від змін, насамперед в соціальній та технологічній сферах діяльності сучасного людства. Але є певні, загальні способи, впровадження яких дозволяє знизити ймовірність успіху SE-атак. Організаціям також важливо встановити чітку та сильну політику безпеки та процеси для зменшення загрози соціальної інженерії. Нижче наведено методи для забезпечення захисту від SE-атак:

1) Тренінги з питань безпеки. Це є найпростішим рішенням для запобігання атакам соціальної інженерії. Кожна особа в організації повинна своєчасно пройти базову підготовку з питань безпеки, щоб він/вона ніколи не надавав жодної інформації без відповідного дозволу та що він/вона повинен повідомляти про будь-яку підозрілу поведінку;
2) Перевірка даних. Існує велика ймовірність того, що зловмисник може приєднатися до компанії як співробітник, щоб збирати інсайдерську інформацію про компанію. Це робить перевірку фону дійсно важливою частиною політики компанії щодо протидії атакам соціальної інженерії. Його слід поширювати не лише на внутрішніх працівників, але й на постачальників та інших контрактних

працівників, перш ніж вони стануть частиною організації або отримають доступ до мережі організації [12];

3) Фізична охорона. Має бути належний механізм контролю доступу, щоб переконатися, що лише уповноважені люди мають доступ до обмежених розділів організації;
4) Обмежений витік даних. Необхідно постійно стежити за тим, яка інформація про організацію шириться в Інтернеті. Будь-які несправності слід негайно усунути. Це ускладнить пасивний збір інформації для зловмисника [12];
5) Імітаційні вправи з соціальної інженерії. Спеціальна соціальна інженерія повинна проводитись із внутрішніми працівниками організації групою безпеки або постачальником, щоб відстежувати рівень обізнаності щодо безпеки в організації;
6) Політика класифікації даних. Повинна бути належна класифікація даних на основі їх рівнів критичності та доступу персоналу. Класифікація даних призначає рівень чутливості до інформації компанії. Кожен рівень класифікації даних включає різні правила для перегляду, редагування та спільного використання даних. Це допомагає запобігти соціальній інженерії, надаючи працівникам механізм розуміння того, яку інформацію можна розголошувати, а якою не можна ділитися без належного дозволу.
7) Встановлення та підтримка брандмауерів, антивірусного програмного забезпечення, антишпигунського програмного забезпечення та фільтрів електронної пошти;
8) Заборона близького контактування та передачі важливої інформації з незнайомими людьми та тими, хто не належить до організації [12];
9) Встановлення для організації належної стратегії реагування на інциденти;
10) Обмеження використання корпоративних ідентифікаторів у публічних доменах, блогах, дискусійних форумах тощо;

11) Звернення уваги на URL-адресу веб-сайту. Хоча зловмисні веб-сайти зазвичай виглядають ідентично легітимним сайтам, але URL-адреса може мати варіант написання або інший домен;
12) Заборона звернення до конфіденційних і важливих даних в Інтернеті в громадських місцях, кафе, готелях тощо, де не можна довіряти безпеці в Інтернеті;
13) Заборона надсилання конфіденційної інформації через Інтернет до того, як буде виконана перевірка безпеки веб-сайтів;
14) Нерозголошення особистої чи фінансової інформації в електронних листах і заборона надання відповіді на листи електронної пошти з запитами щодо цієї інформації;
15) Постійна перевірка захищеності всіх фізичних точок входу та виходу;
16) Заборона надання кому-небудь особистої інформації чи інформації про організацію, якщо немає впевненості в повноваженнях цієї особи мати цю інформацію;
17) Використання віртуальної клавіатури, де це можливо;
18) Дотримання обережності щодо розміщенння інформації на веб-сайті компанії. Необхідно уникати публікації організаційних діаграм або списків ключових людей, де це можливо;
19) Обов’язкове знищення, подрібнення усіх викинутих документів, які можуть містити конфіденційні дані.

Висновки за розділом [12].

