МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри кібербезпеки

_____Анна ІЛЬЄНКО
"_____"_____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ "МАГІСТР"

Тема: Методи забезпечення захисту інформації та операційної скритності в кіберпросторі

Виконавець: Олексій ЧЕБАН

Керівник: д.т.н., професор Сергій ТОЛЮПА

Нормоконтролер: к.т.н., доцент Андрій ПЕТРЕНКО

Київ 2024

ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Факультет комп'ютерних наук та технологій
Кафедра кібербезпеки
Освітній ступінь магістр
Спеціальність 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки

_____Анна ІЛЬЄНКО
«30»___08_____2024 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Чебана Олексія Георгійовича

1. Тема кваліфікаційної роботи «Методи забезпечення захисту інформації та операційної скритності в кіберпросторі» затверджена наказом ректора 30.08.2024 № 1695/ст.

2. Термін виконання роботи: з 30.08.2024 по 15.12.2024.

3. Вихідні дані до роботи: проаналізувати технології атаки у кіберпросторі на особовий склад, основні елементи організації безпеки інформаційного простору; визначити вимоги до механізмів індивідуального захисту особового складу; розробити методи забезпечення захисту інформації та операційної скритності в кіберпросторі в умовах війни.

4. Зміст пояснювальної записки: (перелік усіх розділів) кіберпростір, кібербезпека, нормативна складова кібербезпеки; технічний захист інформації: методи та засоби; практичні поради та методи з операційної секретності та захисту інформації.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: презентація.

6. Календарний план-графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1.	Уточнення постановки задачі	30.08.2024 – 05.09.2024	*Виконано*
2.	Збір інформації	06.09.2024 – 15.09.2024	*Виконано*
3.	Нормативно-правова складова кібербезпеки	16.09.2024 – 25.09.2024	*Виконано*
4.	Розробка методів та засобів захисту інформації та операційної секретності	26.09.2024 – 02.10.2024	*Виконано*
5.	Оформлення роботи	03.10.2024 – 25.10.2024	*Виконано*

7. Дата видачі завдання: 30.08.2024

Керівник кваліфікаційної роботи: _____ Сергій ТОЛЮПА

(підпис керівника)

Завдання прийняв до виконання: _____ Олексій ЧЕБАН

(підпис здобувача вищої освіти)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Методи забезпечення захисту інформації та операційної скритності в кіберпросторі»: 101 с., 29 рис., 2 табл., 3 формули, 45 літературних джерела.

Об’єкт дослідження: методи, які захищають інформацію, що становить таємницю або іншу критичну інформацію, а також інформацію, що може стати такою при поєднані та аналізу некритичної інформації, і особисту інформацію суб’єктів теж.

Предмет дослідження: сучасні методи індивідуального захисту військовослужбовців у кіберсфері.

Мета кваліфікаційної роботи: удосконалення існуючих методів забезпечення захисту інформації та операційної скритності в кіберпросторі, доповнюючи їх підходом з індивідуального захисту суб’єктів.

Методи дослідження: для вирішення завдання проведено дослідження результатів атак агентів російської федерації на колишніх та дійсних військовослужбовців України з 2014 по 2023 роки. Шляхом ітераційної розробки було розроблено концепцію індивідуального захисту військовослужбовців у кіберсфері.

Практична цінність: для індивідуального захисту військовослужбовців розроблені методи захисту інформації у кіберпросторі та від радіоелектронної розвідки.

Наукова новизна: новизна цієї роботи є новітня концепція індивідуального захисту військовослужбовців за рахунок комплексного підходу покращує існуючі методи кіберзахисту..

Результати кваліфікаційної роботи рекомендується використовувати –

КІБЕРБЕЗПЕКА, ОПЕРАЦІЙНА СЕКРЕТНІСТЬ, ВВЕДЕННЯ В ОМАНУ, ЗАХИЩЕНІСТЬ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЕОМ	–	електронна обчислювальна машина
ЗІ	–	захист інформації
ІКТ	–	інформаційно-комунікаційна технологія
ІБ	–	інформаційна безпека
ІТ	–	інформаційна технологія
ІР	–	інформаційний ресурс
ІТС	–	інформаційно-телекомунікаційна система
ІС	–	інформаційна система
КСЗІ	–	комплексна система захисту інформації
НСД	–	несанкціонований доступ
ОС	–	операційна система
ПЗ	–	програмне забезпечення
СЗІ	–	система захисту інформації
ТЗІ	–	технічний захист інформації
OSINT	–	open source intelligence (розвідка з відкритих джерел)
GEOINT	–	geospatial intelligence (геопросторова розвідка)
ЛБЗ	–	лінія бойового зіткнення
КСП	–	командно-спостережний пункт
РЕР	–	радіоелектронна розвідка
VPN	–	virtual private network (приватна віртуальна мережа)
OPSEC	–	operational security (операційна секретність)
EEFI	–	essential elements of friendly information (важливі елементи дружньої інформації)

ВСТУП

Робота є складовою більшого проекту – посібника з індивідуальної та колективної інформаційної безпеки військовослужбовців і малих підрозділів, автором якого є я та мій побратим (його ім'я не вказую на його прохання).

В умовах триваючої збройної агресії російської федерації проти України безпека людини, суспільства і держави суттєво залежать від надійного функціонування об'єктів критичної інфраструктури. Крім фізичних впливів на такі об'єкти летальною зброєю, російська федерація не полишає спроб разом зі своїми сателітами впливати нелетальними засобами -– кіберзброєю на системи управління об'єктів критичної інфраструктури через кіберпростір та з кіберпростору. Враховуючи транскордонність кіберпростору та високий рівень інформатизації об'єктів критичної інфраструктури як в Україні, так і у світі, наприклад, об'єктів ядерної енергетики (Запорізька та Чорнобильська атомні станції) та об'єктів водопостачання (Каховська та Київська ГЕС), систем управління військами та зброєю (Єдиної автоматизованої системи управління Збройними Силами України (ЄАСУ ЗСУ) та її складових) тощо, ризики масштабуються не тільки на національний безпековий вимір, а й становлять загрозу для людства на глобальному рівні на досяжну перспективу. Ситуація ускладнюється тим, що об'єкти критичної інфраструктури, які функціонують в єдиному інформаційному просторі й підтримують широкий спектр сучасних інформаційних технологій, всупереч колосальним зусиллям протидії стороннім втручанням з кіберпростору та через кіберпростір, й надалі залишаються вразливими до загроз нового типу. Після повномасштабного вторгнення російських військ на територію України бойові дії в нашій країні ведуться не лише на передовій. Війна охопила всі аспекти життєдіяльності.

Аналізування інформаційного простору свідчить, що інформаційна війна ведеться з задіянням колосальних ресурсів, фінансування, використовуються всі

можливі методи, технології, зрадники, агентура. Вона здійснює атаки на всіх рівнях: інформаційному, когнітивному, кіберпросторі.

Від 2022 року дотепер кількість кібератак на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури зросла щонайменше втричі [1].

Інформаційні операції рф спрямовані на дискредитацію, дезорганізацію, підрив іміджу та дестабілізацію нашої держави. Збройній агресії передували активні неконвенційні заходи противника, інтенсивність яких не знизилася, а навпаки має тенденцію до зростання. Ба більше, недобросовісне використання інформаційного простору всередині держави призводить до зниження рівня внутрішньої інформаційної безпеки, прямим наслідком чого є дестабілізація соціально-політичної обстановки, спротив прийняттю тих чи інших державних рішень, погіршується ситуація із забезпеченням збереження державної таємниці [2].

Інформація стала ефективною зброєю сучасної війни, багатьом успішним операціям, ударам, штурму передувала інформаційна підготовка, і успішність будь-якої операції можливо прогнозувати від якості системи отримання, обробки та захисту інформації.

Немає сумнівів, що захист критично важливих для інформаційних систем масивів повинен відповідати міжнародним, корпоративним, нормативним і методичним документам. Застосовуються високовартісні технічні засоби і впроваджуються суворо регламентовані організаційні заходи. Однак немає відповіді на найважливіше запитання -– наскільки рішення, яке пропонується або реалізовується, є правильним, яка його запланована і реальна ефективність.

Нерідко замовник СЗІ погано уявляє значення того чи іншого засобу і його необхідність в загальному рівні безпеки, тому в результаті збільшуються витрати за практичної невизначеності досягнутого ефекту. Замовник СЗІ не отримує те, що йому реально потрібно, і не може об'єктивно перевірити і оцінити якість і ефективність запропонованого рішення.

Не дивлячись на роль технологій, головним чинником ризику і джерелом інформації є людина.

Нині більшість з тих, хто залучений до складу сил безпеки і оборони України, не в повному обсязі розуміють існуючі кіберзагрози та потенційно можливі негативні наслідки, які можуть створити небезпеку життєво важливим інтересам громадян, суспільства і держави в цілому під час користування особистими пристроями. Результат такого ставлення – трагічна кількість втрачених життів та можливостей.

На жаль, не всі військовослужбовці можуть самостійно забезпечити безпечне налагодження та експлуатацію тих чи інших додатків / застосунків, програмного забезпечення, набору інструментів, технологій та захистити особисті (службові) дані від несанкціонованого доступу.

Отже, для збереження життя на полі бою необхідно знати і дотримуватися певних вимог і правил користування особистими пристроями та відповідним програмним забезпеченням.

Актуальність теми. Зважаючи на ведення російською федерацією терору проти військовослужбовців, починаючи з залякування в соціальних мережах, закінчуючи спробами фізичного знищення, використовуючи агентуру. Ця робота має велику актуальність для застосування як військовослужбовцями так і волонтерам, громадьско-активних осіб.

Метою роботи є удосконалення існуючих методів забезпечення захисту інформації та операційної скритності в кіберпросторі, доповнюючи їх підходом з індивідуального захисту суб'єктів.

Об'єктом роботи є методи, які захищають інформацію, що становить таємницю або іншу критичну інформацію, а також інформацію, що може стати такою при поєднані та аналізу некритичної інформації, і особисту інформацію суб'єктів теж.

Суб'єкт роботи – носій інформації: військовослужбовець, члени його сім'ї.

Наукова новизна – новизна цієї роботи є новітня концепція індивідуального захисту військовослужбовців за рахунок комплексного підходу покращує існуючі методи кіберзахисту.

Практична значущість роботи – для індивідуального захисту військовослужбовців розроблені методи захисту інформації у кіберпросторі та від радіоелектронної розвідки.

РОЗДІЛ 1
КІБЕРПРОСТІР, КІБЕРБЕЗПЕКА. НОРМАТИВНА СКЛАДОВА КІБЕРБЕЗПЕКИ

1.1. Захищений кіберпростір – запорука успішного розвитку країни. Нормативно-правове забезпечення кібербезпеки

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету здійснюватиметься шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному кіберпросторі [3].

Кіберпростір дедалі частіше розглядається як одна із потенційних арен військових дій нарівні з традиційними фізичними просторами. Активно розвивається практика створення кібервійськ, які виконують не лише завдання із захисту критично важливої інформаційної інфраструктури від атак, а й здійснюють превентивні наступальні дії. Це передбачає виведення з ладу важливих об’єктів інфраструктури противника завдяки знищенню чи порушенню роботи інформаційних систем, які забезпечують їхню діяльність.

російська федерація є однією з основних загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, основану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України [3].

Постійно зростає технічна складність кіберзагроз: створюються нові методи й інструменти для здійснення атак. Кібератаки дедалі частіше використовуються як елемент інформаційних операцій, спрямованих на маніпулювання суспільною думкою чи втручання у виборчі процеси, що підкреслює їхню важливість у сучасних конфліктах. Структурно національну систему кібербезпеки представлено на рис. 1.1.

Рис. 1.1. Загальна структура національної системи кібербезпеки

Кіберпростір дедалі частіше стає інструментом терористичних організацій, і масштаби його використання швидко зростають. Основними мішенями кібертероризму залишаються об'єкти атомної енергетики, системи електро- та водопостачання, електронні комунікації, фінансова та банківська сфери, транспортна інфраструктура (авіація й залізниця), стратегічні сховища сировини, а також хімічні та біологічні об'єкти.

Стратегія ґрунтується на положеннях Конституції України, Законів України «Про національну безпеку України» та «Про основні засади забезпечення кібербезпеки України» (рис. 1.2), Конвенції про захист прав людини і основоположних свобод, Конвенції про кіберзлочинність, Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 р. № 392, Концепції боротьби з тероризмом в Україні, затвердженої Указом Президента України від 5 березня 2019 р. № 53 інших нормативно-правових актів [3-5]. Перспективні напрями розвитку системи кібербезпеки показано на рис. 1.3.

Перелік викликів та кіберзагроз національному кіберпростору, а також чинники, які є загрозами кібербезпеці України представлено на рис 1.4 та рис 1.5.

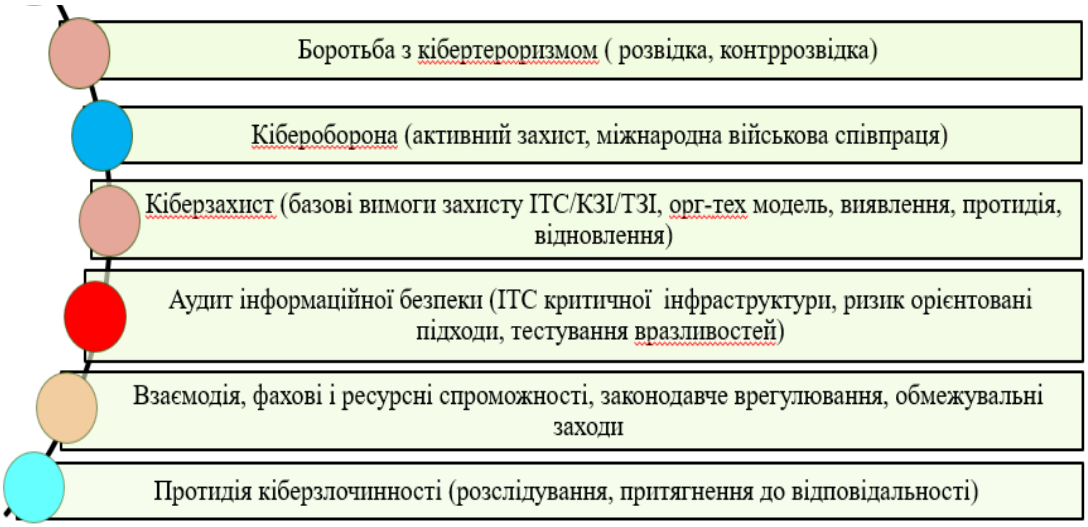

Рис. 1.2. Основні напрями реалізації закону

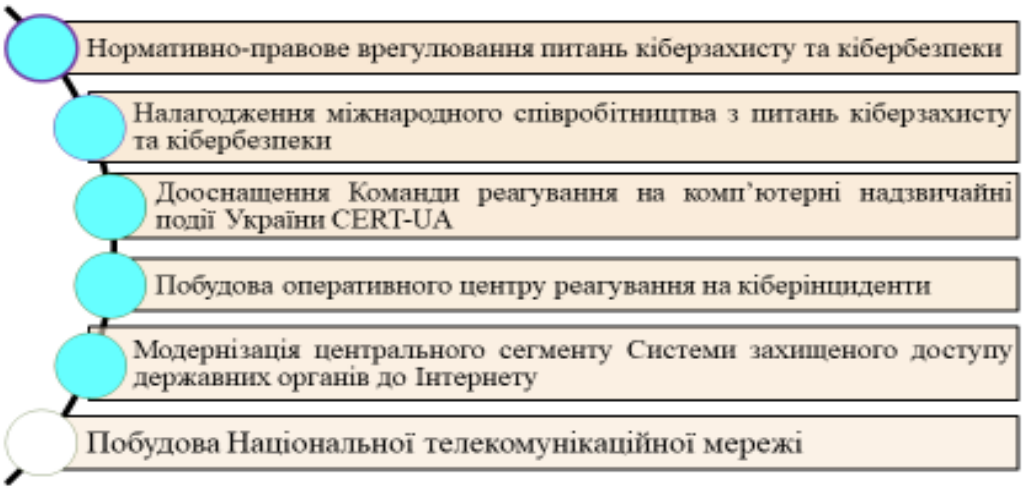

Рис. 1.3. Перспективні напрями розвитку системи кіберзахисту

Рис. 1.4. Виклики та кіберзагрози національному кіберпростору

Рис. 1.5. Системні кіберзагрози національній безпеці

1.2. Організаційно-технічна модель захисту кіберпростору

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, національну систему кібербезпеки, повноваження суб'єктів забезпечення кібербезпеки та засади координації [5].

Одним із ключових напрямів забезпечення функціонування національної системи кібербезпеки, передбачених законодавством, є створення її організаційно-технічної моделі (ОТМ). Ця модель розроблена Держспецзв'язку на основі багаторічного досвіду реалізації норм і положень закону, побудови національної системи кібербезпеки, аналізу міжнародних підходів до кіберзахисту та взаємодії з іншими суб'єктами у цій сфері.

Положення про ОТМ містить опис місії, структури, механізму роботи та цілей моделі, а також вводить визначення ключових понять, таких як сили та засоби кіберзахисту, команди реагування на кіберінциденти, кібергігієна. Архітектура ОТМ побудована на багаторівневому підході й має три взаємопов'язані інфраструктури.

ОТМ є системою заходів і інструментів, спрямованих на ефективне реагування на кіберзагрози, мінімізацію вразливостей комунікаційних систем і запобігання інцидентам. Вона дозволяє консолідувати зусилля всіх суб'єктів кібербезпеки, забезпечуючи захист національних інформаційних ресурсів, кіберстійкість критичної інфраструктури та стабільну роботу інформаційних систем як державного, так і приватного секторів.

ОТМ кіберзахисту має організаційно-керуючу, технологічну та базисну інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки [6]. Такий опис ОТМ зручніше навести у вигляді певної архітектури (рис.1.6.), яка являє собою структуровану систему. Архітектура ОТМ демонструє цілісність системи кіберзахисту, де всі рівні й інфраструктури тісно взаємодіють, доповнюючи один одного.

1.3. Кіберпростір і кібербезпека – головні ознаки нової інформаційної цивілізації

Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» кіберпростір – середовище (віртуальний простір), яке надає

можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [5].

Отже, найбільш відмінними ознаками кіберпростору як субстанції, створенню якої передусім сприяли зміна характеру діяльності людини з прийняття рішень, впровадження електронно-цифрових форм створення, обробки, зберігання і переміщення інформації, перехід від паперового діловодства до електронного тощо, переважна *більшість фахівців вважає* його неперевершені можливості зі створення численних зв'язків між окремими індивідуумами і соціальними групами та з надання різнопланових інформаційних послуг [7]. З урахуванням характерних рис кіберпростору як сфери вчинення заздалегідь спланованих деструктивних дій на кшталт проникнення до ІТС один одного, блокування або виведення з ладу їх найбільш уразливих елементів, дезорганізації оборонних автоматизованих систем управління (АСУ) протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд з наземною, морською й повітряно-космічною сферами) та так званого своєрідного містку між такими поняттями як Internet і кібернетика це також дає можливість:

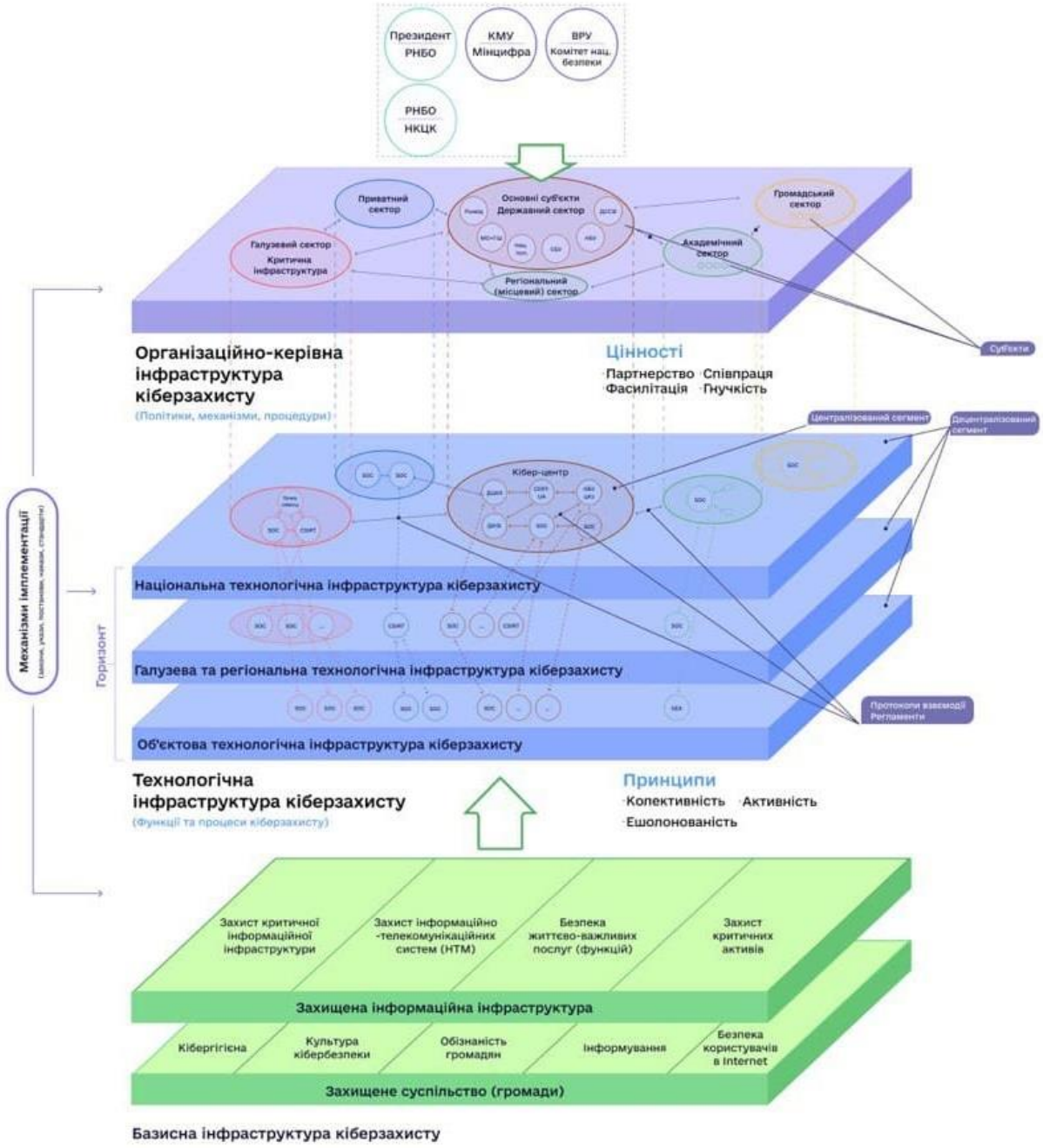

Рис. 1.6.Архітектура організаційно-технічної моделі кіберзахисту кіберпростору

виділити в ньому систему певних відносин між суб'єктами та об'єктами інформаційної й кібернетичної інфраструктури;

виокремити злочини, втручання і загрози, пов'язані з особливостями існування та передачі інформації;

визначитися з його можливими дійовими особами (рис. 1.7);

розглядати його з позицій власне віртуального і реального (електронного, комунікаційного, кібернетичного, інформаційного, особливого психологічного) тлумачення як додатковий вимір бойового простору, розрізняючи водночас фізичний (інфраструктура, кабелі та роутери), семантичний (дані) і синтаксичний (протоколи передачі даних) рівні тощо.

