Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

Магістр
(назва освітнього ступеня)

на тему: Інформаційна безпека малого та середнього бізнесу: сучасний стан, загрози та протидії

Виконав студент 6 курсу, групи СБм-61
спеціальності (напрямку підготовки)
125 «Кібербезпека»
(шифр і назва спеціальності (напряму підготовки))

		Кравчук В.М.
	(підпис)	(прізвище та ініціали)
Керівник		Кульчицький Т.Р.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Лечаченко Т.А.
	(підпис)	(прізвище та ініціали))
Завідувач кафедри		Загородна Н.В.
	(підпис)	(прізвище та ініціали)
Рецензент		Осухівська Г.М.
	(підпис)	(прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека

студенту Кравчуку Віталію Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Інформаційна безпека малого та середнього бізнесу: сучасний стан, загрози та протидії в системі керування розумним будинком

Керівник роботи Кульчицький Тарас Русланович Ph.D в галузі права
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «16» листопада 2023 року № 4/7-1061

2. Термін подання студентом роботи 16.12.2023

3. Вихідні дані до роботи Технічна документація, інтернет-джерела

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Розділ 1. Загрози кібербезпеки для малого та середнього бізнесу. 1.1 Види інформаційних загроз. 1.2 Наслідки кібератак. Розділ 2. Класифікація інформації, що підлягає захисту відповідно до законодавства України. 2.1 Персональні дані. 2.2 Комерційна таємниця. 2.3 Службова таємниця. 2.4 Професійна таємниця.2.5 Процесуальна таємниця. Розділ 3. Захист інформації ЛОМ (локальної обчислювальної мережі) АТ Укрбургаз. 3.1 Аналіз вразливості підприємства. 3.2 Встановлення між мережевого екрану. 3.3 Впровадження криптопровайдера в системі захисту даних. 3.4 Встановлення засобів виявлення вторгнень та антивіруса.Розділ 4. Безпека життєдіяльності, основи охорони праці. 4.1 Охорона праці. 4.2 Безпека в надзвичайних ситуаціях. Висновки. Список використаних джерел. Додатки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титулка. 2. Актуальність, об'єкт, предмет дослідження. 3. Мета кваліфікаційної роботи. 4. Інтерфейс адміністратора у UserGate Proxy & Firewall. 5. Контроль сесій у UserGate Proxy & Firewall. 6. Налаштування обмежень щодо трафіку та між мережевого екранування. 7. Схема обміну захищеними документами. 8. Процес формування та перевірки підпису документа. 9. Процедура оновлення сертифіката у ViPNet CSP. 10. Створення правила трансляції (NAT) 11. Компоненти Security Studio Endpoint Protection. 12. Варіант розміщення засобів захисту інформації у корпоративній мережі. 13. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М. к.т.н. зав. Кафедри КС		
Безпека в надзвичайних ситуаціях	Клепчик В.М, проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 16.11. 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення з завданням до кваліфікаційної роботи	16.11.2023	Виконано
2	Підбір джерел про інформаційну безпеку	16.11.23-20.11.23	Виконано
3	Опрацювання джерел про інформаційну безпеку	21.11.23	Виконано
4	Підбір джерел про існуючі засоби проведення аудиту	23.11.23	Виконано
5	Опрацювання джерел про види інформаційних загроз, наслідки кібератак	23.11.23 – 26.11.23	Виконано
6	Аналіз інформації, що підлягає захисту відповідно до законодавства України	27.11.23-28.11.23	Виконано
7	Аналіз роботи ЛОМ (локальної обчислювальної мережі) АТ Укрбургаз	29.11.23-01.12.23	Виконано
8	Оформлення першого розділу	02.12.23-04.12.23	Виконано
9	Оформлення другого розділу	05.12.23-06.12.23	Виконано
10	Оформлення третього розділу	07.12.23-08.12.23	Виконано
11	Оформлення розділу «Безпека життєдіяльності і основиохорони праці»	08.12.23-09.12.23	Виконано
12	Оформлення кваліфікаційної роботи	10.12.23	Виконано
13	Нормконтроль	11.12.23	Виконано
14	Перевірка на плагіат	20.12.23	Виконано
15	Захист кваліфікаційної роботи	26.12.23	Виконано

Студент _____ Кравчук В.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Кульчицький Т.Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Інформаційна безпека малого та середнього бізнесу: сучасний стан, загрози та протидії. // Кваліфікаційна робота освітнього рівня «Магістр» // Кравчук Віталій Миколайович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль 2023 // С. - 84, рис. - 11, табл. – 2, додат. – 4, бібліогр. – 38.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРАТАКА, ПЕРСОНАЛЬНІ ДАНІ, КОМЕРЦІЙНА ТАЄМНИЦЯ, ЗАХИСТ ДАНИХ.

У роботі досліджено питання інформаційної безпеки в розрізі підприємств малого та середнього бізнесу: сучасний стан, загрози та протидії. Малі та середні компанії найбільше страждають від кібератак. Через це такі компанії можуть втратити конфіденційну інформацію, гроші чи цінну частку ринку. Існує безліч способів, якими зловмисники намагаються досягти своїх цілей.

Областю інформаційної безпеки є управління ризиками та захисту інформації від загроз та небажаного доступу. Вона включає різні заходи і практики, спрямовані на дотримання конфіденційності, цілісності та доступності інформації.

Основна увага присвячена аналізу мережного та програмного забезпечення підприємства АТ Укрбургаз. Визначено склад інформації, схильної до загроз, виявлено вразливості із захисту, а також запропоновані заходи щодо запобігання загрозі інформаційної безпеки у ЛОМ АТ Укрбургаз.

Результати цієї роботи допоможуть підвищити розуміння процесів інформаційної безпеки і розробити рекомендації щодо поліпшення захисту локальної обчислювальної мережі підприємства. Дана кваліфікаційна робота може бути корисною для компаній, які планують підвищити рівень інформаційної безпеки.

ABSTRACT

Information security of small and medium-sized businesses: current state, threats and countermeasures. // Qualification work of the educational level "Master" // Kravchuk Vitalii Mykolayevich // Ternopil National Technical University named after Ivan Pulyu, faculty of computer and information systems and software engineering, department of cyber security, SBм-61 group // Ternopil 2023 // S. - 84, fig. - 11, tab. – 2, add. – 4, bibliography - 38.

Keywords: INFORMATION SECURITY, CYBER ATTACK, PERSONAL DATA, COMMERCIAL SECRET, DATA PROTECTION.

The work examines the issue of information security in the context of small and medium-sized enterprises: the current state, threats and countermeasures. Small and medium-sized companies suffer the most from cyber attacks. Because of this, such companies can lose confidential information, money or valuable market share. There are many ways in which attackers try to achieve their goals.

The area of information security is risk management and protection of information from threats and unwanted access. It includes various measures and practices aimed at maintaining confidentiality, integrity and availability of information.

The main focus is on the analysis of the network and software of JSC Ukrburgaz. The composition of information susceptible to threats was determined, security vulnerabilities were identified, and measures were proposed to prevent the threat of information security in LOM JSC Ukrburgaz.

The results of this work will help increase the understanding of information security processes and develop recommendations for improving the protection of the enterprise's local computer network. This qualifying work can be useful for companies that plan to increase the level of information security.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІБ - Інформаційна безпека

ЛОМ - локальна обчислювальна мережа)

ЕОМ - електронно-обчислювальна машина

МСБ-сегмент - сегмент малого та середнього бізнесу

ПЗ - програмне забезпечення

ОС - операційна система

СКЗІ - засіб криптографічного захисту інформації

SSEP - Security Studio Endpoint Protection

ЛОМ - локальна обчислювальна мережа

ІТ-фахівці - працюючі у сфері інформаційних технологій

ПЕОМ - персональна електронно-обчислювальна машина

ВСТУП

У сучасну цифрову епоху малий і середній бізнес все більше покладається на технології для здійснення своїх операцій. Хоча вони мають багато переваг, але також несуть в собі значний ризик: кібернебезпеку. Підприємства малого та середнього бізнесу особливо вразливі до кібератак, оскільки вони часто мають обмежені ресурси та не мають знань для адекватного управління своєю інформаційною безпекою.

Кібератаки можуть завдати шкоди малому та середньому бізнесу як у фінансовому плані, так і з точки зору шкоди репутації. Підприємства стають мішенню для хакерів, оскільки вони мають слабші заходи безпеки, ніж великі підприємства.

Заходи по підвищенню інформаційної безпеки мають вирішальне значення. Серед засобів захисту – антивірусне програмне забезпечення, брандмауери та регулярне оновлення ПЗ. Однак кібербезпека — це більше, ніж просто технологія. Вона передбачає навчання персоналу небезпеці кібератак, встановлення надійних паролів і засобів контролю доступу, а також розробку політик і процедур захисту.

Підвищення інформаційної безпеки може допомогти у запобіганні фінансових втрат, зниженні юридичної відповідальності та збереженні репутації організації. Клієнти більше хвилюються про захист своїх даних і охочіше співпрацюють із компаніями, які серйозно ставляться до кібербезпеки, що може допомогти малому та середньому бізнесу отримати конкурентну перевагу.

Актуальність дослідження полягає у внесенні пропозицій щодо встановлення захисту і покращення інформаційної безпеки підприємства АТ Укрбкргаз.

Об'єктом дослідження є інформаційна безпека малого та середнього бізнесу на основі інформаційних процесів АТ Укрбургаз, які організовані та функціонують на підприємстві.

Предмет дослідження – методи та способи захисту інформації в процесах АТ Укрбкргаз.

Головною метою даної кваліфікаційної роботи є підвищення рівня захищеності інформації на підприємстві АТ Укрбургаз за допомогою розробки рекомендацій щодо забезпечення захисту даних у ЛОМ та рішень щодо недопущення несанкціонованого доступу до службової та секретної інформації.

З метою досягнення визначеної цілі перед нами були поставлені такі *завдання*:

- визначити види інформаційних загроз та наслідки кібератак;
- провести аналіз уразливості підприємства АТ Укрбургаз (визначити можливі загрози, сценарії їх реалізації та оцінити актуальність загроз);
- розробити рекомендації щодо захисту інформації на підприємстві АТ Укрбургаз.

Практична значимість роботи визначається можливістю реалізації єдиної безпекової політики на підприємстві, що забезпечує належну ступінь захисту службової інформації.

Методи дослідження. У ході даної роботи використано наступні методи: теоретичні (дослідження тематичної літератури, індукції; пояснення; класифікації, аналізу та синтезу) та емпіричні (моделювання; аналіз, порівняння; планування).

Проблематику інформаційної безпеки сектору малого та середнього бізнесу досліджували різні автори О.Буров, В.Биков, О. Пінчук, С.Литвинова, Б.Бистрова, Т.Савчук.

Кваліфікаційна робота структурована наступним чином: вона включає вступ, чотири розділи, висновки та перелік використаних джере і додатків.

РОЗДІЛ 1 ЗАГРОЗИ КІБЕРБЕЗПЕКИ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

1.1 Види інформаційних загроз

Малі та середні підприємства вносять значний внесок у світову економіку, згідно з даними Світової організації торгівлі, МСБ-сегмент становить велику частину всього світового бізнесу. Через кібератаки ці компанії можуть втратити конфіденційну інформацію, гроші чи цінну частку ринку. Існує безліч способів, якими зловмисники намагаються досягти своїх цілей. Важливо визначити загрози, яким можуть наражатися компанії, а також способи їх виявлення та запобігання.

Інформаційна безпека (ІБ) — це галузь, що охоплює інструменти та процеси, які організації використовують для захисту інформації. Вона включає параметри політики, які запобігають доступу неавторизованих осіб до ділової чи особистої інформації. [10].

У питаннях збереження і захисту інформації ключовим є слово «доступ». Саме з його неправильної організації починається хибний шлях, коли «треті особи» отримують можливості проникнення у внутрішні інформаційні ресурси і можуть використовувати дані в будь-яких цілях, у тому числі протиправних і корисливих.

До таких вразливостей схильні підприємства будь-якої форми, але ті, які працюють у невеликих масштабах, «страждають» від них особливо гостро. Ресурси на забезпечення ІБ у них обмежені, а штатні ІТ-фахівці не завжди розуміють, як ефективно побудувати «лінію захисту» від потенційних витоків не лише ззовні, а й зсередини. І тут необхідно правильно розподілити зусилля та бюджет, щоб мінімізувати ризики та забезпечити захист важливих даних та операцій, розуміти — звідки йде загроза, як її промоніторити та припинити.

Питання інформаційної безпеки важливе для бізнесу. Ми визначили основні причини цього:

По-перше, вона забезпечує захист конфіденційності даних. Компанії зберігають і обробляють велику кількість критично важливої інформації, наприклад, про клієнтів, співробітників, підрядників. І порушення безпеки таких відомостей може призвести до витоків і серйозних правових наслідків, а за найгірших сценаріїв — до штрафів та судових позовів.

По-друге, ІБ підтримує репутацію організації. Витік даних та порушення, пов'язані з інформаційною безпекою, можуть завдати серйозної, а часто непоправної шкоди репутації будь-якої компанії. Несприятливий збіг обставин — і ось уже втрачено довіру не лише клієнтів, а й партнерів. Відновити його потім дуже важко, довго, дорого та не завжди можливо.

По-третє, ІБ забезпечує захист від загроз, підтримує бізнес-процеси та продуктивність, допомагаючи зберегти в безпеці важливі дані — фінансові відомості, банківську інформацію, дані про постачання, збут продукції або матеріалів. Крім того, вона може бути джерелом бізнес-переваг та економічної ефективності, запобігаючи фінансовим втратам, пов'язаним з атаками та інцидентами.

Основні загрози інформаційної безпеки можуть бути націлені на різні завдання, але важливим є те, що вони постійно еволюціонують і вдосконалюються.

Найбільш відомі та поширені вразливості інформаційної безпеки — кібератаки, у тому числі DDoS-атаки, фішинг та злами, що здійснюються зловмисниками для несанкціонованого доступу до систем та даних компанії [14]. Інші серйозні загрози — віруси, трояни, шпигунське програмне забезпечення, які можуть завдати непоправної шкоди внутрішній IT-структурі. Важливою проблемою залишаються і витоки інформації, отримані внаслідок хакерських атак чи в результаті необережного поводження з конфіденційною інформацією всередині організації.

Недостатньо оновлений софт, прогалини у політиці безпеки, у тому числі відсутність спеціалізованих цифрових рішень, спрямованих на контроль та моніторинг нормального функціонування інформаційної структури компанії, низькі компетенції IT-фахівців також можуть бути причиною кіберризиків, які злочинці завжди раді використовувати для зламу корпоративних інформаційних систем.

Не слід недооцінювати і внутрішні загрози, які можуть бути викликані діями несумлінних співробітників, які мають привілейовані права доступу до внутрішніх систем та підсистем компанії. Така проблема стає зараз дедалі актуальнішою.

Створення системи безпеки інформації вимагає комплексного підходу і має підґрунтя, що спирається на поглиблений аналіз можливих ризиків та їх негативних наслідків. Жодної дрібниці не можна упустити. Кожен суттєвий аспект має прямий вплив на ситуацію. Негативні наслідки піддаються аналізу. Ним передбачено чітку ідентифікацію потенційних джерел небезпек, факторів, які спричиняють їхній прояв, і як наслідок, встановлення можливих загроз для ІБ.

Проводячи таке дослідження варто переконатися, що всі потенційні джерела небезпек ідентифіковані та зіставлені, викриті усі можливі фактори (уразливості), всім ідентифікованим джерелам та факторам зіставлені загрози безпеки інформації.

Виходячи з дослідження О.Бурова, встановлення, створення моделі та поділ джерел ризику та їх виявлення, необхідно проводити на базі вивчення наступної схеми: джерело небезпеки – фактор уразливості – напад – наслідки [32].

Появою небезпеки вважаються можливі техногенні, людські чи стихійні носії загрози. Ризик [Threat] - це можлива загроза, що передбачається або реально існує. До цього пункту відноситься діяння або бездіяльність, направлена на шкоду об'єкту (ресурсів інформації). Це викликає наслідки, які

отримує користувач чи власник. Вони характеризуються спотворенням та втратою інформації [32].

Фактор уразливості [Vulnerability] - причини з-за яких об’єкт втрачає безпеку інформації. Вони виникають за наявності недоліків у системі функціонування об'єкта інформатизації. Страждають протоколи обміну та інтерфейси, що використовуються програмним забезпеченням та апаратною платформою.

Напад - реалізація загрози через вразливі боки джерела інформації. При нападі реалізується взаємодія «джерела та фактору», відбувається завдання шкоди та вибір методів відповіді для відбиття загрози.

Наслідки - потенційне заподіяння шкоди. На цьому етапі настає встановлення жорсткого зв'язку між юридичною категорією "шкода" та технічними проблемами [32].

Отже, з визначеннями О.Бурова можна погодитись і відповідно до цього ми можемо перейти до певних проявів можливої шкоди, які будуть також різними. Наведена класифікація формується з:

– моральних та матеріальних збитків, спричинених діловій репутації компанії;

– фінансових збитків від потреби відновлення зруйнованих інформаційних ресурсів, які знаходяться під захистом;

– моральних та грошових збитків від порушення діяльності компанії;

– майнових збитків від втрати цінної інформації, яка є конфіденційною;

– фізичних, моральних або майнових збитків, які виникли внаслідок витоку персональних даних деяких осіб;

– матеріальних втрати, які утворилися від неможливості виконати зобов'язання перед третьою стороною;

– майнових та моральних збитків, що виникли внаслідок порушення міжнародних відносин [12].

Збитки можуть бути нанесені будь-яким суб'єктом. Тоді буде йти мова про правопорушення. Можливі також прояви, незалежні від суб'єкта (стихійне лихо або інший вплив, спричинений проявом техногенних чинників). Перший випадок характеризується виною суб'єкта, за діями якого школа встановлюється як склад злочину, скоєного навмисне або з необережності. Такі випадки розглядають з точки зору кримінального права.

Другий випадок характеризується імовірнісним характером. Предмет розгляду сумісний з випадками у цивільному, адміністративному або арбітражному праві.

В правових відносинах шкода - невигідні для власника майнові наслідки, утворені внаслідок правопорушення. Збитки рахуються у зменшенні майна, або недоотриманні доходу, який було б отримано за відсутності правопорушення (втрачена вигода).

При розгляді суб'єкту, який завдав шкоди будь-якій особі, категорія "збитки" справедлива лише тоді, коли є можливість довести, що їх заподіяно, тобто поведінку особи треба кваліфікувати визначеннями правових актів, як склад злочину [12].

Згідно з ст. 361 ч.1 КК України під несанкціонованим втручанням в роботу електронних комунікаційних, інформаційних (автоматизованих), електронних комунікаційних мереж, інформаційно-комунікаційних систем вбачається порушення, яке вимагає грошове покарання від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян. Також є ризик обмеження волі строком до трьох років. [2].