Одним з найефективніших засобів протидії інсайдерським загрозам є стровення і впровадження корпоративних програм пом’якшення внутрішніх загроз, що повинна адаптивно враховувати поточні характеристики розвитку організації та зміни її пріоритетів. В цьому сенсі, найчастіше використовуваними інструментами і заходами для зменшення рівня кіберзагроз від зловмисної діяльності інсайдерів є: - технології моніторингу всього спектру кіберповедінки користувачів (UAM та UBA); - DLP системи та постійні навчання і підвищення рівня обізнаності персоналу.

DLP системи є важливим інструментом, впровадження якого призводить до посилення поточних гарантій безпеки даних в організацій. Слід намагатися підтримувати актуальну стратегію застосування та впровадження DLP систем. При цьому, важливо зробити систему простою у використанні та управлінні, оскільки чим складніша DLP система, тим більша ймовірність того, що цільова система буде скомпрометована.

Особу увагу слід приділити захисту від SE-атак, так як незалежно від того, які засоби контролю реалізовано, завжди є «людський фактор» [24], який не дозволяє стверджувати про абсолютну надійність захисту конфіденційних даних. В даному випадку, до ефективних методів захисту можна віднести проведення тренінгів з питань ІБ та імітаційних тренувань з соціальної інженерії, так як саме постійне навчання персоналу дозволить покращити взаємодію з даними та вберегти їх від витоку.

Для запобігання здійснення фішингових атак на основі кейлогерів насамперед необхідно передбачити активне використання двоспрямованих брандмауерів, біометричних систем автентифікації [25] та антишпигунського ПЗ. Результатом інтеграції цих складових захисту є створення комплексного рішення безпеки, яке ефективно протидіє спробам витоку, як персоніфікованої, так і чутливої корпоративної інформації в сучасних ІС.

ВИСНОВКИ

В роботі проведено аналіз особливостей проблематики доксінгу та запропоновано узагальнення можливостей з комплексної протидії цієї загрозі в ІТ-сфері. Суть явища доксінгу полягає в здійсненні зловмисних дій проти користувачів послуг та/або засобів сучасних ІС, шляхом викрадення конфіденційної інформації чи особистих даних. За результатами проведених досліджень підкреслено, що доксінг є відносно новим явищем, можливість існування котрого обумовлена неперервним розвитком нових ІТ-технологій та масштабною цифровізаціэю всіх сфер сучасного суспільства [26].

Існуючі концепції та механізми забезпечення ІБ не можуть гарантувати повного захисту чутливих даних мережевих користувачів, оскільки будь-які дані при їх обробці та багатопараметрічних узагальненнях *(час, мова, геолокація, пошукові запити, час спілкування з учасниками мережевих груп тощо),* можуть стати зброєю в руках доксерів, мотиви дій яких можуть варіюватися від традиційного булінгу до, навить, політико-економічних цілей [24]. Тому, при розміщенні особистої інформації на веб-сайтах та різних комунікаційних платформах, найкращою лінією поведінки є, по можливості, мінімізація обсягів доступної для широкого загалу, персоніфікованої інформації та чутливих даних користувачів. Така загальна стратегія помітно ускладнює процес попереднього збору інформації про майбутніх жертв доксерів, що дозволяє «розтягнути» терміни підготовки атак на інформаційні ресурси обраних жертв (фішинг, соціальний інжиніринг, сайт парсинг та ін.) і тим самим погіршити показник «часу реакцій» (або оперативності) атакуючої сторони [26].

За результатами попереднього аналізу наявних нормативних актів у сфері забезпечення приватності даних, зроблено висновок що, юридична сторона питання захисту конфіденційної інформації має безліч умовностей, які є причиною існування низки проблем у процедурах притягнення до

відповідальності за порушення відповідних законодавчих норм. З метою запобігання, а також притягнення до відповідальності доксерів-зловмисників у світі існує низка документів, що сприяють процесу підвищення рівня захисту чутливої інформації. Підкреслено, що GDPR та PDPO, які є міжнародними правовими рамками із захисту даних, мають досить схожі основні принципи, стосовно питань конфіденційності. Регламент захисту персональних даних разом з усім пакетом реформ «Privacy» є результатом багаторічного розвитку юридичної думки, що заснована на усвідомленні необхідності захисту приватного життя будь-якого громадянина в сучасному цифровому суспільстві.