ІБ у найбільш загальному вигляді може бути визначена як *стан захищеності інформаційного простору держави, за якого неможливе нанесення збитку властивостям об'єкта безпеки, зумовленим інформацією та інформаційною інфраструктурою та який забезпечує формування, використання і розвиток національної інфосфери в інтересах оборони* (рис. 1.7).

Рис. 1.7. Структура поняття «Інформаційна безпека»

Характерними ознаками, які нині уособлюють поняття кібербезпеки, є: стан захищеності кіберпростору держави в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим,

корпоративним та/або національним інтересам; є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо IP, ІКТ і ІТС (рис. 1.8).

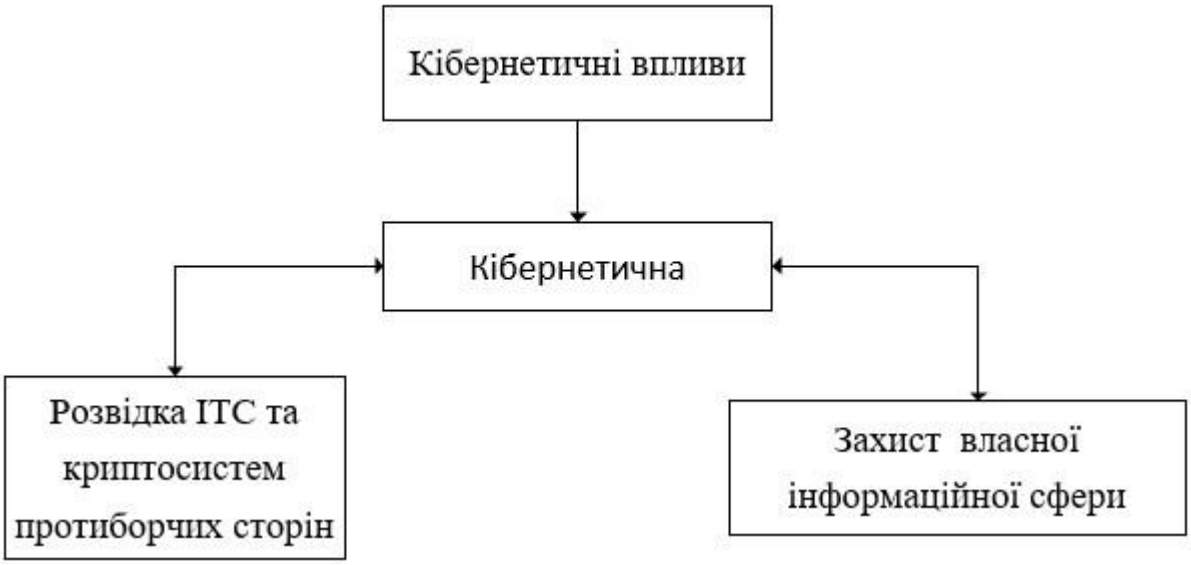

Рис. 1.8. Складові кібернетичної безпеки

Комплексна сутність кібербезпеки за таких умов може бути виражена схемою, поданою на рис. 1.9.

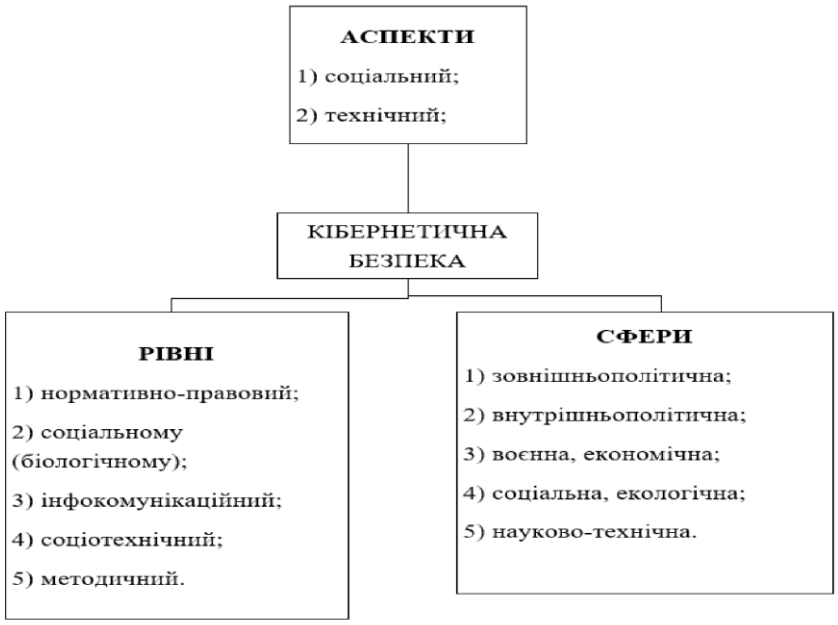

Рис. 1.9. Сутність кібернетичної безпеки

Водночас проблемами забезпечення кібернетичної безпеки нині є:

- відсутність чіткого усвідомлення ролі та значення кібербезпекової складової у системі забезпечення національної безпеки держави;
- дифініційна, термінологічна та нормативно-правова невизначеність у сфері кібербезпеки;
- залежність держави від програмних та технічних продуктів іноземного виробництва;
- відсутність належної координації діяльності відповідних відомств та як наслідок неузгодженість дій зі створення окремих елементів системи кібербезпеки;
- складнощі із методичним забезпеченням та кадровим наповненням відповідних структурних підрозділів.

Висновки до розділу 1

У першому розділі цієї роботи розглянуто такий важливий аспект як нормативно-правове підґрунтя кібербезпеки, детально описано сутність Стратегії кібербезпеки, розглянуто Закон України «Про основні засади забезпечення кібербезпеки України», на основі якого та свого багаторічного досвіду Держспецзв'язок розробив ОТМ кібербезпеки. Також досліджено, що таке кіберпростір, визначено його можливі дійові особи, розкрито комплексну сутність кібернетичної безпеки.

РОЗДІЛ 2
ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ: МЕТОДИ ТА ЗАСОБИ

Сучасний багатосторонній аналіз результатів творчих і практичних робіт дає вагомі підстави стверджувати, що на часі є як об'єктивна необхідність, так і об'єктивні передумови раціональної реалізації Концепції технічного захисту інформації, що дозволить забезпечити необхідний рівень захищеності інформації, без чого не можуть бути вирішені актуальні проблеми інформатизації суспільства [8].

Захист інформації (ЗІ) – це комплекс організаційно-технічних заходів, спрямованих на забезпечення оптимального рівня надійності інформації, які містять захист даних на всіх етапах: її формування, передачі, прийому, обробки, накопичення і використання з метою забезпечення необхідної надійності.

Надійність інформації визначається як інтегральний показник, що охоплює три ключові аспекти:

- фізична цілісність – це збереження структури даних без перекручень чи знищення елементів;
- довіра до інформації – забезпечення її захисту від підміни чи несанкціонованих модифікацій при збереженні цілісності;
- безпека інформації – запобігання несанкціонованому доступу до даних осіб, які не мають відповідних повноважень.

2.1. Класифікація засобів захисту інформації

ЗІ охоплює різноманітні аспекти, які можна умовно розділити на кілька груп залежно від типів загроз і порушень у роботі системи. До цих груп належать морально-етичні, правові, адміністративні, технічні та програмні заходи. Проте межі між ними часто є розмитими, адже сучасні технології нерідко поєднують програмні та апаратні методи для підвищення ефективності.

Морально-етичний підхід базується на правилах поведінки, які формуються із розвитком інформаційних технологій. Ці норми можуть бути як неформальними, так і закріпленими у статутах, наприклад, у вигляді Кодексу професійної поведінки членів Асоціації користувачів ЕОМ США [9]. Їх дотримання підтримує авторитет особи чи організації, навіть якщо не є юридично обов'язковим.

Правові засоби захисту забезпечують регулювання доступу до інформації через закони, укази та нормативні акти. Вони охоплюють питання авторських прав, відповідальності за порушення правил роботи з інформацією та інші аспекти, що стосуються використання інформаційних технологій.

Організаційні заходи, які часто називають адміністративними, стосуються правил функціонування систем і управління їхніми ресурсами. Вони регламентують діяльність користувачів і персоналу для запобігання порушенням безпеки. Ці заходи нерідко застосовуються разом із технічними та програмними інструментами, проте надмірне навантаження адміністративними процедурами може знизити загальний рівень безпеки, якщо користувачі ігнорують складні інструкції.

Фізичні засоби захисту покликані протидіяти загрозам через використання механічних, електронних або електромеханічних пристроїв. Вони захищають інформацію від фізичних загроз, таких як крадіжка, поломки чи стихійні лиха, і часто інтегруються з програмними засобами для підвищення ефективності.

Програмні рішення охоплюють такі заходи, як ідентифікація користувачів, управління доступом, реєстрація дій у системі, криптографічний захист і захист від вірусів. Їхнє завдання полягає в тому, щоб зробити інформацію максимально захищеною на всіх етапах її використання.

Отже, інтеграція різних методів і підходів забезпечує створення багаторівневої системи захисту, що відповідає сучасним викликам і загрозам у сфері інформаційної безпеки.

2.2. Модель порушника

Модель порушника – абстрактний формалізований або неформалізований опис порушника в автоматизованій системі [10].

2.2.1. Поняття порушника інформаційної безпеки

Порушники це особи, які реалізують загрози інформаційній безпеці, проте варто розмежовувати терміни «порушник» та «зловмисник». Порушник може діяти неусвідомлено, наприклад, через недбалість або недостатні знання, тоді як зловмисник діє цілеспрямовано з наміром завдати шкоди.

Аналізування загроз завершується створенням моделі загроз – структурованого опису, який дозволяє систематизувати можливі ризики. Відповідно до нормативних актів України, зокрема Типового положення про службу захисту інформації в автоматизованій системі, загрози класифікуються за їх впливом на ключові властивості інформації та автоматизовані системи (АС):

- конфіденційність – запобігання несанкціонованому доступу до даних;
- цілісність – збереження достовірності й незмінності інформації;
- доступність – забезпечення можливості доступу до інформації у потрібний час;
- спостережність і керованість АС – контроль і управління системою безпеки.

Ключові загрози безпеці інформації можна поділити на три основні категорії залежно від порушення властивостей:

загрози конфіденційності:

- крадіжка або копіювання інформації й засобів її оброблення;
- втрата або витік інформації, зокрема ненавмисний;

загрози доступності:

- блокування доступу до даних;
- знищення інформації чи засобів її оброблення;

загрози цілісності:

- модифікація або спотворення даних;
- підміна автентичної інформації чи нав’язування фальшивої.

Розуміння природи походження цих загроз і їх класифікація дозволяють ефективніше формувати заходи захисту, спрямовані на збереження конфіденційності, цілісності й доступності інформації, а також на забезпечення стабільного функціонування АС.

Модель порушника є структурованим описом потенційних осіб, які можуть завдати шкоди інформаційній системі, і використовується спільно з моделлю загроз для побудови ефективної політики інформаційної безпеки. Нормативними актами України визначено кілька ключових параметрів моделі порушника.

До категорій порушників належать як внутрішні, так і зовнішні суб’єкти. Внутрішніми порушниками можуть бути користувачі, інженерний склад, працівники відділів супроводу програмного забезпечення, технічний персонал, служба безпеки чи навіть керівники. Зовнішні порушники, своєю чергою, включають сторонніх осіб, які не мають безпосереднього доступу до системи, але можуть здійснювати атаки дистанційно або через фізичний доступ.

Мета дій порушника може варіюватися від отримання конфіденційної інформації до внесення змін у дані чи структуру системи. Деструктивні цілі, такі як знищення інформаційних і матеріальних активів, також є поширеними.

Рівень доступу порушника до системи визначає його повноваження. Вони можуть містити запуск фіксованих задач, створення і використання власних програм, внесення змін у конфігурацію системи або підключення нових апаратних засобів.

Технічна оснащеність порушника є важливим фактором аналізування. Вона може містити доступ до апаратних, програмних і спеціальних інструментів, які значно підвищують його можливості.

Припущення про кваліфікацію порушника завжди ґрунтуються на рівні знань і навичок, оскільки це дозволяє створити максимально захищену систему, готову протистояти навіть найскладнішим загрозам.

Розуміння моделі порушника дає змогу передбачити потенційні дії зловмисників і забезпечити адекватний захист критичних систем та інформації, враховуючи усі можливі сценарії загроз.

Наведемо спрощену класифікацію, яка відображає найбільш типові атаки на розподілені автоматизовані системи. Ця класифікація запропонована Пітером Меллом (Peter Mell) [11].

Віддалене проникнення (remote penetration). Атаки, які дозволяють реалізувати віддалене керування комп'ютером через мережу.

Локальне проникнення (local penetration). Атака, що призводить до отримання несанкціонованого доступу до вузла, на якому вона ініційована.

Віддалена відмова в обслуговуванні (remote denial of service). Атаки, що дозволяють порушити функціонування системи або перезавантажити комп'ютер через мережу (в тому числі через Інтернет).

Локальна відмова в обслуговуванні (local denial of service). Атаки, що дозволяють порушити функціонування системи або перезавантажити комп'ютер, на якому вони ініційовані. Приклади атак цього типу: аплет, що перезавантажує процесор (наприклад, відкриттям великої кількості вікон великого розміру), що призводить до неможливості обробки запитів інших програм.

Сканування мережі (network scanning). Аналіз топології мережі і активних сервісів, що доступні для атаки. Атака може здійснюватися за допомогою службового програмного забезпечення.

Використання сканерів вразливостей (vulnerability scanning). Сканери вразливостей призначені для пошуку вразливостей на локальному або віддаленому комп'ютері. Вони насамперед призначені служити діагностичним інструментом системних адміністраторів, але можуть бути використані і як зброя

для розвідки й атаки. Найвідоміші з таких програмних засобів: SATAN, SystemScanner, Xspider, nessus.

Злом паролів (password cracking). Для цього використовуються програмні засоби, що підбирають паролі користувачів. Залежно від надійності системи зберігання паролів, можуть використовуватися методи зламу або підбору пароля за словником.

Аналіз протоколів (sniffing – прослуховування трафіку). Пасивна атака, яка спрямована на розкриття конфіденційних даних, зокрема, ідентифікаторів і паролів доступу.

До цієї класифікації не потрапили численні атаки, що спрямовані на введення в оману протоколів пошуку в мережі, тому можна додати також підміну об'єкта (spoofing). Типові приклади: несправжній DNS-сервер, підміна IP-адреси джерела (IP spoofing), несправжній ARP-запит (ARP spoofing).

Перші чотири класи атак розрізняються здебільшого по кінцевому результату (або меті реалізації), а наступні – способу їх здійснення.

Побудова моделі порушника

Інформаційні ресурси (ІС) у розподіленні бази даних та знань передусім є привабливими з точки зору розташованої на них інформації не тільки для авторизованих користувачів ІС, а також для окремих осіб або певних груп осіб, які прагнуть бути її користувачами. Ця привабливість зумовлена характером і обсягом інформації, що вводиться, обробляється, зберігається й циркулює в ІС [12].

Особа, яка намагається отримати несанкціонований доступ до ресурсів ІС для ознайомлення, модифікації, знищення або зміни режимів роботи системи класифікується як порушник. Дії таких осіб можуть бути як ненавмисними, що виникають через помилки або недбалість, так і зловмисними, коли доступ здійснюється свідомо і з метою завдання шкоди.

Особливу загрозу становлять зловмисні порушники, які діють під впливом кримінальних угруповань, комерційних структур, політичних організацій чи

навіть іноземних спецслужб. Такі особи прагнуть отримати дані для подальшого використання у власних інтересах, модифікації інформації, знищення даних чи досягнення інших переваг для себе, своїх партнерів або для ослаблення конкурентів.

Зловмисники можуть бути як внутрішніми, тобто особами, які мають доступ до системи (працівники, користувачі), так і зовнішніми – сторонніми особами, що перебувають поза межами контрольованої зони, або такими, що проникли до неї незаконним шляхом. Внутрішні порушники мають більший потенціал для завдання шкоди через їхній легітимний доступ до ресурсів системи, тоді як зовнішні зазвичай покладаються на технологічні методи злому.

Розуміння мотивів і характеру дій таких порушників є ключовим для створення ефективних систем захисту, що здатні запобігти потенційним загрозам як з боку недбалих користувачів, так і цілеспрямованих зловмисників.

2.2.2. Можливості порушника

За рівнем можливостей, які надаються штатною інфраструктурою інформаційної мережі, виділяють чотири рівні порушників. Класифікація ієрархічна, тобто кожний наступний рівень містить у собі функціональні можливості попереднього рівня [12]:

- перший рівень, відповідає найбільш низькому рівню можливостей порушника у системі – можливістю запуску фіксованого набору програм, які реалізують певні функції з обробки інформації;
- другий рівень, визначається можливістю створення й запуску власних програм з новими функціями обробки і подальшого одержання потрібної порушнику інформації;
- третій рівень, визначається можливістю управління функціонуванням ІС, тобто впливом на базове програмне забезпечення системи, а також на склад і конфігурацію технічного забезпечення інформаційної системи;

- четвертий рівень, визначається інтегрованим обсягом можливостей працівників, які здійснюють розробку, впровадження й експлуатацію технічних засобів інформаційної системи, а також можливістю введення до складу ІС власних технічних засобів з новими функціями, щодо обробки і отримання інформації.

Ступінь ризику

Персонал ІС відіграє різну роль у її функціонуванні, що безпосередньо впливає на ступінь ризику, пов'язаний із можливістю реалізації загроз або нанесення шкоди системі. Розподіл ризиків здійснюється відповідно до функцій і рівня доступу працівників до критичних ресурсів системи:

- найбільший ризик мають ті працівники, які володіють найширшими повноваженнями та доступом до ключових елементів системи. До них належать системні адміністратори, адміністратори баз даних і адміністратори безпеки. Вони мають прямий доступ до конфігурацій системи, що дає їм змогу модифікувати, видаляти або впливати на роботу критичних даних;
- високий ризик пов'язаний із працівниками, які здійснюють безпосередню обробку даних або працюють із програмним забезпеченням системи. Це оператори, менеджери обробки даних, оператори введення й підготовки даних, а також системні програмісти. Їхні дії можуть впливати на коректність обробки даних, що створює серйозні загрози;
- середній ризик характерний для інженерів системи та менеджерів програмного забезпечення. Їхній доступ до компонентів системи обмежений, але вони все ще можуть впливати на стабільність роботи або окремі функції ІС;
- обмежений ризик мають прикладні програмісти, інженери та оператори зв'язку, бібліотекарі магнітних носіїв, а також оператори периферійного обладнання. Вони мають доступ до менше критичних частин системи, тому їхній потенційний вплив є значно нижчим;
- низький ризик притаманний інженерам по периферійному устаткуванню та бібліотекарям магнітних носіїв. Вони працюють з компонентами, які менш

критичні для основних функцій системи, а їхній доступ до конфіденційної інформації зазвичай обмежений.

Ця ієрархія ризиків допомагає визначити пріоритети у впровадженні заходів безпеки. Особлива увага повинна бути приділена категоріям персоналу з найбільшим ризиком, що передбачає посилений контроль доступу, регулярне навчання з питань кібербезпеки та впровадження механізмів перевірки дій працівників із розширеними повноваженнями.

2.2.3. Цілі порушника

Можливою метою порушника є особиста авторизація, тобто одержати особисті легальні атрибути доступу бажано з найширшими правами щодо доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення відповідно до своїх намірів; авторизувати інших осіб, які б мали можливість одержати легальні атрибути доступу бажано з найширшими правами щодо доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення відповідно до своїх намірів; знайти прихильників або довірених осіб серед персоналу або користувачів ІС, які мають можливість одержувати легальні атрибути доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення відповідно до своїх намірів [13].

2.2.4. Рівень знань порушника

Порушник може знати:

- склад, розміщення, функціональні особливості, умови й режими функціонування елементів ІС, включаючи траси прокладених або можливих ліній зв'язку, комунікаційних мереж зв'язку й трафіки відповідних каналів передачі даних;
- порядок, засоби й режими здійснення охорони елементів ІС, місця їх розташування й прилеглі території;
- порядок, засоби й режими здійснення організаційно правових і технічних заходів захисту ресурсів ІС;
- основні закономірності формування в ІС баз даних і потоків запитів до них.

За характером дій зловмисник може здійснювати: активні або пасивні дії, стосовно ресурсів і функціональних властивостей захищеності інформаційних об'єктів ІС.

Під активною загрозою розуміється спроба навмисної несанкціонованої зміни стану функціонування ІС, а під пасивною – спроба несанкціонованого проникнення в систему без зміни її стану.

Методи, що використовуються порушниками

Порушники можуть використовувати такі методи та засоби:

- агентурні методи одержання відомостей через підкуплених користувачів і персонал, а також прихильників чи довірених осіб з числа штатних працівників або таких, які мають доступ до ресурсів ІС;
- пасивні технічні засоби перехоплення інформаційних сигналів;
- штатні засоби ІС або недоліки проєктування системи захисту інформації від несанкціонованого доступу (НСД);
- методи й засоби активного впливу на елементи ІС, які змінюють конфігурацію ІС (підключення додаткових або модифікація штатних технічних засобів, підключення або «врізання» у канали передачі даних, впровадження й використання спеціального ПЗ тощо).

За місцем здійснення порушень дії зловмисника можна класифікувати:

- без одержання доступу на контрольовану територію із використанням технічних засобів віддаленого доступу через засоби: Internet, електронної пошти,

модемного зв'язку чи дистанційної розвідки (наприклад, по оптичних, акустичних каналах, каналах побічних електромагнітних випромінювань тощо), або з використанням засобів одержання інформації з мережі передачі даних (наприклад, шляхом підключення або «врізання» у лінії зв'язку);

- з одержанням доступу на контрольовану територію ІС або до робочих місць кінцевих користувачів, але без доступу до технічних засобів ІС, також з використанням технічних засобів дистанційної розвідки з подальшим несанкціонованим доступом до будинків, або приміщень, у яких розміщені елементи ІС;
- з одержанням доступу до робочих місць кінцевих користувачів ІС з подальшим несанкціонованим доступом до пристроїв введення / виводу інформації, копіювання, до канального або каналоутворюючого устаткування й до інших елементів ІС;
- з одержанням доступу до засобів управління ІС і засобів управління комплексною системою захисту інформації з подальшими розширеними

2.3. Загрози безпеці інформації

2.3.1. Поняття загрози

Під загрозами безпеці (конфіденційності) інформації розуміють потенційні або реально можливі дії щодо інформаційних ресурсів, які призводять до неправомірного оволодіння відомостями, що охороняються.

Такими діями є :

- ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;
- модифікація інформації у кримінальних цілях – часткова або значна зміна складу і змісту відомостей;
- руйнування (знищення) інформації як акт вандалізму з метою прямого нанесення матеріальних збитків.

