МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

ОПОРНИЙ КОСПЕКТ ЛЕКЦІЙ

з дисципліни

«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

для студентів освітньо-кваліфікаційного рівня «бакалавр»
спеціальність «Кібербезпека»

Тернопіль
ЗУНУ
2023

Опорний конспект лекцій з дисципліни «Управління інформаційною безпекою» для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Яцків В.В., Давлетова А.Я., Драпак В.І. – Тернопіль 2023. – 49с.

Опорний конспект лекцій складається з частин, що рекомендовані програмою на основі галузевого стандарту вищої освіти України з спеціальності «Кібербезпека»

Укладачі: Василь ЯЦКІВ
Аліна ДАВЛЕТОВА
Володимир ДРАПАК

Рецензенти:
Франко Ю.П. к.т.н., доцент, завідувач кафедри комп'ютерних технлогій Тернопільського національного педагогічного університету.
Возна Н.Я. д.т.н., професор, професор кафедри спеціалізованих комп'ютерних систем Західноукраїнського національного університету.

Розглянуто та схвалено на засіданні кафедри кібербезпеки, протокол №10 від 11.04.2023

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека, протокол №4 від 11.04.2023

ЗМІСТ

ІНФОРМАЦІЙНІ РЕСУРСИ, ЩО ПІДЛЯГАЮТЬ ЗАХИСТУ

1. Основні поняття
2. Сфери розповсюдження державної таємниці на інформацію
3. Комерційна таємниця
4. Персональні дані

1. Основні поняття

- **Конфіденційність** - властивість інформації бути захищеною від неправомірного ознайомлення.
- **Цілісність** - умови, за яких інформацію зберігають, передають та приймають без змін.
- **Доступність** - коли суб'єкти, які мають право на безперешкодний доступ до інформації, можуть його реалізувати.

У Законі України «Про захист інформації в інформаційно-комунікаційних системах» наведено означення основних термінів.

2. Сфери розповсюдження державної таємниці на інформацію

Державна таємниця розповсюджується на інформацію з різних галузей життєдіяльності держави, наприклад, у сфері оборони, у сфері економіки, науки і техніки, у сфері зовнішніх відносин, у сфері державної безпеки та охорони правопорядку.

Конкретні відомості можуть бути віднесені до державної таємниці за **ступенями секретності** «особливої важливості», «цілком таємно» та «таємно» лише за умови, що вони належать до категорій, зазначених вище, і їх розголошення завдаватиме шкоди інтересам національної безпеки України.

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

3. Комерційна таємниця

Комерційна таємниця – це відомості, що не є державною таємницею, зв'язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій чи фірм, розголошення, витік і несанкціонований доступ до яких може завдати шкоди їх інтересам.

Комерційну таємницю можуть складати відомості, які відносяться до широкого кола питань підприємницької діяльності. Підприємець, що виготовляє чи придбає законним шляхом конфіденційну інформацію, самостійно встановлює склад і обсяг відомостей, що відносяться до комерційної таємниці, строки, порядок захисту і доступу до неї, правила її використання та умови передачі іншим особам.

4. Персональні дані

Персональні дані – інформація (зафіксована на будь-якому матеріальному носієві) про конкретну людину, яка ототожнена або може бути ототожнена з нею.

Персональні дані умовно можна поділити на різні категорії:

1.За природою відомостей на:

- об’єктивні відомості про фізичну особу (біометричні дані, стан банківського рахунку тощо);
- суб’єктивні відомості про фізичну особу (автобіографія, характеристика, матеріали атестації, опис особистих рис фізичної особи, досьє тощо);

2. За формою обробки відомостей на:

- відомості на паперових носіях;
- відомості на електронних, магнітних, оптичних носіях тощо;

3. За зв’язком з фізичною особою на:

- відомості, що стосуються фізичної особи безпосередньо (особова справа працівника, запис у базі даних медичного закладу, банківський рахунок тощо);
- відомості, що стосуються фізичної особи опосередковано (реєстраційний запис про право власності на об’єкт нерухомого майна, записи відеоспостереження у громадських місцях, записи про технічне обслуговування автомобіля тощо);
- відомості, що можуть стосуватися фізичної особи та впливати на її права й інтереси.

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Основні поняття і класифікація загроз
2. Основні загрози доступності
3. Основні загрози цілісності
4. Основні загрози конфіденційності

1. Основні поняття і класифікація загроз

Загроза – це потенційна можливість певним чином порушити інформаційну безпеку (ІБ). Реалізація загрози спричиняє моральний чи матеріальний збиток, а захист і протидія загрозі покликані знизити його обсяг, в ідеалі – цілком, на практиці – значно або хоча б частково.

Спроба реалізації загрози називається **атакою**, а той, хто робить таку спробу, – **зловмисником** (порушником).

Побудова моделі зловмисника – це процес класифікації потенційних порушників за такими параметрами:

- тип зловмисника (конкурент, клієнт, розробник, співробітник компанії тощо);
- розташування зловмисника відносно об'єктів захисту (внутрішній, зовнішній);
- рівень знань про об'єкти захисту і оточення (високий, середній, низький);
- рівень можливостей доступу до об'єктів захисту (максимальні, середні, мінімальні);
- час дії (постійно, в певні часові інтервали);
- місце дії (місце розташування зловмисника під час реалізації атаки).

Потенційні зловмисники називаються **джерелами загрози**. Найчастіше загроза є наслідком наявності вразливих місць у захисті інформаційної системи (ІС), наприклад, можливість доступу сторонніх осіб до критично важливого устаткування або помилки в програмному забезпеченні (ПЗ).

Проміжок часу від моменту, коли з’являється можливість використати слабке місце, і до моменту, коли пропуск ліквідується, називається **вікном небезпеки**, що асоціюється з даним вразливим місцем.

Загрози класифікуються за такими критеріями:

- за аспектом ІБ (доступності, цілісності, конфіденційності), проти якого загрози спрямовані в першу чергу;
- за компонентами ІС, на які загрози націлені (дані, програми, апаратура, підтримувальна інфраструктура);
- за способом здійснення (випадкові/навмисні дії природного або техногенного характеру);
- за розташуванням джерела загрози (всередині/зовні ІС);
- за обсягом збитку (граничний, після якого фірма може стати банкрутом; значний, але не призводить до банкрутства; незначний, який фірма за якийсь час може компенсувати);
- за ймовірністю виникнення (дуже ймовірна загроза; ймовірна загроза; малоймовірна загроза);
- за характером нанесеного збитку (матеріальний; моральний).