За результатами узагальнення відомих інцидентів безпеки звернено увагу на той факт, що станом на сьогоднішній день, кіберзлочинці мають безліч інструментів для здійснення зловмисних дій у скомпрометованої їми системі чи мережі. Це напряму стосується і їх можливостей щодо викрадення конфіденційної інформації чи особистих даних жертв атаки. При цьому людський фактор є найслабшою ланкою в контурі безпеки, яку можна виправити тільки шляхом неперервності процесу підвищення особистий компетенцій з питань ІБ та вдосконалення існуючих механізмів захисту.

Акцентовано увагу, що користувачам послуг сучасних ІС, важливо мати розуміння різноманітності внутрішніх загроз безпеки, до яких вони повинні підготуватися. Цілістне розуміння багатовекторності існуючих кіберзагроз є запорукою усвідомлення необхідності впровадження комплексного захисту наявних інформаційних ресурсів. Класифікація та об'єктивна характеристика існуючого спектру внутрішніх загроз, сприяє кращій структуризації корпоративних програм безпеки (політик інформаційної безпеки) й впроваджуваних механізмів, щодо захисту від внутрішніх та зовнішніх загроз, в тому числі з питань безпеки конфіденційних даних.

Спираючись на результати проведеного аналізу можливих шляхів з протидії доксінгу, можна стверджувати, що одним з найефективніших засобів протидії витоку чутливих даних (в т.ч. інсайдерським загрозам), є впровадження корпоративних програм пом’якшення внутрішніх загроз, які

повинні адаптивно враховувати поточні характеристики розвитку організації та зміни її пріоритетів. В цьому сенсі, найчастіше використовуваними інструментами і заходами для зменшення рівня кіберзагроз від зловмисної діяльності інсайдерів є: - використання технологій моніторингу наявного спектру кіберповедінки користувачів (UAM і UBA); - впровадження наявних рішень XDR-платформ; - інтеграція DLP систем, як мінімальної складової із можливого переліку відомих технологій і засобів захисту; - постійне навчання та підвищення рівня обізнаності персоналу з питань ІБ.

DLP системи є важливим інструментом для посилення поточних гарантій безпеки чутливих даних, де «простота» її інтеграції та управління, є основним чинником її успішного застосування за призначенням.

Особливу увагу слід приділити захисту від SE-атак, так як незалежно від того, які міри і засоби безпеки було реалізовано, нажаль, завжди є «людський фактор» [24], який не дозволяє стверджувати про абсолютну надійність захисту конфіденційних даних. В даному випадку, до ефективної складової заходів із протидії доксінгу слід віднести проведення тренінгів з питань ІБ та імітаційних тренувань з соціальної інженерії, що дозволить покращити взаємодію з даними та поінформованість персоналу щодо специфіки роботи з різними категоріями (типами) корпоративної інформації.

Для запобігання здійснення фішингових атак на основі кейлогерів необхідно передбачити використання двоспрямованих брандмауерів, біометричних систем автентифікації і антишпигунського ПЗ. Результатом зусиль по інтеграції цих складових є побудова комплексного рішення безпеки, що ефективно протидіє спробам витоку, як персоніфікованої, так і чутливої корпоративної інформації в сучасних ІС. Отже, найефективніший спосіб зменшити ризики безпеки – це володіти інформацією про актуальні загрози та впроваджувати існуючі технології і методи захисту даних, виключно в їх комплексній парадигмі [26].

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Чорна Т. Проблематика доксингу: - міжнародний досвід щодо забезпечення захисту персональних даних [Електронний ресурс] / Т. Чорна, Э. Богданова, К. Погоріла // Study of world opinion regarding the development of science. Proceedings of the IX International Scientific and Practical Conference. Prague, Czech Republic. – 2022. – С. 720–723. – URL: https://isg-konf.com/study-of-world-opinion-regarding-the-development-of-science/ (дата звернення: 01.03.2023)

2 Why They Dox: First Large-Scale Study Reveals Top Motivations and Targets For this Form of Cyber Bullying | NYU Tandon School of Engineering [Електронний ресурс] // Home | NYU Tandon School of Engineering. – URL: https://engineering.nyu.edu/news/why-they-dox-first-large-scale-study-reveals-top-motivations-and-targets-form-cyber-bullying (дата звернення: 01.03.2023)