Протиправні дії з інформацією призводять зрештою до порушення її конфіденційності, повноти, достовірності та доступності, що також призводить до порушення як режиму управління, так і його якості за умов помилкової або неповної інформації.

Кожна загроза тягне за собою певні збитки – моральні чи матеріальні, а захист і протидія загрозам мають знизити їхні обсяги, в ідеалі – повністю, реально – значно або хоча б частково. Але й це вдається не завжди. Зазначене дає змогу провести певну класифікацію загроз безпеці інформації (рис. 2.1).

Рис. 2.1. Класифікація загроз безпеки інформації

Систематизуємо відомі загрози безпеки інформації різноманітного походження (табл. 2.1) і дамо короткий коментар цих ознак класифікації, їхніх значень та змісту.

Походження загроз. У табл. 2.1 виділено два значення цієї ознаки: випадкове і навмисне. Під випадковим розуміють таке походження загроз, яке зумовлюється спонтанними і незалежними від волі людей обставинами, що

виникають у системі у процесі її функціонування. Найбільш відомими явищами такого плану є відкази, збої, помилки, стихійні лиха та побічний вплив. Суть перелічених явищ (крім стихійного лиха, суть якого зрозуміла) визначається в такий спосіб:

Таблиця 2.1

Загрози безпеки інформації

Параметри класифікації	Значення параметрів	Зміст значення параметру
1. Види	1.1. Фізична цілісність 1.2. Логічна структура 1.3. Зміст 1.4. Конфіденційність 1.5. Право власності	Знищення (спотворення) Спотворення структури Несанкціонована модифікація Несанкціоноване отримання Привласнення чужого права
2. Природа походження	2.1. Випадкова 2.2. Навмисна	Відмови, збої, похибки, стихійні лиха, побічні явища Зловмисні дії людей
3. Передумови появи	3.1. Об'єктивні 3.2. Суб'єктивні	Кількісна нестача елементів системи, якісна нестача елементів системи Розвідувальні органи іноземних держав, промисловий шпіонаж, діяльність кримінальних (злочинних) елементів, дії недобросовісних співробітників системи
4.Джерела загроз	4.1. Люди 4.2. Технічні пристрої 4.3. Моделі, алгоритми, програми 4.4. Технологічні системи обробки 4.5. Зовнішнє середовище	Сторонні особи, користувачі, персонал Реєстрація, передача, зберігання, обробка, видача Загального призначення, прикладні, допоміжні Ручні, інтерактивні, машинні, мережні Стан атмосфери, побічні шуми і завади, побічні сигнали

- відмова – порушення працездатності будь-якого елемента системи, що призводить до неможливості виконання ним своїх основних функцій;
- збій – тимчасове порушення працездатності будь-якого елемента системи, наслідком чого може бути помилкове виконання ним у цей момент своєї функції;

- помилка – неправильне (разове чи систематичне) виконання елементом однієї чи декількох функцій, що виникає внаслідок його специфічного (постійного або тимчасового) стану;
- побічний вплив – негативна дія на систему в цілому або окремі її елементи, що викликана будь-якими явищами, які відбуваються всередині системи або в зовнішньому середовищі.

Навмисне виникнення загроз зумовлене зловмисними діями людей.

2.3.2. Джерела загроз

Під джерелом загроз розуміється безпосередній їх генератор або носій. Таким джерелом можуть бути люди, технічні засоби, моделі (алгоритми), програми, зовнішнє середовище.

Визначимо множину загроз, потенційно можливих у сучасних автоматизованих системах. Водночас повинні врахувати не тільки всі відомі (що раніше виявлялися) загрози, а й такі загрози, які раніше не виявлялися, але потенційно можуть виникнути за нинішніх концепцій архітектурної побудови систем і технологічних схем обробки інформації.

Класифікуємо канали несанкціонованого отримання інформації за двома критеріями: необхідності доступу (фізичного або логічного) до елементів систем для реалізації того чи іншого каналу несанкціонованого отримання інформації і залежності появи каналу від стану системи.

За першим критерієм канали несанкціонованого отримання інформації можуть бути поділені на ті, що не вимагають доступу, тобто такі, що дають змогу отримувати необхідну інформацію дистанційно (наприклад, шляхом візуального спостереження через вікна приміщень системи), і ті, що вимагають доступу в приміщення систем. Канали несанкціонованого отримання інформації, скористатися якими можна тільки діставши доступ у приміщення систем, поділяються на такі, що не залишають слідів у системах (наприклад, візуальний перегляд зображень на екранах моніторів або документів на паперових носіях), і

на канали несанкціонованого отримання інформації, використання яких залишає ті чи інші сліди (наприклад, викрадення документів або машинних носіїв інформації).

За другим критерієм канали несанкціонованого отримання інформації поділяються на такі, що потенційно існують незалежно від стану системи (наприклад, викрадати носії інформації можна незалежно від перебування систем у робочому чи неробочому стані), і такі, що існують тільки в робочому стані систем (наприклад, побічне електромагнітне випромінювання та наведення).

Отже, класифікаційну структуру каналів несанкціонованого отримання інформації можна подати у вигляді табл. 2.2.

Таблиця 2.2

Класифікаційна структура каналів несанкціонованого отримання інформації

Залежність від доступу до елементів системи	**Відношення до обробки інформації**	
	Що виявляються безвідносно до обробки	Що виявляються в процесі обробки
Не вимагають доступу	1-й клас – загальнодоступні постійні	2-й клас – загальнодоступні функціональні
Вимагають доступу без зміни елементів системи	3-й клас – вузькодоступні постійні без залишення слідів	4-й клас – вузькодоступні функціональні без залишення слідів
Вимагають доступу із зміною елементів системи	5-й клас – вузькодоступні постійні із залишенням слідів	6-й клас – вузькодоступні функціональні із залишенням слідів

Канали несанкціонованого отримання інформації 1-го класу – канали, що виявляються безвідносно до обробки інформації і без доступу зловмисника до елементів системи. Сюди можна віднести підслуховування розмов, а також

провокування на розмови осіб, що мають стосунок до ІС, і використання зловмисником візуальних, оптичних і акустичних засобів.

Канали несанкціонованого отримання інформації 2-го класу – канали, що виявляються в процесі обробки інформації без доступу зловмисника до елементів ІС. Сюди можна віднести електромагнітні випромінювання різних пристроїв та ліній зв'язку, підключення до інформаційно-обчислювальної мережі генераторів перешкод і реєструючої апаратури.

Канали несанкціонованого отримання інформації 3-го класу – канали, що виявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІС, але без зміни останніх. До них належать всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів.

Канали несанкціонованого отримання інформації 4-го класу – канали, що виявляються в процесі обробки інформації з доступом зловмисника до елементів ІС, але без зміни останніх. Сюди можна віднести запам'ятовування і копіювання інформації у процесі її обробки, використання програмних пасток, недоліків мов програмування і операційних систем.

Канали несанкціонованого отримання інформації 5-го класу – канали, що виявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІС зі зміною останніх. Серед цих каналів – підміна і розкрадання носіїв інформації та апаратури, включення в програми блоків типу «троянський кінь», «комп'ютерний черв'як» тощо, читання залишкової інформації, що міститься в пам'яті, після виконання санкціонованих запитів.

Канали несанкціонованого отримання інформації 6-го класу – канали, що виявляються в процесі обробки інформації з доступом зловмисника до елементів ІС зі зміною останніх. Сюди можна віднести незаконне підключення до апаратури і ліній зв'язку, а також зняття інформації на шинах живлення різних елементів інформаційних систем.

Для вирішення будь-якого завдання в автоматизованій системі повинні бути передбачені адекватні за змістом і достатні по кількості засоби. Вже

розроблено вельми представницький по номенклатурі арсенал різних засобів захисту інформації. Безліч різноманітних можливих засобів захисту визначається передусім способами дії на дестабілізуючі чинники або причини, що породжують їх. Прийнято виділяти такі класи засобів захисту:

фізичні – механічні, електричні, електромеханічні, електронні, електронно-механічні і подібні пристрої і системи, які функціонують автономно, створюючи різного роду перепони на шляху дестабілізуючих чинників;

апаратні – різні електронні, електронно-механічні і подібні пристрої, що схемно вбудовуються в апаратуру автоматизованих систем або що сполучаються з нею спеціально для вирішення завдань захисту інформації;

програмні – спеціальні пакети програм або окремі програми, які використовуються для вирішення завдань захисту;

організаційні – організаційно-технічні заходи, що спеціально передбачаються в автоматизованих системах з метою вирішення задач захисту;

законодавчі – закони й інші нормативно-правові акти, які регламентують права і обов'язки осіб і підрозділів, що мають відношення до функціонування автоматизованої системи, в якій присутня інформація обмеженого доступу, а також встановлюється відповідальність за дії, наслідком яких може бути порушення захищеності інформації;.

морально-етичні – моральні норми або етичні правила, що склалися в суспільстві або в певному колективі, дотримання яких сприяє захисту інформації, а порушення прирівнюється до недотримання правил поведінки в суспільстві або колективі.

Найважливішою концептуальною вимогою до системи захисту інформації (СЗІ) є вимога адаптованості, тобто здатності до цілеспрямованого пристосування за зміни структури, технологічних схем або умов функціонування автоматизованої системи.

2.4. Вимоги до систем захисту інформації

Вимоги щодо ЗІ визначаються власником інформації і узгоджуються з виконавцем робіт з проєктування і створення СЗІ.

ДСТУ 3396.0-96 і ДСТУ 3396.1-96 визначають основні положення і порядок робіт зі створення СЗІ. Ці стандарти встановлюють об'єкт захисту, мету, основні організаційно-технічні положення СЗІ, неправомірний доступ до якої може завдати збитку громадянам, організаціям, державі, а також категорії нормативних документів з СЗІ і вимоги до порядку проведення робіт з технічного захисту. Також цими стандартами визначено, що метою СЗІ є запобігання витоку або порушенню цілісності інформації з обмеженим доступом.

Мета комплексної системи захисту інформації (КСЗІ) може бути досягнута побудовою СЗІ, яка є організованою сукупністю методів і засобів забезпечення СЗІ.

Зміст і послідовність робіт з протидії загрозам або їх нейтралізації повинні відповідати вказаним в ДСТУ 3396.0-96 етапам функціонування систем захисту інформації відповідно до ДСТУ 3396.1-96 і полягати в:

- проведенні обстеження об'єкта (підприємства, установи, організації);
- розробленні реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ;
- прийому робіт з ТЗІ;
- атестації засобів (систем) забезпечення інформаційної діяльності на відповідність вимогам нормативних документів системи ТЗІ.

У процесі формування вимог до СЗІ доцільно знайти відповіді на такі запитання:

- які заходи безпеки пропонується використовувати;
- яка вартість доступних програмних і технічних заходів захисту;
- наскільки ефективні доступні заходи захисту;

- наскільки уразливі підсистемі СЗІ;
- чи є можливість провести аналіз ризику.

Серед сукупності вимог до СЗІ (рис. 2.1) доцільно виділити такі групи вимог: загальні; організаційні; конкретні вимоги до підсистем захисту, технічного і програмного забезпечення, документування, способів і методів захисту.

У сучасних умовах у процесі взаємодії об'єкта і людини виникають події, процеси або явища, які можуть призвести до знищення, втрати цілісності, конфіденційності або доступності інформації. Проте дотепер проєктували СЗІ і розробляли вимоги до їх здійснення без урахування відмінних особливостей систем «людина – об'єкт інформації» або «засіб ЗІ – об'єкт інформації».

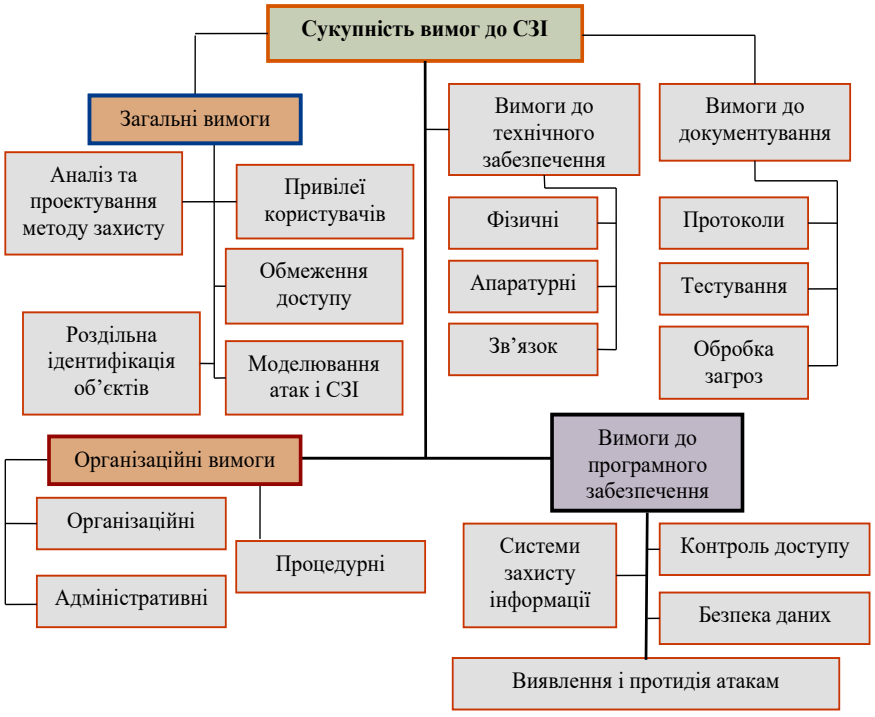

Рис. 2.2. Сукупність вимог до СЗІ

Для вирішення завдань захисту інформації вводиться множина підрівневого захисту L – кінцева множина елементів $l_1, l_2, \ldots, l_k$ кожен підрівень

$l_{i,1} \leq j \leq k$, забезпечується застосуванням m_j-го методу захисту об'єкта $W_i \in W$, тобто $\forall w_i \in W_i l_j(w_i), l_j \in L, m_j \in M, i \in J, j = \overline{1,k}$.

Сумарний рівень захисту, що забезпечується сукупністю $M(W_i)$ методів захисту об'єкта повинен бути не менше базового рівня $J_0(W_i)$ захисту об'єкта W_i:

$$\forall i \in J: J(w_i) = \sum_{j \in J} l_j(w_i) \geq J_0(W_i). \quad (2.1)$$

Підсумовування проводиться лише за тими методами, які належать об'єднанню $M(W_i)$, яке використовується для захисту об'єкта W_i.

Вираз (2.1) і зміст терміну «рівень захисту об'єкта» визначають принципову відмінність задач захисту об'єкта від задач створення систем захисту.

Отже, необхідно також оцінити множину вартостей захисту $s_1, s_2, \ldots, s_k$. Елемент $s_j \in S, j = \overline{1,k}$ характеризує величину затрат за реалізації m_j-го методу захисту об'єкта $w_i \in W$ і який забезпечує l_j-й рівень захисту. Потужність множин M, L та S збігаються.

Злом системи або порушення системи захисту об'єкта w_i характеризується вірогідністю злому кожного методу захисту і всієї сукупності методів в цілому, сумарною вартістю злому або несанкціонованого проникненню через неї, а також тимчасовими витратами, необхідними для подолання всіх методів, які вживаються для подолання системи захисту об'єкта w_i. Сумарна вартість несанкціонованих дій, що вживаються для подолання системи захисту повинна бути більше вартості засобів, що вживаються для захисту об'єкта і самого об'єкта. Тимчасові витрати об'єкта СЗІ на об'єкті повинні бути максимальними, принаймні більшими, ніж для базового обмеження тимчасових витрат нападу системи захисту об'єкта. Тільки за цих умов можна вважати за доцільне вибір цієї сукупності методів захисту об'єкта і виконання вимог до СЗІ.

Будь-яка атака або несанкціонована дія на об'єкт засобу захисту, що є у розпорядженні СЗІ, вплине на нього по-різному: деякі із засобів можуть бути

зруйновані повністю, деякі виведені з ладу частково, а для якихось засобів атака виявиться безпечною. Облік цих відмінностей у результатах дії атаки на засоби захисту є важливим за проєктування, моделювання будь-якої КСЗІ, а також за встановлення стійкості СЗІ передбачуваному супротивникові.

Для формування кожного обліку необхідно:

визначити математичний параметр, що характеризує об'єкт за його використовуваного математичного представлення, якісне застосування якого буде відмінне залежно від характеру збурюючої дії;

вибрати спосіб формального представлення атак СЗІ так, щоб він, будучи простим в обчислювальному сенсі, дозволяв відобразити безпосередню спрямованість атаки;

вибрати простий в обчислювальному сенсі спосіб представлення результату атаки.

Вирішення поставлених завдань дає можливість для створення моделі СЗІ, що дозволяє максимально швидко визначити наслідки організованої атаки, виділяючи «постраждалі» і «незаймані» засоби захисту.

Традиційним шляхом для представлення групи людей з відображенням взаємних стосунків між ним є використання теорії графів. Це зумовлено рядом чинників, серед яких: наочність отримуваної моделі, можливість адекватного віддзеркалення за допомогою стандартних операцій на графах реальних дій над групами і подій у групах, існуванням розробленого математичного апарату для роботи з графами, включаючи велику кількість тих, що добре зарекомендували себе на практиці евристичних методів обробки.

Вибір сукупності методів захисту об'єкта повинен здійснюватися з урахуванням певних каналів витоку для кожного конкретного об'єкта з метою їх перекриття. Потім для кожного окремого методу захисту повинна бути визначена вартість проєктування та експлуатації під час реалізації цього методу, вірогідність і вартість його злому, атаки або несанкціонованої дії.

Наступні характеристики досить складні для визначення: оцінка вартості об'єкта, оцінки рівнів для кожного окремого методу захисту і рівня захисту

самого об'єкта, а також оцінки величини витрат у разі несанкціонованого одержання інформації, нейтралізувавши кожний окремий метод захисту інформації.

Тимчасові заборони необхідні для подолання кожного з методів і часу, необхідного для реалізації однієї спроби подолання кожного методу захисту.

Вказаним характеристиками є початкові дані, необхідні для створення і оцінки якості системи захисту об'єкта і всієї системи в цілому.

Важливість інформації повинна оцінюватися за двома групами критеріїв (рис 2.3) – за призначенням інформації і за умовами її обробки.

Рис. 2.3. Критерії оцінки важливості інформації

У першій групі варто виділити два критерії:

- важливість самих завдань для забезпечення діяльності;
- ступінь важливості інформації для ефективного розв'язання відповідного завдання.

У другій групі виділяються дві складових критерію:

рівень втрат у випадку небажаних змін інформації в процесі обробки під впливом дестабілізуючих факторів;.

рівень витрат на відновлення порушеної інформації.

Якщо позначити K_{BI} – коефіцієнт важливості інформації; $К_{ВЗ}$ – коефіцієнт важливості тих завдань, для забезпечення яких використовується інформація; $К_{ЕЗ}$ – коефіцієнт важливості оцінюваної інформації для ефективного розв'язання завдань; $К_{ВОІ}$ – коефіцієнт важливості оцінюваної інформації з огляду на втрати під час порушення її якості; K_{CB} – коефіцієнт важливості оцінюваної інформації з огляду вартості відновлення її якості. Тоді отримаємо:

$$K_{BI} = f(K_{B3}, K_{E3}, K_{BOI}, K_{CB}). \quad (2.2)$$

Тобто для оцінки важливості інформації необхідно вміти визначати значення перерахованих вище коефіцієнтів і знати вид функціональної залежності K_{BI}. Але натепер невідомі ні ті, ні інші, і є вагомі підстави стверджувати, що і у найближчому майбутньому ця проблема не буде вирішена. Однак іноді для цих цілей, конкретної інформації і конкретних умов можна використовувати підхід, заснований на неформально-евристичних методах.

Для оцінки захищеності інформації досліджують такі її властивості:

повнота інформації – це показник, що характеризує міру достатності оцінюваної інформації для розв'язання відповідних завдань. Звідси випливає, що цей показник, є відносним: повнота інформації оцінюється відносно цілком конкретного завдання або групи завдань. Тому щоб мати можливість визначити показник повноти інформації, необхідно для кожного суттєво значимого завдання або групи завдань скласти перелік тих відомостей, які необхідні для їхнього розв'язання. Для надання таких відомостей зручно використовувати так звані об'єктивно-характеристичні таблиці, які являють собою двомірні матриці. У них по рядках наведено перелік найменувань тих об'єктів, процесів або явищ, які належать до кола інтересів відповідного завдання, а по стовпцях – найменування тих характеристик (параметрів) об'єктів, процесів або явищ, значення яких необхідні для розв'язання завдання. Отже, саме значення характеристик розташуються на перетині відповідних рядків і стовпців;

адекватність інформації – ступінь її відповідності дійсному стану тих об’єктів, процесів, явищ, які відображає оцінювана інформація. У загальному випадку адекватність інформації визначається двома параметрами:

об’єктивністю генерування (знімання, визначення, встановлення) інформації про об’єкт, процес або явище;

тривалістю інтервалу часу між моментом генерування інформації і моментом її адекватності.

Об’єктивність генерування інформації залежить від способу одержання значень характеристик об’єкта, процесу, або явища і якості реалізації (використання) способу в процесі одержання цих значень. Класифікацію характеристик за можливими способами отримання значень представлено на рис. 2.4.

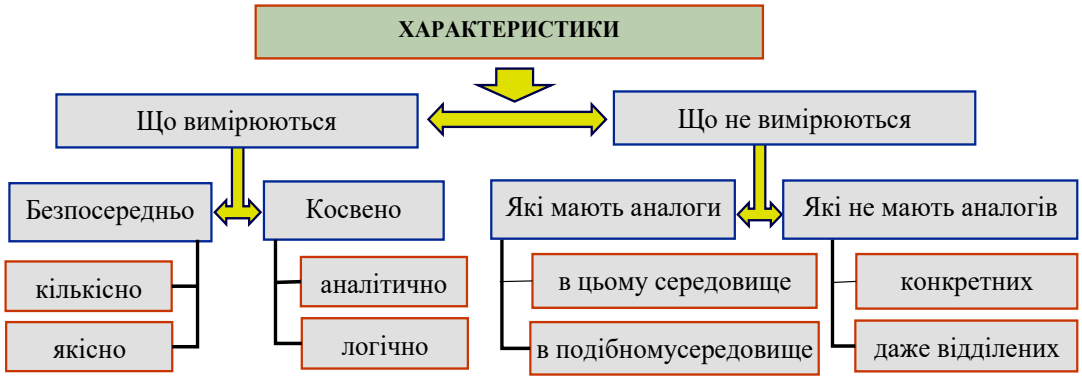

Рис. 2.4. Класифікація характеристик за способами отримання їх значень

Розглянемо адекватність інформації з іншого названого параметра – тривалості інтервалу часу між моментом генерування інформації і теперішнім моментом. Для оцінки адекватності по цьому параметру цілком підходящим є відомий у теорії інформації так званий закон старіння інформації (рис. 2.5).