2. Основні загрози доступності

Загрози доступності класифікуються за компонентами ІС, на які спрямовані загрози:

- відмова користувачів;
- внутрішня відмова ІС;
- відмова інфраструктури, що підтримує ІС.

Стосовно користувачів розглядаються такі загрози:

- небажання працювати з ІС (найчастіше виявляється, коли необхідно

освоювати нові можливості і в разі розбіжності між запитами користувачів і фактичними можливостями та технічними характеристиками);

- неможливість працювати із системою через відсутність відповідної підготовки (недолік загальної комп'ютерної освіти, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією і т.п.);
- неможливість працювати із системою через відсутність технічної підтримки (неповнота документації, нестача довідкової інформації тощо).

Основними джерелами внутрішніх відмов є:

- порушення (випадкове або навмисне) правил експлуатації;
- вихід системи зі штатного режиму експлуатації;
- помилки при (пере)конфігурації системи;
- відмови програмного і апаратного забезпечення.

Як засіб виведення системи зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (звичайно – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). Для виведення систем з штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок.

Віддалене споживання ресурсів –скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю прямують цілком легальні запити на з'єднання та/або обслуговування. Якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною спроможністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність украй важко.

Відмови ПЗ часто провокуються впровадженням в ІС так званого шкідливого ПЗ, дії якого спрямовані на:

- руйнування даних;
- руйнування або пошкодження апаратури (носіїв даних).

Таке пошкодження може викликатися як природними причинами так і штучними. Джерела безперебійного живлення не захищають від потужних короткочасних імпульсів (наприклад, блискавок), і випадки вигорання устаткування – не рідкість. Потужній короткочасний імпульс, здатний зруйнувати дані на магнітних носіях, можна згенерувати і штучним чином – за допомогою так званих високоенергетичних радіочастотних гармат.

Стосовно інфраструктури розглядаються такі загрози:

- порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо- і/або теплопостачання, кондиціонування;
- руйнування або пошкодження приміщень;
- неможливість або небажання обслуговуючого персоналу і/або користувачів виконувати свої обов'язки (цивільні безлади, аварії на транспорті,

терористичний акт або його загроза, страйк тощо).

3. Основні загрози цілісності

У більшості випадків винуватцями загроз цілісності є штатні співробітники організацій, добре знайомі з режимом роботи і заходами захисту. З метою порушення цілісності зловмисник може:

- ввести неправильні дані;
- змінити дані;
- знищити дані.

Потенційно вразливі з погляду порушення цілісності не тільки дані, але і програми. Впровадження шкідливого ПЗ – приклад подібного порушення.

Загрозами динамічної цілісності є:

- порушення атомарності транзакцій,
- переупорядковування,
- крадіжка,
- дублювання даних або внесення додаткових повідомлень.

4. Основні загрози конфіденційності

У загальному випадку, конфіденційну інформацію можна поділити на **службову** та **предметну**.Службова інформація (наприклад, паролі користувачів) не належить певній предметній галузі, в ІС вона грає технічну роль, але її розкриття особливо небезпечно, оскільки воно може забезпечити несанкціонований доступ до всієї інформації, зокрема предметної. Навіть якщо інформація зберігається в комп’ютері або призначена для комп’ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер.

Перехоплення даних – дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються багатьма каналами, їх захист може виявитися достатньо складним і дорогим. Технічні засоби перехоплення доступні, прості в експлуатації, а встановити їх, наприклад на кабельну мережу, може хто завгодно, тому цю загрозу потрібно брати до уваги стосовно не тільки зовнішніх, а й внутрішніх комунікацій.

Крадіжки устаткування є загрозою не тільки для резервних носіїв, але і для комп’ютерів, особливо портативних. Часто ноутбуки залишають без нагляду на роботі або в автомобілі, іноді просто гублять.

Небезпечною не технічною загрозою конфіденційності є методи соціальної інженерії. До загроз, від яких важко захищати інформацію, можна віднести зловживання повноваженнями. Інший приклад – нанесення збитку при сервісному обслуговуванні. Звичайно сервісний інженер дістає необмежений доступ до устаткування і має можливість діяти в обхід програмних захисних механізмів.

ХАРАКТЕРИСТИКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1. Характеристики основних видів безпеки.

2. Рівні та види безпеки.

3. Задачі забезпечення цілісності, доступності, конфіденційності та приватності.

1. Характеристики основних видів безпеки.

Суть національної безпеки - у протидії і компенсації будь-яких деструктивних заворушень, що формуються всередині суспільства або за його межами, які шкодять потребам життєдіяльності і розвитку суспільства та особистості.

У зв'язку з цим у національній безпеці виділяють три рівні безпеки:

- **Безпека особистості** - положення, при якому особистості не загрожує небезпека. Безпека особистості полягає у формуванні комплексу правових і моральних норм, суспільних інститутів та організацій, які дозволили би їй розвивати й реалізовувати соціально значимі здібності й потреби, не зазнаючи при цьому протидії держави й суспільства.
- **Безпека суспільства** - наявність суспільних інститутів, норм, розвинених форм суспільної свідомості, які дозволяють реалізувати права та свободи усіх груп населення і протистояти діям, що ведуть до розколу суспільства (у тому числі і зі сторони держави).
- **Безпека держави** - положення, при якому державі не загрожує небезпека. Досягається наявністю ефективного механізму управління і координації діяльності політичних сил та суспільних груп, а також активних інститутів (органів) їхнього захисту.

2. Рівні та види безпеки

Політична безпека [political security] - здатність і можливості нації та її державних інститутів самостійно вирішувати питання державного устрою, незалежно проводити внутрішню і зовнішню політику в інтересах особистості та суспільства.

Економічна безпека [economy security] - положення, при якому економіці держави не загрожує небезпека, проте створення замкненого самодостатнього господарства в межах окремої країни або їх групи, спрямоване на обмеження імпорту, розвиток експорту товарів і капіталу, а також економічна залежність руйнують системи економічної безпеки.

Соціальна безпека базується на психічному та психологічному стані населення держави. Залежить від багатьох інших видів безпеки та чинників (наявність безробітних, багатодітних родин, кримінальних угруповань, правоохоронних органів і т.ін.). Відчутно змінюється під час воєн, епідемій,

підвищення цін, проведення виборів.

Воєнна безпека [military security] - положення, що характеризує можливість забезпечення національної безпеки засобами збройного насильства.