При стихійних лихах злого наміру особистості не вбачається. Відомий факт, що стихія не буде використовувати конфіденційну інформацію задля власної вигоди. В обох випадках власник інформації отримує шкоду і втрачає важливі дані.

В залежності від того, чи заподіяло шкоди будь-яке природне чи техногенне явище, збитки можна компенсувати за рахунок страхової компанії або за рахунок особистих коштів особи, яка володіє інформацією[15].

Носіями загроз ІБ є джерела ризиків. В їх ролі можуть бути об'єктивні прояви або суб'єкт (особистість). Ці джерела можуть бути внутрішніми, тобто знаходитись всередині компанії, та зовнішніми. Такий розподіл є виправданим згідно з попередньою думкою щодо вини чи ризику порушення ІБ. Розмежування на внутрішні та зовнішні фактори потрібно для того, аби встановлювати різні джерела ризиків.

Найбільш розповсюджені групи джерел загроз ІБ:

- Викликані антропогенними чинниками.
- Спричинені техногенними факторами.
- Є наслідком стихійного лиха [16].

До антропогенних джерел ризиків для ІБ відносять суб'єкти, що діють навмисно або випадково, створюючи злочин. Ця група є наймасштабнішою і викликає найбільший інтерес по темі створення захисту. Дії суб'єкта можна передбачити, вжити запобіжних заходів.

Антропогенне джерело загрози визначається суб'єктом, маючим доступ (санкціонований або несанкціонований) до таємної інформації. Джерела ризику поділяються на зовнішні і внутрішні.

Зовнішніми прийнято поділяти на випадкові та навмисні. До їх складу входять одиниці:

- кримінальних структур;
- потенційних злочинців та хакерів;
- недобросовісних партнерів;
- технічного персоналу постачальників телематичних послуг;
- представників організацій, які мають завдання ведення нагляду та аварійного реагування;
- представників силових структур [17].

Внутрішніми суб'єктами бувають висококваліфіковані фахівці з доступом до програмного забезпечення та технічних засобів. Вони можуть використати штатне обладнання та технічні засоби мережі.

В даному випадку приходиться рахуватися з:

– основним персоналом (користувачами, програмістами, розробниками);

– представниками служби охорони інформації;

– допоміжним персоналом;

– технічним персоналом [17].

Як правило, враховують фактори особливої групи антропогенних джерел внутрішнього середовища. Шкода може бути завдана особами з порушеннями психіки або навмисно впровадженими агентами, які можуть входити в основний чи технічний персонал.

Іншим джерелом загроз є технократична діяльність людства в його цивілізаційному розвитку. Наслідки такої діяльності непередбачувані і часто виходять з-під контролю. Їх неможливо спрогнозувати. Їм приділяють особливу увагу. Цей клас небезпек заслуговує особливої уваги у наш час, тому що обладнання застаріває і вихід із строю технічного парку може завдати великої шкоди.

Джерела потенційних загроз ІБ, виражені технічними засобами, можуть бути зовнішніми і виявитися у вигляді:

– засобів зв'язку;

– мереж комунікації (інтернет, вода);

– транспорту.

та внутрішніми:

– неякісними технічними засобами опрацювання інформації;

– неякісними програмними шляхами обробки даних;

– допоміжними засобами (охорони, сигналізація, телефонна мережа);

– іншими технічними засобами, які працюють у системі установи [20].

Наступна група джерел ризиків поєднує обставини непереборної сили та ті, які характеризуються об'єктивністю та абсолютністю, що поширюється на всіх. Непереборною силою в юридичній практиці вважаються стихійні лиха та інші фактори, які не піддаються передбаченню чи запобіганню. Ці ризики неможливо прогнозувати і захищатись від них треба стандартними засобами.

Непередбачувані джерела потенційних загроз інформаційної безпеки зазвичай є зовнішніми відносно об'єкта, який знаходиться під захистом і вони керуються насамперед природними катаклізмами:

– пожежами;
– землетрусами;
– повенями;
– ураганами;
– різними непередбачуваними обставинами;
– незрозумілими явищами;
– іншими форс-мажорними обставини [20].

Джерелам ризику притаманні різні міри небезпеки, які можна кількісно оцінити. В першу чергу це визначається ступенем доступності до захисного об'єкта:

1) високий ступінь по доступу має антропогенне джерело загроз, що споряджене повним доступом до технічного та програмного застосування захищених даних;

2) перший середній ступінь доступності притаманний антропогенному джерелу загроз, якому доступні опосередковані функціональні обов'язки, доступ до техніки та ПЗ для роботи з захищеною інформацією;

3) другий середній ступінь включає в себе ризики, породжені антропогенними джерелами загроз в яких обмежений доступ до устаткування, функціональні обов'язки;

4) низький ступінь доступності мають антропогенні джерела ризиків з дуже обмеженою можливістю доступу до технічного та програмного забезпечення.

5) відсутність доступу для антропогенного джерела [23].

Визначивши ступінь доступності до об’єкта, можна перейти до визначення рівня віддаленості від об'єкта, що також є вкрай значущим.

Ступінь віддаленості від об'єкта захисту, описаний наступними факторами:

– види об'єктів збігаються - форми захисту включають в себе джерела техногенних вразливостей і їх розподіл за територією є неможливим;

– об'єкти поблизу - їх встановлено у безпосередній близькості відповідно від джерел техногенних вразливостей і прояв таких загроз може істотно вплинути на об'єкт, що захищається;

– об'єкти на середній відстані розташовуються на віддаленні джерела техногенних вразливостей де прояв таких загроз може подіяти на об'єкт захисту;

– дистанційно розташовані об'єкти виключає можливість прямого впливу на нього.

– найбільш віддалені об'єкти стоять на значній відстані від джерел загрози. Тому, таке положення не передбачає жодних впливів на об'єкт, включаючи вторинні прояви. [20].

Після того, як будуть встановлено параметри ступеню віддаленості від об’єкта, який захищається, можна звернути увагу на особливості розташуванням об'єктів захисту у різних природних, кліматичних, сейсмологічних, гідрологічних та інших умовах та проаналізувати ситуацію.

Обставини можуть відрізнятися:

– вкрай небезпечними умовами – об'єкт перебуває у ділянці дії природних явищ;

– небезпечними умовами - розташування об'єкт, де спостереження показує ризик виникнення природних катаклізмів;

– помірно небезпечними умовами - в районі, де немає небезпеки природних катаклізмів, проте існують умови для виникнення стихійних загроз безпосередньо на об'єкті;

– слабко небезпечними умовами - роль розташована за межами зони впливу природних явищ, але на об'єкті існують умови для виникнення стихійних вразливостей;

– безпечними умови вважаються тоді, коли об'єкт знаходиться поза за межами зони впливу природних явищ і на об'єкті відсутні умови для виникнення стихійних вразливостей [23].

Оскільки характеристика джерел небезпеки будується на різних факторах, буде актуальним перелічити їх максимальну кількість, аби зробити більш точний аналіз. Тому після особливостей розташування об’єкта варто розглянути кваліфікацію антропогенних джерел. Вона відіграє суттєву дію у визначенні можливостей щодо протиправних діянь.

Наведемо таку класифікацію рівня можливості взаємодії з мережею:

– рівень нульової дії – не надає жодної можливості будь-якого використання програм;

– рівень першого лаштунку - дозволяє діяти обмежено при запуску програм фіксованого набору, призначеного для обробки даних (рівень некваліфікованого користувача);

– рівень другого лаштунку - передбачає створення та запуск користувачем власних захисних програм із оновленими функціями з обробки інформації (рівень програміста);

– рівень третього лаштунки - визначає фахове управління функціонування мережі, тобто впливає на базове ПЗ, його склад та конфігурацію (рівень системного адміністратора);

– рівень четвертого лаштунку - володіє повним спектром можливостей для суб'єктів, що розробляють та відновлюють технічні засоби, включаючи інтеграцію в мережу власних технічних засобів з оновленими функціями обробки інформації (рівень розробника і адміністратора) [20].

На нульовому рівні мінімум можливостей для встановлення контакту джерела ризику з захищеною мережею.

Після встановлення рівня мережі доцільним буде оцінити привабливість діяння із боку джерел загроз. Вона встановлюється за наступною градацією рівнів:

– дуже привабливим рівнем є захищені інформаційні ресурси, в них, міститься інформація, здатна знищити організацію, яка захищає;

– привабливим рівнем є ресурс інформації, який містить секретну інформацію, якою можна скористатися заради вигоди;

– з помірною привабливістю є рівень інформаційних ресурсів, розголошення яких може принести великі збитки;

– зі слабким рівнем привабливості вважаються ресурси з інформацією, накопиченою протягом певного періоду;

– не привабливим рівнем є інформація, яка не викликає інтересу для джерела ризику [23].

Після того як буде дана оцінка привабливості впливу на об’єкт, треба визначити готовність джерела. Вона виникає в умовах можливості здійснення тієї чи іншої загрози у певних умовах місцезнаходження об'єкта. За готовністю джерела визначають:

– з реалізованою загрозою за сприятливих умов;

– ризик за поміркованих умов, коли вони сприятливі, але спостереження не вказують на можливість здійснення;

– слабко реалізованою загрозою, коли причини не дають втілити план в життя;

– не реалізована загроза без передумов для її реалізації [33].

Коли буде визначена готовність реалізації загрози постає питання аналізу ступеня невідкладності наслідків (фатальності). Вони можуть відрізнятися за характером:

– непереборність як результат впливу небезпеки, призводить до знищення та руйнування об'єкту захисту;

– відносна непереборність, коли є можливість відновити втрачені ресурси;

– часткове усунення наслідків та обмеження часу доступу до інформації;

– усунення наслідків, коли об’єкт частково зазнав руйнації і не треба багато витрачати на відновлення;

– відсутні наслідки без впливу загроз [35].

Визначення актуальних (найнебезпечніших) загроз дозволяє проаналізувати розміщення об'єктів захисту та схеми інформаційної системи, і навіть інформаційних ресурсів, підлягають захисту.

Загрози встановлюються через вразливості на конкретному об'єкті інформатизації. Вона відомі об'єкту охорони, утворюють з ним одне ціле та характеризуються вадами процесу роботи, характеристиками створення автоматизованих систем, протоколами обміну та інтерфейсами, які відносять до програмного забезпечення та апаратної платформи, диктують умови використання та знаходження.

Джерела ризиків можуть скористуватися вразливостями задля втрати безпеки інформації, незаконної вигоди (навмисної шкоди).

До вразливостей ІБ слід прирахувати об'єктивні, суб'єктивні, випадкові [20].

Слабкими місцями об'єктивних вразливостей є побудова та технічна характеристика устаткування, що використовується на захищеному об'єкті. Повністю усунути їх неможливо, але доступно суттєво послабити методами технічного та інженерно-технічного впливу на відбиття ризиків. Їх список можна доповнити:

– супутніми технічними засобами впливу;

– електромагнітними підсилювачами;

– електричними ланцюгами живлення та нерівномірним споживанням струму в мережі;

– акустичними;

– апаратними;

– програмними перешкодами, нелегальним ПЗ;

– елементами з можливістю електроакустичного перетворення;

– елементами з впливом на електромагнітне поле;

– в залежності від місцезнаходження об’єкту;

– в залежності від наявних методів передачі інформації через канали обміну [20].

За об’єктивними вразливостями переходять до розгляду суб'єктивних. На них впливають дії співробітників та, в основному, усуваються організаційними та програмно-апаратними методами. Такими чинниками можуть бути:

1) похибки:

– провокує неправильна підготовка та використання ПЗ (невірна розробка алгоритмів, встановлення програм, використання додатків, невірно введені дані);

– складність в управління системою (універсальні налаштування сервісів, організовані потоки обміном інформації);

– помилки при використанні техніки (експлуатація технічних засобів, можливості обміну інформацією);

2) навмисна шкода:

– порушення правил доступу до об'єкта та технічного оснащення;

– перешкоджання використання енергозабезпечення;

– спотворення використання режиму інформації;

– порушення конфіденційності звільненими працівниками [30].

За помилками та вмисними порушеннями слід розглянути випадкові вразливості. Вплив здійснюють особливості оточуючого середовища навколо об'єкта і невідкладні обставини. Передбачити такі фактори майже нереально, ефективність виникає після комплексної організації, технічних інженерних заходів процедур з протидії ризикам:

1) операційні збої:

– неможливість роботи по причині несправності техніки;

– старіння носіїв інформації;

– неадекватність роботи ПЗ;

– відсутність електропостачання.

2) пошкодження:

– - життєво важливі комунікацій (комунальні та кондиціонування повітря);

– - огорожі (паркани, стіни, перекриття) [35].

Кожна з вразливостей володіє мірою небезпеки, яка піддається кількісній оцінці. При цьому, за критерії порівняння (показників) можна вибрати розмір дії ризику на непереборність наслідків. Інформативність - одна з головних задатностей прибирати вразливості без спотворень, є засобом передавання корисного інформаційного сигналу.

Що одним з критеріїв може бути доступність, яка визначає здатність ризику використовувати різні фактори (великі розміри, спеціалізована апаратура).

Одним з найбільш вживаних критеріїв є визначення кількості складових об'єкта, які володіють деякою вразливістю. Окрім вищезгаданих, важливе

місце займає фатальність. Вона визначається, як відношення добутку вказаних показників до їх максимального значення.

Кожному показнику надається оцінка експертним методом у розмірі п’яти балів. Один бал означає мінімальну міру впливу окремо взятого показника на розрахунок вразливості, а п’ять - максимальну [19].

Розрахунок актуальних ризиків дає зрозуміти, як піддається впливу загроз, як приймаються вразливості, що допомагають реалізації загроз.

Виходячи з результатів спостереження утворюють матрицю взаємовпливу ризиків та вразливостей, де обчислюються наслідки реалізації атак та коефіцієнт небезпеки цих атак. При цьому враховується, що атаки з коефіцієнтом менше 0,1 (припущення експертів), надалі можуть не розглядатися через малу ймовірність їх вчинення на об'єкті. Така матриця складається окремо кожної загрози.

1.2 Наслідки кібератак

На сьогоднішній день проблема кібербезпеки є однією з найбільш пріоритетних у світі. Існують відмінності в поняттях інформаційного захисту та кібербезпеки. Передусім варто відзначити, що кібербезпека є підмножиною інформаційної безпеки.

Сьогодні безліч величезних корпорацій та дрібних компаній забезпечує зберігання даних саме на десктопах, серверах ноутбуках або у хмарних сховищах інтернету. Але буквально років десять тому перед тим, як вся важлива інформація перейшла в онлайн, вона займала простір кількох кабінетів. Щодо завдання інформаційної безпеки, то вона полягає в тому, щоб захищати і зберігати дані будь-якої форми, цим і проявляється масштабність визначення інформаційної безпеки у порівнянні з кібербезпекою.

Атаки проводяться з різних напрямків: SMTP, DNS, HTTP, SSL. Щоб захиститися від них, потрібні спеціальні рішення. Щоб розпочати кібератаку, необхідно створити комп'ютерну мережу. Вона може містити кілька сотень

тисяч комп'ютерів. Ці комп'ютери направляють у ціль дуже багато запитів. Сервери не витримують навантаження та відмовляють [33].

Кібербезпека ж полягає у захисті даних, які розміщуються в електронній формі. А також у визначенні найбільш важливих даних, де вони розміщуються, та які технології необхідно застосовувати для захисту.

Ми живемо у світі, який сьогодні пов'язаний з мережею та інформаційними технологіями, від інтернету банкінгу до державної інфраструктури і саме тому кібербезпека є важливою необхідністю. Таке явище як кібератаки увійшло в буденність і набуває ще більш масштабного характеру в наші дні, тому що основні хакерські атаки здатні наприклад: наносити непоправна шкода іміджу будь-якої країни або, що ще гірше, підірвати всю її економіку.

Згідно з дослідженням Juniper Research загальносвітові збитки від кібератак виросли у чотири рази. Якщо цей рівень кібератак не зміниться, то цілком можливо, що до 2029 року загальні збитки світової економіки становитимуть $2,1 трильйона. В якості прикладу можна навести дані про останні кібератаки. Збитки на суму 81 мільйона доларів були завдані центральному банку міста Бангладеш у лютому 2016 року. Також у результаті даної кібератаки була зроблена спроба крадіжки ще 850 мільйонів доларів, але вона була відбита [28].

Сьогодні ці проблеми поширені і на менш глобальному рівні, і їх не можна оминати стороною. Вони включають розуміння та усвідомлення використання кожною людиною своїх особистих даних у мережі інтернет та на різних переносних носіях. Через нехтування елементарними заходами безпеки, щодня відбувається крадіжка та злом персональної інформації та банківських даних користувачів по всьому світу.

Найбільш популярними видами атак є:

1. Атаки WEB додатків: на їхню частку припадає 24% від усіх атак. Даний вид несанкціонованого злому включає SQL ін'єкції, він же SQLI (45% від усіх атак WEB додатків) та міжсайтовий скриптинг (XSS).

2. Шкідливий код займає 19%. Такий вид кібератак буває різноманітних видів та розмірів, від банальних вірусів та черв'яків до високотехнологічного шпигунського програмного забезпечення. Сьогодні, від цього виду атак немає захисту в жодного користувача чи компанії.

3. Атаки спрямовані на певні програми: їх частка займає 19%. Їхня назва говорить сама за себе. Ці атаки спрямовані на певний тип додатків та їх головною метою є перехоплення найважливіших пакетів даних, які проходять через ці додатки. За допомогою аналізу вхідних пакетів через програму можна отримати інформацію про потенційну жертву, наприклад, якою ОС користується, її мережевий трафік, а також отримати достовірну інформацію про додатки, які запускає користувач.

4. Dos/DDoS Attacks займають 9%. DoS (Denial of Service) означає "відмова в обслуговуванні". Такий тип кібератак полягає в тому, що хакер починає перевантажувати сервер за допомогою великої кількості запитів, внаслідок чого сервер перестає функціонувати. Існує ще один вид кібератак, які мають назву DDoS (Distributed Denial of Service) "розподілена відмова в обслуговуванні". Він схожий на попередній вигляд атак, але проводиться за допомогою набагато більшої мережі відомої як ботнет.

5. Розвідувальний вид атаки займає 9%. Існує 2 типи розвідувальної атаки: пасивна та активна. Пасивна розвідувальна атака - це така атака, при якій хакер шукає важливу інформацію, при цьому не втручається в свою систему жертви. Активна ж коли хакер втручається у систему жертви. Варто зазначити, що в різних випадках пасивний та активний вид розвідувальної атаки називають пасивним, тому що замість того щоб використовувати знайдену вразливість, зловмисник займається виключно збиранням різних даних для того, щоб підготуватися до ще більшої кібератаки [29].