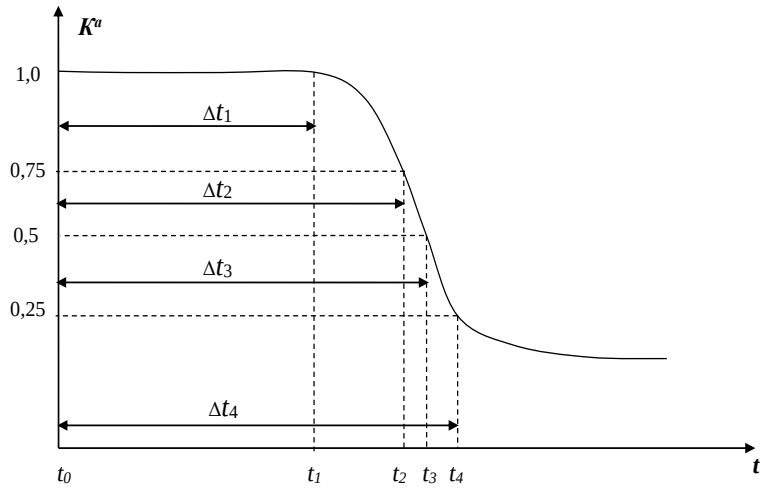

Рис. 2.5. Графічне представлення закону старіння інформації

При цьому під t_0 – розуміється момент часу генерування (одержання) оцінюваної інформації; Δt_1 – тривалість часу, протягом якого оцінювана інформація повністю зберігає свою адекватність; Δt_2 – тривалість часу, протягом якого, адекватність інформації падає на 25%; Δt_3 – тривалість часу, протягом якого, адекватність інформації падає на половину; Δt_4 – тривалість часу, протягом якого, адекватність інформації падає на 75%.

Враховуючи те, що обидві складові адекватності інформації $K^{a'}$ і $K^{a''}$ залежать від великої кількості факторів, багато з яких носять випадковий характер, мається підстава стверджувати, що вони також носять випадковий характер і тому можуть інтерпретуватися як імовірності того, що інформація відповідного параметру є адекватною. Оскільки для переважної більшості теоретичних досліджень і практичних додатків важливо, щоб інформація була адекватної одночасно по обом параметрам, то відповідно до теореми множення ймовірностей загальний показник адекватності інформації може бути визначений як: $K^a = K^{a'} \cdot K^{a''}$. Незалежність значень a'і a''представляється цілком природньою.

Релевантність інформації – це показник, який характеризує відповідність її потребам розв'язуваного завдань. Для кількісного виразу цього показника використовують так званий коефіцієнт релевантності K_p – відношення обсягів релевантної інформації N_pдо загального обсягу аналізованої інформації N_0, тобто

$$K_p = \frac{N_p}{N_0}. \qquad (2.3)$$

Сутність коефіцієнта релевантності зрозуміла, але труднощі практичного його використання пов'язані з кількісним виразом обсягу інформації. Тому завдання обчислення цього коефіцієнта на практиці ставиться до досить невизначеної і такої, що важко розв'язується проблеми.

Толерантність інформації – це показник, що характеризує зручність сприйняття і використання інформації в процесах розв'язку того завдання, для розв'язку якого вона використовується. Вже з визначення зрозуміло, що поняття толерантності є дуже широким, значною мірою невизначеним і суб'єктивним. Тому не можна сподіватися на розробку строго формальної методики визначення толерантності інформації.

Необхідний рівень ЗІ повинен визначатися з урахуванням значень усіх розглянутих показників. Однак в цей час методика такого визначення відсутня і розробка її вимагає самостійних досліджень. У якості виходу з цього положення можна використовувати таку напівевристичну процедуру:

усі показники інформації діляться на три категорії: визначальні, істотні і авторські, причому основним критерієм для такого розподілу повинна служити та мета, для досягнення якої здійснюється ЗІ.

Необхідний рівень захисту встановлюється за значеннями визначальних показників інформації.

Обраний рівень за необхідності може бути скорегований з урахуванням значення істотних показників. Значення другорядних показників також можуть ігноруватися.

Отже, здійснимо класифікацію методів і засобів ЗІ.

Методи захисту можна розділити на організаційні, технічні, криптографічні і програмні.

Засоби захисту так само можна розділити на постійно діючі; і такі, що долучають за виявлення спроб нападів.

По активності вони діляться на: пасивні; напівактивні; активні.

За рівнем забезпечення ЗІ засоби захисту підрозділяються на класи:

1 клас: системи слабкого захисту;

2 клас: системи сильного захисту;

3 клас: системи дуже сильного захисту;

4 клас: системи особливого захисту.

Розглянемо предметну область ЗІ з позицій структурної ієрархії.

Вибір СЗІ (головна проблема) від передбачуваного способу нападу (зворотна проблема) і способів виявлення факту нападу (проміжна проблема).

Розв'язок завдання вибору залежить від форми надання інформації (відео, звукова, електромагнітний сигнал), а спосіб захисту – від передбачуваної форми впливу на інформацію (копіювання, знищення, викривлення), використовуваного носіями інформації (папір, магнітний диск тощо), стану інформаційного масиву (перебуває в стані передачі, обробки або зберігання), від того, чи проводиться ЗІ безперервно або під час виявлення факту нападу. Такий тип ієрархії наглядно може бути представлений у вигляді семантичної схеми (рис. 2.6).

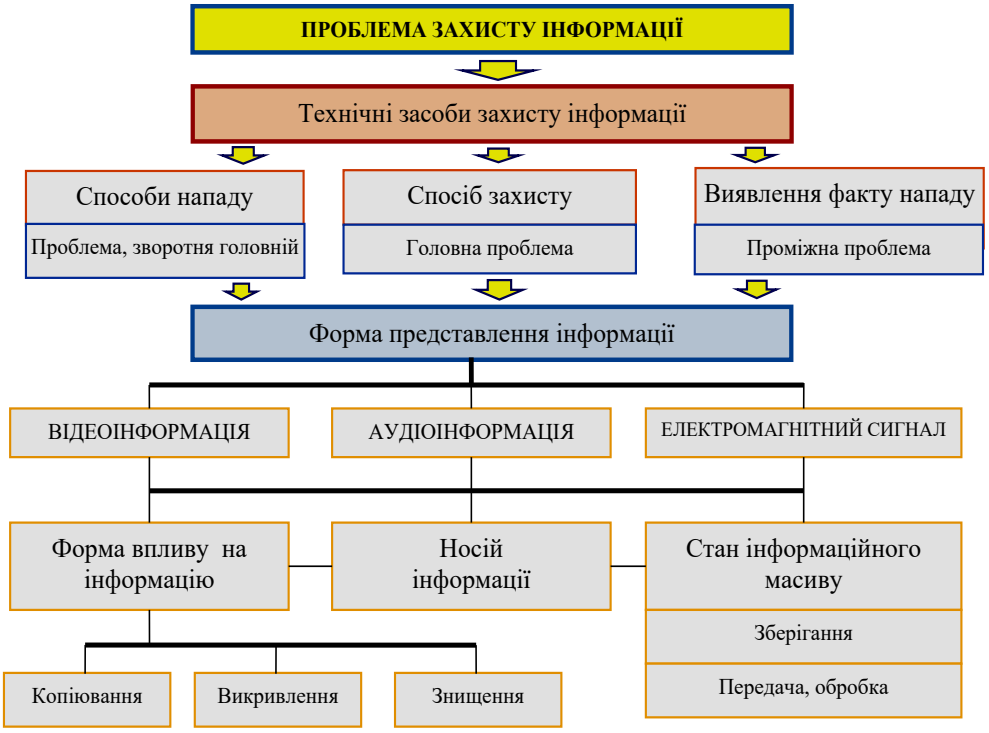

Рис. 2.6. Семантична схема проблеми захисту інформації за допомогою технічних засобів з позиції структурної ієрархії

З погляду функціональної ієрархії СЗІ обмежує доступ, оперативно знищує носії інформації, і в тому числі ставить перешкоди для блокування активних дій порушників (рис. 2.7).

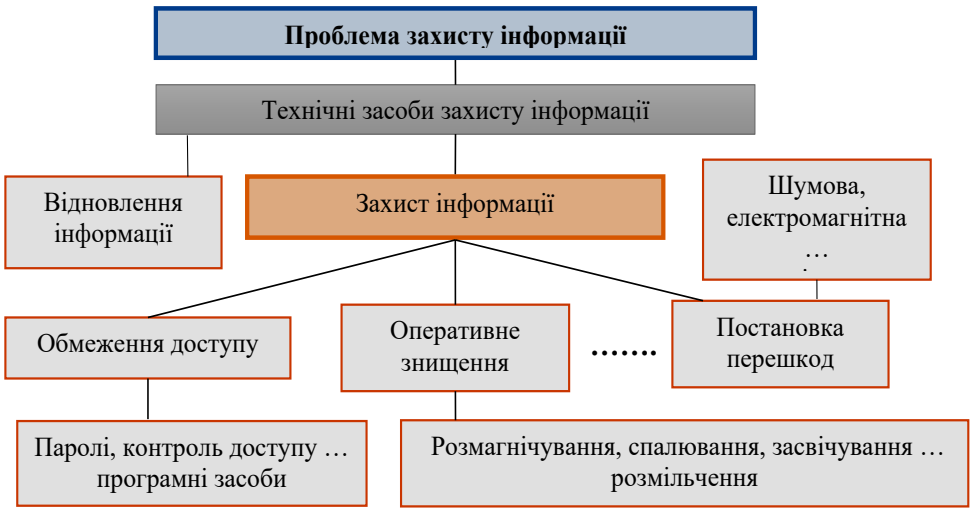

Рис. 2.7. Семантична схема проблеми захисту інформації за допомогою технічних засобів з позиції функціональної ієрархії

З погляду причинно-слідчої ієрархії (рис. 2.8) у першому випадку СЗІ повинна виявити факт нападу. За виявлення факту нападу СЗІ реалізує деякий спосіб захисту. Виявлення факту нападу і реалізація конкретного способу захисту відбувається за умови, що заздалегідь відомо кілька передбачуваних способів нападу. Сам спосіб нападу так само залежить від стану інформаційного масиву і форми надання інформації.

У другому випадку СЗІ працює безперервно, також передбачається, що напад на інформацію може бути здійснений в будь-який час. СЗІ безперервно захищає інформаційний масив від декількох передбачуваних способів нападу з метою копіювання, викривлення знищення інформації шляхом її оперативного знищення, обмеження доступу, постановки перешкод тощо.

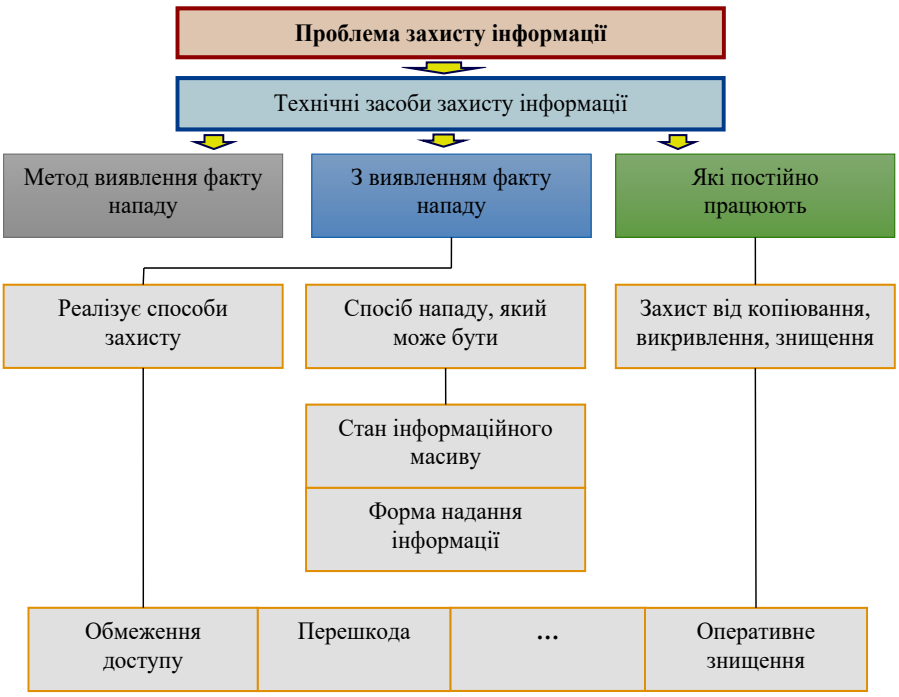

Рис. 2.8. Семантична схема «проблеми захисту інформації за допомогою технічних засобів з позиції причинно-слідчої ієрархії»

Висновки до розділу 2

У другому розділі роботи розкрито основні положення захисту інформації, модель порушника, визначені загрози безпеки інформації та математичне підґрунтя вимог до систем захисту інформації.

Зокрема, описано загрози безпеці конфіденційності, розділено на три групи джерела загроз безпеці інформації

Наголошено, що під час аналізу загроз необхідно завжди припускати найвищу кваліфікацію порушника.

Розглянуто спрощену класифікацію Пітера Мелла – типізація найбільш типових атак на розподілені автоматизовані системи.

Проведено класифікацію загроз за такими параметрами: за об’єктом, за збитками, за обсягом збитків, за відношенням до об’єкта, за ймовірністю виникнення, за характером дії, за причинами появи.

РОЗДІЛ 3
МЕТОДИ З ЗАХИСТУ ІНФОРМАЦІЇ ТА ОПЕРАЦІЙНОЇ СЕКРЕТНОСТІ

Стан захищеності всієї системи є станом захищеності найуразливішого її елемента. Як показує досвід окремих військових, можливо взяти позицію, яка успішно стримувала атаки ворога, здійснивши тиск на одного чи декілька військовослужбовців через погрози їх родинам. Особливо це питання загострилося після повномасштабного вторгнення російської федерація.

Надважливим фактом є існування військовослужбовців, члени родин яких знаходяться на окупованих територіях або на території російської федерації.

Треба розуміти, що знайти вразливих людей використовуючи сучасні засоби пошуку з відкритих джерелах, не є складним завданням. Ворогом досить давно використовуються автоматизовані засоби для створення і наповнення баз даних про громадян України, які є у соціальних мережах. Доповнювати та корегувати такі бази даних їм допомагають різноманітні витоки інформації, такі як зламування державних реєстрів України та баз клієнтів приватних підприємств. Ворогом створено низку організацій для виконання цієї роботи. Найвідоміша з них це «Фабріка тролєй», творцем якої нібито є відомий лідер (у минулому) ЧВК «Вагнер». Попри свою назву, основними цілями цієї організації є створення та наповнення баз даних, а не суперечки в коментарях [14].

Особливо ворога цікавить така інформація: робота на підприємствах інфраструктури або оборони, служба у Силах оборони, адреса проживання, наявність родини, належність до соціальних груп. Також ворог шукає інформацію, яка явно несе військове значення: кількість виготовленої оборонної продукції, фото колон військової техніки тощо.

3.1. Соціальні конструкти

3.1.1. Соціальна комунікація

Натепер витік інформації через недотримання суб'єктами операційної секретності встановлених рекомендацій та правил користування соціальними мережами, комунікацій з іншими суб'єктами, а також людьми, що не є суб'єктами, є найбільшим серед інших каналів витоку.

Витік інформації через розмови на вулиці є давно відомою проблемою. Вимоги операційної секретності потребують обговорення чутливої інформації у спеціально відведених для цього місцях. Але не тільки розмови наражають на небезпеку вас та інших. Пересування поза контрольованої зони у характерній формі, носіння знаків розрізнення, все це дає ворогу необхідну йому інформацію.

Небажано пересуватися у місцях, де є цивільні у військовій формі зі знаками розрізнення без потреби. Кожна дія повинна мати мету. Не дозволяється обговорювати чутливі речі в громадських місцях. Ці рекомендації не стосуються тих випадків, коли на меті є ввести противника в оману.

Необхідно уникати явних ознак, про ваше місце розташування, великої кількості машин з характерними номерами в одній будівлі, характерні шлагбауми, відкрите розташування чатового тощо.

У розмовах з цивільними без потреби не називайтесь справжнім ім'ям, використання різних імен залежно від місцевості дасть вам можливість зрозуміти звідки стався витік інформації, також це ускладнить пошук інформації про вас з відкритих джерел.

Ваша сім'я є таким же суб'єктом операційної секретності як і ви. Вся інформація, що стосується вас, повинна бути видалена з відкритих джерел та не повинна розголошуватися без нагальної потреби.

Помилкою буде приховування інформації про себе від близьких. У випадку, коли їм необхідно буде знайти ваше місцезнаходження, вони звернуться за допомогою до інших людей і як показує практика, якщо вами не

був залишений контакт особи, до якої ваша сім'я може звернутися, з великою вірогідністю вона натрапить до ворожих осіб.

Ще однією помилкою буде явне приховування інформації у громадських місцях. Підозріла поведінка може призвести до детального вивчення вас ворогом та/або увагу союзних контррозвідувальних служб. Головним правилом буде поводити себе так, як поводить більшість навколо, наприклад, якщо більшість людей ходить у військовій формі, то, не зважаючи на попередню рекомендацію, носіння цивільного одягу навпаки приверне до вас увагу.

Не довіряйте випадковим знайомим, існує багато агентів противника, які були завербовані ще на початку незалежності нашої держави.

3.1.2. Соціальні мережі OSINT, GEOINT

Витік інформації через соціальні мережі є наслідком активного розвитку та використання так званих OSINT та GEOINT.

OSINT – це процес та методи збору інформації з публічно доступних джерел для аналітичного використання, містить аналіз даних з медіа, офіційних документів, публічних записів, Інтернету та інших відкритих платформ. OSINT може бути ключовим методом отримання інформації у сучасній війні. Шляхом проведення моніторингу відкритих і відносно відкритих джерел та соціального інжинірингу про об'єкти розвідки добувається від 35 % до 95 % розвідувальних даних, які інколи не тільки не відрізняються від військових і державних таємниць, але й часто можуть перевершувати їх за своєю цінністю.

GEOINT – процес отримання інформації про просторове знаходження об'єкта та його характеристик, використовуючи зображення та геопросторових даних.

Наявність автоматизованих інструментів значно спростили використання цих методів порівняно з минулими десятиліттями. Якість інформації, що була знайдена за допомогою OSINT, є тим більша, ніж її кількість. Введення активного життя у соціальних мережах видає величезну кількість відкритої

інформації про вас. Вказування реальних даних про себе дозволяє досить просто за допомогою програмного забезпечення зібрати вичерпну інформацію про вас. Вказування недостовірної інформації, але додавання у список друзів, які таку інформацію вказали, дозволяє опосередковано визначити вас. Людина, досвідчена у GEOINT, з великою точністю знайде місце, де було зроблено фото, використовуючи характерні місцеві предмети, положення небесних світил, хмар. Її робота значно спроститься, якщо у фотографію були додані метадані геолокації – більшість телефонів робить це за замовчуванням.

До того ж велика кількість інформації у соціальній мережі, коментарі, пости, список груп, до яких ви доєдналися, дозволяє зробити ваш психологічний аналіз, час, коли ви в мережі, дозволить визначити ваш режим сну, а через нього опосередковано час заступання на чергування / пост.

Припустимо, у 1998 році ви закінчили військову кафедру та зробили фото у формі, яке згодом розмістили у соціальній мережі. Ворог, побачивши це фото, може зробити висновок, що ви закінчили військову кафедру, і визначити приблизний рік, виходячи з форми. Далі ворог може припустити, що ви зараз на службі, отримали звання капітана і, ймовірно, є командиром роти. Навіть без вашого імені і прізвища ворог може розпочати збирати додаткову інформацію про вас.

Тепер уявіть, що це фото супроводжувалося детальною інформацією: датою, спеціальністю, повним ім'ям. Навіть якщо ви не викладали це фото, але хтось із ваших друзів розмістив фото вашого взводу і зазначив вас в описі, ворог все одно може зібрати інформацію. Якщо у списку ваших друзів багато військових, ворог може припустити, що ви теж військовий або волонтер.

Наслідки отримання інформації про вас ворогом можуть бути критичними для вас, ваших рідних, вашого підрозділу та можливо може вплинути на тактичне становище на полі бою.

Якщо ворог зміг поєднати вашу цивільну особистість з військовою, він може вдатися до шантажу через ваших рідних. Реально існують випадки, коли

ворог дізнавшись про адресу проживання, висилав фото будинку / квартири з текстом «ти наш». Після чого висилав вимоги на певні дії – здати позицію, спостережний пункт, робити хибні доповіді і так далі. У разі відмови діяти за вказівкою ворога, використовують підставних осіб, що виконують дії фізичного характеру над родиною військовослужбовця. Також існують випадки залякування та фізичних дій до осіб, що вже перестали бути військовослужбовцями, тим самим залякуючи наше суспільство.

Що робити, якщо вас почали шантажувати:

1. Доповідь командиру. Негайно повідомте свого командира.

2. Звернення до людей, що можуть допомогти вам захистити вашу родину, як-от побратими, що проходять лікування або були комісовані, громадські організації, що підтримують військових, інші люди, яким ви безумовно довіряєте та які можуть запобігти фізичному насиллю від ворожих осіб.

3. Звернення до спеціальних служб – контррозвідка Збройних Сил України, Служба Безпеки України.

3.1.3. Методика поводження у соціальних мережах

За наявності соціальної сторінки рекомендується поступово редагувати інформацію, бо видалення, фактично її приховує, але залишає її в системі, збереження попередніх версій, реалізовано не скрізь та є більш затратною операцією. Інформації, яка однозначно ідентифікує вас як військовослужбовця бути не повинно. Можливо трохи змінити ім’я, якщо було вказано ваше реальне, змініть букву в імені або прізвищі.

Обмежити доступ до особистої інформації. Перевірте налаштування приватності у соціальних мережах і обмежте доступ до вашої особистої інформації, сховайте список ваших друзів, груп, спільнот.

Не публікуйте детальну інформацію про себе. Уникайте розміщення фотографій у військовій формі або будь-якої іншої інформації, яка може розкрити вашу військову службу.

Зробіть вашу сторінку приватною.

Відпишіться від спільнот, за якими ви перестали слідкувати, видаліть друзів, яких ви не знаєте або знаєте погано.

Прослідкуйте за інформацією, яку публікують ваші друзі та родичі. Попросіть їх не публікувати інформацію про вас без вашого дозволу.

Особливу увагу зверніть на існуючі фото.

Якщо вам необхідно створити військову соціальну сторінку, краще за все працювати з нею з окремого пристрою. У цьому випадку уникайте зв'язків з вашою цивільною особистістю, не додавайтесь до старих друзів, не підписуйтесь на старі групи, спільноти. За можливості не використовуйте ваше фото, навіть зі схованим обличчям, безпечніше буде використовувати картинку з інтернету, попередньо очистивши її метадані.

Якщо необхідно зробити і виставити фото, замальовуйте його, піксілізація піддається дешифруванню. Чим менше об'єктів буде на фото, тим менша вірогідність, що спеціалісти по GEOINT зможуть дізнатися ваші координати, бо вирішальною може стати травинка в кадрі – цілком можливо, що така трава росте тільки на певній місцевості.

Створіть декілька облікових записів, для перегляду використовуйте один, для спілкування з рідними інший, для військових потреб третій. За потреби створюйте додаткові облікові записи.