Екологічна безпека - це стан системи "природа - техніка - людина", який забезпечує збалансовану взаємодію природних, технічних та соціальних систем, формування природно-культурного середовища, яке відповідає санітарно-гігієнічним, естетичним і матеріальним потребам людей при збереженні природно-ресурсного та екологічного потенціалу природних систем і здатності біосфери в цілому до саморегулювання. Важливою її складовою є стан захищеності особистості, суспільства і держави від загроз, які створюються стихійними лихами і техногенними катастрофами.

Науково-технологічна безпека характеризується станом фундаментальних, пошукових і прикладних наукових досліджень, які забезпечують стабільний розвиток науково-технічного, технологічного й соціально-економічного потенціалу держави на світовому рівні.

Забезпечення безпеки в інформаційній сфері. Стрімке зростання ІТ призвело до початку перерозподілу у суспільстві реальної влади від традиційних структур до центрів управління інформаційними потоками. ІТ широко застосовуються Будь-яка диверсія у таких сферах, як фінансовий обіг і ринок цінних паперів, зв'язку, транспорті, високотехнологічних виробництвах, державних системах управління і т.ін. може призвести до тяжких наслідків.

3. Задачі забезпечення цілісності, доступності, конфіденційності та приватності

Для характеристики основних критеріїв інформаційної безпеки застосовують **модель тріади CIA** Confidentiality, Integrity and Availability (CIA)). Ця система передбачає основні характеристики ІБ: конфіденційність, цілісність та доступність.

ІС аналізуються для того, щоб ідентифікувати і застосувати промислові стандарти ІБ, як механізми захисту і запобігання, на **трьох рівнях**:

- фізичному;
- особистому;
- організаційному

в **трьох головних секторах**:

- технічних засобах;
- програмному забезпеченні;
- комунікаціях.

По суті, процедури або правила запроваджуються для інформування адміністраторів, користувачів та операторів щодо використовування захисної продукції для гарантування ІБ в межах організацій.

У Концепції державної інформаційної політики України визначено сучасний стан інформаційної сфери, окреслено коло проблем, на розв'язання яких спрямована державна інформаційна політика та встановлюються пріоритетні завдання державної інформаційної політики.

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Механізми реалізації інформаційної безпеки.
2. Методи забезпечення інформаційної безпеки.
3. Положення щодо політики безпеки.

1. Механізми реалізації інформаційної безпеки

Фактично, реалізація ІБ має дві частини:

- Код – це програми в довірчій обчислювальній базі (в комплексі засобів захисту).

- Налаштування – це всі дані, які керують операціями цих програм: списки контролю доступу, членство в групі, користувацькі паролі, ключі шифрування і т.д.

Задача реалізації захисту повинна протидіяти загрозам, які зустрічаються в таких основних формах:

- шкідливі (помилкові або ворожі) програми;
- шкідливі (ворожі) агенти – користувачі (або програми), які надають хорошим, але легковірним програмам свідомо помилкові команди;
- шкідливі агенти, які підключаються до комунікацій і заповнюють їх своїми повідомленнями.

У загальному випадку існують чотири **стратегії захисту**.

- **Нікого не впускати.** Це повна ізоляція. Вона забезпечує найкращий захист, але перешкоджає використанню інформації або послуг від інших, і передачі їх іншим користувачам. Це непрактично для всіх.
- **Не впускати порушників.** Програми всередині цього захисту можуть бути легковірними. Це дозволяє зробити електронні цифрові підписи програм і міжмережеві екрани (МЕ).
- **Пустити порушників, але перешкодити їм в заподіянні шкоди.** Традиційним способом захисту служить динамічне ПЗ типу на основі процесів операційної системи.
- **Захопити порушників і переслідувати їх**. Передбачає здійснення аудиту силовими та правоохоронними структурами.

Щоб зробити роботу захищеною використовуються **комплекс засобів захисту** (КЗЗ) – набір апаратних засобів, ПЗ та інформації з налаштування (setup), від якої залежить захист системи.

Хорошим способом запобігання шкоди, яку можуть заподіяти дефекти в КЗЗ є використання **захисту в глибину** (ешелоновану оборону), тобто надлишкові механізми захисту. При цьому порушникові буде складно одночасно використовувати слабкості різних систем на всіх рівнях. Ешелонована оборона не дає строгих гарантій, але насправді, практично допомагає.

2. Методи забезпечення інформаційної безпеки

Діяльність із забезпечення ІБ здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану та можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення ІБ є **методи опису і класифікації**. У якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються **методи дослідження причинних зв'язків. Вибір методів аналізу** стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери ІБ, то у ній зазвичай виділяють такі рівні:

- **На фізичному рівні** здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій.
- **На програмно-технічному рівні** здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.
- **На рівні управління** здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення інформаційної безпеки.
- **На технологічному рівні** здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.
- **На рівні користувача** реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на об'єкти інформаційної безпеки, унеможливлення інформаційного впливу з боку соціального середовища.
- **На мережевому рівні** дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою.

- **На процедурному рівні** вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Виділяють декілька типів методів забезпечення інформаційної безпеки:

- однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;
- багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;
- комплексні методи - багаторівневі технології, які об'єднані у єдину систему координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;
- інтегровані високоінтелектуальні методи - багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів з організаційним управлінням.

Важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від різних загроз. Отже, система має відповідно реагувати і гарантувати ефективну діяльність у цьому напрямі.

3. Положення щодо політики безпеки

Політика безпеки – це сукупність документованих рішень, що приймаються керівництвом організації і спрямовані на захист інформації та асоційованих з нею ресурсів.

Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для ІС організації. Коли ризики проаналізовано і стратегію захисту визначено, тільки тоді складається програма забезпечення ІБ, під яку виділяються ресурси, призначаються відповідальні, визначається порядок контролю виконання програми тощо.

Розробка політики безпеки. З практичної точки зору політику безпеки доцільно розглядати на декількох рівнях деталізації.

До верхнього (адміністративного) рівня належать рішення, що стосуються організації в цілому. Вони мають загальний характер і, як правило, виходять від керівництва організації. До адміністративного рівня інформаційної безпеки відносяться заходи загального характеру, що реалізуються

керівництвом організації.

Головна мета заходів адміністративного рівня – сформувати програму робіт у галузі інформаційної безпеки і забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан подій.

До середнього рівня відносять питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних експлуатованих організацією систем. Приклади таких питань – ставлення до передових (але, можливо, недостатньо перевірених) технологій, доступ до Internet (як сумістити свободу доступу до інформації із захистом від зовнішніх загроз?), використання домашніх комп'ютерів, застосування користувачами неліцензійного програмного забезпечення і т.д.