Інші форми атак займають решту 20% від інших кібератак. У результаті при дії даних атак об'єкт зазнає серйозних збитків і проблеми із громадськістю. На превеликий жаль, на сьогоднішній день немає єдиного плану дій щодо

запобігання кібератакам. Держави всього світу розробляють стандарти кібербезпеки [29].

Першими кроками на шляху до скорочення кібератак є створення різноманітних відділів з управління всілякими інформаційними ризиками, які б у свою чергу визначали рівень захисту вже в галузі кібербезпеки, з якими може зіткнутися об'єкт і розробляли політику боротьби з ними. Об'єкт повинен застосовувати заходи щодо захисту інформації та використовувати нові технології в сфері кібербезпеки, а також він повинен керуватися тим як сама система налаштована і використовується. Також необхідно виключати непотрібні функції та підтримувати свіжі версії використовуваного софту, в якому підвищена стабільність та виправлені критичні помилки.

Також слабкою точкою захисту будь-якої організації є мережева складова, так що дуже важливо правильне проектування самої мережі та правильне налаштування пристроїв за вже прийнятим стандартом безпеки.

Що стосується переносних пристроїв, які схильні до великої вразливості з боку кіберзлочинців, то вони повинні в першу чергу сканувати на наявність шкідливого коду. Також необхідний ліміт на передачу інформації між носієм та ПК.

Самому ж користувачу необхідно надавати лише ті привілеї, які необхідні у його роботі. Це стосується доступності до акаунту системного адміністратора, він не повинен бути доступний звичайному користувачеві. А активність користувача має перевірятися.

У міру того як інформаційні технології все глибше проникають в усі сфери сучасного суспільства, а повсякденне життя людей інтегрується з високими технологіями, все частіше у кібернетичному просторі проявляються терористичні атаки нового типу. Подібні проблеми та загрози виникли у зв'язку з широким розповсюдженням інформаційних технологій. Сучасний кібертероризм із повною впевненістю можна поставити в один ряд з тероризмом і організованою злочинністю, що вважаються традиційними

видами злочинності, - такі великі масштаби, технічні можливості та наслідки цього сучасного протиправного явища [35].

В даний час істотні зміни в політичній, соціальній та економічній сферах життя суспільства спричиняють зростання злочинів терористичного характеру у всьому світі. Метою терористичної пропаганди може бути визначено маніпулювання окремими людьми чи групами людей для підриву у них віри у традиційні цінності, підміни або трансформації цінностей, поширення серед населення почуття підвищеної тривоги, страху та паніки, розпалювання радикальних настроїв. Зрештою подібні маніпуляції створюють умови для впливу на різні соціальні групи. Аналіз причин зростання злочинів терористичної спрямованості дозволяє сучасному суспільству розуміти ступінь загрози громадянам та державі загалом, визначати напрямки здійснення протидії кібертероризму.

До причин зростання терористичних актів найчастіше відносять боротьбу за політичну владу, міжетнічні конфлікти, фінансову підтримку терористичних організацій, зростання організованої злочинності, поширення ідей тероризму через інформаційно-телекомунікаційну мережу Інтернет, історичні події глобального масштабу (пандемії, війни, фінансові кризи). Так період пандемії Covid-19 ознаменувався сплеском кібератак. Причому кіберзлочинці намагалися атакувати насамперед профільні міністерства, а також окремі лікарні та навіть безпосередньо деяких лікарів. І це у ситуації, коли на медичну сферу у період лягло найбільше навантаження. Масованій DDoS-атаці навесні 2020 р. зазнали всіх серверів Міністерства охорони здоров'я та соціальних служб США (HHS). Тоді ж постраждали бази даних Університетської клініки у Брно – одного з найбільших центрів аналізу крові на COVID-19 у Чехії. В результаті лікарі були змушені скасувати кілька хірургічних операцій, оскільки не могли працювати із тестами на коронавірус. Організації, що проводили боротьбу з COVID-19, ставали жертвами цільових атак просунутих кіберзлочинців. [26]

У звіті про кіберзлочинність у період пандемії, який опублікував Інтерпол, йдеться, що для максимального збільшення фінансової вигоди шахраї почали переносити свої основні цілі з малого бізнесу та приватних осіб на великі корпорації, держкомпанії, критично важливі інфраструктури, включаючи медичні установи. Інтерпол підкреслює, що у боротьбі з кібертероризмом потрібна більш тісна співпраця між державним та приватним секторами. Крім того, дуже важливо приділяти більше уваги підвищенню рівня технічної та інформаційної безпеки різних життєво важливих установ, оскільки це пов'язано з інтересами держави та збереженням її стабільності. [26]

Результати кіберзагроз різноманітні: вони можуть деструктивно впливати і на окремо взяту особу, і на працю державного апарату чи галузі економіки. Наприклад, у ЗМІ висвітлювалася ситуація, коли хакери високого рівня угруповання DarkSide 7 травня 2022 р. порушили шифрування енергетичної системи Colonial Pipeline (США), тим самим викликавши кризу. Як наслідок, у 17 федеральних штатах було введено режим надзвичайної ситуації.

Проведений аналіз звітів Cybersecurity threatscape та Інтерполу 2020–2022 років дозволив виявити тенденції у застосуванні у зазначений період кіберзагроз та їх основну спрямованість, а також різновиди завданих збитків. На наш погляд, доцільно зробити класифікацію кіберзагроз за низкою ознак (таблиця 1.1), де максимальний рівень загрози/частота використання – +++, середній рівень – ++, слабкий – +. Зазначимо, що ранжування усереднене, оскільки навіть окремий хакер може завдати дуже значний збиток. [27]

Таблиця 1.1 – Види кіберзагроз (2019–2022 рр.), частота застосування та ступінь їх небезпеки для суспільства

Частота застосування	Середній рівень небезпеки	Спрямованість впливу	Об'єкт впливу	Мета/ наслідки	Збитки
Інтернет-бот					
+++	+	Слабозахищені пристрої або DDoS-атаки	Фізособи, держустанови	Зупинити роботу онлайн-сервісу	Втрата прибутку; репутаційні витрати
Кіберсталкінг					
++	++	Індивідуальні кібепристрої	Фізичні особи (часто діти та підлітки)	Залякування, крадіжка онлайн-особи, шантаж, шпигунство	Моральний збиток (страх чи занепокоєння за свою безпеку), репутаційні втрати
Хакінг					
+++	+++	Вразливість мережі або пристроїв	Фізичні особи, організації, держустанови, банки	Отримання інформації; псування кредитної історії; крадіжка фінансів, шантаж за допомогою блокування кіберінфраструктури, банківських рахунків	Репутаційні та фінансові втрати

Продовження таблиці:

Підбір облікових даних (brute-force)					
+++	++	Корпоративні та глобальні мережі; використання пристроїв для здійснення злочинної діяльності	Фізособи, організації, держустанови, банки, великі компанії, банки, системоутворюючі компанії	Контроль над сервером, збір персональних даних, крадіжка грошей, у тому числі цифрових, або облікового запису в соцмережі; виведення з ладу особливо захищених пристроїв, шпигунство, руйнування критичної інфраструктури	Фінансові та репутаційні витрати
Сканування мережі					
++	+++	Корпоративна мережа, в якій використовуються пристрої для здійснення злочинної діяльності	Юрособи, організації, держустанови, банки	Отримання великої кількості службової закритої інформації	Репутаційні витрати, витік важливої інформації
Соціальна інженерія					
++	+++	Електронна пошта, соцмережі використовують пристрої для здійснення злочинної діяльності	Фізособи, організації	Залякування, крадіжка онлайн-особи, крадіжка грошей, у тому числі цифрових	Фінансові та репутаційні витрати
Фішинг					
+	+	Електронна пошта (використовують пристрої для здійснення злочинний діяльності)	Фізособи, організації, держустанови, банки	Крадіжка онлайн-особи, крадіжка грошей, у тому числі цифрових, вимагання	Фінансові та репутаційні витрати

Продовження таблиці:

Шкідливе ПЗ					
+++	+++	Мережі або пристрої	Фізособи, організації, держустанови, банки	Порушення роботи ПЗ та пристрої IoT; контроль над сервером; збір персональних даних, крадіжка грошей, у тому числі цифрових	Втрата прибутку; репутаційні витрати, блокування роботи складних пристроїв

Таким чином, найбільш поширеними є інтернет-боти, хакінг, шкідливе програмне забезпечення, підбір облікових даних. Інтернет-боти займаються зупинкою онлайн-сервісів. Хакінг вражає мережу або пристрої. Шкідливе ПЗ порушує роботу пристроїв, викрадає персональні дані. При підборі облікових даних здійснюється викрадання даних, шпигунство, руйнування критичної інфраструктури.

У період пандемії злочинці часто застосовували інформаційний тероризм задля дестабілізації суспільства та досягнення незаконних цілей. Одним із проявів кібертероризму можна вважати фейк. Небезпека недостовірної інформації у тому, що вона не тільки підриває довіру аудиторії до мас-медіа, а й сприяє економічній та політичній дестабілізації в країні. У міру збільшення в інформаційному просторі частки фейкових новин, пов'язаних із COVID-19, кібертерористи активізували атаки на громадян та організації. Фейкові новини про вірус та про вакцини поширювалися у всіх країнах. Західні держави лобіювали свої інтереси, просуваючи у тому числі розробки вчених. Недостовірна інформація поширювалася блискавично, що сприяло глобальній політичній та економічній дестабілізації. Довіра до офіційних ЗМІ була підірвана, населення відмовлялося від вакцинації; поширювалися панічні настрої. Таким чином, статистичні дані підтверджують, що своїми діями екстремісти знизили рівень безпеки у багатьох країнах [26].

Спроби виключити або хоча б мінімізувати наслідки поширення дезінформації з використанням Всесвітньої павутини роблять уряди багатьох

країн: розробляють правові норми та приймають нові закони, укладають угоди тощо запобігання поширенню фейкової інформації та на підвищення відповідальності операторів зв'язку спрямоване уточнення існуючих забезпечувальних заходів у сфері інформаційно-цифрового простору низки держав.

У західних країнах зроблено зусилля щодо запобігання поширенню рейкових новин: пошукова система Google блокувла мільйони повідомлень; припинялася робота сайтів, публікували недостовірну інформацію; адміністрація месенджера WhatsApp також провела заходи, завдяки яким вдалося на 25% уповільнити поширення шкідливої інформації [29]

Методи боротьби із кібертероризмом. Законодавче регулювання діяльності у віртуальному просторі стало важливим завданням у світовому масштабі. В другій половині 2010-х рр. у різних державах було прийнято закони, що обмежують поширення небезпечного контенту та фейків. 15 травня 2019 р. у Парижі з ініціативи новозеландської та французької сторін проведено саміт за участю урядових лідерів 17 держав, Єврокомісії та представників восьми технологічних компаній, в результаті якого було підписано Крайстчерцький заклик – план дій, що регламентує низку заходів, які слід вжити авторам документа. Ці заходи обмежують можливості терористів використовувати Мережу як інструмент для протиправних дій.

Крайстчерцький заклик – це своєрідне державно-приватне партнерство, яке об'єднує 48 країн, ЮНЕСКО, Раду Європи, Європейську комісію та вісім технологічних компаній. Урядові органи зобов'язуються коригувати законодавство та контролювати соціальну сферу; технологічні компанії, у свою чергу, повинні встановити контроль за контентом та розробити заходи щодо вилучення та блокування недостовірної та небезпечної інформації [32].

У 2019 р. британська влада класифікувала погрози в Мережі та системно описала їх у документі Online Harms White Paper. У ньому представлений огляд усіх небезпек, з якими може зіткнутися користувач, працюючи в

Інтернеті. У документі приділено особливу увагу легальному контенту, який потенційно може становити небезпеку для дітей.

Рамки протиправної діяльності інтернет-платформ у Німеччині визначаються Законом про соціальні мережі (The Network Enforcement Act, NetzDG) (набув чинності 2017 р.).

У 2018 р. у Франції ухвалили закон про боротьбу з хибними новинами та деструктивним контентом. У Туреччині, згідно із законом, деструктивний контент повинен бути видалений на першу вимогу місцевого управління телекомунікацій та зв'язку. У 2020 році Єврокомісія запропонувала масштабний проект цифрового регулювання – законопроект «Про цифрові послуги» (Digital Services Act, DSA). Його мета – боротьба з порушенням прав людини та протидія розпалюванню ненависті у мережі Інтернет. Особливу увагу приділено інтернет-платформам, якими користується більше 10 % населення Євросоюзу: Google і YouTube, а також Twitter і Facebook. «Закон зобов'яже ці послуги забезпечити прозорість роботи та прояснити власні алгоритми рекомендацій. Велика увага в DSA приділяється боротьбі з нелегальним контентом, послугами та товарами [33].

Нові історичні виклики та розвиток цифрових технологій створюватимуть плідний ґрунт для діяльності кібертерористів. При цьому їх атаки стають більш цинічними, вони здатні впливати на великі соціальні групи та у глобальних масштабах. Мета таких нападів не лише заволодіння матеріальними цінностями чи владою, а й психоемоційний та фізичний вплив на суспільство.

В результаті ламаються стереотипи поведінки та катастрофічно знижується рівень довіри до державі та офіційним ЗМІ. У результаті люди навіть під загрозою смерті не схильні вчиняти розумні дії. Неможливо переоцінити важливість конструктивного обговорення цифрових загроз. Масштаб проблеми великий, а супротивник надзвичайно небезпечний, оскільки витончено прагне обійти нові правила та заходи із забезпечення цифрової гігієни.

У ряді європейських держав та на американському континенті накопичено позитивний досвід протидії терористичним правопорушенням у Мережі. Через різноманітні портали та сайти інтернет-користувачі знайомляться з превентивною державною діяльністю щодо терористичних організацій та їхньої ідеології. Багато держав скоригували законодавство, яке регулює інтернет-комунікацію. Розроблено комплекс заходів щодо протидії кібер- та інформаційному тероризму [34].

Однак далеко не всі і не завжди адекватно оцінюють рівень небезпеки кібератак і, відповідно, не реагують на те, що відбувається належним чином. Наприклад, технологічні компанії не надто серйозно сприймають сенс боротьби з тероризмом. Хоча найбільші технологічні платформи досягли великих успіхів у протистоянні терористичному контенту, вони все ще можуть працювати краще і потребують конкретних рекомендацій співтовариства фахівців боротьби з тероризмом.

Рада Безпеки ООН наголошує на важливості цифрових технологій у боротьбі з глобальною загрозою тероризму та закликає держави – члени організації розвивати спільну діяльність у цій галузі: знайти способи активізувати та прискорити обмін оперативною інформацією про використання інформаційних технологій терористичними групами та припиняти вербування терористів [35].

27 червня 2017 року відбувся напад комп'ютерного вірусу "Ransom:Win32/Petya" на підприємства приватного та державного сектору економіки України. Відбулися порушення в роботі банків, аеропортів, державної залізничної компанії, телекомпаній, телекомунікаційних компаній, великих мережевих супермаркетів, енергетичних компаній, державної фіскальної служби, структур державної управління та органів місцевого самоврядування і так далі.. Вірус вразив суб'єкти інших держав, але найбільших збитків зазнала Україна [36].

Країна не витримала атаку, яка викрила незахищеність життєво важливих інтересів суспільства та держави у сфері кіберпростору.

Впровадження законодавчого регулювання питання кібербезпеки, зможе захистити кіберпростір і запобігти масовим кібератакам. Законодавство вводить важливі базові поняття в галузі інформаційного захисту та окреслює права та обов'язки державних органів щодо ІБ [9]. До обов’язків державної служби захисту інформації входить обслуговування та координування діяльності суб'єктів галузі. Служба контролює виконання вимог законодавчих та нормативних актів, що регулюють сферу захисту інформації, інспектує виконання Закону про захист інформації в інформаційно-телекомунікаційних системах, що діє на сьогодні. Таким чином, в Україні проводиться системна робота з питань національної кібербезпеки [1].

Аналізуючи питання інформаційної безпеки, можна сказати, що вона є дуже актуальна в нинішній час. Малі та середні компанії найбільше страждають від кібератак. Через це такі компанії можуть втратити конфіденційну інформацію, гроші чи цінну частку ринку. Існує безліч способів, якими зловмисники намагаються досягти своїх цілей.

Областю інформаційної безпеки є управління ризиками та захисту інформації від загроз та небажаного доступу. Вона включає різні заходи і практики, спрямовані на дотримання конфіденційності, цілісності та доступності інформації.

Інформаційний захист підтримує репутацію організації. Витік даних та порушення, пов'язані з інформаційною безпекою, можуть завдати серйозної, а часто непоправної шкоди репутації будь-якої компанії. Виконується захист від загроз, підтримка бізнес-процесів та продуктивності.

Злочинці часто застосовують інформаційний тероризм задля дестабілізації суспільства та досягнення незаконних цілей. Одним із проявів кібертероризму можна вважати фейк. Небезпека недостовірної інформації у тому, що вона не тільки підриває довіру аудиторії до мас-медіа, а й сприяє економічній та політичній дестабілізації в країні. Найбільш поширеними є інтернет-боти, хакінг, шкідливе програмне забезпечення, підбір облікових даних. Інтернет-боти займаються зупинкою онлайн-сервісів. Хакінг вражає

мережу або пристрої. Шкідливе ПЗ порушує роботу пристроїв, викрадає персональні дані. При підборі облікових даних здійснюється викрадання даних, шпигунство, руйнування критичної інфраструктури.

У ряді європейських держав та на американському континенті накопичено позитивний досвід протидії терористичним правопорушенням у Мережі. Через різноманітні портали та сайти інтернет-користувачі знайомляться з превентивною державною діяльністю щодо терористичних організацій та їхньої ідеології. Багато держав скоригували законодавство, яке регулює інтернет-комунікацію. Розроблено комплекс заходів щодо протидії кібер- та інформаційному тероризму

Питання забезпечення кібербезпеки надзвичайно актуальні і для України. Впровадження законодавчого регулювання питання кібербезпеки, зможе захистити кіберпростір і запобігти масовим кібератаким.

Впровадження законодавчого регулювання питання кібербезпеки, зможе захистити кіберпростір і запобігти масовим кібератаким. Законодавство вводить важливі базові поняття в галузі інформаційного захисту та окреслює права та обов'язки державних органів щодо ІБ [9]. До обов’язків державної служби захисту інформації входить обслуговування та координування діяльності суб'єктів галузі. Служба контролює виконання вимог законодавчих та нормативних актів, що регулюють сферу захисту інформації, інспектує виконання Закону про захист інформації в інформаційно-телекомунікаційних системах, що діє на сьогодні.