Для спілкування зі знайомими використовуйте кодові слова, сучасні технології дозволяють підробити голос та зображення у реальному часі, тому за необхідності уточнюйте особу, наприклад, якщо вас просять відправити гроші нібито у госпіталь на ліки.

3.1.4. Цілеспрямовані дії ворожих сил

У будь-який момент, ви можете стати об'єктом дії ворожої агентури. Дотримуючись наданих рекомендацій, ви збережетеся від найпростіших методів отримання інформації. Треба розуміти, що ворожим агентом може бути хто

завгодно, тому навіть, якщо вас просить розголосити інформацію особа, вища за вас званням, без погодження власника інформації або іншої уповноваженої особи ви не повинні це робити. Не давайте фотографувати ваші документи.

Враховуйте, що інформацію, що вам надається або надаєте ви, може бути перехоплена ворогом. Не розкривайте маршрути та час висування на позиції без крайньої необхідності.

Якщо ви маєте підозру, що ви стали об'єктом атаки ворожої агентури, зверніться у службу контррозвідки вашого підрозділу.

Ще одним вектором атаки є дія ворожої пропаганди, на відміну від дій агентури, цей вектор спрямований на все суспільство та його складові, а не на особистість. Характерною рисою нинішньої пропаганди ворога є: висування великої кількості версій, думок з різних джерел. Водночас ці версії зазвичай мають розбіжності, дещо протирічать одна одній. Але ворогом також використовується пропаганда негативних рис нашого суспільства, у більшості випадків перебільшуючи їх та замовчуванні всіх інших. Позитивні новини сприймаються гірше, ніж негативні. Такий вид ворожої пропаганди зазвичай спирається на декілька основних джерел, після чого, використовуючи агентуру, вразливі частини населення та робить провокативні пости та відео у соціальних мережах, тим самим стимулюючи інші верстви населення повторити за ними, створюючи вигляд, великої кількості однодумців.

Іншим видом пропаганди є використання так званих ботів. Вони не є самостійним методом, а підсилюють інші методи пропаганди. Велика кількість ботів діє у західній частині соціальних мереж, використовуючи штучний інтелект.

Операційна секретність – відповідальність кожного її суб'єкта.

Більшість перерахованих методів та рекомендацій буде не ефективними, якщо хоча б декілька суб'єктів в колективі не буде їх притримуватися. Якщо один із суб'єктів постійно розголошує інформацію у громадських місцях, виставляє у соціальні мережі критичну інформацію, то дії по підтриманню

операційної секретності індивідуальних суб'єктів не несуть достатньої захищеності. Такий суб'єкт є вразливим для дій ворожої агентури. Якщо будь хто з суб'єктів активно піддається ворожій пропаганді, це знижує морально-психологічний стан всього колективу, а з часом такий суб'єкт почне робити спроби підмовляти інших.

Суб'єкт може не притримуватися правил та рекомендацій через природні складові характеру, не вважаючи це чимось важливим, не бути в змозі їм слідувати через психологічні вади або з інших установлених причин. В такому випадку, його необхідно усунити від джерел критичної інформації. Але варто наголосити, що такий суб'єкт є оптимальним кандидатом для введення в оману, шляхом розголошення такому суб'єкту дезінформації, всі інші кроки по розповсюдженню інформації він зробить сам. З боку противника таке джерело отримання інформації буде вважатися як помилка з нашої сторони.

Варто слідкувати за іншими суб'єктами – наявність шкідливих звичок, як-то лудоманія, алкоголізм, вживання наркотиків, робить такого суб'єкта не надійним і до того ж вірогідним вектором атаки агентури, шляхом шантажу, позики грошей або інших товарів та послуг.

3.2. Мобільні системи

Насамперед необхідно знати, що порядок користування військовослужбовцями мобільними телефонами та іншими електронними засобами визначає командир військової частини (стаття 143 Статуту внутрішньої служби Збройних Сил України) [15]. Тобто командир приймає рішення і визначає, коли, як і де можна здійснювати дзвінки.

Телефон як ідентифікатор особистості нової ери, який є джерелом всеохоплюючої, досить повної інформації про користувача та його оточення.

Найдосконалішу систему операційної секретності і захисту інформації зводить нанівець фізична втрата телефона.

Телефон військовослужбовця містить інформацію про його родину, фотографії, контакти, банківські дані, повну інформацію про нього самого, Найголовніше те, що він містить вичерпну інформацію про значну частину свого підрозділу, батальйону або бригади, місця дислокації, контакти, фотографії, ієрархію. Отримання будь-якої інформації ворогом про родину, особисто про вас, ваш підрозділ буде однозначно використано для знищення.

Зламування мобільного пристрою несе велику небезпеку для військовослужбовців. Від можливості прослуховувати розмови та відмови у роботі, до виходу з режиму радіомовчання, що дозволить засобам радіо та радіоелектронної розвідки дізнатися місце знаходження власника пристрою.

Для збереження стану захищеності інформації потрібно вірно організувати систему індивідуального захисту пристроїв та інформації на них.

Першим етапом системи повинно стати розуміння, що життя безповоротно змінилося війною, запорукою виживання стала швидка адаптація до нових умов та вимог. І цією вимогою стала диференціація громадського та військового життя, максимальне розділення цих сфер на всіх рівнях інформаційної взаємодії.

Ваш телефон – це ваша особиста річ. Не дозволяйте його використання без вашого дозволу та без спостереження за діями користувача.

Для військової діяльності потрібно створити нову інформаційну (віртуальну) особистість. Модифікувати початкову прибравши з неї всю небезпечну інформацію. Цивільне і військове життя мають бути відокремленими інформаційними сутностями.

Побудувати індивідуальну організаційну систему в двох формах цивільного і військового захисту, частиною якої є політика (правила) взаємодії з мобільними телефонами варто спираючись на чотири рівні інформаційної взаємодії починаючи від найнижчого фізичного рівня.

3.2.1. Фізичний вектор

Початком є наявність мінімум двох в оптимальному варіантів трьох фізичних пристроїв мобільного зв'язку (телефонів), якщо другий телефон відсутній потрібно придбати його та 2-3 сім-карти. (Правильним буде активувати військову сім-карту вже в межах прифронтової зони).

Перший телефон стосується виключно цивільної діяльності і повсякденного використання поза зоною бойових дій тільки для цивільних потреб, на ньому не може зберігатися інформація військового характеру взагалі, а та, яка потрапила повинна бути правильним шляхом видалена. Другий телефон це військова особистість, на ньому зберігається виключно військова інформація, програми, контакти можливо фотографії, все що стосується і чого вимагає військова діяльність. Третій телефон потрібен у випадку активної діяльності безпосередньо на або за рубежем лінії бойового зіткнення (ЛБЗ).

Концепція використання:

перший телефон використовується в зоні 100 км безпосередньо від ЛБЗ, правила користування ним послаблені, на ньому дозволено з перевірених джерел перегляд фільмів та відвідування ресурсів, зберігання цивільних фотографій, контактів, програм. Цей телефон повинен вимикатися за 100 км від ЛБЗ і не функціонувати в периметрі, вмикатися тільки за умови залишення прифронтової зони. На ньому може бути тільки та військова інформація, без якої неможливо відмовитися в найобмеженішому вигляді;

другий телефон, який функціонує в радіусі ближче за 100 км від ЛБЗ та знаходиться у вимкненому стані після залишені ЛБЗ. Він існує для військової діяльності – програми, контакти, переписки, фотографії. Правила безпеки на ньому посилені, відвідувати посилання і сайти заборонено. Використовується тільки необхідне і перевірене;

третій телефон існує для того, щоб брати його з собою безпосередньо на рубіж ЛБЗ, де він може бути будь-якої миті втрачений та потрапити до рук

ворога. Цей телефон повинен мати лише необхідні 2-3 контакти, 1-2 програми, вся інша інформація та фотографії на ньому мають бути елементами введення ворога в оману, якщо ця мобільна система буде ним отримана.

Ці телефони стають фундаментом захисту і подальшої побудови системи захисту.

3.2.2. Апаратний вектор загроз

Мобільний телефон є радіовипромінювальним пристроєм, тому власник такого пристрою разом з оточуючими завжди знаходяться під «прицілом», розкриваючи ворогу своє місцезнаходження. Навіть звичайний дзвінок або повідомлення додому, що «в мене все добре, завтра висуваємося», може обернутися засідкою, артобстрілом або чимось гіршим.

Також слід розуміти, що деякі оператори мобільного зв'язку є громадянами інших держав, у тому числі російської федерації, тому спецслужби цих держав можуть отримувати інформацію про переговори та навіть місцезнаходження методом триангуляції (аналіз сили сигналу на трьох найближчих базових станціях).

Мобільний телефон це засіб зв'язку, який вже прослуховується противником.

Це просте правило збереже багато життів.

Необхідно вимикати телефон повністю або вмикати «режим польоту», коли перебуваєте на командно-спостережному пункті (КСП) чи на позиції.

Дозволено увімкнути WiFi за потреби скористатися Інтернетом від іншого пристрою (Starlink, GSM-роутер), але не ризикуйте роздавати Інтернет з інших мобільних телефонів та приєднуватися до невідомих WiFi-мереж.

Не варто користуватися мобільним зв'язком одночасно кільком особам із однієї точки, телефонуйте по черзі з певними часовими проміжками. Безпечніше дзвонити з місць, віддалених від розташування позицій. Якщо ви знаходитесь на передовій позиції, то не користуйтеся телефоном або модемом взагалі. Якщо це

неможливо, то намагайтеся використовувати їх на зворотній від противника стороні пагорба або у низині. Це допоможе захиститись від радіоелектронної розвідки (РЕР).

Окупанти використовують «підробні» базові станції на літаках (типу Орлан-10) чи наземних приладах (авто, радіовежі тощо). За їх допомогою вони можуть встановити саму позицію, кількість бійців на ній, час та обсяг ротації та навіть, іноді, шлях від ППД до позиції.

Тож необхідно взяти за правило, що одночасно повинно бути ввімкнено не більше одного телефону і на термін не більше, ніж треба для передачі інформації. З цих же «підробних» станцій окупанти можуть розсилати звичайні СМС з демотивуючими чи шахрайськими повідомленнями, або здійснювати дзвінки з підміною номера та імені абонента (наприклад, вам зненацька може зателефонувати «Дружина», «Мати» або «Начальник»). Не реагуйте на ці повідомлення, а потрібному абоненту передзвоніть самі, через месенджер.

Чим ближче до фронту – тим менше довіри до того, що вам надходить на телефон по звичайних GSM-каналах. Неможливо звичайному абоненту зрозуміти чи підключився телефон до ворожої базової станції. Ви, імовірно, зможете здійснити голосовий виклик та відіслати СМС, але ворог прослухає його, прочитає зміст повідомлення та буде знати кому ви дзвонили.

Мобільний Інтернет-трафік, якщо він буде дозволений, буде теж спостерігатися ворогом, але зміст його, найімовірніше, він прочитати не зможе. Не приєднуйтеся до невідомих WiFi-мереж на передовій, особливо до тих, які працюють без вводу пароля. В налаштуваннях вашого модема або роутера Starlink – встановіть мінімальну потужність WiFi, це захистить від РЕР.

Фізична безпека апаратного рівня: встановіть надійний пароль розблокування не менш ніж з шести цифр, або цифро-літерний пароль. Не використовуйте розповсюджені паролі, типу: 111111, 123321, qwerty. Налаштуйте автоблокування телефону в найкоротший термін (1–5 хв.).

Налаштуйте видалення даних або повне блокування після п’яти невдалих спроб вводу пароля.

Не використовуйте графічний ключ та розблокування обличчям. Це не надійний захист.

Не підключайте до телефону чужих сім-карт, карт пам’яті, флешок, павербанків, шнурів, зарядних пристроїв та інших речей, походження яких має сумніви. Ці речі можуть як заразити ваш телефон вірусами, так і фізично знищити його. Не використовуйте телефон, як флешку для переносу інформації з комп’ютера.

3.2.3 Програмний вектор загроз

Правила надавання доступів

Перевірка дозволів програм на Android є обов’язковою частиною аналізу мобільного пристрою на факт ураження. Їх необхідно перевіряти для впевненості, що додатки не отримують доступу до інформації або функцій, які не є необхідними для їх роботи. Це допомагає уникнути небажаного збору даних та потенційних безпекових ризиків.

Дозвіл на автозапуск дозволяє додаткам на Android працювати у фоновому режимі або запускатися автоматично після перезавантаження пристрою. Це може бути корисним для додатків, які виконують важливі функції без безпосередньої участі користувача, наприклад, поштових клієнтів чи месенджерів. Проте шкідливі програми також намагаються отримати цей дозвіл, щоб запускати себе без відома користувача.

Наприклад, шпигунське ПЗ або рекламне ПЗ може використовувати автозапуск для відновлення своєї активності після перезапуску пристрою, що ускладнює їх виявлення та видалення. Це також може впливати на продуктивність пристрою та час його роботи від акумулятора, оскільки фонові процеси споживають ресурси системи. Важливо ретельно контролювати дозволи на автозапуск та надавати їх тільки перевіреним додаткам, які вам дійсно

необхідні. На більшості пристроїв Android ви можете управляти дозволами на автозапуск через налаштування системи або використовувати спеціалізовані додатки для керування автозапуском

Вкладка «Використання даних» в налаштуваннях Android показує скільки даних споживає кожен додаток. Якщо ви помітите несподівано високе використання даних для додатку, який не повинен інтенсивно використовувати інтернет, це може бути ознакою шпигунського програмного забезпечення.

Додатки, які працюють у фоновому режимі, можуть швидко розряджати батарею. Особливо це стосується шпигунських програм, які активно моніторять діяльність користувача і передають дані, що призводить до значного енергоспоживання.

Паролі

Паролі повинні стояти на всіх чутливих елементах, програмах, контактах, альбомах фотографій.

Двофакторна аутентифікація

Надважливий елемент захисту, що робить зламування програмним чином надскладним завданням. Дозволяє запобігти втраті інформації, навіть якщо система була вражена вірусними програмами. Це засіб важливий засіб мінімізації збитку та відновлення системи, обов'язковий до використання на всіх платформах, що на це розраховані.

Геолокація

У налаштуваннях телефону – вимкніть служби геолокації та вмикайте їх тільки за потреби ними користуватися (для мап, для польотів на дроні). Подивіться, яким додаткам надані права на користування геолокацією, вимкніть її для тих, кому вона не потрібна для роботи. Наприклад: камера, месенджери, калькулятор, ігри тощо.

Встановіть додаток, який підміняє ваші координати, наприклад FakeGPS, для польотів на дроні.

ВАЖЛИВО: встановлюйте тільки ту програму, яку ви отримали від фахівців підрозділу.

Android

Ніколи не встановлюйте root на свій телефон. Зареєструйте новий Google аккаунт на новий номер, використовуючи стійкий пароль.

Налаштуйте двофакторну автентифікацію та інші налаштування приватності. Встановлюйте додатки лише з офіційного Play Market.

За винятком тих, що були розроблені для ЗСУ та розповсюджуються фахівцями підрозділу.

Не встановлюйте додатки, у яких розробники з росії (Yandex, Mail.ru, VK, Одноклассники та ін. непотріб).

Не встановлюйте додатки, які пересилають в месенджерах або електронною поштою.

Якщо додаток прийшов від фахівця підрозділу – впевніться, чи дійсно він його повинен був надіслати. Видаліть з телефону все зайве, що не потрібно для виконання завдань. Встановлюючи додаток, звертайте увагу до чого додаток запитує доступ. Не надавайте доступи, якщо це викликає у вас підозру. Оминайте додатки, які «видаляють віруси», «чистять пам'ять» чи «прискорюють телефон». Не встановлюйте «зламані» ігри.

У більшості випадків – це шкідливе п/з, яке буде просто з'їдати ресурси телефону або заразить його вірусами. Уникайте «кастомних прошивок» для телефонів. Чим більш популярна програма в маркеті, тим вона менш небезпечна. Звертайте увагу на кількість інсталяцій (сотні тисяч) та відгуки.

Окремі ознаки шкідливого програмного забезпечення на Android

1. Наявність розділу «Для розробників» («Для разработчиков») у налаштуваннях телефону. За замовчуванням на більшості телефонів не відображається. Дає доступ до окремих налаштувань телефону (наприклад, «режим налагодження» та дає змогу підключати телефон до комп'ютера як для

зчитування службової інформації операційної системи «Android», так і для встановлення програмного забезпечення.

2. Активація можливості встановлення програмного забезпечення з невідомих джерел («Неизвестные источники»). Надає можливість встановлювати програмне забезпечення, що не пройшло перевірку та відсутнє у загальному доступу в магазині застосунків «Google Play». Має бути вимкнутим.

3. Наявність у розділі «Застосунки» («Приложения») програм, для яких активовано розширені права доступу до пристрою та візуально схожих на системні застосунки операційної системи «Android». Видаліть такі застосунки або вимкніть зайві права.

4. Поява спливаючої реклами під час звичайного користування телефоном.

5. Поява додатків, яких ви не встановлювали.

6. Телефон нагрівається і розряджається.

7. Виросло споживання Інтернет-трафіку, а в деталізації з'явилися невідомі програми.

8. На ваш телефон приходять СМС з авторизацією в банківські додатки, а з рахунку намагаються перевести гроші.

9. Від вас вашим контактам приходять підозрілі або явно шахрайські повідомлення в месенджерах або СМС.

За наявності таких ознак припиніть використовувати такий телефон, проведіть скидання до заводських налаштувань та, за можливості, перепрошийте у довіреному сервісному центрі. Для більшої безпеки можна встановити системні паролі на застосунки, які зберігають приватну інформацію (галерея, месенджери, соціальні мережі):

активуйте функцію «Екранний час» у відповідному підпункті меню «Налаштування»;

натисніть на сенсорну кнопку «Використовувати код-пароль» і введіть будь-яку відому лише вам послідовність символів;

торкніться графіка статистики використання програм на вашому пристрої та виберіть потрібну програму зі списку. Знизу екрана розташовуватиметься

«кнопка» з написом «Додати ліміт». Необхідно її натиснути та встановити час, наприклад, 1 хвилину. Після цього достатньо активувати тумблер навпроти пункту Блокувати в кінці списку. Після закінчення встановленого часу (у прикладі однієї хвилини) програма заблокується. Для його розблокування достатньо натиснути на кнопку «Ігнорувати ліміт» і ввести вибраний під час налаштування пароль.

Антивіруси

Якщо ви ще не користуєтесь Антивірусом, наполегливо радимо встановити його. Питання вибору певного вендору є дуже особистим. Однак важливо: не встановлювати декілька Антивірусних програм на одному ПК; завантажувати файл для встановлення Антивірусної програми лише з офіційного сайту розробника; перезавантажити комп'ютер одразу після встановлення Антивірусу.

Популярні в Україні вендори, продукти яких мають україномовний інтерфейс: Avast, Eset, Zillya!.

Створіть в системі Windows свого ПК обліковий запис користувача, який не матиме прав адміністратора. Працюйте саме під цим користувачем. Так ви не зможете під ним видаляти чи встановлювати програми, змінювати налаштування системи. Проте якщо будете працювати під обліковим записом користувача, без прав адміністратора, то навіть, якщо запуститься троянська програма, вона не зможе нашкодити системі. У такий спосіб ви можете захистити себе навіть без антивірусу. Використання облікового запису без прав адміністратора дозволить вберегтися від більшості шкідливих програм.

Безпека електронних фінансів

Найкращою практикою для захисту ваших фінансів є створення окремої карти для онлайн платежів, на яку будете переводити кошти перед проведенням транзакції. Краще мати декілька карт. Наприклад, однією розраховуватися фізично в терміналах магазинів, іншою проводити онлайн платежі, а основну використовувати лише для переказів коштів на попередні дві.

Захист персональної інформації

Не варто встановлювати прості паролі, наприклад, 1111; 12345 чи qwerty. За статистикою подібні паролі використовуються у 70 % чи навіть 80 % випадків. Звісно, подібні паролі можна легко підібрати. Не використовуйте один і той самий пароль для всіх акаунтів. У цьому Вам стануть у пригоді спеціальні програми (менеджери паролів), вони будуть самі генерувати потрібні паролі для кожного сайту, а вам необхідно буде запам'ятати тільки один пароль для входу в акаунт цієї програми. Варто періодично змінювати паролі (раз на 1-2 місяці). Якщо зловмисники отримали ваш логін і пароль, це не означає, що ця інформація буде одразу використана, шахраї можуть до неї повернутися за декілька місяців чи років. Тому періодично змінюйте паролі!

Створення резервної копії

Широкого попиту у зловмисників набули віруси вимагачі-шифрувальники. Потрапляючи на ваш ПК та активізувавшись, шкідливий код шифрує всі дані без можливості їх відновлення. Якщо ви працюєте з великою кількістю даних, необхідно періодично робити резервні копії на переносний жорсткий диск (SSD) або використовувати хмарні сховища.

Сучасні хмарні сховища є досить зручними і простими у використанні. Потрібно лише періодично копіювати або зберігати необхідну інформацію у відповідній папці.

Доводимо до відома популярні сервіси хмарних сховищ (у дужках наведено, який обсяг інформації надається безкоштовно):

1. DropBox (2ГБ, додатково можна отримати ще до 48ГБ). Один із найпопулярніших сервісів, який має багато додаткових функцій, зокрема: історія зміни файлів; можливість поділитись файлом за допомогою посилання; створення спільних папок із іншими користувачами сервісу та багато інших.

2. GoogleDrive (15ГБ). Для використання цього сервісу достатньо мати акаунт Google (пошту на gmail). Цей сервіс має схожий із попереднім функціонал. До того ж одразу надається більше місця у безкоштовній версії.

3. OneDrive (15ГБ, додатково можна отримати ще до 8ГБ). Сервіс від Microsoft, який раніше мав назву SkyDrive. Наразі даний сервіс також є одним із флагманів хмарних сховищ.

Інтернет-провайдери

Крім техгігантів, існує ще одна не дуже очевидна загроза – інтернетпровайдер як стаціонарний, так і мобільний. Через них проходить інформація про всю інтернет-активність. Зібрану провайдерами інформацію можна доволі легко отримати та розкрити. Наприклад, джерела журналістів, або їхні методики розслідувань та пошуку інформації, або навіть зробити якісь маніпуляції з трафіком. Але і тут є можливість приховувати свою активність в мережі. Використовуйте VPN або послуги з шифрування ваших DNS-запитів. Простіше кажучи, ваш інтернет-провайдер не знатиме, які сайти ви відвідуєте і якими застосунками користуєтеся. Адже ми платимо грошима за послугу доступу до інтернету, а не даними, як у випадку з тим же Google.

Про VPN

Обираючи VPN, важливо розуміти його спосіб монетизації. Оскільки на ринку багато безкоштовних сервісів, то часто вони замість вашого інтернет-провайдера збирають інформацію про ваші дії і відповідно монетизують. Існують надійні застосунки, наприклад, Psiphon та 1.1.1.1, які безкоштовно надають послуги, але з обмеженням в швидкості. Вони так само надійні, як і платні версії, але менш комфортні у використанні. Зазвичай ці обмеження будуть ледь помітні. Почати користуватися ними дуже легко, оскільки і Psiphon, і 1.1.1.1 доступні для всіх основних платформ.