3 Chen M. Doxing: What Adolescents Look for and Their Intentions [Електронний ресурс] / Mengtong Chen, Anne Cheung, Ko Chan // International Journal of Environmental Research and Public Health. – 2019. – Т. 16, № 2. – С. 218. DOI: 10.3390/ijerph16020218

4 Чорна Т. Явище доксингу: Узагальнення характерних методів атаки та шляхів протидії цій загрозі. [Електронний ресурс] / Т. Чорна, В. Коршенко, С. Малахов // Теоретичне та практичне застосування результатів сучасної науки: матеріали III Міжнародної студентської наукової конференції, м. Біла Церква. – 2022. – № 3. – С. 226–229. DOI: 10.36074/liga-inter-07.10.2022

5 What Is Doxing? What Does It Mean to Dox Someone? | Fortinet [Електронний ресурс] // Fortinet. – URL: https://www.fortinet.com/resources/cyberglossary/doxing (дата

звернення: 18.03.2023)

6 Kai-Yi Wong S. EU GDPR and HK PDPO: What's the Difference? | Hong Kong Lawyer [Електронний ресурс] / Stephen Kai-Yi Wong // Home | Hong Kong Lawyer. – URL: https://www.hk-lawyer.org/content/eu-gdpr-and-hk-pdpo-what's-difference (дата звернення: 20.03.2023)

7 An Update on European Union General Data Protection Regulation 2016 [Електронний ресурс]. – 2018. – С. 45–100. – URL: http://www.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf (дата звернення: 21.03.2023)

8 General Data Protection Regulation (GDPR) – Official Legal Text [Електронний ресурс] // General Data Protection Regulation (GDPR). – URL: https://gdpr-info.eu/ (дата звернення: 21.03.2023)

9 Hong Kong e-Legislation [Електронний ресурс] // Hong Kong e-Legislation. – URL: https://www.elegislation.gov.hk/hk/cap486 (дата звернення: 21.03.2023)

10 Document 02002L0058-20091219 [Електронний ресурс]. – URL: https://eur-lex.europa.eu/eli/dir/2002/58 (дата звернення: 25.03.2023)

11 EUR-Lex - 32016L1148 - EN - EUR-Lex [Електронний ресурс] // EUR-Lex – Access to European Union law – choose your language. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення: 26.03.2023)

12 Shetty D. Social engineering - the human factor | www.securityxploded.com [Електронний ресурс] / Dinesh Shetty // Home Page - www.SecurityXploded.com. – URL: https://securityxploded.com/social-engineering-the-human-factor.php#gsc.tab=0 (дата звернення: 28.03.2023)

13 Cybersecurity and Infrastructure Security Agency. Insider Threat Mitigation Guide : Defining, Detecting, Assesing, and Managing Insider Threats: Cybersecurity and Infrastructure Security Agency [Електронний ресурс] / Cybersecurity and Infrastructure Security Agency. – [Б. м.] : Independently Published, 2022. – 133 с. – URL: https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf (дата звернення: 01.04.2023)

14 Naitlho E. A. Keylogger detection and prevention [Електронний ресурс] : capstone design / Naitlho El Amine. – Ifrane, 2022. – 50 с. – URL: http://www.aui.ma/sse-capstone-repository/pdf/fall-2022/KEYLOGGER%20DETECTION.pdf (дата звернення: 05.04.2023)

15 2020 Ponemon Cost of Insider Threats Global Report | Proofpoint US [Електронний ресурс] // Proofpoint. – URL: https://www.observeit.com/cost-of-insider-threats/ (дата звернення: 09.04.2023)

16 Tahboub R. Data Leakage/Loss Prevention Systems (DLP) [Електронний ресурс] / Radwan Tahboub, Yousef Saleh // 2014 World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, Tunisia, 17–19 січ. 2014 р. – [Б. м.], 2014. – С. 15. DOI: 10.1109/wccais.2014.6916624

17 Data Loss Prevention (DLP) Systems: What They Are & Key Benefits | Ekran System [Електронний ресурс] // Ekran System. – URL: https://www.ekransystem.com/en/blog/dlp-systems-pros-and-cons (дата звернення: 12.04.2023)