Політика безпеки нижнього рівня стосується конкретних інформаційних сервісів. Вона включає два аспекти – цілі і правила їх досягнення, тому її інколи важко відокремити від питань реалізації.

При формулюванні цілей політики нижнього рівня можна виходити з міркування цілісності, доступності і конфіденційності, але не можна на цьому зупинятися. Її цілі повинні бути конкретнішими.

Програма реалізації політики безпеки. Після того, як сформульована політика безпеки, можна складати програми її реалізації.. Щоб зрозуміти і реалізувати будь-яку програму, її потрібно структурувати за рівнями відповідно до структури організації. В поширеному випадку достатньо двох рівнів – верхнього, або центрального, який охоплює всю організацію, і нижнього, або службового, який стосується окремих послуг або груп однорідних сервісів.

СОЦІОТЕХНІЧНА БЕЗПЕКА

1. Поняття соціотехнічної системи та її властивостей
2. Рекомендації щодо захисту від соціотехнічних атак
3. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки
4. Методи соціального інжинірингу
5. Соціальні мережі: особливості, основні поняття та визначення
6. Менеджмент персоналу у сфері інформаційної безпекою

1. Поняття соціотехнічної системи та її властивостей

Загалом під **системою** слід розуміти цілісність взаємопов'язаних елементів та взаємозв'язків між ними, яким притаманні певні властивості, мета, цілі та функції. Систему, як правило, характеризує **структура**, що відбиває взаємодію між її елементами і випливає з властивостей останніх або оточення, а також **функціонал**, який регламентує відношення між певним елементом

системи і системою в цілому та визначає можливість керувати нею. Якщо в системах існують не самі лише однобічні причинно-наслідкові залежності, то говорять про **комплексні**, або, як їх ще називають, **складні системи**. Основні властивості складних систем такі:

- **інтегративність** - властивість, що визначає фактори, які утворюють і зберігають систему;
- **комунікативність** - ступінь зв'язку із зовнішнім середовищем;
- **рівновага** - здатність зберігати деякий стан за відсутності збурень;
- **стійкість** - здатність системи повертатись до попереднього стану після того, як її було з нього виведено;
- **адаптація** - здатність системи до цілеспрямованого пристосування.

Ці властивості визначаються як зворотними зв'язками системи, так і особливостями окремих її елементів.

Складні **соціотехнічні системи** (СТС) - це системи, складовою яких є людина-оператор, знання, уміння, настрої, ціннісні переваги й ставлення до виконуваних обов'язків якої у взаємодії з технічним пристроєм у процесі, наприклад, виробництва матеріальних цінностей, управління певними процесами, обробки інформації тощо сприяють підвищенню ефективності розв'язання відповідних завдань або поліпшенню їх результативності.

Головні характеристики СТС наступні:

1) **організаційна філософія**, що базується на розумінні працівниками своїх цілей і призначення підприємства, на їхній постійній готовності поділити з адміністрацією всю повноту відповідальності за результати господарської діяльності;

2) **організаційна структура управління**, що забезпечує рядовим робітникам та службовцям реальні права щодо участі в керуванні;

3) новий підхід до розробки робочих місць і визначення ролі виконавця в процесі ухвалення управлінських рішень;

4) **нова схема розміщення обладнання**, яка має відповідати потребам перспективної форми організації праці, забезпечуючи прискорене проходження матеріальних потоків на виробництві;

5) **нові форми й методи підготовки та перепідготовки кадрів**, що спираються на гнучку кадрову політику, спрямовану на гарантування зайнятості;

6) **нові критерії в оцінюванні економічної ефективності** використання сучасних технологій та здійснення капіталовкладень у розвиток виробництва.

2. Захист від соціотехнічних атак

Крім комплексності використання методів інформаційного захисту слід також враховувати пряму або опосередковану соціальну залежність кожного

напряму захисту. З огляду на сказане вище, взаємозалежність ризиків порушення ІБ та інших типів безпеки СТС можна представити у вигляді структури, яка зображена на рисунку 1.

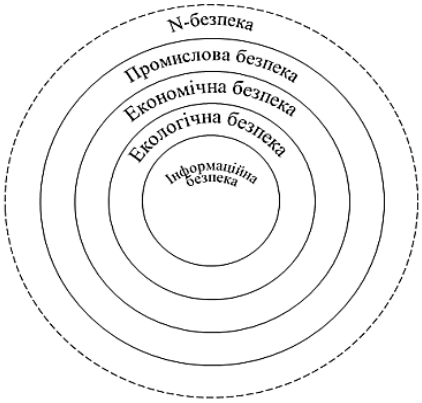

Рисунок 1 - Взаємозалежність ризиків порушення інформаційної безпеки

3. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки

В епоху глобальної інтенсифікації інформаційних процесів і їх проникнення в усі сфери діяльності людини, коли практично кожній людині доводиться виконувати різні завдання, взаємодіючи з численними елементами ІТ-інфраструктури, залежність кожного індивіда від інформаційних систем і мереж та його уразливість щодо стороннього кібернетичного впливу постійно зростають. Зрештою травмується психіка людини, а це, у свою чергу, може спонукати її до розголошення інформації з обмеженим доступом (ІзОД). Саме тому соціальні інженери в пошуках об’єктів своїх атак беруть до уваги передусім **психологічний стан** причетних до них осіб.

У сучасних організаціях (установах, компаніях) **потенційними жертвами** таких зловмисників можуть бути адміністратори, начальники, користувачі та навіть знайомі будь-кого зі згаданих категорій осіб. Особистісно-професійні характеристики осіб, що приваблюють атакувальників і можуть стати джерелом витоку ІзОД, якою вони володіють, а також можливі дії соціальних інженерів ілюструє рисунок 2.