Веб-браузери

Веб-браузери Google Chrome легко можна назвати не браузером, а шпигуном. Google створив цей браузер якраз для того, щоб шпигувати за діями користувачів поза гуглівськими сервісами, щоб знати, як поводяться люди на інших сайтах, куди клікають, що читають, що дивляться. Також за допомогою

цього браузера Google зміг потрапити на закриті сайти й збирати інформацію там, куди не дотягнули його сервіси, такі як Google-аналітика. Якщо ви користуєтеся Google Chrome то виправити нічого не вийде. Надійніше просто змінити браузер. Перейдіть на форки браузера Firefox, який спеціалізується на приватності, також це суттєво зменшить стеження за вашими діями в Інтернеті.

Звичайно, ці альтернативні браузери не ідеальні, адже вбудована пошукова система в одному з них також Google, але добре мати альтернативу.

Пошукові системи

DuckDuckGo – прекрасна альтернатива Google. Це пошукова система, яка не збирає і не продає інформацію про користувачів. Звичайно якість результатів видачі та якісь індивідуалізованих запитів буде гірша ніж в Google. Цьому є просте пояснення тим, що Google про вас знає так багато інформації і завжди це враховує за формування результатів. А от у DuckDuckGo, цих даних немає. DuckDuckGo прекрасно справляється з більшістю повсякденних запитів, для яких не потрібні супер алгоритми. DuckDuckGo цілком може стати основним шукачем, а Google користуйтеся тоді коли потрібно знайти щось специфічне. Та й статистика говорить, що аудиторія DuckDuckGo зростає. В Україні він вже на 4 місці по використанню.

3.2.4. Вектор соціальних мереж

Соціальні мережі стали невід'ємною частиною нашого життя, але вони також є потенційним джерелом загроз. Неправильне використання соціальних мереж може призвести до витоку конфіденційної інформації, яка може бути використана зловмисниками для різних цілей, включаючи крадіжку особистих даних, шантаж, та навіть фізичну небезпеку.

Ось кілька основних аспектів, які варто враховувати для захисту в соціальних мережах.

Метадані фотографій

Метадані фотографій містять інформацію про дату, час та місце зйомки, а також технічні характеристики пристрою, що використовувався. Видаляйте метадані перед публікацією фотографій в Інтернеті або налаштуйте пристрій так, щоб він не зберігав ці дані.

Правила налаштування профілів

Закриття особистої інформації: Видаліть із налаштувань або закрийте для загалу всю особисту інформацію. Номер телефону (перереєструйтесь, використовуючи службову сім-карту), дату народження, інформацію про місце проживання, місце роботи, посаду, військову частину, рід військ тощо.

Аватари: використовуйте нейтральні зображення без відкритого обличчя.

Ім'я акаунту: замініть на нейтральне або псевдонім.

Контент: не поширюйте фото та відео, які можуть ідентифікувати ваше місцезнаходження, техніку, позиції тощо.

Друзі та контакти: не додавайте в друзі сторонніх осіб. Переконайтеся, що людина, з якою ви спілкуєтеся, не видає себе за когось іншого.

Посилання та файли: не відкривайте файлів та посилань від незнайомців і навіть від знайомих, якщо вони викликають сумніви.

Активність: відключіть можливість бачити вашу останню активність.

Повідомлення: обмежте надсилання повідомлень тільки для контактів.

Безпека месенджерів

Месенджери часто використовуються для обміну конфіденційною інформацією. Ось кілька рекомендацій для забезпечення їхньої безпеки:

номер телефону: використовуйте службову сім-карту. Дату народження, місце проживання, місце роботи, посаду тощо;

налаштування приватності: використовуйте нейтральне ім'я та аватар. Відключіть видимість останньої активності та можливість надсилати повідомлення від сторонніх акаунтів;

чати з наскрізним шифруванням: використовуйте месенджери, що підтримують наскрізне шифрування;

двофакторна аутентифікація: налаштуйте двофакторну аутентифікацію для захисту акаунтів;

приватність: налаштуйте приватність так, щоб вашу інформацію бачили лише довірені особи;

перевірка прив'язаних пристроїв: періодично перевіряйте прив'язані до акаунтів пристрої та відключайте невідомі;.

зникаючі повідомлення: налаштуйте зникаючі повідомлення на 7 днів або менше.

Наскрізне шифрування

Лише відправник і одержувач мають доступ до вмісту повідомлення. Індивідуальні та групові повідомлення видаляються з серверів одразу після доставки. Захищає персональні розмови від розповсюдження.

Навіщо необхідне наскрізне шифрування? При спілкуванні в Інтернеті ваші дані подорожують мережею, що дає можливість прослуховувати ваші чати та повідомлення електронної пошти всім бажаючим. Наскрізне шифрування дозволяє уникнути стороннього проникнення. Коли ви використовуєте засоби зв'язку із наскрізним шифруванням, ніхто, крім адресата, не може бачити та читати ваші повідомлення.

Використовуючи вище наведені методи, сформуємо концепцію індивідуального захисту військовослужбовця (рис 3.1).

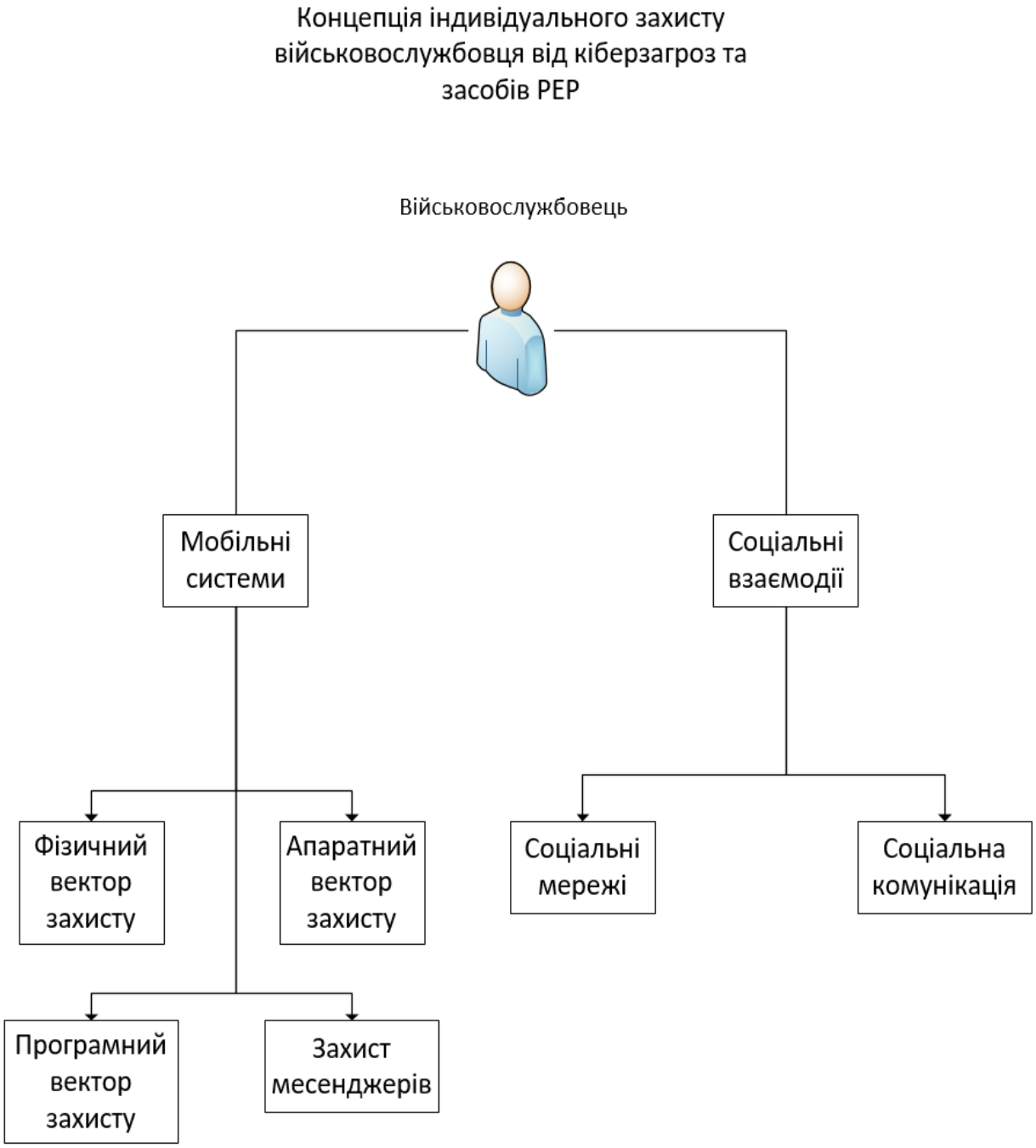

Рис. 3.1. Концепція індивідуального захисту військовослужбовця від кіберзагроз та засобів РЕР

3.3. VPN небезпека, впровадження

Протоколи захищеного каналу, як правило, використовують у своїй роботі механізм тунелювання. За допомогою цієї методики пакети даних транслюються через загальнодоступну мережу як за звичайним двоточковим з'єднанням. Між кожною парою «відправник – одержувач даних» встановлюється своєрідний тунель – безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого (рис 3.2).

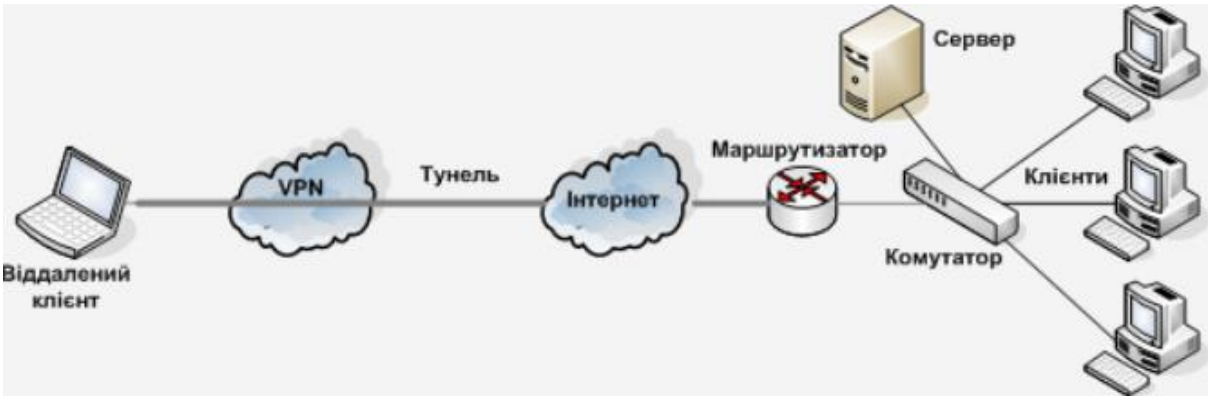

Рис. 3.2. Принцип роботи VPN

Приватна віртуальна мережа (VPN) – це виділена мережа на базі загальнодоступної мережі, що підтримує конфіденційність переданої інформації завдяки використанню тунелювання та інших процедур захисту. У основі технології VPN лежить ідея забезпечення доступу віддалених користувачів до корпоративних мереж, що містять конфіденційну інформацію, через мережі загального користування.

VPN-пристрій розташовується між внутрішньою мережею і Internet на кожному кінці з'єднання. Під час передачі даних через VPN, вони зникають «з поверхні» в точці відправлення і знову з'являються тільки в точці призначення. Завдяки тунелюванню приватна інформація стає невидимою для інших користувачів. Перш ніж потрапити в Internet-тунель дані шифруються, що

забезпечує їх додатковий захист. Протоколи шифрування визначаються VPN-рішенням.

Ролі VPN-пристроїв

VPN-клієнт є програмним або програмно-апаратним комплексом, що зазвичай виконується на базі персонального комп'ютера;

VPN-сервер є програмним або програмно-апаратним комплексом, що встановлюється на комп'ютері, що виконує функції сервера;

шлюз безпеки VPN – це мережевий пристрій, що підключається до двох мереж, а також виконує функції шифрування та аутентифікації для численних хостів розташованих за ним.

VPN-сервер та шлюз безпеки можуть бути одним пристроєм. Найефективнішим вибором буде використання спеціалізованих пристроїв безпеки, для малих та середніх мереж прикладом може існувати лінійка пристроїв FortiGate, Cisco ASA.

Використовуючи VPN, необхідно бути впевненим в сервері VPN та шлюзі безпеки, оскільки через них проходить весь ваш трафік і вони можуть як прослуховувати, так підробити його. Тому використання безкоштовних VPN є великим ризиком. Виходом буде або використання перевірених VPN, як правило вони не безкоштовні, або розвертання особистого серверу VPN. Розвертати свій сервер бажано використовуючи спеціалізовані пристрої мережевої безпеки або звичайні роутери, але не всі роутери здатні це зробити. Іншим простим варіантом буде використання персонального комп'ютера в ролі VPN-сервера та шлюза безпеки.

Розвертання свого серверу vpn, використовуючи технологію OpenVPN

OpenVPN – це набір open source програм, який заслужено є одним із найпопулярніших і найлегших рішень для реалізації захищеної VPN мережі.

Завантажте MSI інсталятор OpenVPN для вашої версії Windows з офіційного сайту (https://openvpn.net/community-downloads/), після чого починайте установку. Залиште налаштування за замовчуванням.

Наступним кроком (рис 3.3) буде створення ключів шифрування та сертифікатів. Для цього будемо використовувати утиліту easy-rsa.

Запускаємо утиліту командою EasyRSA-Start.bat та ініціалізуємо інфраструктуру ключів командою ./easyrsa init-pki.

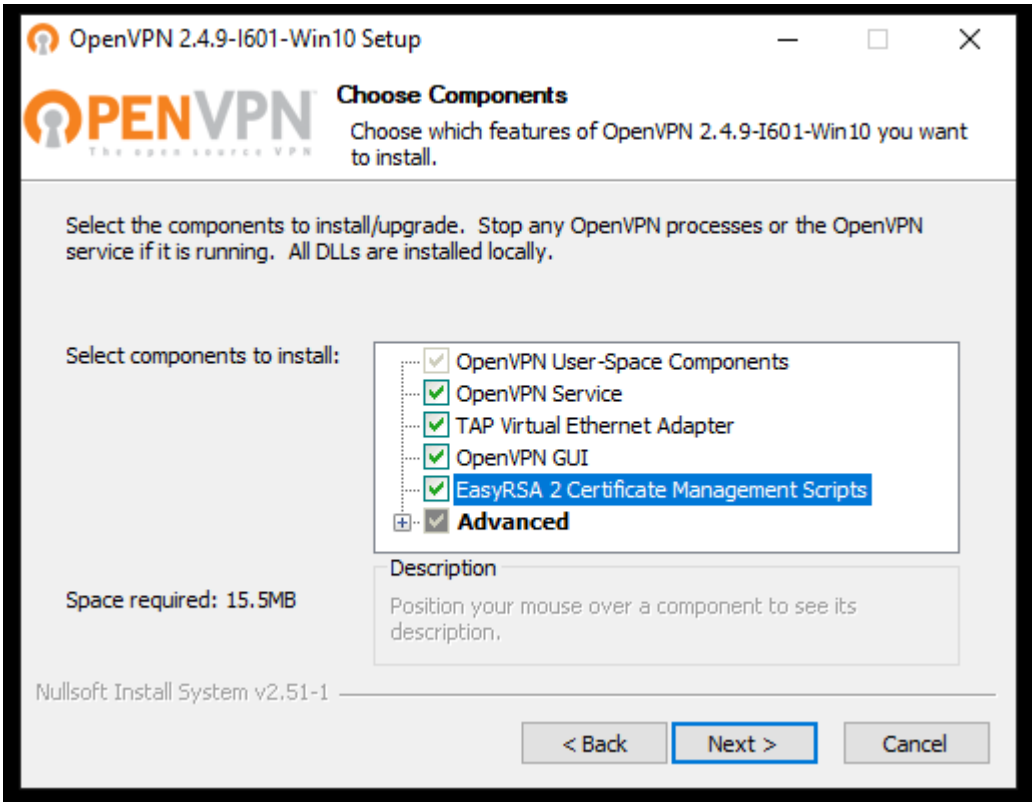

Рис. 3.3 Встановлення OpenVPN та EasyRSA

Відкриваємо файл vars.bat. Та виставляємо змінні DH_KEY_SIZE значення 2048, «set DH_KEY_SIZE=2048». Зберігаємо файл та вводимо команду ./easyrsa clean-all

Генеруємо сертифікати, командами «./easyrsa build-ca nopass» «./easyrsa build-server-full server», «./easyrsa build-client-full Client1 nopass», «./easyrsa gen-dh», в реальних умовах необхідно замінити «nopass» на пароль для клієнта.

Згенеровані файли, *ca.crt*, *server.crt*, *server.key*, *dh2048.pem*, копіюємо до *OpenVPN\config*, далі копіюємо файл прикладу конфігурації сервера *OpenVPN\sample-config*, до *OpenVPN\config* і називаємо його server.ovpn. У файлі

нам необхідно перевірити, щоб співпадали назва параметрів DH, в нашому випадку dh2048.pem (рис 3.4).

```
# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
dh dh2048.pem
```

Рис. 3.4. Необхідне значення параметра dh

Тепер запускаємо сервер, для цього знаходимо программу OpenVPN GUI і натисаємо Connect.

Для клієнтів нам необхідно встановити OpenVPN, передати їм файли ca.crt, client.crt, client.key та client.ovpn. Останній файл знаходиться в *OpenVPN\sample-config*, і в файлі необхідно IP адресу сервера. Знаходимо рядок «remote my-server-1 1194», та замінюємо *remote my-server-1* на адресу сервера.

На клієнті файли необхідно помістити у OpenVPN\config. По аналогії з сервером через ПЗ OpenVPN GUI запускаємо роботу OpenVPN.

3.4. Резервування даних

Резервування даних (або бекап) – це процес створення копій даних для захисту від їхньої втрати або пошкодження. Це важливий елемент управління інформацією, який допомагає забезпечити безперебійність роботи та захистити важливі дані від непередбачених подій, таких як апаратні збої, кібератаки або фізичне знищення носія інформації.

Основні методи резервування даних

Повне резервування: створюється повна копія всіх даних. Цей метод забезпечує найвищий рівень безпеки, але займає багато часу та ресурсів;

інкрементальне резервування: зберігаються тільки ті дані, які були змінені або додані з моменту останнього резервування. Це зменшує обсяг збережених даних і прискорює процес резервування;

диференційоване резервування: створюються копії всіх змін з моменту останнього повного резервування. Це компроміс між повним і інкрементальним резервуванням, забезпечуючи швидке відновлення даних.

Стратегії резервування

Резервування на місці (on-site backup): дані зберігаються на локальних носіях, таких як жорсткі диски, стрічкові накопичувачі або інші пристрої. Це швидкий метод, але він не захищає від фізичних загроз;

віддалене резервування (off-site backup): дані зберігаються в іншому фізичному місці, що підвищує безпеку від локальних катастроф;

хмарне резервування (cloud backup): дані зберігаються у віддалених дата-центрах через інтернет. Це зручний та масштабований метод, що забезпечує високу доступність та відновлення даних.

Найкращі практики резервування даних

Правило 3-2-1: зберігати три копії даних на двох різних носіях, одна з яких в іншому фізичному місці;

автоматизація процесу: використання програмного забезпечення для автоматичного резервування даних, що зменшує ризик людської помилки;

регулярне тестування: Періодичне перевіряння резервних копій для впевненості в їхній працездатності та швидкому відновленні.

Шифрування даних: захист резервних копій від несанкціонованого доступу.

Популярні інструменти для резервування

Acronis True Image

Backblaze

Carbonite

Veeam Backup & Replication

Google Drive, Dropbox, OneDrive, Delta Drive

Резервування даних є критично важливим для забезпечення безпеки та безперервності процесів.

Використання точки відновлення Windows 10

Натисніть «Налаштування відновлення системи». Ще один спосіб потрапити в потрібне вікно – натиснути клавіші Win + R на клавіатурі і ввести systempropertiesprotection після чого натиснути Enter.

Відкриється вікно параметрів (вкладка «Захист системи»). Точки відновлення створюються для всіх дисків, для яких увімкнено захист системи. Наприклад, якщо для системного диска С захист вимкнено, ви можете увімкнути його, вибравши цей диск і натиснувши кнопку «Налаштувати».

Після цього виберіть «Увімкнути захист системи» та вкажіть кількість місця, яку ви бажаєте виділити для створення точок відновлення: чим більше місця, тим більша кількість точок зможе зберігатися, а в міру заповнення простору старі точки відновлення будуть видалятися автоматично.

Для того, щоб створити точку відновлення системи, на тій же вкладці «Захист системи» (потрапити в яку також можна через правий клік по «Пуск» – «Система» – «Захист системи») натисніть кнопку «Створити» та задайте ім'я нової точки, після чого ще раз натисніть «Створити». Через деякий час операцію буде виконано.

Тепер на комп'ютері міститься інформація, яка дозволить вам скасувати останні зроблені зміни в критично важливих системних файлах Windows 10, якщо після інсталяції програм, драйверів або інших дій ОС почала працювати неправильно.

Створені точки відновлення зберігаються у прихованій системній папці System Volume Information у корені відповідних дисків або розділів, однак доступу до цієї папки у вас за замовчуванням немає.

Для того щоб відновити систему з раніше створення точки відновлення використайте один із таких способів:

через інтерфейс Windows 10 ;

за допомогою інструментів діагностики в спеціальних варіантах завантаження;

в середовищі відновлення запущеного з флешки (якщо комп'ютер не завантажується);

в командному рядку.

Найпростіший спосіб за умови, що система запускається – зайти в панель управління, вибрати пункт «Відновлення», після чого натиснути «Запуск відновлення системи».

Запуститься майстер відновлення, у першому вікні якого вам можуть запропонувати вибрати рекомендовану точку відновлення (створену автоматично), а в другому, якщо ви оберете «Вибрати іншу точку відновлення», ви зможете самі вибрати одну із точок відновлення, створених вручну або автоматично. Натисніть «Готово» (рис 3.5).

Після завершення автоматичного перезавантаження комп'ютера вам повідомлять, що відновлення пройшло успішно.