Отже, кібербезпека відіграє критичну роль у захисті активів, клієнтів, підрядників та репутації бізнесу, а також забезпечує дотримання законодавчих вимог та норм. Можна сказати про те, в сучасному світі безпека в інтернеті є надзвичайно важливою. Комп'ютерна мережа від дня її створення була і буде піддаватися атакам зловмисників та ймовірно кількість загроз кібератак тільки зростатиме. З належним рівнем кваліфікації та підготовкою обладнання і фахівців можна ефективно керувати збитками, відновлювати втрати від кібератак та ефективно протистояти їм..

РОЗДІЛ 2 КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ, ЩО ПІДЛЯГАЄ ЗАХИСТУ ВІДПОВІДНО ДО ЗАКОНОДАВСТВА УКРАЇНИ

2.1 Персональні дані

Інформація в залежності від доступності буває загальнодоступною та з обмеженим доступом. Закон України «Про захист персональних даних» регулює відносини, пов'язані з обробкою персональних даних, що здійснюється органами державної влади, органами місцевого самоврядування, іншими муніципальними органами, юридичними особами та фізичними особами з використанням автоматизованих засобів обробки, включаючи інформаційні та телекомунікаційні мережі, або не збираючи дані з цих засобів. Коли обробляються персональні дані без спеціальних засобів характер дій відповідає засобам автоматизації, виконується дозвіл на проведення пошуку персональних даних, що зберігаються на матеріальному носії та внесені в картотеки або інші систематизованих бази збору персональних даних. [4]

Метою вказаного закону є гарантування захисту прав і свобод людини і громадянина під час обробки його особистих даних, включаючи захист прав на недоторканність приватного життя, особистих інтересів та сімейної таємниці. Для кращого розуміння термінології слід розглянути статтю 2 Закону України «Про захист персональних даних» у якій висвітлено основні поняття що стосуються персональних даних які зображені на рисунку 2.1.

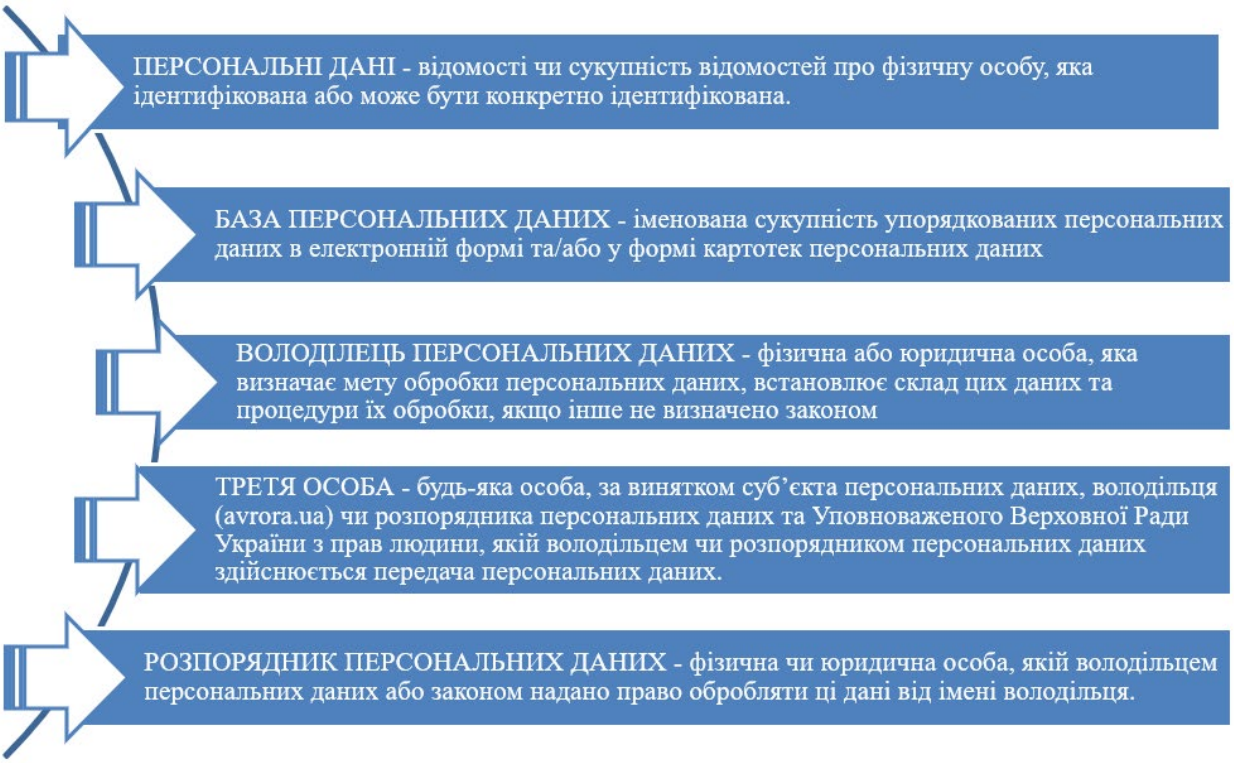


Рисунок 2.1 – Основні терміни згідно ЗУ «Про захист персональних даних» [4]

У статті 6 ЗУ «Про захист персональних даних» встановлено правила обробки персональних даних у загальнодоступних джерелах персональних даних.

1. Джерела зі зберігання персональних даних можуть бути загальнодоступними. В такі примірники додають ПІБ рік, місто місця народження, домашню адресу, абонентський номер, професійні відомості та інше.

2. На вимогу суб'єкта або за рішенням суду персональні дані повинні негайно видалятися.

Закон «Про захист персональних даних» обумовлює його використання в різних сферах суспільного життя. Даним Законом не передбачене створення персональних баз даних з фізичними особами, журналістами, професійним творчим працівником [4].

Як вказує зарубіжний досвід, Закон України «Про захист персональних даних» варто доповнити списком принципів обробки персональних даних. В

основу можна покласти перелік принципів, будь то: принцип законного підгрунтя – персональні дані збираються виключно чесно без омани; принцип вузького використання – вони використовуються для визначених цілей; принципу персональної участі – особа відокремлена від даних, які про неї зібрані, повинен бути доступ до даних, що стосуються його або її, і суб'єкт даних має право вимагати виправлення неточної або оманливої інформації.

2.2 Комерційна таємниця

Поняття комерційної таємниці згідно з ст. 505 ЦКУ трактується як «інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію» [5].

Статтею 420 ЦКУ визначено, що «комерційна таємниця є об'єктом інтелектуальної власності. Відповідно майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором» [5].

Зокрема, ст. 506 ЦКУ відносить до майнових прав інтелектуальної власності на комерційну таємницю:

- можливість користуватися комерційною таємницею;
- безперешкодне право дозволу викриття комерційної таємниці;
- пряме право відміняти неправомірне розголошення, або обробку інформації щодо комерційної таємниці;
- інші права за законом [5].

Отже, інформація, яка є секретною, не повинна бути легко доступною для різних осіб, не пов’язаних з її зберіганням та обробкою. Комерційну таємницю відносять до майнових прав інтелектуальної власності.

2.3 Службова таємниця

Службова таємниця є видом конфіденційної інформації, та декларація про службову таємницю виступає самостійним об'єктом права [29].

Інформація представляє собою основні види службової таємниці:

1) інформація службового характеру:

- військових;
- слідства;
- судочинства;

2) охороноздатна конфіденційна інформація, що стала відомою в силу виконання службових обов'язків посадовим особам державних органів місцевого самоврядування: комерційна таємниця, банківська таємниця, професійна таємниця, а також конфіденційна інформація про приватне життя особи.

На документах (у необхідних випадках та на їх проектах), що містять службову інформацію обмеженого розповсюдження, проставляється позначка «Для службового користування».

Таким чином, за розголошення службової інформації обмеженого поширення, а також порушення порядку поводження з документами, що містять таку інформацію, державний службовець (працівник організації) може бути притягнений до дисциплінарної чи іншої передбаченої законодавством відповідальності [29].

2.4 Професійна таємниця

Професійна таємниця — інформація, що захищається за законом, довірена або яка стала відомою особі виключно з чинності виконання ним своїх професійних обов'язків, не пов'язаних з державною або муніципальною службою, поширення якої може завдати шкоди правам і законним інтересам іншої особи, до що вірив ці відомості, і яка не є державною або комерційною таємницею [13].

Інформація може вважатися професійною таємницею, якщо вона відповідає наступним вимогам:

– довірена чи стала відома особі лише через виконання ним своїх професійних обов'язків;

– особа, якій довірена інформація, не перебуває на державній або муніципальній службі (інакше інформація вважається службовою таємницею) (наприклад, виклик ветеринара додому відноситься до службової таємниці);

– заборона на поширення довіреної або відомої інформації, яке може завдати шкоди правам та законним інтересам довірителя;

– інформація не відноситься до відомостей, складаючи державну та комерційну таємницю [7].

Відповідно до цих критеріїв можна виділити наступні об'єкти професійної таємниці:

Лікарська таємниця - відомості про факт звернення громадянина за наданням медичної допомоги, стан його здоров'я та діагноз, інші відомості, отримані ним при медичному обстеженні та лікуванні. Основні принципи охорони здоров’я зображені на рисунку 2.2. :

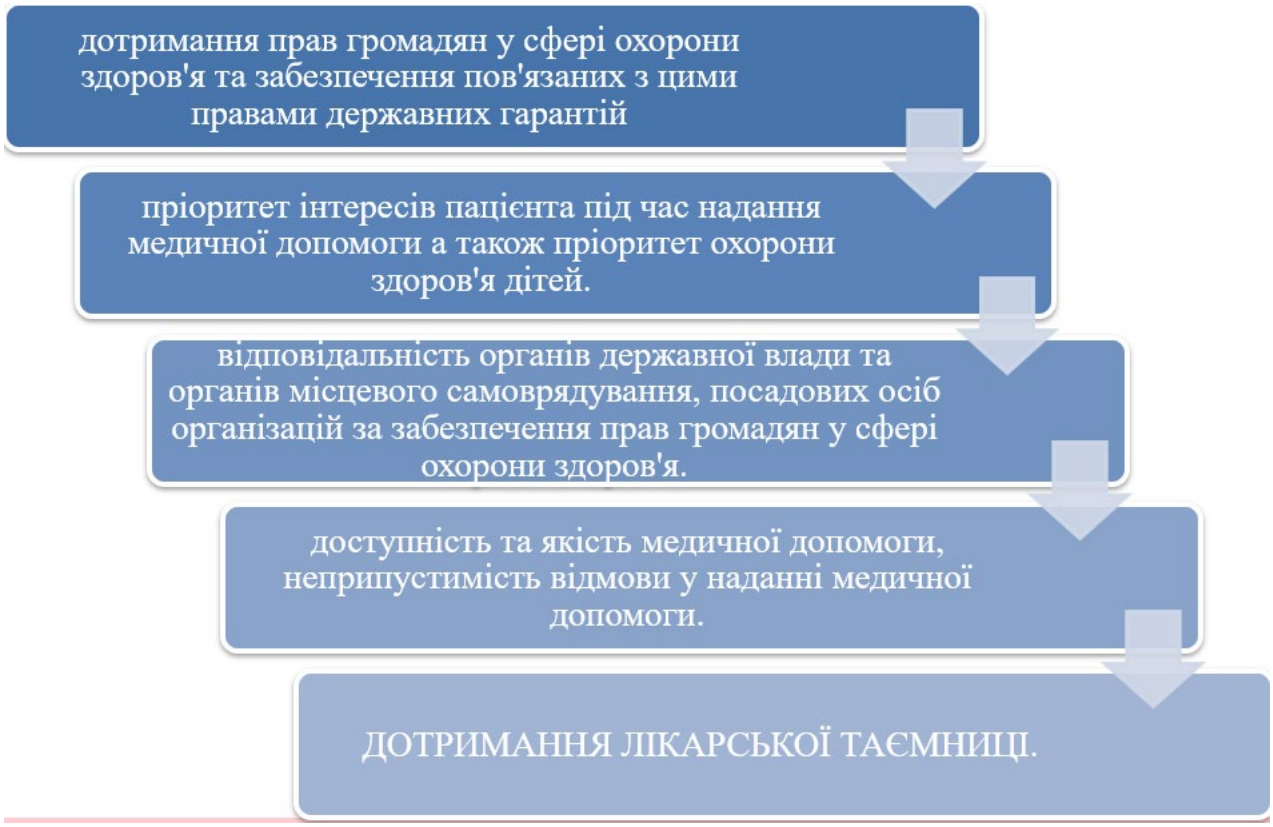


Рисунок 2.2 – Основні принципи охорони здоров’я[7]

Таємниця зв'язку. На території України гарантується таємниця листування, телефонних переговорів, поштових відправлень, телеграфних та інших дій, що передаються мережами електрозв'язку та мережами поштового зв'язку.

Оператори зв'язку зобов'язані забезпечити дотримання таємниці зв'язку. Огляд поштових відправлень особами, які не є уповноваженими працівниками оператора зв'язку, розкриття поштових відправлень, огляд вкладень, ознайомлення з інформацією та документальної кореспонденцією, що передаються мережами електрозв'язку та мережами поштового зв'язку, здійснюються тільки на підставі рішення суду.

Відомості про передані по мережах електрозв'язку та мережі поштового зв'язку в повідомленнях, про поштові відправлення та поштові перекази грошових коштів, а також самі ці повідомлення, поштові відправлення та перекладені кошти можуть видаватися лише відправникам та одержувачам або їх уповноваженим представникам, якщо інше не передбачено законами.

Нотаріальна таємниця. Нотаріусу при виконанні службових обов'язків, особі, яка замінює тимчасово відсутнього нотаріуса, а також особам, які працюють у нотаріальній конторі, забороняється розголошувати відомості, оголошувати документи, які стали їм відомі у зв'язку зі здійсненням нотаріальних дій, у тому числі і після складання повноважень або звільнення.

Відомості (документи) про нотаріальні дії можуть видаватися тільки особам, від імені або за дорученням яких вчинено ці дії, якщо інше не встановлено законом. Відомості про скоєні нотаріальні дії видаються на вимогу суду, прокуратури, органів слідства.

Довідки про видачу свідоцтв про право спадщину та про нотаріальне посвідчення договорів дарування направляються до податкового органу у випадках і в порядку, які передбачені законодавством. Довідки про заповіти видаються лише після смерті заповідача.

Адвокатська таємниця - будь-які відомості, пов'язані з наданням адвокатом юридичної допомоги своєму довірителю.

Таємниця усиновлення. Судді, які винесли рішення про усиновлення дитини, або посадові особи, які здійснили державну реєстрацію усиновлення, а також особи, іншим чином обізнані про усиновлення, зобов'язані зберігати таємницю усиновлення дитини.

Таємниця страхування. Страховик не має права розголошувати отримані ним внаслідок своєї професійної діяльності відомості про страхувальника, застрахованої особи та вигодонабувача, стан їх здоров'я, а також про майновий стан цих осіб.

Таємниця сповіді – відомості, довірені громадянином священнослужителю на сповіді. В країні гарантуються свобода віросповідання. Священнослужитель не може бути притягнутий до відповідальності за відмову від дачі показань щодо обставин, які стали відомі йому на сповіді.

Банківська таємниця. Кредитна організація, яка здійснює функції з обов'язкового страхування вкладів, гарантують таємницю про операції, про рахунки та вкладах своїх клієнтів та кореспондентів [7].

Проаналізувавши різні види професійної таємниці, ми робимо висновок, що велика кількість інформації не повинна бути доступною для більшості людей.

2.5 Процесуальна таємниця

Таємниця слідства пов'язана з інтересами законного провадження при розгляді справи. З метою забезпечення державного захисту суддів, посадових осіб правоохоронних та контролюючих органів, а також окремих категорій службовців та співробітників органів державної охорони, вони виконують функції, реалізація яких може призвести до посягань на їх безпеку, а також створення належних умов для здійснення правосуддя, боротьби зі злочинами та іншими порушеннями закону.

Державний захист мають:

- робітники судів;
- прокурори;
- слідчі;
- особи, які роблять дізнання;
- ведучі оперативно-розшукової діяльності;
- працівники органів внутрішніх справ, що охороняють громадський порядок, надають громадянам безпеку;

1) співробітники установ та органів кримінально-виконавчої системи;

2) військовослужбовці, які брали безпосередню участь у припинення дій озброєних злочинців, незаконних озброєних формувань та інших організованих злочинних груп;

3) військовослужбовці ЗСУ;

- співробітники органів служби безпеки;

– співробітники Слідчого комітету;

– судові виконавці;

– співробітники органів держохорони;

– працівники органів митниці та податкової, антимонопольних органів.

Можливість забезпечення заходів державного захисту може розповсюджуватися і на кримінальні справи, пов'язані з особою, яка подає заяву, служить свідком чи стає жертвою злочину, або іншими особами, що сприяють запобіганню або розкриттю злочину.

Інформація в залежності від доступності буває загальнодоступною та з обмеженим доступом. Закон України «Про захист персональних даних» регулює відносини, пов'язані з обробкою персональних даних, що здійснюється органами державної влади, органами місцевого самоврядування, іншими муніципальними органами, юридичними особами та фізичними особами з використанням автоматизованих засобів обробки, включаючи інформаційні та телекомунікаційні мережі, або не збираючи дані з цих засобів. Коли обробляються персональні дані без спеціальних засобів характер дій відповідає засобам автоматизації, виконується дозвіл на проведення пошуку персональних даних, що зберігаються на фізичному носії та внесені в картотеки або інші систематизовані бази збору персональних даних.

Крім персональних даних, які охороняються законом, існують інші джерела інформації, яку не розголошують. До них відносять: комерційну, службову, професійну, процесуальну таємницю. Інформація, яка є секретною, не повинна бути легко доступною для різних осіб, не пов’язаних з її зберіганням та обробкою. Комерційну таємницю відносять до майнових прав інтелектуальної власності. За розголошення службової інформації обмеженого поширення, а також порушення порядку поводження з документами, що містять таку інформацію, державний службовець (працівник організації) може бути притягнений до дисциплінарної чи іншої передбаченої законодавством відповідальності. Проаналізувавши різні види професійної таємниці, ми робимо висновок, що велика кількість інформації не повинна бути доступною для більшості людей.