18 Data Loss Prevention and Challenges Faced in their Deployments [Електронний ресурс] / Victor O. Waziri [та ін.] // International Conference on Information and Communication Technology and its

Applications. – 2016. – URL: http://repository.futminna.edu.ng:8080/jspui/handle/123456789/2438 (дата звернення: 19.04.2023)

19 Sagiroglu S. Keyloggers [Електронний ресурс] / Seref Sagiroglu, Gurol Canbek // IEEE Technology and Society Magazine. – 2009. – Т. 28, № 3. – С. 10–17. DOI: 10.1109/mts.2009.93415

20 Рондалєв Д. Особливості функціонування корпоративного міжмережевого екрану та питання взаємодії з системою IDS [Електронний ресурс] / Д. Рондалєв, О. Мелкозьорова, О. Нарєжній. – 2019. – № 3. – С. 11–21. – URL: https://periodicals.karazin.ua/cscs/article/view/15614/14707 (дата звернення: 10.05.2023)

21 Vavilis S. Data Leakage Quantification [Електронний ресурс] / Sokratis Vavilis, Milan Petković, Nicola Zannone // Lecture Notes in Computer Science. – Berlin, 2014. – С. 98–113. DOI: 10.1007/978-3-662-43936-4_7

22 Prokopets M. How to Prevent Keylogging Attacks [Електронний ресурс] / Marie Prokopets // Nira. – URL: https://nira.com/how-to-prevent-keylogging-attacks/ (дата звернення: 15.05.2023)

23 Anti-Spyware Coalition Definitions and Supporting Documents [Електронний ресурс] // yumpu.com. – URL: https://www.yumpu.com/en/document/view/48017412/anti-spyware-coalition-definitions-and-supporting-documents (дата звернення: 19.05.2023)

24 Гайкова В. Суть аналогий кибербуллинга и эксперимента Милгрэма [Електронний ресурс] / Валерия Гайкова // Ricerche scientifiche e metodi della loro realizzazione: esperienza mondiale e realta domestiche / chair С. Малахов. – [Б. м.], 2021. DOI: 10.36074/logos-14.05.2021.v1.39

25 Fingerprint verification using the traveling salesman problem solution and decomposition of the vicinity of the minutiae [Електронний ресурс] // Computer Science and Cybersecurity. – 2020. – № 2. DOI: 10.26565/2519-2310-2020-2-03

26 Чорна Т. Інсайд, фишинг і SE-атаки, як складові проблематики доксінгу. [Електронний ресурс] / Т. Чорна, Ю. Лєсная, С. Малахов // Proceedings of the XXII International Scientific and Practical Conference. Helsinki, Finland. – 2023. – С. 506–510. – URL: https://isg-konf.com/modern-theories-and-improvement-of-world-methods (дата звернення: 01.06.2023)