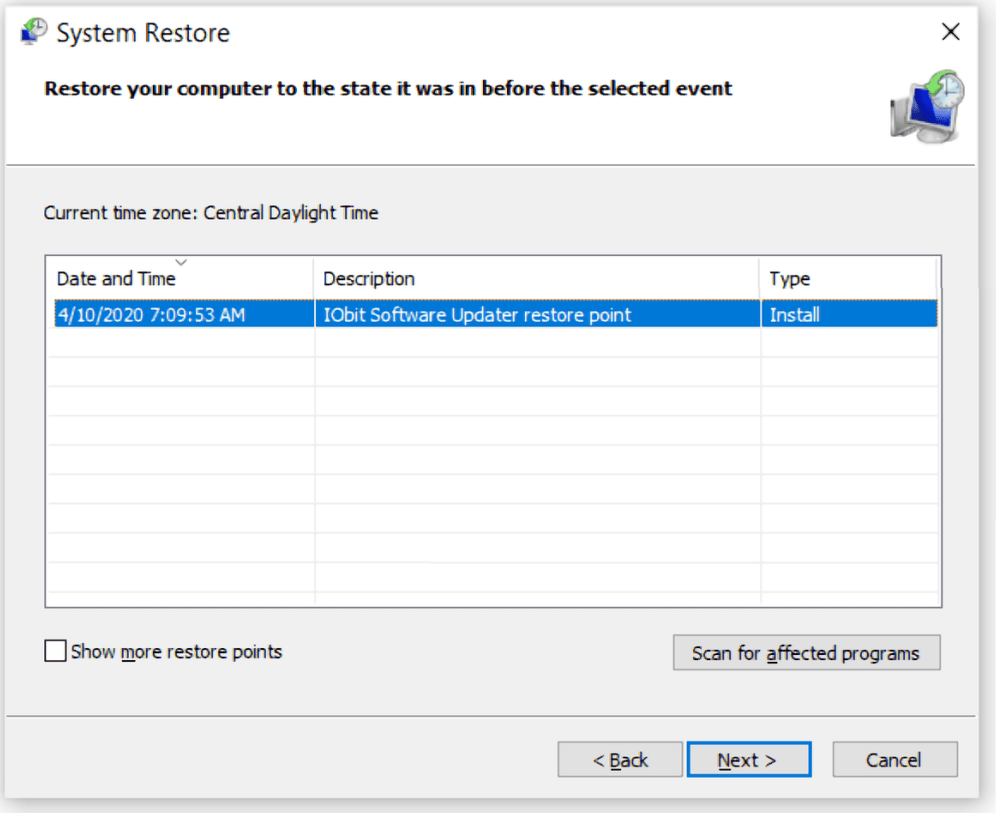

Рис. 3.5. Відновлення з системи з бекапу

Другий метод використовувати точку відновлення – за допомогою особливих варіантів завантаження, потрапити в які можна через Параметри – Оновлення та відновлення – Відновлення або ж ще швидше, прямо з екрана блокування: натиснути по кнопці «живлення» справа внизу, а потім, утримуючи Shift, натиснути «Перезавантаження». Або декілька разів вимкнути комп'ютер відразу, як з'явиться заставка завантаження Windows.

На екрані особливих варіантів завантаження виберіть пункт «Пошук та усунення несправностей» – «Відновлення системи» (або «Діагностика» – «Додаткові параметри» – «Відновлення системи» в попередніх версіях Windows 10), далі ви зможете скористатися наявними точками відновлення (у процес потрібно ввести пароль облікового запису) (рис 3.6).

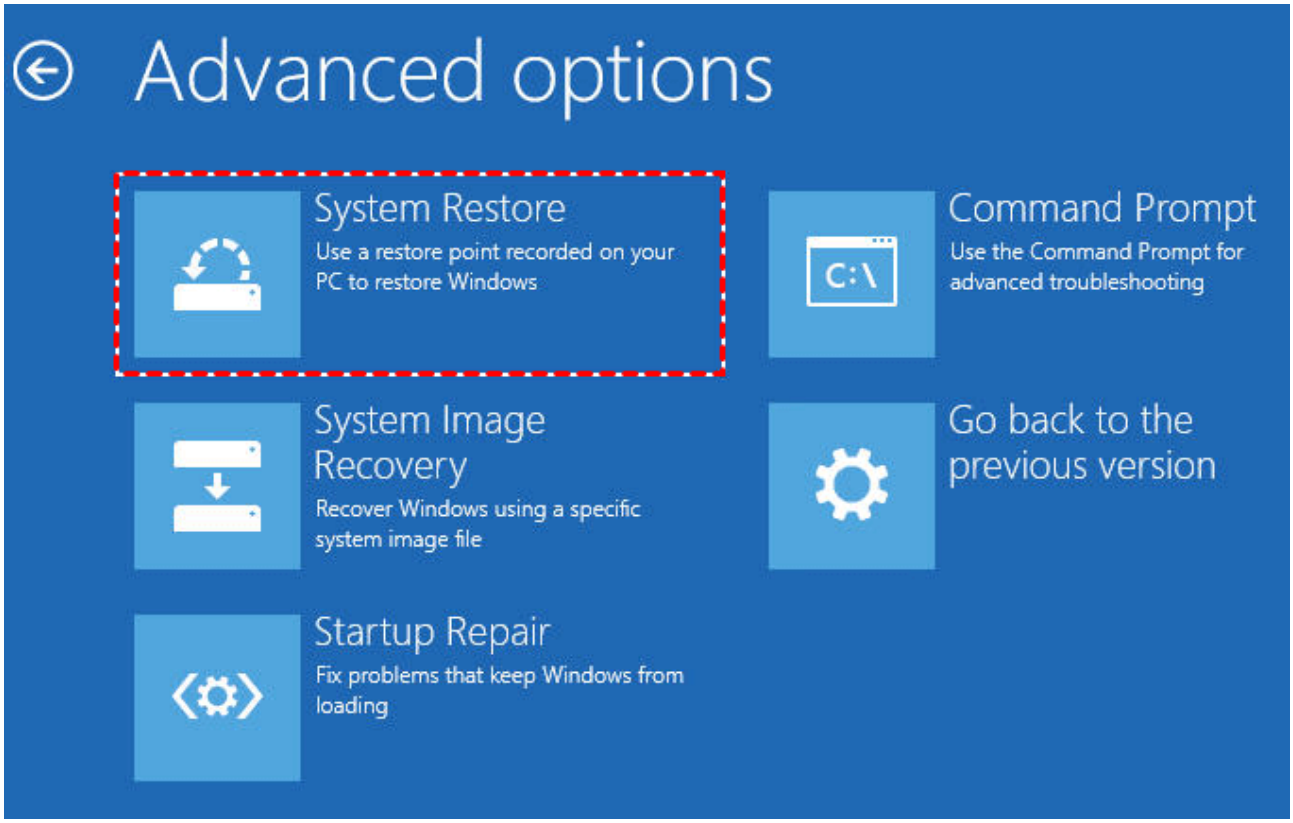

Рис. 3.6. Відновлення системи при завантеженні

Якщо Windows 10 не завантажується, ви можете використовувати точки відновлення: для цього вам знадобиться завантажувальна флешка з Windows 10

(яку доведеться зробити на іншому комп'ютері), або диск відновлення. За використання завантажувальної флешки достатньо вибрати пункт «Відновлення системи» на другому екрані програми установки (рис. 3.7).

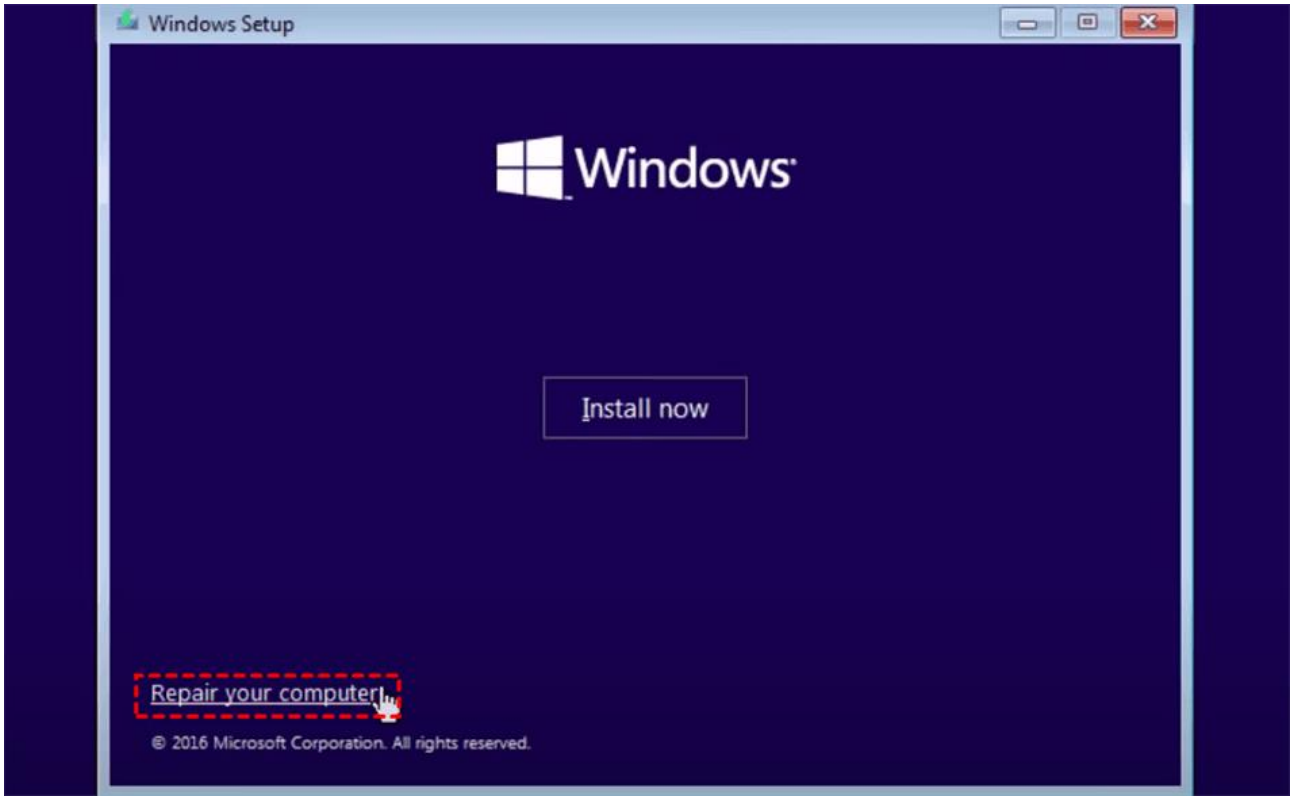

Рис. 3.7. Відновлення з накопичувача з образом ОС Windows 10

І ще один спосіб – запуск відкату до точки відновлення з командного рядка. Він може знадобитися в тому випадку, якщо єдиний працюючий варіант завантаження Windows 10 – безпечний режим з підтримкою командного рядка (рис 3.8).

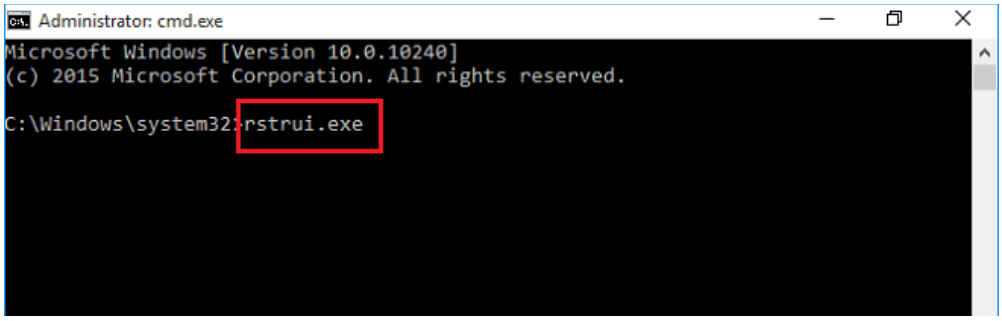

Рис. 3.8. Відновлення з командного рядка у безпечному режимі

Використання Acronis True Image

Після завершення установки заходимо в ПЗ Acronis True Image. На головному екрані вибираємо «Резервне копіювання», «Додати копію» (рис 3.9).

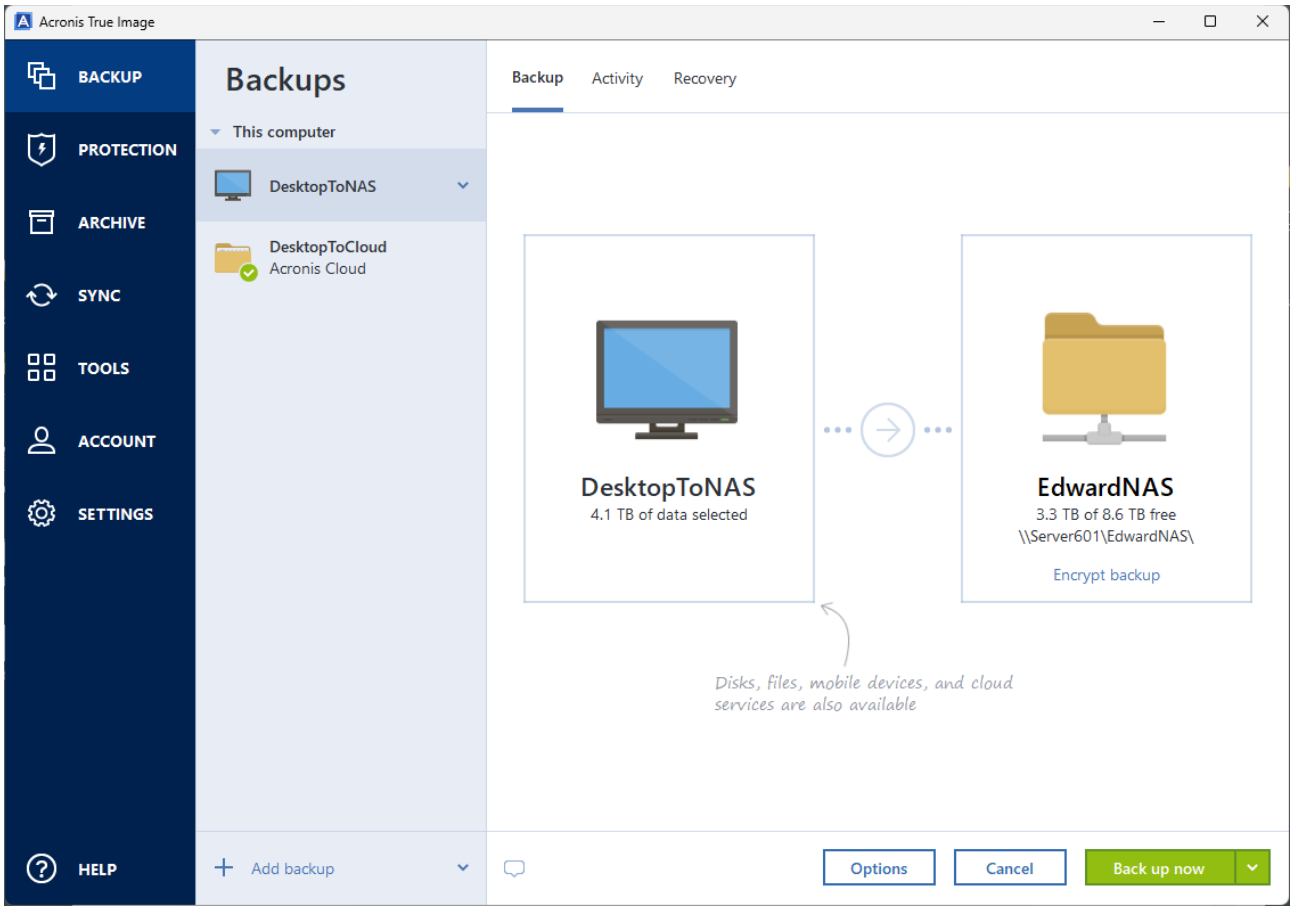

Рис. 3.9. Створення резервної копії у ПЗ Acronis True Image, крок 1

Далі натискаємо «Параметри», вибираємо бажані дати, коли буде робитися бекап, та ставимо галочки в Додаткових налаштуваннях (рис 3.10).

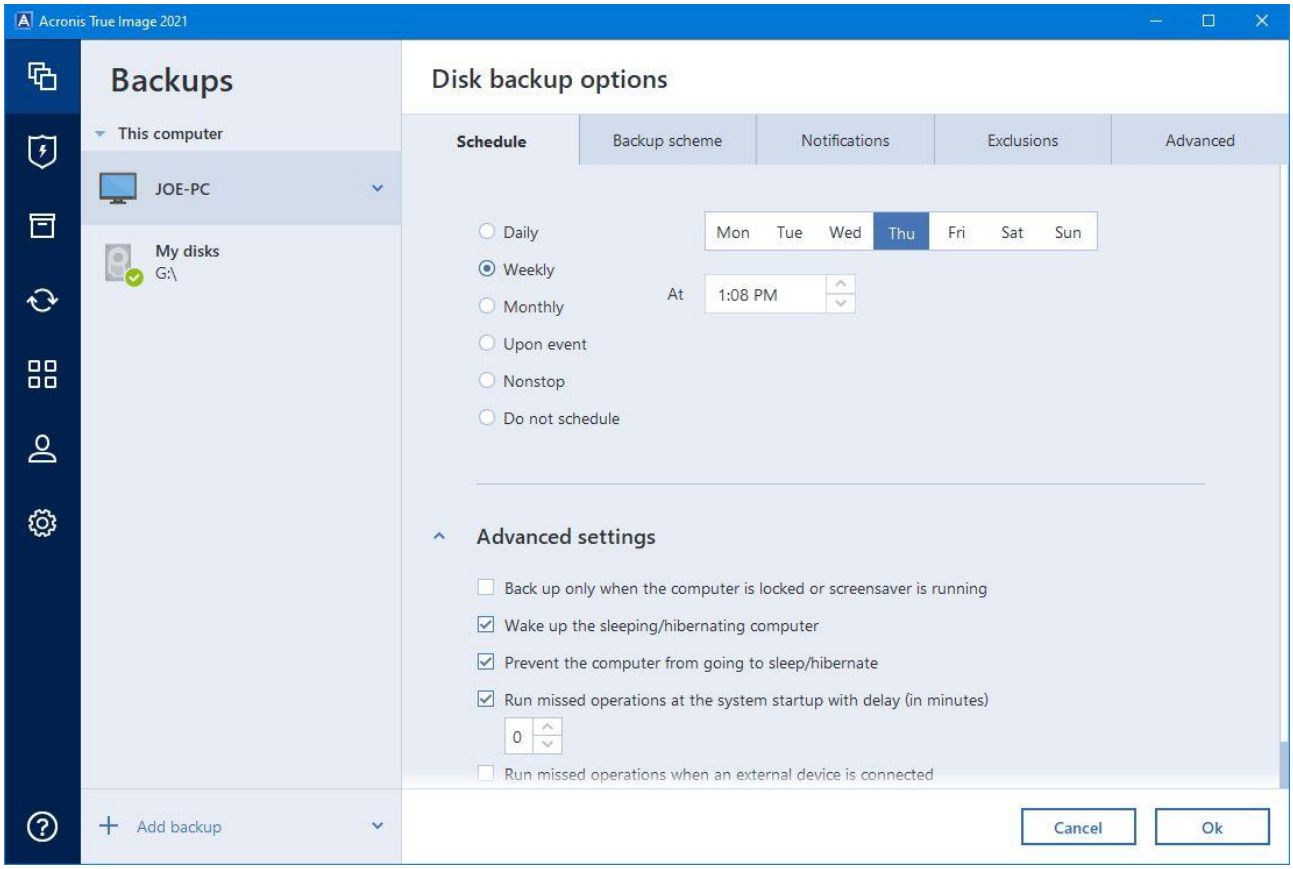

Рис. 3.10. Створення резервної копії у ПЗ Acronis True Image, крок 2

У розділі схеми вибираємо бажану схему, для прикладу взято Інкрементну (рис 3.11).

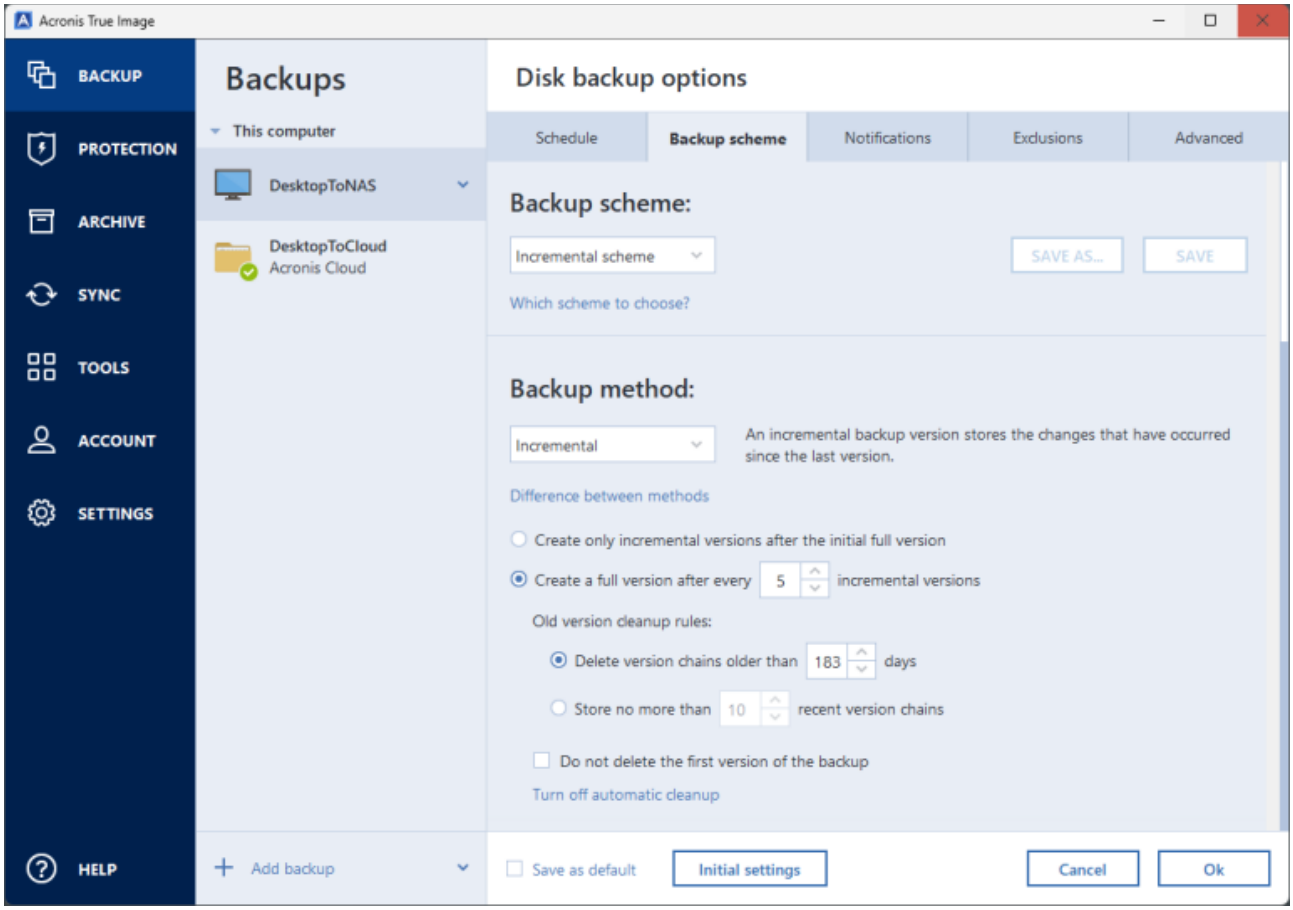

Рис. 3.11. Створення резервної копії у ПЗ Acronis True Image, крок 3

За потреби налаштовуємо сповіщення та винятки (які файли та папки не будуть входити в бекап.