РОЗДІЛ 3 ЗАХИСТ ІНФОРМАЦІЇ ЛОМ (ЛОКАЛЬНА ОБЧИСЛЮВАЛЬНА МЕРЕЖА) АТ УКРБУРГАЗ

3.1 Аналіз вразливості підприємства

Під час проведення аналізу захищеності інформації для підприємства АТ Укрбургаз було встановлено, що існує ймовірність реалізації наступних загроз несанкціонованого доступу:

– здійснення несанкціонованого доступу до активів, що захищаються, використовуючи штатні засоби інфраструктури АТ Укрбургаз;

– використання безконтрольно залишених штатних засобів інфраструктури АТ Укрбургаз або розкрадання порушниками та втрата елементів інфраструктури (у тому числі роздруківок, носіїв інформації);

– здійснення несанкціонованого візуального перегляду інформації, що захищається, що відображається на засобах відображення (екранах моніторів), ознайомлення з документами, що роздруковуються;

– дії щодо аналізу мережевого трафіку, сканування обчислювальної мережі, атаки, спрямовані на відмову в обслуговуванні, виявлення парольної інформації, підміна довіреного об'єкта мережі, нав'язування хибного маршруту мережі з використанням позаштатних технічних та програмних засобів, доступних порушнику;

– маскування під адміністраторів інфраструктури АТ Укрбургаз;

– компрометація (перегляд, підбір тощо) парольної інформації на доступ до інформаційних ресурсів АТ Укрбургаз

– здійснення перехоплення керування завантаженням ОС.

Вид ресурсів, потенційно схильних до загрози – цільова та технологічна інформація (комерційна інформація).

Характеристики безпеки активів, що порушуються конфіденційність.

Можливі наслідки реалізації загрози – несанкціоноване ознайомлення з інформацією, що захищається.

Проведемо оцінку актуальності загроз інфраструктурі.

У таблиці 3.1 наведено перелік актуальних загроз інфраструктури АТ Укрбургаз, виявлений під час аналізу загроз несанкціонованого доступу до інформації.

Таблиця 3.1 – Перелік загроз інфраструктури АТ Укрбургаз

№	Загроза безпеці	Ступінь актуальності	Заходи щодо протидії загрозі	
			Технічні	Організаційні
1	Крадіжка носіїв інформації	актуальна		Інструкція для персоналу
2	Крадіжка паролів	актуальна		Інструкція користувача, облік паролів
3	Крадіжки, модифікації, знищення інформації	актуальна	Налаштування засобів захисту, політика безпеки	Резервне копіювання та інструкція користувача
4	Несанкціоноване відключення засобів захисту	актуальна	Налаштування засобів захисту	Інструкція адміністратора безпеки
5	Дії шкідливих програм (вірусів)	актуальна	Антивірусне ПЗ	Інструкція з антивірусного захисту
6	Недекларовані можливості ПЗ	актуальна	Налаштування засобів захисту	Сертифікація
7	Установка ПЗ не пов'язаного з виконанням обов'язків	актуальна	Налаштування засобів захисту, політика безпеки	Інструкція користувача, інструкція адміністратора безпеки
8	Ненавмисна модифікація (Знищення) інформації співробітниками	актуальна	Налаштування засобів захисту, політика безпеки	Інструкція користувача
9	Вихід з ладу апаратно-програмних засобів	актуальна	Резервне копіювання	Охорона, Інструкція для персоналу

Продовження таблиці:

10	Збій системи електропостачання	актуальна	Використання ДБЖ, резервне копіювання	Охорона
11	Розголошення інформації, модифікація, знищення співробітниками	актуальна	Налаштування засобів захисту, політика безпеки	Інструкція для персоналу, підписка про не розголошення
12	Перехоплення в межах контрольованої зони	актуальна	Засоби криптографічного захисту, фізичний захист каналу	Охорона
13	Загрози віддаленого запуску додатків	актуальна	Міжмережевий екран, Антивірусне ПЗ	
14	Загрози застосування по мережі шкідливого ПЗ	актуальна	Міжмережевий екран, Антивірусне ПЗ	
15	Загрози витоку видової інформації	актуальна		Інструкція користувача
16	Крадіжка ПЕОМ	неактуальна		Пропускний режим, охорона, відеоспостереження
17	Виведення з ладу вузлів ПЕОМ, каналів зв'язку	неактуальна		Пропускний режим, охорона, відеоспостереження
18	Загроза "Аналіз мережевого трафіку" з перехопленням переданої та прийнятої із зовнішніх мереж інформації	неактуальна	Міжмережевий екран	Інструкція користувача, інструкція адміністратора безпеки

Отже, стосовно інфраструктури АТ Укрбургаз можна зробити такі висновки:

1. Неактуальність крадіжки ПЕОМ. У будівлі введено цілодобовий контроль доступу до контрольованої зони, що здійснюється охороною, двері, зачиняються на замок, винесення комп'ютерної техніки за межі будівлі можливий лише за спеціальними перепустками.

2. Неактуальність виведення з ладу вузлів ПЕОМ, каналів зв'язку. У будівлі введено контроль доступу в контрольовану зону, двері зачиняються на замок.

3. Неактуальність дій, спрямованих на перехоплення акустичної інформації. Основний обсяг даних консолідовано зберігається на сервері БД, сервер БД розміщений в окремому приміщенні всередині контрольованої зони. Тому ймовірність проникнення зовнішніх порушників або фізичного знищення даних мінімальна – необхідно доопрацьовувати програмно-апаратний комплекс засобів захисту комп'ютерної інформації по напрямкам: забезпечити захист мережевого периметра та вибрати міжмережевий екран; вибрати криптографічні засоби захисту; визначити засоби виявлення вторгнень та антивірусу.

3.2 Встановлення між мережевого екрану

Однією з перших рекомендацій у ході аналізу захисту даних АТ Укрбургаз є установка міжмережевого екрану, яка є зовнішньою.

Міжмережні екрани призначені в першу чергу для захисту комп'ютерних мереж або окремих вузлів від зовнішніх атак. Міжмережевий екран робить можливою фільтрацію вхідного та вихідного трафіку, що йде через систему. Для корпоративної мережі фірми було обрано програмний міжмережевий екран UserGate Proxy & Firewall 5.2 F, який є ефективною альтернативою дорогим програмним та апаратним міжмережевим екранам і

маршрутизаторам, які використовуються для захисту конфіденційної інформації та даних у захищених системах.

Продукт використовує комплексний підхід до забезпечення безпеки локальної мережі та сучасні методи боротьби з Інтернет-загрозами, призначений для організації безпечної міжмережевої взаємодії, обліку трафіку та захисту локальної мережі організації від зовнішніх загроз і є сертифікованим засобом міжмережевого екранування та безпечного доступу до Інтернету для захищених систем.

Дане комплексне рішення UserGate Proxy дозволяє:

– підтримувати передачу трафіку через протоколи PPTP та L2TP для з'єднання VPN-сервера з VPN-клієнтами локальної мережі з подальшою публікацією мережевих ресурсів з метою віддаленого використання;

– розробити стратегію доступу до Інтернету та проводити повний моніторинг використання мережевого трафіку в організації із веденням детальної статистики;

– розробити норми для регулювання швидкості передачі даних між локальною мережею та Інтернетом, обмежуючи обсяг трафіку та час перебування в мережі для користувачів і груп;

– спростити мережеве адміністрування.

На рисунках наведено приклади функціонування UserGate Proxy & Firewall.

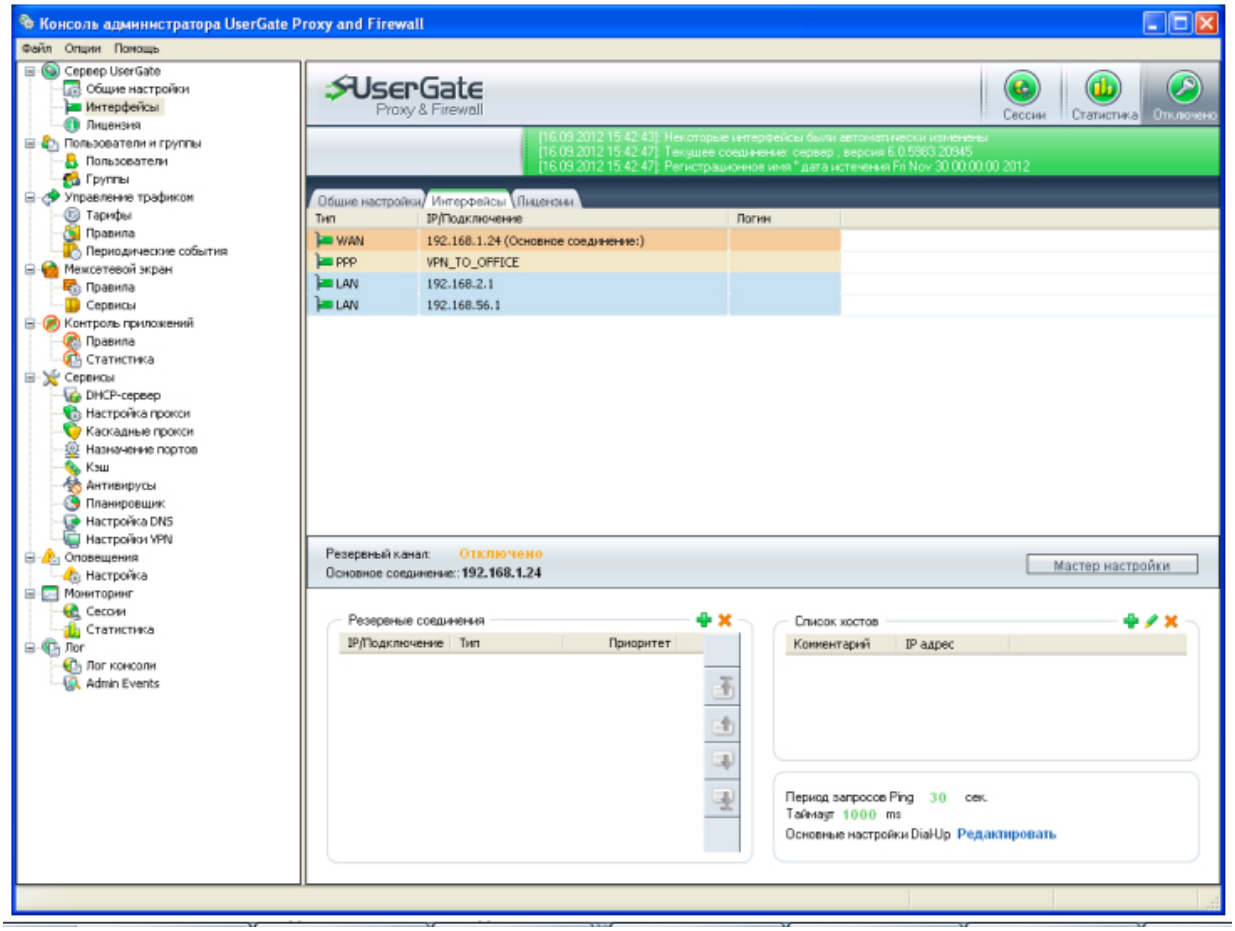


Рисунок 3.1 – Інтерфейс адміністратора у UserGate Proxy & Firewall

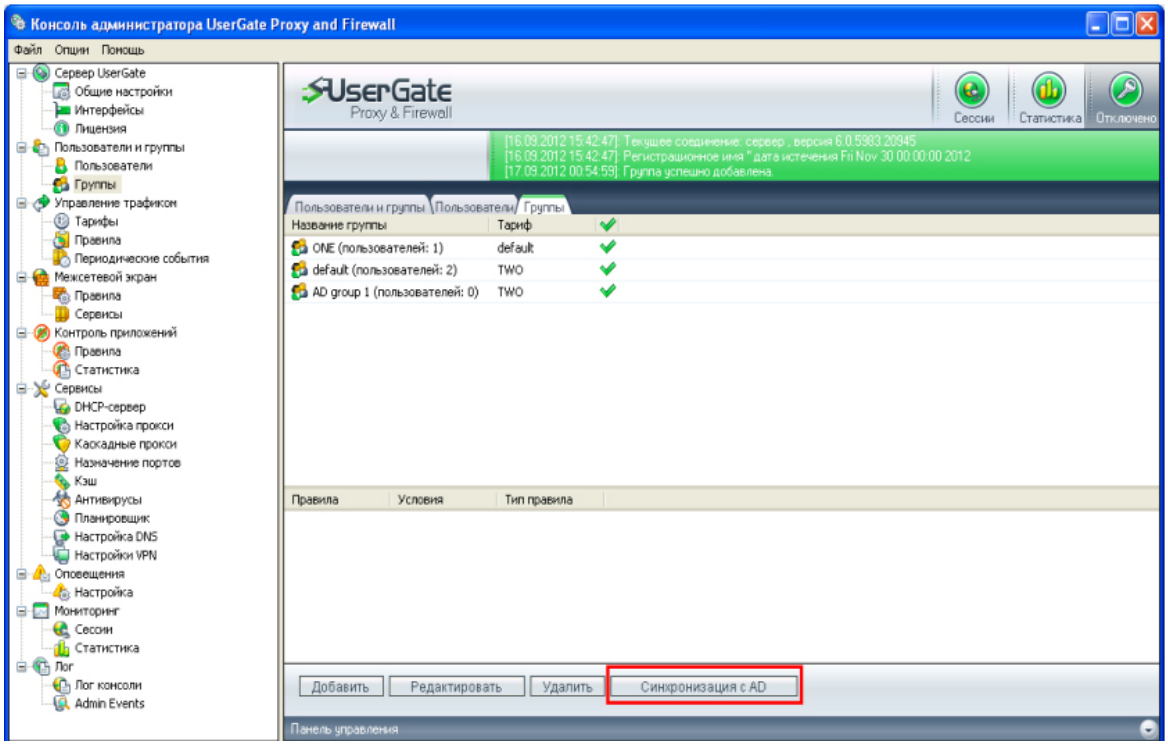


Рисунок 3.2 – Контроль сесій у UserGate Proxy & Firewall

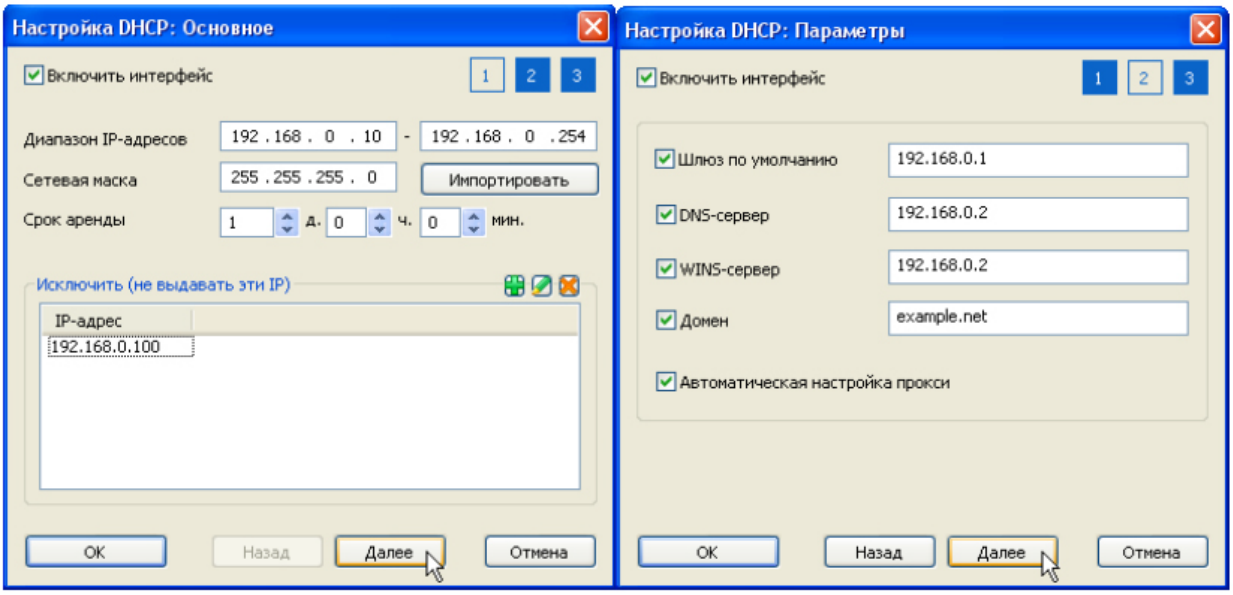


Рисунок 3.3 – Налаштування обмежень щодо трафіку та між мережевого екранування

3.3 Впровадження криптопровайдера в системі захисту даних

Особливий інтерес становить засіб криптографічного захисту інформації «ViPNet CSP», який:

– призначено для формування ключів шифрування та ключів електронного підпису, шифрування та імітозахисту даних;

– забезпечення цілісності та справжності інформації. СКЗІ «ViPNet CSP» може використовуватися в державних та комерційних структурах, а також фізичними особами шляхом вбудовування в прикладне програмне забезпечення;

– забезпечує зберігання та обробку персональних даних, конфіденційної, службової, комерційної та ін. інформації, що не містить відомостей, що становлять державну таємницю, а також забезпечує обмін такою інформацією і юридичну значимість електронного документообігу.

Обмін інформацією в електронній формі здійснюється всередині та між державними органами, органами місцевого самоврядування, організаціями, і навіть громадянами (фізичними особами).

СКЗІ «ViPNet CSP» підходить для вбудовування в прикладне програмне забезпечення інших виробників та для постачання кінцевим користувачам та забезпечує:

– Створення ключів електронного підпису. Перевірку електронного підпису, обчислення та перевірку електронного підпису.

– Хешування даних.

– Шифрування та імітозахист даних. Генерацію випадкових та псевдовипадкових чисел, сесійних ключів шифрування.

– Аутентифікацію та вироблення сесійного ключа при передачі даних за протоколами SSL/TLS. Зберігання сертифікатів відкритих ключів безпосередньо у контейнері ключів.

– Підтримка різних пристроїв зберігання ключів (eToken, Shipka та ін.).

Для здійснення функцій шифрування та перевірки електронного підпису криптопровайдер ViPNet CSP використовує відкритий ключ, що знаходиться в сертифікат того користувача, якому адресовано зашифрований документ або від якого надійшов документ із електронним підписом. Для розшифрування та формування електронного підпису криптопровайдер використовує закритий ключ користувача, який здійснює дані операції (Той ключ, який буде вказано самим користувачем). Процес передачі конфіденційного повідомлення Outlook схематично представлений нижче (рис. 3.4).