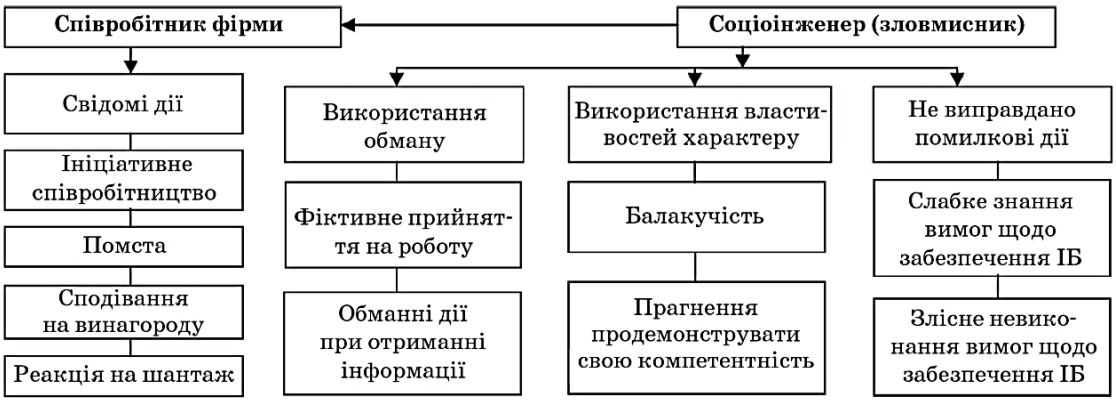

Рисунок 2 - Дії зловмисників

Для **досягнення мети** зловмисники використовують різну тактику, наприклад:

- видають себе за іншу особу;
- відвертають увагу потенційної жертви;
- нагнітають психологічну напругу тощо.

4. Методи соціального інжинірингу

Соціальний інжиніринг – це метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів. Основна мета соціальних інженерів – це отримання доступу до захищених систем з метою крадіжки інформації, паролів, даних, тощо. Основною відмінністю від простого злому – це те, що в ролі об'єкта атаки вибирається не машина, а людина.

Заходи протидії методам соціальної інженерії. Основним способом захисту від методів соціальної інженерії є навчання співробітників. Усі працівники компанії повинні бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації компанії, а також способи запобігання витоку даних.

5. Соціальні мережі: особливості, основні поняття та визначення

Під **соціальною мережею** в цьому сенсі розуміють множину дійових осіб, які можуть взаємодіяти один з одним. Така мережа, як результат розвитку ІТ, становить частину соціальної структури суспільства. Водночас соціальна мережа як **соціотехнічний об'єкт** відбиває наявні зв'язки між дійовими особами (різноманітні соціальні контакти) в термінах вузлів і сполучних ланок, починаючи з випадкових знайомств і закінчуючи тісними родинними вузами. Вузли отожнюються з акторами в мережах, а зв'язки відповідають стосункам між акторами.

Останнім часом мережа Інтернет перетворилась на справжню зброю в руках незадоволених споживачів і співробітників, за допомогою якої вони успішно атакують фірми (організації, утанови), їхню продукцію та керівництво шляхом розміщення в мережі негативної інформації. Вплив воцмереж на формуваня суспільної думки також є вагомим.

Регулярний моніторинг (відстеження) інформації в соціальних мережах дозволяє відповідним дійовим особам оцінювати ефективність своєї діяльності, заздалегідь виявляти й розв'язувати можливі ризики, а також мінімізувати негативні наслідки їх реалізації.

6. Менеджмент персоналу у сфері інформаційної безпеки

Людина, як активний елемент СТС може впливати різним чином на розвиток такої системи і, як наслідок, впливати на стан і розвиток множини середовищ, що її оточують. Більша частина порушень пов'язана з людиною.

Однак, у цій статистиці не наведено дані, які можна ідентифікувати, як дії людини, що потрапила під дію ІПО. Це означає, що загальний стан інформаційної безпеки СТС доцільно аналізувати через призму інформаційної війни, ефективне проведення якої може суттєво змінити початковий або стійкий стан СТС.

Стан СТС значною мірою визначає особливості процесу проведення проти неї ІПО і характеризується набором значень відповідних параметрів, наприклад, ймовірнісними оцінками порушень цілісності, конфіденційності та доступності інформаційних ресурсів системи як об’єкта захисту. Це дозволяє розглянути стан системи, як множину точок n-вимірного простору, який характеризується значеннями досліджуваних параметрів.

ОСНОВНІ ПОНЯТТЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1. Визначення національної безпеки.
2. Основні категорії теорії національної безпеки.
3. Принципи забезпечення національної безпеки.
4. Характеристики національної безпеки.
5. Фактори забезпечення національної безпеки.
6. Основні засоби забезпечення національної безпеки.

1. Визначення національної безпеки

Безпека [security, safety] - стан, при якому кому-небудь, чому-небудь не загрожує небезпека будь-якого виду, існує захист від небезпеки.

Національна безпека [national security] - це категорія політичної науки (політології), яка характеризує стан соціальних інститутів, який забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості та суспільства. Вона відображає зв'язок безпеки з нацією.

Нація [nation] (від лат. natio - народ, плем'я) - це стійка історична спільність людей, що визначається соціальними зв'язками певної формації і характеризується специфічними етнічними рисами, зумовленими особливостями економічного і культурного розвитку, спільністю території, мови, побуту, традицій і звичаїв, а також відображенням цих факторів у суспільній свідомості і суспільній психології.

Життєво важливі інтереси - сукупність потреб, задовольняння яких надійно забезпечує існування і можливості прогресивного розвитку особистості, суспільства і держави.

Особистість [personality] - це людина як суб'єкт відносин і свідомої діяльності. До життєво важливих інтересів особистості відносяться, насамперед, права і свободи людини і громадянина, в тому числі інформаційні.

Суспільство [society] - це сукупність форм сумісної діяльності людей, що утворилися в процесі історичного розвитку. Життєво важливі інтереси суспільства зв'язані зі створенням і розвитком вільного, гуманного, високоосвіченого, гармонійного суспільства, заснованого на принципах демократії, бережливого відношення до своїх традицій і національного надбання, суспільства, що підтримує і всіляко охороняє основний свій осередок - сім'ю.

Держава [State, country, nation] - сукупність офіційних органів влади в цій чи іншій країні, основний заклад і спосіб політико-правової організації життя суспільства на чолі з одноосібним або колективним правителем, органами виконавчої та інших видів влади і вертикальною системою управління, за допомогою якої здійснюється влада, охороняється існуючий лад, забезпечується нормальне життя людей.

До характеристик, за допомогою яких можна описати дану систему, належать:

- доступність - можливість за прийнятний час отримати шукану інформаційну послугу будь-яким суб'єктом виконавчої влади;
- цілісність - актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни;
- конфіденційність - захист від несанкціонованого ознайомлення.

ІБ як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. Водночас, ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку у різних суспільних груп і окремих осіб, почасти не співпадають. Саме у цьому знаходить свій безпосередній вираз вплив держави, яка за допомогою системи методів виражає загальні цінності у сфері ІБ.

2. Основні категорії теорії національної безпеки

Теорія національної безпеки [national security theory] - це наука, яка поєднує в собі прикладні аспекти соціальних, воєнних, гуманітарних, технічних, психологічних, біологічних та інших наук з метою дослідження суті, змісту, методів, форм і засобів забезпечення безпеки особистості, суспільства та держави.