ДОДАТОК А

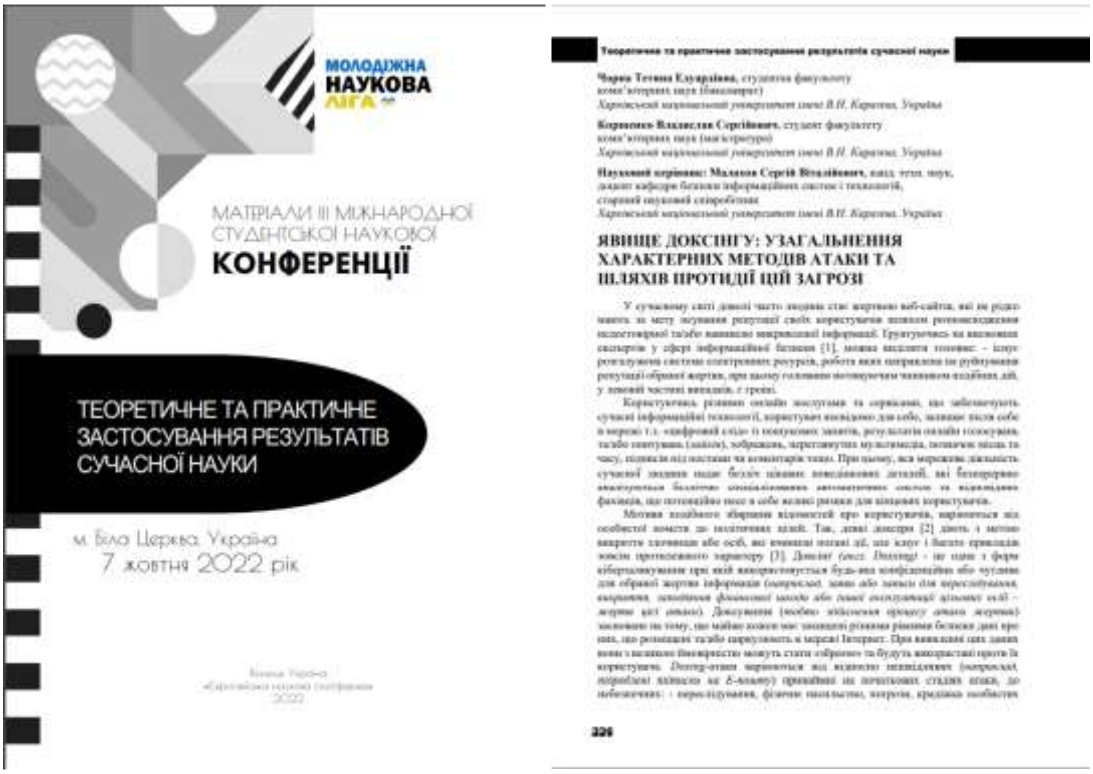

Рисунок А.1 — Наукове видання [4], сторінка 226

Рисунок А.2 – Сертифікат участі для роботи [4]

STUDY OF WORLD OPINION REGARDING THE DEVELOPMENT OF SCIENCE

Proceedings of the IX International Scientific and Practical Conference

Prague, Czech Republic
November 22 – 25, 2022

ПРОБЛЕМАТИКА ДОКСИНГУ: - МІЖНАРОДНИЙ ДОСВІД ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Чорна Тетяна Едуардівна
студентка факультету комп'ютерних наук, (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Богданова Єлизавета Сергіївна
студентка факультету комп'ютерних наук, (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Погоріла Каріна Валеріївна
студентка факультету комп'ютерних наук, (магістрат)
Харківський національний університет імені В.Н. Каразіна, Україна

В сучасному суспільстві, проблематика доксингу є однією з найбільш обговорюваних тем. Це відносно нове явище, що є поступово формування парадигми існування сучасного інформаційного суспільства. Актуальність цього напряму, спонукає профільних фахівців проводити ретельний аналіз відповідних інцидентів, з метою завчасного усунення передумов виникнення подібних загроз у майбутньому. Так наприклад, учасниками дослідження Нью-Йоркського університету 2017 року було виявлено та проаналізовано понад 5500 файлів, що були пов'язані із доксуванням [1]. Їх результати свідчать, що понад 90% доксованих файлів містили адресу жертви, 61% - номер телефону, в 53% - адресу електронної пошти жертви атаки. Більш того, сорок відсотків імен онлайн користувачів були оприлюднені, і такий же самий відсоток IP-адрес жертв атаки, було викладено в загальний доступ. Менш поширена, персоніфікована інформація, така як, номери кредитних карток (4,3%), номери соціального страхування (2,6%) або інша фінансова інформація (8,8%), також була розкрита (див. рис. 1).

Здійснюючи спробу захистити особисту інформацію, яка розміщена в соціальних мережах: - 32% жертв доксингу «закрили» або змінили особисті налаштування конфіденційності у своєму обліковому записі Instagram, а 25% змінили поточні налаштування облікового запису Facebook (після атаки). Приблизно 10% жертв цієї атаки змінили свій обліковий запис у Instagram, а 3% змінили свої налаштування у Facebook, після того, як було вжито заходів щодо боротьби зі зловмисниками.