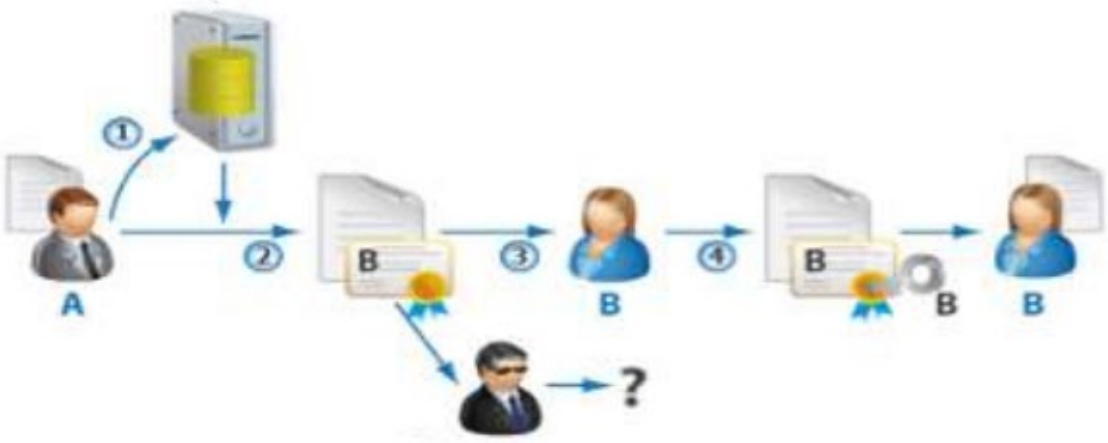


Рисунок 3.4 – Схема обміну захищеними документами

Користувачеві А необхідно передати користувачеві В конфіденційне повідомлення Outlook:

– Користувач А запитує з мережевого сховища сертифікат відкритого ключа користувача В та зіставляє його з контактом В у програмі Outlook.

– А зашифровує документ із використанням відкритого ключа з сертифіката Ст.

– А надсилає користувачеві В зашифроване повідомлення.

– Розшифровує документ за допомогою свого закритого ключа.

– Таким чином користувач отримує конфіденційне повідомлення від користувача А.

Якщо повідомлення перехопить зловмисник, прочитати листа йому не вдасться, оскільки у нього немає закритого ключа користувача. Якщо користувач не зможе розшифрувати повідомлення, що надійшло від А, це означає, що лист був змінений сторонніми особами або пошкоджено в процесі пересилання. У такому випадку може запитати у користувача А повторне надсилання повідомлення.

Процес формування та перевірки електронного підпису наведено нижче.

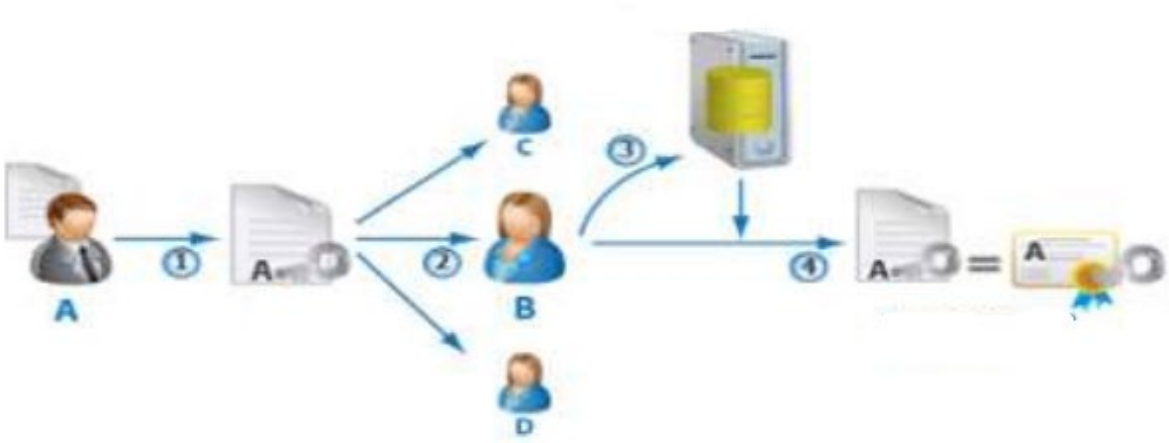


Рисунок 3.5 – Процес формування та перевірки підпису документа

Користувачеві А необхідно завірити документ (наприклад, повідомлення Outlook) електронним підписом, для того щоб інші користувачі не змогли внести до нього зміни і кожен міг переконатися, що автор цього документа – користувач А;

– Користувач А підписує документ своїм закритим ключем.

– А надсилає цей документ усім зацікавленим особам (Користувачі B, C і D) або викладає для загального доступу.

– Користувач В запитує в Сховищі сертифікатів сертифікат відкритого ключа А.

– У перевіряє документ за допомогою відкритого ключа А, який знаходиться у його сертифікаті.

СКЗІ «ViPNet CSP» призначено для роботи на IBM-сумісних комп'ютерах (стаціонарних, переносних чи мобільних) з наступною рекомендованою конфігурацією: процесор з архітектурою x86 чи x86-64; ОЗУ – не менше 512 мегабайт; вільне місце на жорсткому диску – не менше ніж 30 мегабайт.

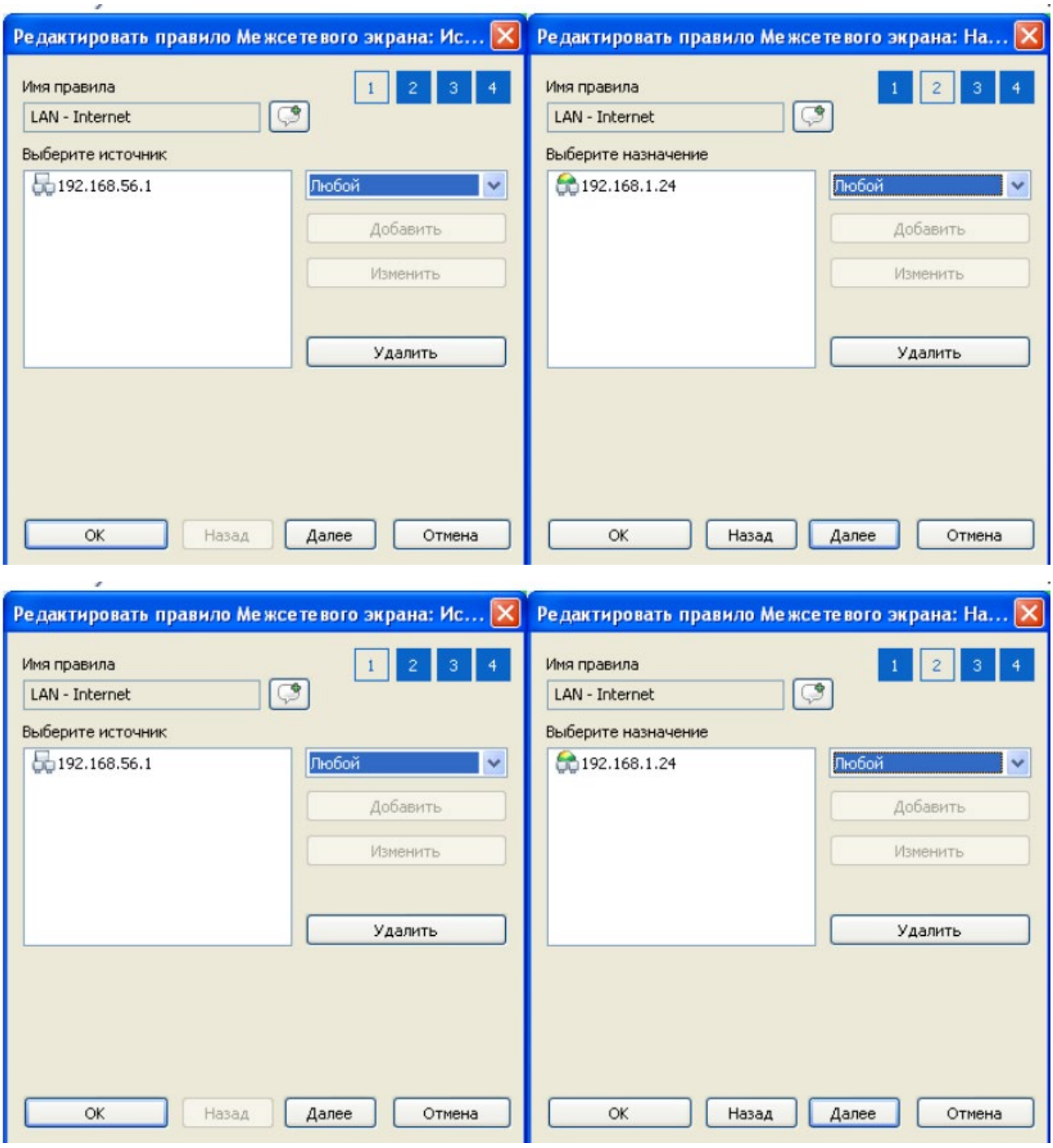


Рисунок 3.6 – Створення правила трансляції (NAT)

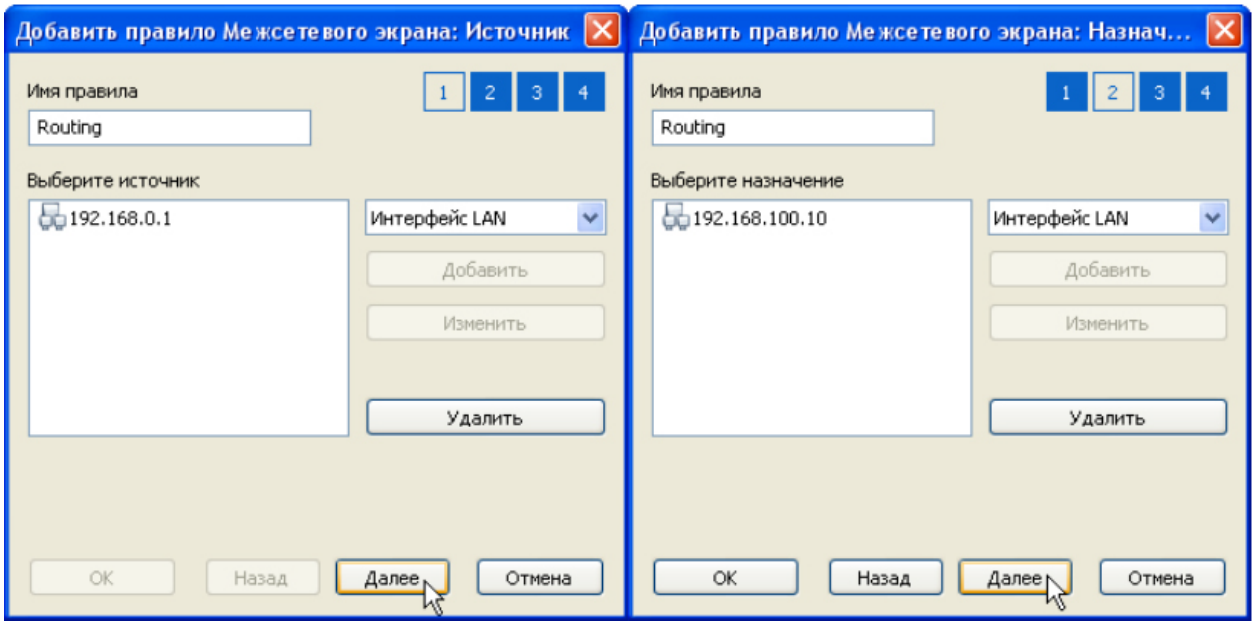


Рисунок 3.7 – Процедура оновлення сертифіката у ViPNet CSP

3.4 Встановлення засобів виявлення вторгнень та антивіруса

Security Studio Endpoint Protection 6.0 забезпечує захист комп'ютера з застосуванням міжмережевого екрану, антивіруса та засоби виявлення вторгнень. Забезпечує безпечну та комфортну роботу з мережею Інтернет, запобігаючи будь-яким спробам проникнення на комп'ютер шкідливого програмного забезпечення та блокуючи небажаний трафік.

Security Studio Endpoint Protection 6.0 захищає комп'ютер від мережевих вторгнень, шкідливих програм та спаму:

- безпечний доступ до мережі;
- захист від відомих вірусів та програм-шпигунів;
- захист від невідомих загроз;
- безпечне використання мережевих ресурсів та захист від спаму;
- централізоване управління.

Security Studio Endpoint Protection (SSEP) забезпечує захист комп'ютера із застосуванням міжмережевого екрану, антивірусу та засоби виявлення вторгнень. Забезпечує безпечну та комфортну роботу з мережею інтернет,

запобігаючи будь-яким спробам проникнення на комп'ютер шкідливого програмного забезпечення та блокуючи небажаний трафік.

Сертифікована версія Security Studio Endpoint Protection дозволить виконати вимоги щодо захисту персональних даних. SSEP може бути використаний спільно з СЗІ від Secret Net для забезпечення комплексного захисту автоматизованого робочого місця.

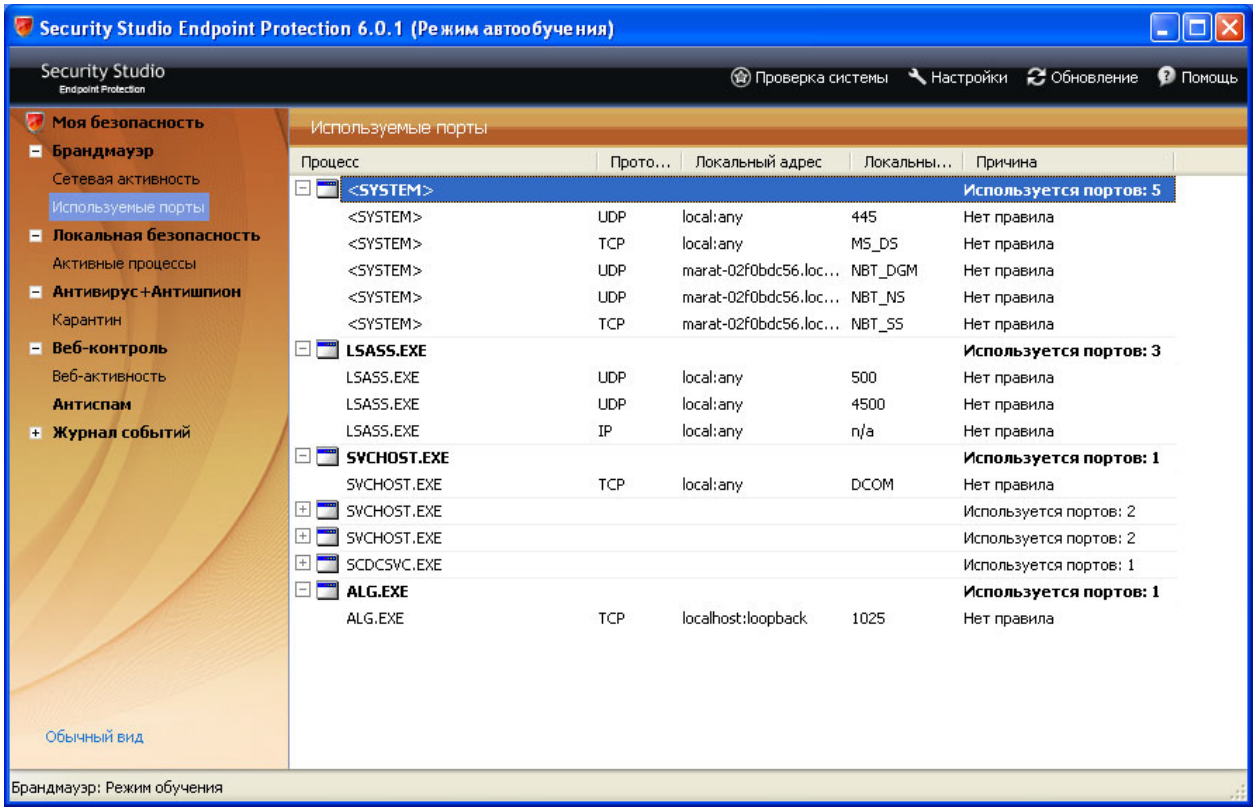


Рисунок 3.8 – Компоненти Security Studio Endpoint Protection

Компоненти Security Studio Endpoint Protection:

– Міжмережевий екран. Двосторонній контроль трафіку дозволяє припинити спроби несанкціонованого доступу до комп'ютера з локальної мережі Інтернету.

– Антивірус та антишпигун. Швидкий та ефективний сканер, що поєднує антивірус та антишпигун, виявляє та знешкоджує шкідливе програмне забезпечення.

– Засіб виявлення вторгнень. Модуль "Детектор атак" запобігає понад 25 типовим атакам, а «Локальна безпека» контролює взаємодію програм, захищаючи систему від нерозпізнаних загроз.

– Web-контроль. Інтерактивні елементи web-серверів можуть завдати шкоду комп'ютеру та призвести до витоку конфіденційної інформації. Для запобігання цьому виду загроз SSEP контролює роботу інтерактивних елементів, які вбудовані в веб-сторінки, що завантажуються.

– Централізоване управління. Центр адміністрування SSEP дозволяє зробити централізовану установку або оновлення SSEP на робочих станціях, віддалену настройку механізмів захисту та моніторинг подій безпеки.

Переваги та переваги Security Studio Endpoint Protection.

– Засіб виявлення вторгнень – одне з найбільш технічно досконалих засобів протидії витокам інформації.

– Можливість роботи паралельно з антивірусом іншого виробника.

– Можливість впровадження комплексного рішення спільно із Secret Net.

– SSEP рекомендовано до встановлення в інфраструктурі АТ Укрбургаз на всіх робочих станціях.

Таким чином, внаслідок відпрацювання проектного рішення щодо захисту інформації від несанкціонованого доступу до корпоративної мережі АТ Укрбургаз, були рекомендовані до встановлення наступні СЗІ:

– криптографічний засіб захисту від НСД – СКЗІ «ViPNet CSP»;

– міжмережевий екран UserGate Proxy & Firewall 5.2 F;

– засіб виявлення вторгнень та антивірус – SSEP.

Варіант розміщення засобів захисту інформації у корпоративній мережі АТ Укрбургаз зображено рис. 3.9.