Концепція (основи державної політики) національної безпеки України схвалена Верховною Радою України 16 січня 1997 р. **Концепція складається з п'яти частин:**

1. Загальні положення й принципи.
2. Національні інтереси України.
3. Загрози національній безпеці України.
4. Основні напрями державної політики національної безпеки України.
5. Система забезпечення національної безпеки України.

Основні категорії, які складають зміст теорії національної безпеки наведені на рисунку 1.

Рисунок 1 - Основні категорії теорії національної безпеки держави

Основна ідея теорії та практики забезпечення національної безпеки держави формулюється в **концепції національної безпеки**.

Національна безпека - це стан захищеності життєво важливих інтересів особистості, суспільства й держави від внутрішніх і зовнішніх загроз.

Національні інтереси держави відображають фундаментальні цінності та прагнення народу, його потреби в гідних умовах життєдіяльності, а також цивілізовані шляхи їх створення й способи задоволення. Національні інтереси держави та їх пріоритетність обумовлюються конкретною ситуацією, що складається в країні та за її межами.

Загроза [threat] - це можлива небезпека, тобто здатність заподіяти будь-яку шкоду, призвести до будь-якого нещастя. Стан безпеки визначається характером зовнішніх і внутрішніх загроз.

Основні можливі загрози національній безпеці держави проявляться у найбільш важливих сферах її життєдіяльності: політичній, економічній, соціальній, воєнній, екологічній, науково-технічній, інформаційній.

Головними об'єктами національної безпеки є:

- громадянин - його права й свободи;
- суспільство - його духовні та матеріальні цінності;
- держава - її конституційний лад, суверенітет, територіальна цілісність і недоторканість кордонів.

3. Принципи забезпечення національної безпеки

Основними принципами забезпечення національної безпеки є:

- пріоритет прав людини;
- верховенство права;
- пріоритет договірних (мирних) засобів у вирішенні конфліктів;

- адекватність заходів захисту національних інтересів реальним та потенційним загрозам;
- демократичний цивільний контроль за воєнною сферою, а також іншими структурами в системі забезпечення національної безпеки;
- додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;
- чітке розмежування повноважень органів державної влади.

Методи та засоби забезпечення національної безпеки

Реалізація принципів забезпечення національної безпеки можлива за рахунок створення системи безпеки, основним функціями якої повинні стати:

- виявлення й прогнозування внутрішніх і зовнішніх загроз життєво важливим інтересам об'єктів безпеки;
- здійснення комплексу оперативних та довготривалих заходів щодо попередження й нейтралізації загроз;
- створення й підтримання у готовності сил та засобів забезпечення національної безпеки у повсякденних умовах або при надзвичайних ситуаціях;
- здійснення системи заходів щодо нормального функціонування об'єктів безпеки в регіонах, які постраждали в результаті виникнення надзвичайної ситуації;
- участь у заходах із забезпечення безпеки за межами держави згідно з міжнародними договорами й угодами, що укладені даною державою.

Національна безпека держави досягається шляхом проведення виваженої державної політики відповідно до прийнятих доктрин, стратегій, концепцій і програм у таких сферах, як політична, економічна, соціальна, воєнна, екологічна, науково-технологічна, інформаційна тощо.

Конкретні засоби й шляхи забезпечення національної безпеки держави обумовлюються:

- пріоритетністю національних інтересів,
- необхідністю своєчасного вжиття заходів, адекватних характеру й масштабам загроз цим інтересам, і ґрунтуються на засадах правової демократичної держави.

4. Характеристики національної безпеки

До числа найважливіших характеристик національної безпеки відносяться її риси, які є основними показниками зовнішнього і внутрішнього аспектів національної безпеки і виступають необхідними умовами або вимогами її існування та збереження.

Зовнішній аспект національної безпеки характеризують такі риси: національний суверенітет, національна незалежність, національні особливості, територіальна цілісність, непорушність кордонів, державна могутність тощо.

Внутрішній аспект національної безпеки характеризують такі риси: прогресивність національного розвитку, політична стабільність, демократичний плюралізм, національна єдність, національна злагода, соціальна справедливість, суспільне благополуччя тощо.

5 Фактори забезпечення національної безпеки

У сучасному розумінні національної безпеки особлива роль належить визначенню факторів її забезпечення, під якими розуміють усі можливості суспільства щодо вирішення завдань відвернення війни й забезпечення мирних умов функціонування безпеки.

Система факторів забезпечення національної безпеки є складною і багатогранною. Існують різні способи класифікації цих факторів, так, зокрема, їх поділяють на внутрішні й зовнішні, об'єктивні й суб'єктивні. Особливе місце серед них посідають внутрішні фактори. Втілення в життя зазначених факторів повинно супроводжуватися оптимізмом і надією на здатність і спроможність збереження людської цивілізації.

6. Основні засоби забезпечення національної безпеки

Успіхи в реалізації сучасної концепції національної безпеки, як зазначалося вище, залежить від багатьох обставин, у тому числі від комплексного використання економічних, політичних, науково-технічних, соціальних, духовних і воєнних факторів.

Будь-які зміни основ політичного або воєнно-політичного мислення вимагають переосмислення місця й ролі кожної з них, визначення їхніх взаємозв'язків. В першу чергу це торкається **співвідношення політичних та воєнних засобів забезпечення безпеки**.

КІБЕРЗЛОЧИННІСТЬ

1. Характеристика кіберзлочинності.
2. Стан кіберзлочинності в Україні.
3. Засоби протидії кіберзлочинності.
4. Класифікація кіберзлочинів.
5. Протидія кіберзлочинності в Україні.
6. Боротьба із кіберзлочинами.
7. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення.

1. Характеристика кіберзлочинності

Кіберзлочин – дія, що порушує закон, яке вчинено з використанням інформаційно-комунікаційних технологій (ІКТ) і/або націлене на мережі, системи, дані, веб-сайти і/або технології, або сприяє вчиненню злочину.

Кіберзлочин відрізняється від традиційного злочину тим, що він «не визнають фізичні або географічні кордони» і можуть відбуватися з меншими зусиллями, більшою легкістю і з більшою швидкістю, ніж традиційні злочини (хоча це залежить від виду кіберзлочинів і виду традиційного злочину, з яким вони порівнюється). Коли ІКТ є частиною способу вчинення злочину, кіберзлочинність включає в себе традиційний злочин, вчиненню якого сприяють мережа Інтернет та цифрові технології.