Розглядаючи питання захисту конфіденційної інформації з юридичного боку, розкривається вся складність цієї проблеми. Зазвичай, в таких випадках, можна говорити про порушення законодавства про персональні дані, але коли йдеться про наслідки інциденту, важко притягти до відповідальності конкретну людину (виконавця та/або замовника атаки). Проте з метою запобігання, а також

Рисунок А.3 – Наукове видання [1], сторінка 720

CERTIFICATE

Google Scholar
Bowker
INTERNATIONAL SCIENCE GROUP
OUCI
Open Ukrainian Citation Index
doi
Crossref

is awarded to

Чорна Тетяна Едуардівна

for active participation
IX International Scientific and Practical Conference
«STUDY OF WORLD OPINION REGARDING THE DEVELOPMENT OF SCIENCE»

November 22 – 25, 2022, Prague, Czech Republic
24 Hours of Participation
(0,8 ECTS credits)

Organizing committee Ekaterina Zvereva

Рисунок А.4 – Сертифікат участі для роботи [1]

MODERN THEORIES AND
IMPROVEMENT OF WORLD METHODS

Proceedings of the XXII International Scientific and Practical Conference

Helsinki, Finland
June 06 – 09, 2023

TECHNICAL SCIENCES
MODERN THEORIES AND IMPROVEMENT OF WORLD METHODS

ІНСАЙД, ФІШИНГ ТА SE-АТАКИ ЯК СКЛАДОВІ ПРОБЛЕМАТИКИ ДОКСІНГУ

Чорна Тетяна Едуардівна
студентка факультету комп'ютерних наук, (бакалаврiат)
Харківський національний університет імені В.Н. Каразіна, Україна

Лєсная Юлія Євгенівна
студентка факультету комп'ютерних наук, (магістратура)
Харківський національний університет імені В.Н. Каразіна, Україна

Малахов Сергій Віталійович
канд. техн. наук, ст. науковий співробітник, доцент кафедри
Харківський національний університет імені В.Н. Каразіна, Україна

Вступ.

На сьогоднішній день корпоративні дані є одним із найважливіших активів організацій, які в межах своєї діяльності здійснюють її зберігання і обробку. До таких даних, в тому числі, належить інформація про їх клієнтів: - їх професійну діяльність, інтереси, фінансове і майнове становище, стан здоров'я тощо. В умовах постійного розширення відомих кіберзагроз, шахрайства та крадіжки особистих даних, потреба у захисті корпоративної й персоніфікованої інформації має першочергове значення. При цьому, несанкціонований доступ та/або крадіжка чутливої інформації здійснюється не лише за рахунок зловмисної діяльності зовнішніх кіберзлочинців (хакерів) але й завдяки хибних дій персоналу та навмисної діяльності внутрішніх інсайдерів [1-2].

Узагальнення відомостей, стосовно кількості інцидентів безпеки, пов'язаних із витоком інформації, як на побутовому рівні, так і на рівні організацій, вказує на появу нових та постійне вдосконалення відомих методів і інструментів незаконного збору чутливої корпоративної інформації, та персоніфікованих даних власників звичайних гаджетів та/чи користувачів онлайн сервісів сучасних інформаційних систем (ІС) [3-6].

Тому розгляд питань, стосовно безпеки персоніфікованої інформації та чутливих корпоративних даних, є безумовно актуальним і потребує проведення ретельного аналізу поточного стану загроз й оцінки можливостей з протидії несанкціонованому витоку даних та спробам реалізації доксінгу.

Завчасна оцінка актуальних ризиків інформаційної безпеки (ІБ) та методична робота, щодо виключення передумов виникнення інсайду і витоку даних технічними каналами, здатні мінімізувати наслідки хибних або навмисних дій персоналу, що забезпечує недопущення передумов для реалізації доксингу чутливої інформації.

Рисунок А.5 – Наукове видання [26], сторінка 506

CERTIFICATE

Google Scholar
Bowker
INTERNATIONAL SCIENCE GROUP
OUCI
Open Ukrainian Citation Index
doi
Crossref

is awarded to

Чорна Тетяна Едуардівна

for active participation
XXII International Scientific and Practical Conference
«MODERN THEORIES AND IMPROVEMENT OF WORLD METHODS»

June 06-09, 2023, Helsinki, Finland
24 Hours of Participation
(0,8 ECTS credits)

Organizing committee Ekaterina Zvereva

Рисунок А.6 – Сертифікат участі для роботи [26]