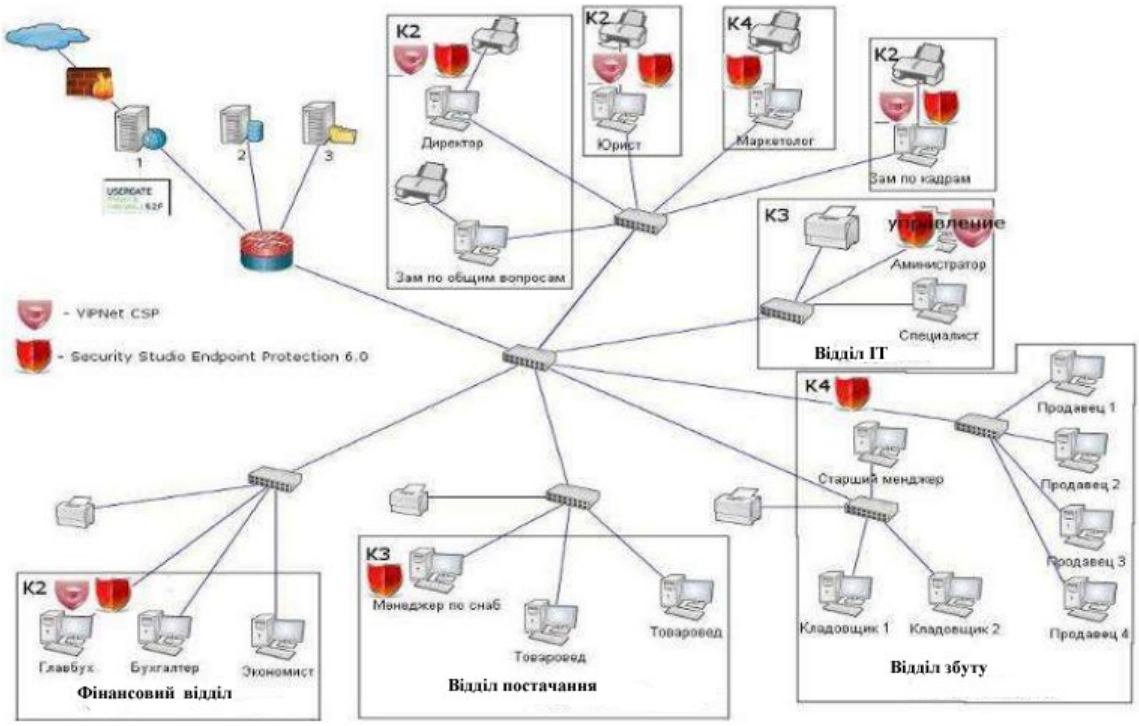


Рисунок 3.9 – Варіант розташування СЗІ у корпоративній мережі АТ Укрбургаз

В даному розділі здійснено оцінку мережного та програмного забезпечення підприємства, визначено склад інформації, схильної до загроз, виявлено вразливості із захисту, а також запропоновані заходи щодо запобігання загрозі інформаційної безпеки у ЛОМ АТ Укрбургаз.

Встановлено сертифіковану версію Security Studio Endpoint Protection, яка дозволить виконати вимоги щодо захисту персональних даних. SSEP може бути використаний спільно з СЗІ від Secret Net для забезпечення комплексного захисту автоматизованого робочого місця.

Також був впроваджений криптопровайдер в системі захисту даних. «ViPNet CSP» виконує формування ключів шифрування та ключів електронного підпису, шифрування та імітозахисту даних; забезпечує цілісність та справжність інформації. Його використовують в державних та комерційних структурах шляхом вбудовування в прикладне програмне забезпечення. Криптопровайдер забезпечує зберігання та обробку персональних даних, конфіденційної, службової, комерційної та ін.

інформації, що не містить відомостей, що становлять державну таємницю, а також забезпечує обмін такою інформацією і юридичну значимість електронного документообігу.

Отже, після відпрацювання проектного рішення щодо захисту інформації від несанкціонованого доступу до корпоративної мережі АТ Укрбургаз, були встановлені засіб виявлення вторгнень та антивірус – SSEP, криптографічний засіб захисту від НСД – СКЗІ «ViPNet CSP», та міжмережевий екран UserGate Proxy & Firewall 5.2 F.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Охорона праці

Використання ПЕОМ у роботі може негативно позначитися на здоров’ї спеціаліста з інформаційної безпеки, особливо якщо комп'ютер використовується постійно або значну частину робочого часу.

Виконуючи свої професійні обов’язки, спеціаліст з інформаційної безпеки може піддаватися впливу небезпечних і шкідливих виробничих чинників. Під впливом таких факторів може виникнути тимчасове погіршення здоров'я та, відповідно, знизитися працездатність, виникнути головний біль, різь в очах і погіршення зору, загальна втома, дратівливість. Як побічні ефекти роботи з комп’ютером можуть виникнути безсоння, біль у суглобах, попереку, кистях рук.

Перерахуємо можливі шкідливі та (або) небезпечні виробничі фактори, які можуть вплинути на працюючих:

– підвищений рівень електромагнітних випромінювань; підвищений рівень іонізуючих випромінювань;

– підвищена яскравість світла; пряма та відбита блискітність;

– статичні перевантаження кістково-м'язового апарату та динамічні локальні навантаження м'язів кистей рук; перенапруга зорового аналізатора; розумова перенапруга; емоційні навантаження; монотонність праці [21].

На підприємстві АТ Укрбургаз працюючі зобов'язані:

– знати та дотримуватись вимог експлуатаційних документів організацій-виробників використовуваної ПЕОМ;

– дотримуватися режиму праці та відпочинку, встановленого законодавством, правилами внутрішнього трудового розпорядку організації, трудової дисципліни, виконувати вимоги з охорони праці, правил особистої

гігієни; виконувати вимоги пожежної безпеки; палити лише у спеціально призначених для цього місцях;

– піклуватися про особисту безпеку та особисте здоров'я, а також про безпеку оточуючих у процесі виконання робіт або під час перебування на території організації;

– утримувати робоче місце у порядку та чистоті;

– знати місцезнаходження аптечки першої медичної допомоги;

– повідомляти безпосереднього керівника або іншої уповноваженої посадової особи про несправність ПЕОМ та периферійних пристроїв (принтера, сканера, клавіатури ПЕОМ, електричних комп'ютерних мережевих пристроїв, блоку безперебійного живлення та інших пристроїв) (далі – обладнання) та інших неполадках та інших неполадках розпочинати роботу до їх усунення;

– негайно повідомляти безпосереднього керівника або іншої уповноваженої посадової особи про будь-яку ситуацію, яка загрожує життю або здоров'ю працюючих та оточуючих; виконувати інші обов'язки, передбачені законодавством [21].

На підприємстві АТ Укрбургаз не допускається знаходження працюючих у стані алкогольного, наркотичного або токсичного сп'яніння, а також розпивання спиртних напоїв, споживання наркотичних засобів, психотропних речовин, їх аналогів, токсичних засобів на робочому місці та у робочий час.

Працюючі мають право відмовитися від виконання дорученої роботи у разі виникнення безпосередньої небезпеки для життя та здоров'я їх та оточуючих до усунення цієї небезпеки.

На підприємстві АТ Укрбургаз перед початком роботи з ПЕОМ працівник з інформаційної безпеки повинен оглянути робоче місце та переконатися:

– у стійкості положення устаткування робочому столі;

– у відсутності видимих пошкоджень обладнання;

– у справності та цілісності живильних та сполучних кабелів, роз'ємів та штепсельних з'єднань, захисного заземлення (занулення);

– у справності загального та місцевого освітлення, меблів [22].

Для збереження здоров’я та профілактики професійних захворювань необхідно дотримуватись наступних норм з використання комп’ютерної техніки. Клавіатуру ПЕОМ необхідно розташувати на поверхні робочого стола на відстані 10-30 см від краю, зверненого до працюючого, або на спеціальній, що регулюється по висоті поверхні, відокремленої від основної стільниці.

Екран відеомонітора розміщується на відстані 60-70 см від очей, але не ближче 50 см з урахуванням розмірів алфавітно-цифрових знаків та символів, щоб рівень очей при вертикально розташованому екрані відеомонітора припадав на центр або 2/3 висоти екрану. Лінія погляду повинна бути перпендикулярна центру екрану, і оптимальне її відхилення від перпендикуляра, що проходить через центр екрана у вертикальній площині, не повинно перевищувати +/-5 градусів, допустиме +/-10 градусів.

Необхідно переконатися у відсутності відблисків на екрані відеомонітора, зустрічного світлового потоку. Можливі відбиття, що заважають, і відблиски на екрані відеомонітора та іншому обладнанні усуваються шляхом відповідного їх розміщення, розташування світильників місцевого освітлення. Для зниження яскравості в полі зору при природному освітленні необхідно застосувати жалюзі, що регулюються, щільні штори.

При необхідності – увімкнути місцеве освітлення, протерти поверхню екрана відеомонітора сухою м'якою тканинною серветкою, провітрити приміщення.

На підприємстві АТ Укрбургаз забороняється: встановлювати системний блок у закритих отворах меблів, безпосередньо на підлозі; використовувати для підключення обладнання розетки, подовжувачі, які не оснащені заземлюючим контактом (шиною); включати охолоджене (принесене з вулиці взимку) обладнання; розташовувати екрани

відеомоніторів назустріч один одному при рядному розміщенні робочих столів з метою унеможливлення їх взаємного відображення; приступати до роботи з ПЕОМ під час миготіння зображення на екрані відеомонітора, у разі виявлення несправності обладнання, кабелів чи проводів, роз'ємів, штепсельних з'єднань, за відсутності чи несправності захисного заземлення (занулення) обладнання [21].

Роботу за екраном відеомонітора слід періодично переривати на регламентовані перерви, які встановлюються для забезпечення працездатності та збереження здоров'я або замінювати іншою роботою з метою скорочення робочого навантаження біля екрана.

Тривалість безперервної роботи з ПЕОМ без регламентованої перерви не має перевищувати двох годин.

Час регламентованих перерв протягом робочого дня (зміни) встановлюється залежно від його (її) тривалості, виду та категорії трудової діяльності.

При восьмигодинному робочому дні (зміні) та роботі з ПЕОМ регламентовані перерви слід встановлювати:

– при виконанні робіт зі зчитування інформації з екрану ПЕОМ із попереднім запитом до 20 000 знаків (робота з введення інформації до 15 000 знаків або творча робота в режимі діалогу з ПЕОМ до 2 годин) – через 2 години від початку робочого дня (зміни) та через 2 години після обідньої перерви тривалістю 15 хвилин кожен;

– при виконанні робіт з зчитування інформації з екрану ПЕОМ із попереднім запитом до 40 000 знаків (робота з введення інформації до 30 000 знаків або творча робота в режимі діалогу з ПЕОМ до 4 годин) – через 2 години від початку робочого дня (зміни) та через 1,5-2 години після обідньої перерви тривалістю 15 хвилин кожен або тривалістю 10 хвилин через кожну годину роботи;

– при виконанні робіт з зчитування інформації з екрана ПЕОМ із попереднім запитом до 60 000 знаків (робота з введення інформації до 40 000

знаків або творча робота в режимі діалогу з ПЕОМ до 6 годин) – через 1,5-2 години від початку робочого дня (зміни) і через 1,5-2 години після обідньої перерви тривалістю 20 хвилин кожен або тривалістю 15 хвилин через кожну годину роботи [22].

Під час регламентованих перерв, з метою зниження нервово-емоційної напруги, втоми зорового аналізатора, усунення впливу гіподинамії та гіпокінезії, запобігання розвитку статичної втоми, необхідно виконувати фізичні вправи та вправи для очей.

З метою зменшення негативного впливу монотонності праці доцільно застосовувати чергування операцій.

Після закінчення роботи з ПЕОМ на підприємстві АТ Укрбургаз спеціаліст з інформаційної безпеки зобов'язаний:

- коректно закрити усі активні завдання;
- витягти магнітні носії (флеш-носії, диски);
- вимкнути живлення системного блоку;
- вимкнути живлення всіх периферійних пристроїв;
- вимкнути блок безперебійного живлення;
- відключити стабілізаторр напруги (якщо вона використовується);
- відключити кабель живлення від мережі;
- оглянути і упорядкувати робоче місце; за необхідності протерти поверхні периферійних пристроїв (клавіатура ПЕОМ, маніпулятор «миша», принтер, сканер та інше) і вимити з милом руки [21].

Протирання периферійних пристроїв проводиться м'якою ганчіркою із застосуванням спеціальних або побутових засобів для чищення, що не містять кислот і відбілювачів, при вимкненому обладнанні методом і засобами, що не впливають на працездатність даних пристроїв, не рідше одного разу на тиждень.

4.2 Безпека в надзвичайних ситуаціях

При пошкодженні обладнання, кабелів, проводів, несправності заземлення (занулення), появі запаху гару, виникненні незвичайного шуму та інших несправностях спеціаліст з інформаційної безпеки на підприємстві АТ Укрбургаз зобов'язаний негайно відключити електроживлення обладнання та повідомити про безпосередній керівник або іншу уповноважену посадову особу.

У разі збою в роботі обладнання або програмного забезпечення працівник зобов'язаний повідомити про це фахівця, який здійснює технічне обслуговування обладнання організації, для усунення несправностей.

У разі виникнення загоряння або пожежі спеціаліст з інформаційної безпеки на підприємстві зобов'язаний відключити від електромережі обладнання, вжити заходів щодо евакуації працюючих у безпечне місце, викликати підрозділ з надзвичайних ситуацій за телефоном 101, вказавши адресу об'єкта та ділянку загоряння, повідомити про те, що сталося безпосередньому керівнику або іншій уповноваженій посадовій особі. Розпочати гасіння пожежі наявними засобами пожежогасіння.

Застосування води та пінних вогнегасників для гасіння електрообладнання, що знаходиться під напругою, не допускається. Для цих цілей і використовуються вуглекислотні та порошкові вогнегасники [21].

При нещасному випадку працюючий зобов’язаний:

– негайно повідомити про нещасний випадок безпосереднього керівника або іншої уповноваженої посадової особи;

– вжити заходів щодо запобігання впливу травмуючих факторів на потерпілого, надання потерпілому першої допомоги, виклику на місце події медичних працівників або доставки потерпілого до організації охорони здоров'я [22].

У разі отримання травми та (або) раптового погіршення здоров'я (посилення серцебиття, появи головного болю та іншого) працівник повинен припинити роботу, вимкнути обладнання, повідомити про це безпосереднього керівника або іншу уповноважену посадову особу та за необхідності звернутися до лікаря.

Спеціалісти з інформаційної безпеки на підприємстві АТ Укрбургаз зобов'язані:

– знати та дотримуватись вимог експлуатаційних документів організацій-виробників використовуваної ПЕОМ;

– дотримуватися режиму праці та відпочинку, встановленого законодавством, правилами внутрішнього трудового розпорядку організації, трудової дисципліни, виконувати вимоги з охорони праці, правил особистої гігієни;

– виконувати вимоги пожежної безпеки;

– палити лише у спеціально призначених для паління місцях;

– піклуватися про особисту безпеку та особисте здоров'я, а також про безпеку оточуючих у процесі виконання робіт або під час перебування на території організації;

– утримувати робоче місце у порядку та чистоті; знати місцезнаходження аптечки першої медичної допомоги;

– повідомляти безпосереднього керівника або іншої уповноваженої посадової особи наймача про несправність ПЕОМ та периферійних пристроїв (принтера, сканера, клавіатури ПЕОМ, електричних комп'ютерних мережевих пристроїв, блоку безперебійного живлення та інших пристроїв) та інших неполадок, що перешкоджають виконанню усунення;

– негайно повідомляти безпосереднього керівника або іншої уповноваженої посадової особи про будь-яку ситуацію, яка загрожує життю або здоров'ю працюючих та оточуючих; виконувати інші обов'язки, передбачені законодавством [22].

В результаті аналізу вимог щодо охорони праці на підприємстві АТ Укрбургаз було визначено, що можна використовувати такі методи впливу на мотиви, які стимулюють безпечну поведінку працівників: встановити працівникам чітку мету щодо дотримання правил безпеки; створити умови для можливості досягнення цієї мети. Під час виконання кваліфікаційної роботи з дослідження інформаційної безпеки малого та середнього бізнесу було дотримано всіх вищевказаних норм щодо охорони праці.

Були перераховані можливі шкідливі та (або) небезпечні фактори, які можуть вплинути на працюючих, встановлений час регламентованих перерв протягом робочого дня (зміни) залежно від його (її) тривалості, виду та категорії трудової діяльності. Вказані обов’язки після закінчення роботи з ПЕОМ.

Було описано як себе поводити при пошкодженні обладнання, кабелів, проводів, несправності заземлення (занулення), появі запаху гару, виникненні незвичайного шуму та інших несправностях. Також визначено, що робити у разі виникнення загоряння або пожежі, у разі збою в роботі обладнання або програмного забезпечення.

ВИСНОВКИ

В ході виконанні кваліфікаційної роботи було широко розкрито поняття інформаційної безпеки підприємств малого та середнього бізнесу. Були вирішені поставлені завдання: визначені види інформаційних загроз та наслідки кібератак; проведено аналіз уразливості підприємства АТ Укрбургаз та розроблені рекомендації щодо захисту інформації на підприємстві АТ Укрбургаз.

Аналізуючи питання інформаційної безпеки, можна сказати, що вона є дуже актуальна в нинішній час. Малі та середні компанії найбільше страждають від кібератак. Через це такі компанії можуть втратити конфіденційну інформацію, гроші чи цінну частку ринку. Існує безліч способів, якими зловмисники намагаються досягти своїх цілей.

Областю інформаційної безпеки є управління ризиками та захисту інформації від загроз та небажаного доступу. Вона включає різні заходи і практики, спрямовані на дотримання конфіденційності, цілісності та доступності інформації.

Інформаційна безпека підтримує репутацію організації. Витік даних та порушення, пов'язані з інформаційною безпекою, можуть завдати серйозної, а часто непоправної шкоди репутації будь-якої компанії. Виконується захист від загроз, підтримка бізнес-процесів та продуктивності.

Злочинці часто застосовують інформаційний тероризм задля дестабілізації суспільства та досягнення незаконних цілей. Одним із проявів кібертероризму можна вважати фейк. Небезпека недостовірної інформації у тому, що вона не тільки підриває довіру аудиторії до мас-медіа, а й сприяє економічній та політичній дестабілізації в країні. Найбільш поширеними є інтернет-боти, хакінг, шкідливе програмне забезпечення, підбір облікових даних. Інтернет-боти займаються зупинкою онлайн-сервісів. Хакінг вражає мережу або пристрої. Шкідливе ПЗ порушує роботу пристроїв, викрадає

персональні дані. При підборі облікових даних здійснюється викрадання даних, шпигунство, руйнування критичної інфраструктури.

У ряді європейських держав та на американському континенті накопичено позитивний досвід протидії терористичним правопорушенням у Мережі. Через різноманітні портали та сайти інтернет-користувачі знайомляться з превентивною державною діяльністю щодо терористичних організацій та їхньої ідеології. Багато держав скоригували законодавство, яке регулює інтернет-комунікацію. Розроблено комплекс заходів щодо протидії кібер- та інформаційному тероризму

Питання забезпечення кібербезпеки надзвичайно актуальні і для України. Впровадження законодавчого регулювання питання кібербезпеки, зможе захистити кіберпростір і запобігти масовим кібератакам.

Законодавство використовує базові терміни в галузі ІБ і визначає права та обов'язки державних органів щодо захисту від інформаційних злочинів. Державні службовці забезпечують кіберзахист об'єктів критичної інформаційної інфраструктури; координувати діяльність інших суб'єктів кібербезпеки; забезпечувати створення та функціонування національної телекомунікаційної мережі; запобігати, виявляти та реагувати на кіберінциденти та кібератаки та усувати їх наслідки; інформувати про кіберзагрози та методи захисту від них.