Кіберзлочини вчиняються фізичними особами, групами осіб, комерційними організаціями і державами. Хоча ці суб'єкти можуть застосовувати схожі тактичні методи (наприклад, використовувати шкідливе програмне забезпечення) і атакувати схожі цілі (наприклад, комп'ютерну систему), вони мають різні мотиви і наміри при здійсненні кіберзлочинів.

Кіберзлочинність є одним з видів транснаціональної злочинності, виконавці і жертви якої можуть перебувати в будь-якій точці світу, де є підключення до мережі Інтернету. У зв'язку з цим слідчим, який веде розслідування кіберзлочинів, найчастіше потрібен транскордонний доступ до даних і обмін ними. Це завдання може бути виконано у разі, якщо запитувані дані зберігаються постачальниками послуг і приймаються заходи, що дозволяють правоохоронним органам отримувати доступ до даних.

Кіберзлочинці часто використовують як технічні, так і соціальні підходи до скоєння злочинів.

2. Стан кіберзлочинності в Україні

Сучасні процеси цифрової трансформації економіки пов’язані з розвитком бізнес-моделей, що використовують цифрові платформи. Фактично протягом останнього десятиріччя відбувається революція платформ. **Особливістю цифрових платформ** є об’єднання різних груп споживачів, виробників, власників ресурсів на одному віртуальному майданчику.

Вітчизняний цифровий капітал перебуває на стадії формування, але вже спостерігається велика кількість позитивних прикладів, оскільки можливості розвитку цифрової економіки в Україні пов’язані з розширенням використання цифрових платформ, що є точками зростання сучасної інформаційної економіки, при цьому перспективним напрямом розвитку цифрових платформ виступає технологія блокчейн (ланцюжок блоків транзакцій).

Найбільш поширеними напрямами загроз інформаційній безпеці є шахрайські шкідливі платіжні програми, що ускладнюють, порушують або блокують роботу банківських терміналів, використовуються для крадіжки даних громадян, взлому паролей від банківських карток для заволодіння коштами цих громадян, шахрайства у сфері електронної комерції та застосування інших кримінальних інструментів і послуг в різноманітніших

сферах злочинної діяльності.

Зростання ділової активності із застосуванням ІТ, придбання товарів через мережу Інтернет, Інтернет-банкінгу, он-лайн розрахунки сприяють зростанню економічних злочинів із застосуванням ІТ-технологій.

3. Засоби протидії кібезлочинності

До ефективних засобів протидії кіберзлочинності у сфері ІБ є розробка, створення та впровадження сучасних систем захисту інформації, а також вдосконалення існуючої законодавчої та нормативно-правової бази, здатної забезпечити протидію сучасним кіберзагрозам.

Для підвищення ефективності боротьби з кіберзлочинністю, розвинені країни світу ведуть відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Інциденти в сфері кібербезпеки позначаються на життєдіяльності споживачів інформаційних і багатьох інших послуг та кібератаки, націлені на різноманітні об’єкти інфраструктури систем електронних комунікацій чи управління технологічними процесами.

Розглядаючи стан кіберзлочинності у світі, необхідно сказати, до слабких сторін України можна віднести захист прав на інтелектуальну власність, насамперед існування піратства, банківські і фінансові сервіси, високі інвестиційні ризики, а також рівень кібербезпеки. Проте позитивні зміни є у побудові законодавчої бази для гарантування кібербезпеки держави; стійкість державних ініціатив щодо підвищення кібербезпеки у сфері ІКТ; значне покращення кіберстійкості організацій за останній рік незважаючи на збільшення цілеспрямованих атак.

4. Класифікація кіберзлочинів

Щодо класифікації кіберзлочинів, то в Конвенції Ради Європи про кіберзлочинність, яку Верховна Рада України ратифікувала й імплементувала до українського законодавства починаючи з 11.10.2005, виокремлено **4 основні типи кіберзлочинів**:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем – незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями;
- правопорушення, пов'язані з комп'ютерами, – підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами;
- правопорушення, пов'язані зі змістом, – правопорушення, пов'язані з дитячою порнографією;
- правопорушення, пов'язані з порушенням авторських і суміжних прав.

Український Кримінальний кодекс передбачає 4 статті за інформаційні злочини.

- Ст. 361 передбачає притягнення до відповідальності за незаконне

проникнення до комп'ютерів, систем чи мереж і втручання в їхню роботу (або її блокування).

- Ст. 361-1 передбачає санкції за написання та поширення вірусів, незалежно від того, робиться це безкорисливо чи за гроші.
- Ст. 361-2 покликана карати за зловживання правом доступу до інформації. Наприклад, співробітника компанії, який продав конкурентам базу даних клієнтів своєї компанії, доступ до якої мав через свої службові обов'язки.
- Ст. 362 передбачає покарання для тих, хто мав право доступу до комп'ютера чи мережі, але скористався ним для інших цілей. Якщо ви перед звільненням знищите на своєму службовому комп'ютері важливу інформацію, то ваші дії підпадатимуть під цю статтю.

5. Протидія кіберзлочинності в Україні

Україна має продовжувати застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, розвивати роботу відповідних органів, що здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО.

Важливо підвищувати рівень обізнаності щодо кібербезпеки на всіх рівнях: від діючих центрів комп'ютерної безпеки до розгортання відповідних освітніх програм. За умов небезпек у кіберпросторі, організаціям потрібно змінити ставлення до ІБ, а для цього треба підвищувати обізнаність про важливість інвестування у кібербезпеку як невід'ємну складову будь-якої національної стратегії розвитку ІКТ.

Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України CERT-UA функціонує для взаємодії з Cisco Talos Intelligence Group та іншими державами-членами CERT щодо питань подолання наслідків кібератак на інформаційну інфраструктуру, виявлення причин та обставин таких інцидентів. CERT-UA також допомагає усунути загрози безпеці приватного сектору України та іноземних партнерів. Відповідно до закону «Про основні засади забезпечення кібербезпеки України» (2017), CERT-UA та Центр реагування на кіберзлочини координують заходи, спрямовані на оперативне реагування на кібератаки, а також контролюють впровадження контрзаходів, що передбачають мінімізацію вразливості систем зв'язку.

Україна бере участь у роботі Агентства ЄС з кібербезпеки, Європейського центру з досліджень і компетенції в сфері кібербезпеки, а також у навчаннях з реалізації Спільної оперативної схеми реагування ЄС і держав-членів на

кібератаки.