У вкладці додатково ми можемо налаштувати ще декілька параметрів, як от виключення комп'ютера, після того як буде зроблена резервна копія, ступінь стискання бекапу, та встановлення Acronis True Image на носій, куди буде робити бекап (корисно, якщо робить бекап системного диску на окремий носій, у такому разі носій можна буде вибрати для завантаження).

Щоб відновити інформацію є вкладка Відновлення.

3.5. Забезпечення операційної скритності

Основна мета операційної скритності – захистити інформацію, зберегти контроль над кібероперaціями та уникнути виявлення як з боку систем, що здійснюють атаки, так і сторонніх аналітиків або служб безпеки.

Управління ризиками – для того щоб OPSEC був ефективним, необхідно чітко та реалістично визначити можливість збору інформації противником, а також негативні ефекти за витоку інформації.

Неважливу інформацію можна агрегувати, щоб сформувати більш повну картину операцій і запланованої діяльності. Засоби обміну інформацією та технічні інструменти, такі як соціальні медіа, смартфони та геотеги, дозволяють збирати та обмінюватися великою кількістю, здавалося б, не пов'язаної інформації. Відповідальні за OPSEC повинні оцінити ризики для роботи загальнодоступної інформації, зібраної з часом. Противники намагатимуться збирати інформацію протягом усього часу навчання та підготовки до розгортання операції.

OPSEC – це більше, ніж набір конкретних правил та інструкцій. Як циклічний процес, його слід застосовувати до будь-якої операції чи діяльності, щоб захистити критичну інформацію. Він здійснюється за п'ятиетапним процесом (рис 3.11), який є безперервним на всіх етапах операцій, у тому числі після конфлікту. Він не є лінійним, а є безперервним циклом.

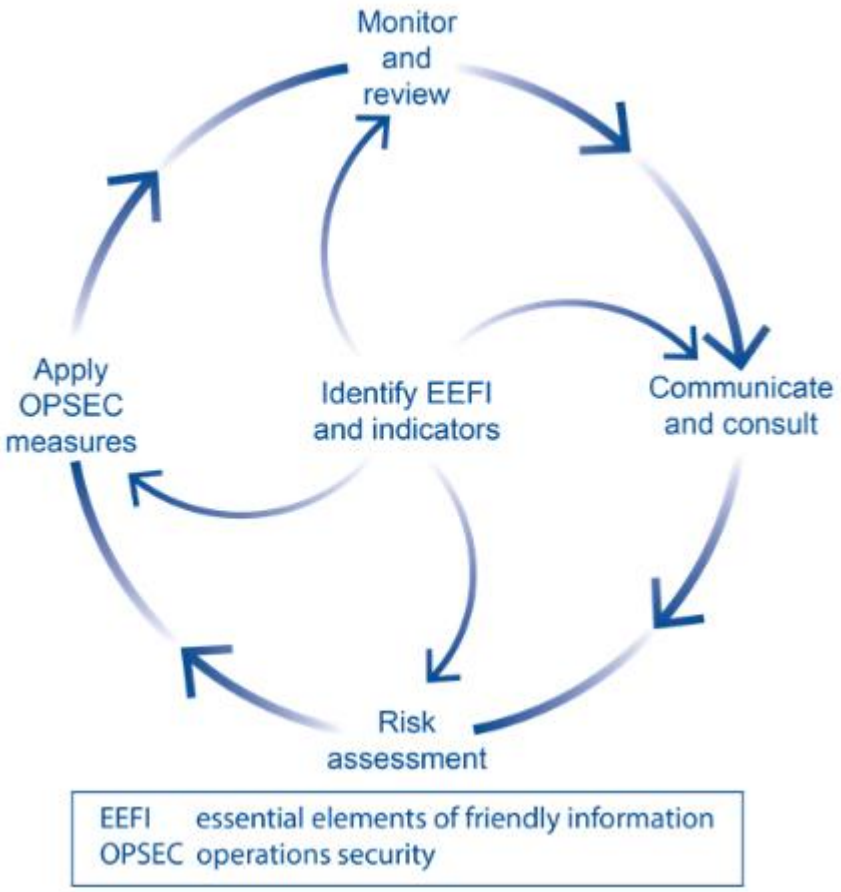

Рис. 3.12. Процес OPSEC

Крок 1: визначте EEFI.

Процес OPSEC повинен визначити контекст ризику. Працівники OPSEC повинні переконатися, що EEFI, специфічні для плану, операції чи діяльності, отримані від відповідного персоналу. Наміри, вимоги, можливості та вразливі місця командувань і формувань компонентів становитимуть основу критичної інформації, яка стосується всіх елементів операційної структури. Оскільки суттєва інформація змінюється на етапах операції, операційну структуру слід оновлювати відповідно. Нові загрози або угода про новий EEFI вимагатимуть переоцінки ризиків і існуючих заходів.

Крок 2: оцінка ризиків.

За оцінки OPSEC відповідає навчений персонал OPSEC, хоча для цього знадобиться допоміжна інформація від іншого персоналу. Працівники OPSEC

повинні тісно співпрацювати з персоналом розвідки, щоб виявити ризики, їх проаналізувати і оцінити. Планування або проведення операцій і заходів підвищить вірогідність індикаторів і створить вразливі місця для використання, особливо за взаємодії цивільних і військових. Уразливість OPSEC існує, коли противник здатний збирати EEFI, аналізувати їх і має час діяти та використовувати ситуацію. Оцінки OPSEC встановлюють базову лінію для відповідної одиниці.

Крок 3: застосування заходів OPSEC. Це має містити необхідні ресурси, синхронізацію, оцінку операцій. Цей процес постійно підживлюється оцінкою ризику. Це може містити відмову від ризику та припинення діяльності по ньому або прийняття та, можливо, збільшення ризику, щоб скористатися можливістю. Це також може передбачати усунення джерела ризику або зміну наслідків, які можуть містити обман. Усі дружні сили відіграють певну роль у застосуванні заходів OPSEC.

Крок 4: моніторинг і перегляд ефективності заходів OPSEC. Постійна оцінка обробки ризиків, яку забезпечує процес OPSEC. Це повинно бути запланованою частиною процесу, який повинен передбачати постійний моніторинг і перегляд. Плани OPSEC можуть провалитися, якщо EEFI буде розкрито ненавмисно. Постійний моніторинг і перегляд процесу OPSEC є важливими.

Крок 5: обговорення та консультація на всіх етапах.

Працівники OPSEC повинні забезпечити оприлюднення перевіреного списку EEFI серед усього персоналу. Спілкування та консультації з командирами та штабом мають відбуватися на всіх етапах процесу OPSEC. OPSEC повинен бути скоординованим з іншими відділами персоналу, щоб забезпечити зворотний зв'язок щодо ефективності OPSEC і виконуватися в об'єднаних силах. Це є важливим для вирішення сприйняття ризику та повинно стосуватися ідентифікованих ризиків, причин, їхніх наслідків (якщо вони відомі) та заходів, необхідних для ліквідації ризиків. Тому особи, відповідальні за оприлюднення інформації, повинні мати необхідну інформацію для розгляду OPSEC перед

оприлюдненням інформації. Працівники OPSEC повинні гарантувати, що агрегування СМІ Організації Північноатлантичного договору (НАТО), військових релізів із громадськістю, командної інформації, соціальних мереж і контрактних документів не розкриває EEFI.

Висновки до розділу 3

У розділі наведено практичні поради (рекомендації) для військовослужбовців з індивідуального захисту себе у кіберпросторі та від засобів радіорозвідки противника. Наголошено, що соціальний простір несе велику небезпеку для операційної секретності, що сім'я військовослужбовця також є суб'єктом операційної секретності та повинна дотримуватися її правил, що не бажаним є приховування інформації про себе від своїх близьких.

Також поверхнево розглянуто методи захисту від розвідки шляхом проведення моніторингу відкритих і відносно відкритих джерел та соціального інжинірингу.

Також вказано порядок дій під час атаки на військовослужбовця ворожої агентури у кіберпросторі.

Сформовано концепцію захисту мобільних пристроїв, чотири її компоненти: фізичний, апаратний, програмний та соціальні мережі (месенджери).

Надано інструкцію з розгортання особистого VPN-сервера та підключення до нього, використовуючи OpenVPN.

Показано способи резервування даних, та розглянуто принципи забезпечення операційної секретності.

ВИСНОВКИ

Робота є складовою більшого проєкту – посібника з індивідуальної та колективної інформаційної безпеки військовослужбовців і малих підрозділів, автором якого є я та мій побратим (його ім'я не вказую на його прохання).

У сучасному суспільстві задоволення потреб в інформації є критичним елементом, що впливає на рівень інформованості особистості, суспільства та держави. Слід зазначити, що задоволення потреб в інформації будь-якою мірою призводить до оволодіння відомостями про навколишній світ та процеси, що протікають в ньому, тобто інформованості особистості, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і, як наслідок, обґрунтованість рішень та дій, що приймаються.

Створення систем інформаційної безпеки ґрунтується на таких принципах:

1. Комплексний підхід до побудови системи захисту, що означає оптимальне поєднання взаємопов'язаних організаційних, програмних, апаратних, фізичних та інших властивостей, підтверджених практикою створення вітчизняних і зарубіжних систем захисту і застосовуються на всіх етапах технологічного циклу обробки інформації.

2. Принцип безперервного розвитку системи є одним з основних для комп'ютерних інформаційних систем, ще більш актуальний для систем інформаційної безпеки. Способи реалізації загроз інформації безперервно удосконалюються, а тому забезпечення безпеки інформаційних систем не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення систем інформаційної безпеки, безперервному контролі, виявленні її вузьких і слабких місць, потенційних каналів витоку інформації та нових способів несанкціонованого доступу,

3. Забезпечення надійності системи захисту, тобто неможливість зниження рівня надійності за виникнення в системі збоїв, відмов, навмисних дій зломщика або ненавмисних помилок користувачів і обслуговуючого персоналу.

4. Забезпечення контролю за функціонуванням системи захисту, тобто створення засобів і методів контролю працездатності механізмів захисту.

5. Забезпечення всіляких засобів боротьби зі шкідливими програмами.

6. Забезпечення економічної доцільності використання системи. Захисту, що виражається в перевищенні можливого збитку від реалізації загроз над вартістю розробки та експлуатації систем інформаційної безпеки.

У результаті вирішення проблем безпеки інформації сучасні інформаційні системи повинні мати такі основні ознаки:

- Наявність інформації різного ступеня конфіденційності;
- Забезпечення криптографічного захисту інформації різного ступеня конфіденційності при передачі даних;
- Обов'язкове управління потоками інформації як в локальних мережах, так і при передачі по каналах зв'язку на далекі відстані;
- Наявність механізму реєстрації та обліку спроб несанкціонованого доступу, подій в інформаційній системі та документів, що виводяться на друк;
- Обов'язкове забезпечення цілісності програмного забезпечення та інформації;
- Наявність засобів відновлення системи захисту інформації;
- Наявність фізичної охорони засобів обчислювальної техніки і магнітних носіїв;
- Наявність спеціальної служби інформаційної безпеки системи.

У продуманій архітектурі безпеки усі вони мають бути присутніми.

З практичної точки зору важливими також є такі принципи архітектурної безпеки:

- безперервність захисту у просторі та часі, неможливість оминути захисні засоби;

- наслідування визнаних стандартів, використання апробованих рішень;
- ієрархічна організація ІС з невеликим числом сутностей на кожному рівні;
- посилення найслабкішої ланки;
- неможливість переходу в небезпечний стан;
- мінімізація привілеїв;
- розділення обов'язків;
- ешелонування оборони;
- різноманітність захисних засобів;
- простота і керованість інформаційної системи.

Україні бракує як нормативно правової бази, наявності відповідних інституцій, так і систем, що могли б задовольняти основні ознаки сучасної та безпечної інформаційної системи.

Стосовно нормативної бази, то в Україні немає власної доктрини операційної секретності. Існують схожі документи, зокрема Доктрина Військ зв'язку та кібербезпеки Збройних Сил України, але вони не достатньо розкривають питання. В основному такі публікації частково керуються документом AJP-3.10.2 – Доктрина безпеки операцій та приховування НАТО.

Через відсутності власної доктрини по операційній скритності ми постійно стикаємося з витоками інформації по відкритих джерелах, особовий склад не повною мірою розуміє перелік критичної інформації, не проводяться навчання та немає штатної посадової особи, яка б відповідала за ці питання.

Треба розуміти, що кібервійна ніколи не припинялась, а отже, і гібридна війна також. Більшість часу Україна лише пасивно захищалася, будь-які активні дії зупинялися державою.

Важливим фактом є те, що ворог вже має великі обсяги інформації про громадян України. У цьому їм допомогли як чисельні зламування державних реєстрів, так і активний збір інформації з відкритих джерел.

З цього можна виділити декілька проблем. У часи проведення мобілізації стати військовослужбовцем може кожний як людина, що не мала присутності у соціальних мережах, так і людина, яка веде активне соціальне життя.

У другому випадку у противна вже є велика, а деколи вичерпна, інформація про людину. Видалення соціальних сторінок лише приверне увагу автоматизованих засобів, так само як і кардинальне змінення поведінки у мережі. Але зазвичай такі особи, навпаки, публікують інформацію, що вони задіяні у Силах Оборони України і навіть додають інформацію про конкретний підрозділ.

Отже, велика кількість людей, задіяних у важливих для держави сферах як Збройні Сили, Міністерство з питань стратегічних галузей промисловості України, Міністерство соціальної політики України тощо, є слабким місцем в інформаційній безпеці, оскільки ворожій агентурі достатньо здійснити вплив на вразливу особу шантажем, погрозами або використанням в «темну».

Наприклад. Знайшовши адресу проживання, наявність дитини або інших близьких осіб, противник може вдатися до фізичних дій шантажування – напис на дверях, залякування особи тощо. В більшості випадків особі, на яку чинять вплив, дають інструкції щодо не звернення у відповідні структури, поліцію, керівництво організації, де вона працює, колег. Це має свій вплив, оскільки існує проблема довіри суспільства до силових структур в плані вирішення подібних питань. У випадку, коли особа, на яку чинять вплив, прийняла правила гри противника, вона становить велику загрозу інформаційній безпеці не тільки до структури до якої вона причетна, але і до інших структур.

Для вирішення таких проблем у цій роботі представлено чотирирівневу концепцію захисту військовослужбовця та його мобільних пристроїв:

фізичний – захист персональних та службових пристроїв від спроб фізичного зламування: важлим є використання двох, а у випадку роботи безпосередньо біля лінії бойового зіткнення трьох мобільних пристроїв, що дозволяє розмежувати інформацію, яка на них зберігається; компрометація

«військового телефону» не призведе до компрометації цивільної особистості військовослужбовця;

апаратний – захист від засобів радіорозвідки ворога та використання надійних паролів і не використання невідомих пристроїв (зарядок, шнурів, накопичувачів), найвідомішим з яких є Леер-3, розписано необхідність пріорітації використання мережі інтернет для зв'язку, не використання невідомих точок доступу, мереж WiFi;

програмний – важливість вірного налаштування дозволів у телефоні, методи перевірки мережевого трафіку на телефоні та маркери можливої компрометації мобільного пристрою;

соціальних мереж (месенджери) – розкрито важливість адаптації соціальної мережі військовослужбовця, видалення метаданих.

Окремо охарактеризовано захист від соціального вектору, від класичного через соціальну комунікацію, виділення у соціумі через характерні ознаки: форма; машина з характерними номерами; статутні засоби контролювання доступу, шлагбаум, вартовий, таблички. Наведено визначення OSINT, GEOINT та у який спосіб ці методи добувають інформацію. Наголошено про наслідки поєднання цивільної та військової особистості військовослужбовця і наведено порядок дій за спроби шантажування такого військовослужбовця. Розписані рекомендації з поводження у соціальних мережах та проінформовано про можливі цілеспрямовані дії ворожих сил.

Надано інструкції з використання особистих VPN-мереж та комплексного підходу з резервування даних.

Впровадження цієї концепції не потребує великих витрат та може бути достатньо швидким у державній сфері.

У роботі представлено саме індивідуальний захист, включаючи родину суб'єкта, але важливим є те, що «операційна секретність – відповідальність кожного її суб'єкта». Тільки у разі використання представленої концепції всіма суб'єктами підрозділу, вона буде найбільш ефективною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Болтрик Є., Манжело А. Ексклюзивне інтерв'ю із заступником голови Держспецзв'язку України з питань цифрового розвитку, цифрових трансформацій і цифровізації Віктором Жорою агентству «Інтерфакс-Україна». Інтерфакс-Україна. URL : https://interfax.com.ua/news/interview/911979.html (дата звернення: 01.10.2024).

2. Медіаграмотність. Практичні поради військовослужбовцям Збройних Сил України : порадник від 29.07.2021 № ВП 1-185(49)03.01.

3. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021.

4. Про національну безпеку України : Закон України від 09.08.2024

5. Про основні засади забезпечення кібербезпеки України : Закон України від 28.08.2024.

6. Про організаційно-технічну модель кіберзахисту : постанова Кабінету Міністрів України від 29.12.2021 №1426.

7. Інформаційна і кібербезпека: соціотехнічний аспект. [Підручник]. / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа / За заг. ред. д.т.н., проф. В. Б. Толубко. К. : ПВП «Задруга», 2014. 317 с. ISBN 978–966–2970–86–9

8. Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Вінниця : ВНТУ, 2018. 316 с.

9. Економічна безпека підприємств, організацій та установ / Ортинський В. Л., Керницький І. С., Живко З. Б., Керницька М. І., Гук О. В., Шимечко Г. І., Живк, 2011. 704 с. ISBN 978-617-566-035-5

10. Про затвердження Зводу відомостей, що становлять державну таємницю : наказ Служби Безпеки України від 23.12.2020 № 383.

11. Peter Mell. Computer Attacks: What They Are and How to Defend Against Them. NIS I . Computer Security Division, 1999. URL : http://cskc.nist.gov/publications/nistbul/html- archive/may-99.html

12. Інформаційна безпека держави. Конспект лекцій для здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 262 «Правоохоронна діяльність» / Укл.: Ю. М. Ткач, С. М. Семендяй. Чернігів : НУ «Чернігівська політехніка», 2022. 133 с.

13. Методика оцінки загроз для інформації автоматизованих систем : Будько М. / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 10, 2005. УДК 681.3.

14. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія / О. В. Левченко. Житомир : Видавець ПП «Євро-Волинь», 2021. 172 с. ISBN 978-617-7992-08-9.

15. Про Статут внутрішньої служби Збройних Сил України : Закон України від 04.05.2024.

16. Allied Joint Doctrine for Operations Security and Deception: AJP-3.10.2.

17. Кібервійна росії проти України. SPEKA Media. 2024. URL : https://speka.media/kiberviina-rosiyi-proti-ukrayini-9qy4ok (дата звернення: 01.10.2024).

18. Greenberg A. The Underground History of Russia's Most Ingenious Hacker Group. Wired. 2023. URL : https://www.wired.com/story/turla-history-russia-fsb-hackers/ (дата звернення: 01.10.2024).

19. Tanriverdi H., Flade F., Frey L. The Elite Hackers of the FSB. Bayerischer Rundfunk. 2022. URL: https://interaktiv.br.de/elite-hacker-fsb/en/index.html (дата звернення: 01.10.2024).

20. Горбулін В. Как победить Россию в войне будущего. Київ : Брайт Букс, 2020. 256 с..

21. Лисичкин, В. А. Третья мировая информационно-психологическая война [Електронний ресурс] / В. Лисичкин, Л. Шелепин. М. : Академия социальных наук, 1999. [Електронний ресурс]: http://www.duel.ru/publish/lisichkin/voina.html.

22. Рада національної безпеки і оборони України: Експертні консультації Україна – НАТО з питань кібернетичного захисту. [Електронний ресурс]. Режим доступу: http://www.rainbow.gov.ua/news/ 1076.html

23. Остроухов, В. В. Інформаційна безпека [Електронний ресурс]. http://westudents.com.ua/glavy/51894-12-nformatsyna-vyna-yak-forma-vedennya-nformatsynogoprotiborstva.htm

24. Карнаух А. А., Шевчук З. Ю. Інформаційна війна на сучасному етапі розвитку суспільства / А. А. Карнаух, З. Ю. Шевчук./ *Науковий часопис НПУ імені М. П. Драгоманова*. Серія 18. Економіка і право. 2015. Вип. 29. С. 98–103.

25. Малик Я. Інформаційна війна і Україна. Демократичне врядування. 2015. Вип. 15. [Електронний ресурс]:http://nbuv.gov.ua/UJRN/DeVr_2015_15_3.

26. Носов В. Манжай О. Оремі аспекти протидії інформаційної війни в Україні. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. Вип. 1. С. 26 – 32.

27. P. J. Sun, «Privacy protection and data security in cloud computing: a survey, challenges, and solutions», IEEE Access, vol. 7, pp. 147 420–147 452, 2019.

28. Положення про Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України у новій редакції, затверджене наказом Адміністрації Держспецзв'язку від 26.10.2020 № 686.

29. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22;

30. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22;

31. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53;

32. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22;

33. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 № 60;

34. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 № 125;

35. Wang J. Encyclopedia of Data Warehousing and Mining/J.Wang; Second Edition. Hershey : Information Science Reference, 2009. 2227 p.

36. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Том 19, № 2 (2013). С. 118–129.

37. Українці стали частіше користуватися інтернетом, 80 % – онлайн щодня: соцопитування URL : https://www.undp.org/uk/ukraine/press-releases/ukrayintsi-staly-chastishe-korystuvatysya-internetom-80-onlayn-shchodnya-sotsopytuvannya (дата звернення: 20.10.2024).

38. Служба внешней разведки России создает ботов для социальных сетей за 30 млн рублей. URL : http://habrahabr.ru/post/150269 (дата звернення: 15.01.2021).

39. Дубов Д. В. «Активні заходи» СРСР проти США: пролог до гібридної війни : аналіт. доп. / Д. В. Дубов, А. В. Баровська, Т. О. Ісакова, І. О. Коваль, В. П. Горбулін ; за заг. ред. Д. В. Дубова. Київ : НІСД, 2017. 88 с.

40. Левченко О. В., Косогов О. М. Методика виявлення заходів негативного інформаційного впливу на основі аналізу відкритих джерел. *Системи обробки інформації*. Харків : ХУПС, 2016. № 1 (138). С. 100–102.

41. Ланде Д. В., Фурашев В. М. Інформаційні операції крізь призму системи моніторингу та інтеграції інтернет-ресурсів. *Правова інформатика*. 2009. № 2 (202). С. 49–57.

42. U. S. National Strategy for Public Diplomacy and Strategic Communication. URL : http://www.au.af.mil/au/awc/awcgate/state/natstrat_strat_comm.pdf (дата звернення: 29.07.2020).

43. Баровська А. Стратегічні комунікації: досвід НАТО. *Стратегічні пріоритети*. Київ : НІСД, 2015. № 1 (34). С. 147–152.

44. Ліпкан В. А., Попова Т. В. Стратегічні комунікації : словник. Київ : ФОП О. С. Ліпкан. 2016. 416 с.

45. Панченко В. М. Структурно-функціональний аналіз загальнодержавної системи забезпечення інформаційної безпеки. *Інформаційна безпека людини, особи, держави*. 2009. № 1. С. 34–39.