Отже, кібербезпека відіграє критичну роль у захисті активів, клієнтів, підрядників та репутації бізнесу, а також забезпечує дотримання законодавчих вимог та норм. Можна сказати про те, що забезпечення кібербезахисту стало надзвичайно важливим у сучасному світі. Комп'ютерна мережа від дня її створення була і буде піддаватися атакам зловмисників, і схоже, що кількість загроз кібератак тільки зростатиме. Протистояння кібератакам та відновлення збитків можливі при належному рівні підготовки обладнання та кваліфікації фахівців.

Інформація буває загальнодоступною та обмеженого доступу в залежності від категорії доступу до неї. ЗУ «Про захист персональних даних»

встановлені норми регулюють взаємовідносини, пов'язані з обробкою персональних даних, здійснюваною органами державної влади, органами місцевого самоврядування, іншими муніципальними установами, юридичними особами та фізичними особами.

Крім персональних даних, які охороняються законом, існують інші джерела інформації, яку не розголошують. До них відносять: комерційну, службову, професійну, процесуальну таємницю. Інформація, яка є секретною, не повинна бути легко доступною для різних осіб, не пов’язаних з її зберіганням та обробкою. Комерційну таємницю відносять до майнових прав інтелектуальної власності. Щодо розголошення службової інформації обмеженого поширення, а також порушення порядку поводження з документами, що містять таку інформацію, державний службовець (працівник організації) може бути притягнений до дисциплінарної чи іншої передбаченої законодавством відповідальності. Проаналізувавши різні види професійної таємниці, ми робимо висновок, що велика кількість інформації не повинна бути доступною для більшості людей.

Було проведено аналіз мережного та програмного забезпечення підприємства, визначено склад інформації, схильної до загроз, виявлено вразливості із захисту, а також запропоновані заходи щодо запобігання загрозі інформаційної безпеки у ЛОМ АТ Укрбургаз.

Встановлено сертифіковану версію Security Studio Endpoint Protection, яка дозволить виконати вимоги щодо захисту персональних даних. SSEP може бути використаний спільно з СЗІ від Secret Net для забезпечення комплексного захисту автоматизованого робочого місця.

Також був впроваджений криптопровайдер в системі захисту даних. «ViPNet CSP» виконує формування ключів шифрування та ключів електронного підпису, шифрування та імітозахисту даних; забезпечує цілісність та справжність інформації. Його використовують в державних та комерційних структурах шляхом вбудовування в прикладне програмне забезпечення. Криптопровайдер забезпечує зберігання та обробку

персональних даних, конфіденційної, службової, комерційної та ін. інформації, що не містить відомостей, що становлять державну таємницю, а також забезпечує обмін такою інформацією і юридичну значимість електронного документообігу.

Отже, після відпрацювання проектного рішення щодо захисту інформації від несанкціонованого доступу до корпоративної мережі АТ Укрбургаз, були встановлені засіб виявлення вторгнень та антивірус – SSEP, криптографічний засіб захисту від НСД – СКЗІ «ViPNet CSP», та міжмережевий екран UserGate Proxy & Firewall 5.2 F.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Дата звернення: 30.11.2023)
2. Кримінальний кодекс України [Електронний ресурс]. Режим доступу: URL:https://zakon.rada.gov.ua/laws/show/2341-14#Text (Дата звернення: 30.11.2023)
3. Закон України «Про інформацію» [Електронний ресурс]. Режим доступу: URL:https://zakon.rada.gov.ua/laws/show/2657-12#Text (Дата звернення: 30.11.2023)
4. Закон України «Про захист персональних даних» [Електронний ресурс]. Режим доступу: URL:https://zakon.rada.gov.ua/laws/show/2297-17#Text(Дата звернення: 30.11.2023)
5. Цивільний Кодекс України [Електронний ресурс]. Режим доступу: URL:https://zakon.rada.gov.ua/laws/show/435-15#Text (Дата звернення: 30.11.2023)
6. Закон України «Про державну таємницю» [Електронний ресурс]. Режим доступу: URL:https://zakon.rada.gov.ua/laws/show/3855-12#Text (Дата звернення: 30.11.2023)
7. Закон України «Про національну безпеку України» [Електронний ресурс]. Режим доступу: URL:https://zakon.rada.gov.ua/laws/show/2469-19/ed20180621#n24. (Дата звернення: 30.11.2023)
8. Про електронні документи та електронний документообіг [Електронний ресурс]. Режим доступу: URL:https://zakon.rada.gov.ua/laws/show/851-15#Text (Дата звернення: 30.11.2023)
9. Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс]. Режим доступу:

URL:https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (Дата звернення: 30.11.2023)

10. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. CS&CS, 2019. Issue 1(13). С.17-29.
11. Биков В., "Теоретико-методологічні засади створення і розвитку сучасних засобів та етехнологій навчання". Розвиток педагогічної і психологічної наук в Україні 1992 – 2002. Збірник наукових праць до 10–річчя АПН України . Академія педагогічних наук України. Частина 2.Харків: “ОВС”, 2002. С. 182-199.
12. Буров О., В. В. Камишин, Н. І. Поліхун, та А. Т. Ашеров, Технології використання мережевих ресурсів для підготовки молоді до дослідницької діяльності : Монографія, О. Ю. Буров, Ред. К.:тТОВ «Інформаційні системи», 2012.
13. В. Ю. Биков, та М. П. Лещенко, «Цифрова гуманістична педагогіка відкритої освіти», Теорія і практика управління соціальними системами: філософія, психологія, педагогіка, соціологія, № 4, 115-130, 2016.
14. Даник Ю. Г., Вдовенко С. Г. Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління збройних сил. Сучасні інформаційні технології у сфері безпеки та оборони, 2017. № 2(29). С. 98–107.
15. Даник Ю. Г., Супрунов Ю. М. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України. Проблеми створення, випробування та експлуатації складних інформаційних систем: збірник наукових праць. Житомир: ЖВІНАУ. 2011. Вип. 5. С. 5–22. 317
16. Даник Ю.Г., Корнейко О.В. Основи методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони України. Information Technology and Security. 2018. Том 6. № 2(11). С. 105-123
17. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ. 2016. 636 с.

18. Даник Ю. Г. Основні аспекти парадигми кібернетичної безпеки. [Електронний ресурс]. Режим доступу: URL:http://jrnl.nau.edu.ua/index.php/IMV/article/view/3171. (Дата звернення: 30.11.2023)
19. Даник Ю. Г., Катков Ю. І., Пічугін М. Ф. Національна безпека: запобігання критичним ситуаціям: монографія. Київ: МО України; Житомир: Рута. 2006. 388 с.
20. Кузьменко Б.В., Заіка Ю.О. Кібертероризм: світові й українські реалії. Науковий вісник Академії внутрішніх справ. 2012. № 2(81). С. 92-98.
21. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання «БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ». В.С. Стручок – Тернопіль: ФОП Паляниця В. А., 156 с. [Електронний ресурс]. Режим доступу: https://elartu.tntu.edu.ua/handle/lib/39196 (Дата звернення: 30.11.2023)
22. Навчальний посібник «ТЕХНОЕКОЛОГІЯ ТА ЦИВІЛЬНА БЕЗПЕКА / автор-укладач В.С. Стручок. Тернопіль: ФОП Паляниця В. А., 156 с. [Електронний ресурс]. Режим доступу: http://elartu.tntu.edu.ua/handle/lib/39424 (Дата звернення: 30.11.2023)
23. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека: соціально-правові аспекти: підручник; за заг.ред. Скулиша Є.Д.. 2010. 512 с.
24. Пінчук О., С. Г. Литвинова, та О. Ю. Буров, "Синтетичне навчальне середовище – крок до нової освіти", Інформаційні технології та засоби навчання. [Електронний ресурс]. Режим доступу: URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/1831 . (Дата звернення: 30.11.2023)
25. Різун, В. В. (2008). Теорія масової комунікації: підруч. для студ. галузі 0303 “Журналістика та інформація”. К.: Видавничий центр «Просвіта. 55.

26. Рік червоного локдауну - як COVID-19 вплинув на кібербезпеку [Електронний ресурс]. Режим доступу: URL:https://www.kaspersky.ru/blog/pandemic-year-in-infosec/30316/ (дата звернення: 30.11.2023).
27. Савчук Т., «Соціальна інженерія: як шахраї використовують людську психологію в інтернеті». [Електронний ресурс]. Режим доступу: URL: https://www.radiosvoboda.org/a/socialna-inzhenerijashaxrajstvo/29460139.html (Дата звернення: 30.11.2023)
28. Статистичні дані з усього світу [Електронний ресурс]. Режим доступу: URL: https://www.juniperresearch.com/home (Дата звернення: 30.11.2023)
29. Apau R. Youth and violent extremism online: countering terrorists exploitation and use of the Internet // African Journal on Terrorism. 2018. Vol. 7. № 1. P. 16–23.
30. B. Bystrova, “Comparative analysis of curricula for bachelor’s degree in cyber security in the USA and Ukraine”, Comparative professional pedagogy, 7(4), 114–119, 2017.
31. European Commission, Digital Single Market News, “EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity — Cybersecurity Strategy and Proposal for a Directive”, February 7, 2013.
32. Fishman B. Crossroads: Counter-terrorism and the Internet. The Texas National Security Review. 2019. № 2 (2). P. 83–100. 1.
33. Freund J., Jones J. Measuring and managing information risk. A FAIR approach: Jack Freund, Jack Jones. Oxford:Butterworth of Elsevier. 2017. 391 c.
34. Minchev Z., Bogdanoski M. Countering Terrorist Activities in Cyberspace. Amsterdam, Berlin, Washington, 2018.
35. O. Ju. Burov, «Educational Networking: Human View to Cyber Defense», Information Technologies and Learning Tools, 52, 144—156, 2016.
36. O. Burov, "Virtual Life and Activity: New Challenges for Human Factors/Ergonomics", in Symp. Beyond Time and Space STO-MP-HFM-231, STO NATO, 2014, pp. 8-1…8-8.

37. Theil S. The Online Harms White Paper: comparing the UK and German approaches to regulation // Journal of Media Law.2019. № 11 (1). P. 1–11.
38. Tucker D. What Is New about the New Terrorism and How Dangerous Is It?. Terrorism and Political Violence. 2001.№ 13 (3). P. 1–14.

ДОДАТКИ

Додаток А – Тези

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004.49+005
Віталій Кравчук, магістр спеціальності 125 - Кібербезпека
Тернопільський національний технічний університет імені Івана Пулюя

ПРОБЛЕМА ЗАХИСТУ КІБЕРПРОСТОРУ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

Vitaliy Kravchuk, master's degree in 125 – Cybersecurity

CYBERSECURITY ISSUES FOR SMALL AND MEDIUM-SIZED BUSINESSES

У сучасних реаліях важко уявити побудову успішної бізнес-моделі без кіберпростору. Компанії дедалі більше переходять на віддалену роботу, це призводить до розвитку IT-інфраструктури і водночас збільшення кількості кібератак на дану галузь.

Багато власників компаній малого і середнього бізнесу не розуміють потреби у витратах на захист компанії від кіберзагроз. Однак така ситуація триває доти, доки власник не зіткнеться з кібератакою, яка може призвести до блокування процесів і сервісів підприємства, фінансових втрат, а в гіршому випадку до повної зупинки чи втрати бізнесу [3].

Щороку експерти Міжнародної спілки електрозв'язку ООН (International Telecommunication Union) складають рейтинг країн за рівнем кібербезпеки під назвою «Глобальний індекс кібербезпеки» (Global Cybersecurity Index). У відповідній доповіді фахівці ITU оцінюють комп'ютерну безпеку всіх країн світу за п'ятьма параметрами: юридична, технічна, організаційна підготовленість, готовність до співпраці, розвиток освітнього та дослідницького потенціалу країни. Найбільш актуальна версія дослідження була випущена у 2020 році. За кількістю кібератак Україна знаходиться на 86-у місці у світі [1].

З вище написаного ми можемо зробити висновок, що найчастіше проблеми та загрози зустрічаються у малому та середньому бізнесі. Серед них:

Незахищеність периметру. Неналаштований мережевий захист, неналаштований захист серверів і кінцевих пристроїв, відсутність систем моніторингу та системи резервного копіювання рано чи пізно призводить до злому IT-інфраструктури.

Незахищеність інформації та баз даних. Бухгалтерська інформація, фінансова інформація, звіти до контролюючих органів, база даних клієнтів, листування з важливими клієнтами або партнерами, особиста конфіденційна інформація тощо.

Незахищеність каналів передачі. Більшість компаній нині потребує доступу до своєї IT-інфраструктури 24/7 з будь-якої точки світу. Для ефективної роботи необхідний швидкий, безпечний канал передачі інформації. Це розуміють керівники, а також зловмисники, тому часто замість атаки на IT-інфраструктуру вибирають атаку на канали передачі інформації.

Неналежний антивірусний захист. Комп'ютерний вірус - вид шкідливих програм, здатних впроваджуватися в код інших програм, системні області пам'яті, завантажувальні сектори та розповсюджувати свої копії різноманітними каналами зв'язку.

Основна мета вірусу – його поширення. Крім того, часто його супутньою функцією є порушення роботи програмно-апаратних комплексів — видалення файлів, видалення операційної системи, непридатність структур розміщення даних, порушення працездатності мережевих структур, крадіжка особистих даних, вимагання, блокування роботи користувачів тощо[4].

Щодня з'являються нові комп'ютерні віруси, виконують певні завдання: від простих – збирання інформації, до складніших процесів – шифрування інформації або використання шкідливих дій.

Неналежний захист сайту. Говорять, якщо вас немає в інтернеті, вас немає у бізнесі. Сайт – це обличчя і вітрина компанії, нікому не хочеться втратити обличчя.

Неналежний захист програм і додатків. Пошта, месенджери, інші програми, які використовують для роботи та спілкування з клієнтами. Якщо програми і канали спілкування зламають, отримають з них конфіденційні дані та почнуть розсилати через них шкідливу інформацію, це може призвести до втрати репутації, коштів, а іноді й клієнтів.

У результаті всіх вищезазначених загроз є ризик втрати дуже важливих даних (sensitive data). Sensitive data - дуже важливі дані, такі як: персональні дані користувачів; банківські та медичні дані; паролі; інформація про фінансові операції тощо. [2] Саме за ними, як правило, полюють хакери, прогнози їх втрат досить великі.

Аби запобігти втраті даних треба ідентифікувати ризики і загрози та почати працювати над запровадженням кіберзахисту компанії. Ідентифікація ризиків і загроз починається з аналізу вразливості підприємства. Параметри аналізу формуються під кожну компанію індивідуально, як правило, проходять у таких напрямках: аудит інформаційних потоків, аудит баз і середовища зберігання, права доступу до інформації, кіберзагроз, мережі, серверів, програм, сервісів, додатків і робочих місць кінцевих користувачів. За результатами перевірки формується звіт, на основі якого будується проект захищеної IT-інфраструктури [5].

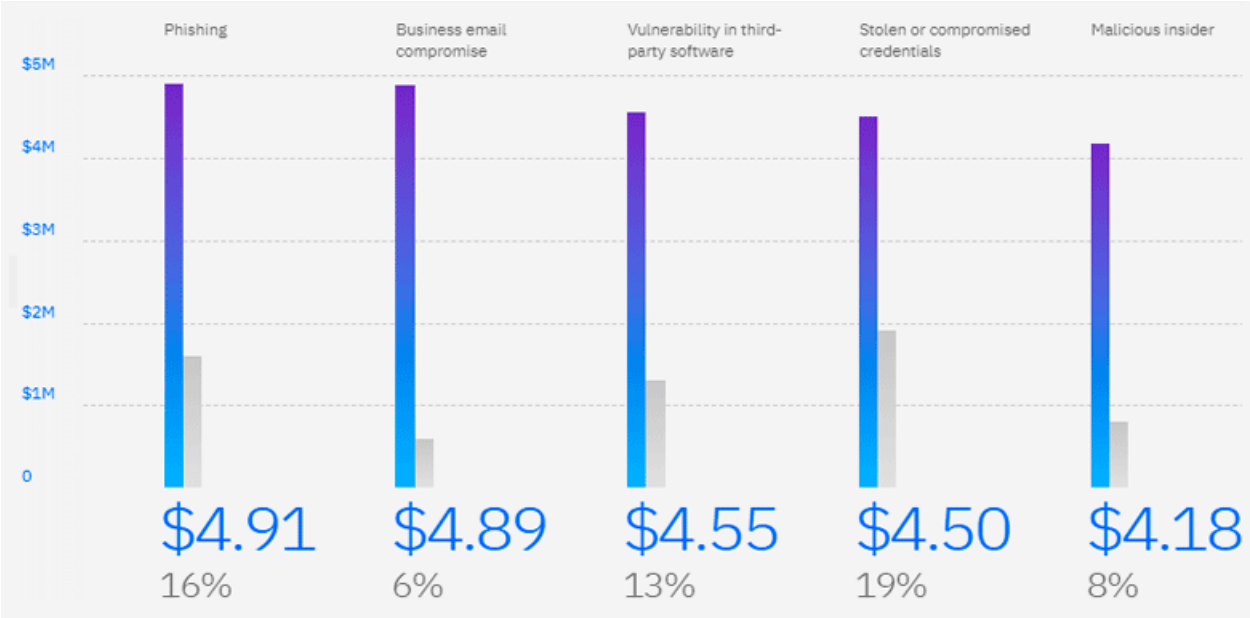
Таким чином, безпечне функціонування бізнесу залежить від системи захисту даних, яка впроваджена на підприємстві. Щорічна статистика показує, що кількість кібератак у світі зростає, від чого несе збитки бізнес-сектор. Якщо компанія прагне стійко зростати, треба визначити потенційні ризики та загрози і почати розробку заходів для підвищення кібербезпеки.

Література

1. https://nonews.co/directory/lists/countries/cybersecurity-index
2. https://www.dataprivacyframework.gov/s/article/1-Sensitive-Data-dpf
3. Pescatore J. SANS 2021 Top New Attacks and Threat Report [Електронний ресурс] / John Pescatore. – 2021. – Режим доступу до ресурсу: https://fs.hubspotusercontent00.net/hubfs/8645105/white-paper/sans-attack-threatreport-2021.pdf.
4. Дубов, Дмитро Володимирович. "Стратегічні аспекти кібербезпеки України." Стратегічні пріоритети 4 (2013): 29.
5. Гриник, Р. О. Дослідження проблем захисту сучасного кіберпростору України / Р. О. Гриник, М. В. Маржан // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 30–31.

Додаток Б – Кількість кібератак у світі

Додаток В - Середня вартість витоку даних від кібератак у розрізі галузей



Додаток Г - Викрадені або скомпрометовані облікові дані коштують дорого