Загалом усі заходи, що проводить світова спільнота у сфері кібербезпеки, – це спроба допомогти країнам вдосконалити цю сферу, а також мотивувати їх на вжиття заходів для покращення їхнього рейтингу, допомагаючи у такий

спосіб підвищити загальний рівень кібербезпеки в усьому світі. Рейтинг «Глобального індексу кібербезпеки» допомагає аналізувати та використовувати найкращі засоби боротьби в ІТ-сфері для подолання та упередження кіберзлочинів та зростання стану їх кібербезпеки.

6. Боротьба із кіберзлочинами

Сьогодні особлива увага приділяється саме питанням міжнародного співробітництва при запобіганні, протидії й розслідуванні комп'ютерних злочинів. У багатьох країнах світу для запобігання і протидії цим видам злочинів створені спеціалізовані кіберпідрозділи, що займаються виявленням, розслідуванням комп'ютерних злочинів та збором іншої інформації з цього питання на національному рівні.

Законом «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. законодавчо закріплені доктринальні засади забезпечення кібербезпеки нашої країни, а також закладені правові основи діяльності Національного координаційного центру кібербезпеки. Він згідно з положеннями є робочим органом Ради національної безпеки і оборони України, який здійснює координацію та контроль за діяльністю суб'єктів сектора безпеки й оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засадвнутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена Законом «Про основні засади забезпечення кібербезпеки України» та іншими законами України. Загальна декларація прав людини, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана ВР України, укази Президента, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України фактично закладають міцний міждержавний правовий, організаційний, процедурний фундамент забезпечення кібербезпеки інформаційного простору в Україні, Європі і світі.

7. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення

Можна виділити 4 основні складові національних інтересів України в інформаційній сфері.

Перша складова національних інтересів України в інформаційній сфері полягає у д**отриманні конституційних прав і свобод людини і громадянина в галузі одержання інформації й користування нею**, забезпеченні духовного

відновлення України, збереження й зміцненні моральних цінностей суспільства, традицій патріотизму, гуманізму, культурного й наукового потенціалу країни.

Друга складова національних інтересів України в інформаційній сфері полягає у **інформаційному забезпеченні державної політики України**, доведенні до громадян України та міжнародної громадськості достовірної інформації про державну політику України, її офіційної позиції щодо соціально значимих подій у житті держави і міжнародного життя, із забезпеченням доступу громадян до відкритих державних інформаційних ресурсів.

Третя складова національних інтересів України в інформаційній сфері полягає у **розвитку сучасних інформаційних технологій, вітчизняної індустрії інформації**, у тому числі індустрії засобів інформатизації, телекомунікації та зв'язку, забезпеченні потреб внутрішнього ринку її продукцією та вихід цієї продукції на світовий ринок, а також забезпеченні накопичення, зберігання та ефективного використання вітчизняних інформаційних ресурсів. У сучасних умовах тільки на цій основі можна вирішувати проблеми створення наукоємних технологій, технологічного переозброєння промисловості, збільшення досягнень вітчизняної науки й техніки. Держава повинна зайняти гідне місце серед світових лідерів мікроелектронної й комп'ютерної промисловості.

Четверта складова національних інтересів України в інформаційній сфері полягає у **захисті інформаційних ресурсів від технічних розвідок**, несанкціонованого доступу, забезпеченні безпеки інформаційних і телекомунікаційних систем.

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО. ІНФОРМАЦІЙНА ВІЙНА

1. Визначення поняття інформаційне протиборство.
2. Визначення поняття інформаційна війна.
3. Інформаційний тероризм. Інформаційна злочинність.
4. Інформаційне протиборство як форма забезпечення інформаційної безпеки.
5. Концепція інформаційної війни. Органи інформаційної війни.
6. Основні форми інформаційної війни на державному рівні.
7. Інформаційна зброя в інформаційній війні.

1. Визначення поняття інформаційне протиборство

Для розв'язання соціальних конфліктів різноманітного масштабу останнім часом усе частіше використовується інформаційна сфера, яка породжує таке явище як **інформаційне протиборство** [information confrontation], яке

характеризується, з однієї сторони, впливом на системи добування, оброблення, розповсюдження та зберігання інформації противника, а з іншої - застосуванням заходів захисту своїх подібних систем від деструктивного та керуючого впливу.

Інформаційна сфера - це сфера діяльності суб'єктів, зв'язана із створенням, перетворенням і споживанням інформації.

Інформаційне протиборство – форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів для впливу на інформаційне поле суперника та захисту власного інформаційного поля в інтересах досягнення поставлених цілей. На сьогодні відомі такі сфери протиборства: світоглядна, політична, дипломатична, воєнна, науково-технологічна, соціальна та гуманітарна, ідеологічна, екологічна тощо.

Інформаційне протиборство здійснюється між різноманітними видами соціальних суб'єктів (особистостей, суспільств, держав, наднаціональних утворень), проте цілий ряд таких конфліктних взаємодій має певні відносно стійкі ознаки, які у їхній сукупності утворюють окремі форми - інформаційна війна, інформаційний тероризм, інформаційна злочинність.

2. Визначення поняття інформаційна війна

Інформаційна війна: процес боротьби між суб'єктами із застосуванням інформаційної зброї.

Інформаційна зброя є інструментом встановлення контролю над інформаційними ресурсами потенційного суперника, тому вона втручається в роботу систем управління та інформаційних систем, систем зв'язку, з метою порушення їх працездатності аж до цілковитого виведення їх з ладу, вилучення, перекручення даних, які в них містяться, або цілеспрямованого введення спеціальної інформації.

Інформаційна зброя враховує різні варіанти протидії, тому чим більше таких варіантів ураховано, тим більша ймовірність успіху в тій чи іншій інформаційній агресії.

Інформаційна загроза: вхідні дані, початково призначені для активізації в інформаційній системі алгоритмів, що відповідають за звичайний режим функціонування.

Сугестія: прихований інформаційний вплив на інформаційну систему, що самонавчається.

Сугестивний вплив: вплив з формування у інформаційної системи, що самонавчається, прихованих від неї самої цілей.

Відомі два трактування поняття "інформаційні війни": гуманітарне і технічне. У гуманітарному розумінні інформаційна війна представляє собою

активні методи перетворювання інформаційного простору, тобто нав'язування громадянам України таких моделей суспільства, які забезпечують бажані типи поведінки, а також породжують інформаційні процеси міркувань.

Інформаційна війна при використанні інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності містить такі **складові**:

- **здійснення впливу на інфраструктуру систем життєзабезпечення** – телекомунікації, транспортні мережі, електростанції тощо;
- **промисловий шпіонаж** – порушення прав інтелектуальної власності, розкрадання патентованої інформації, викривлення або знищення важливих даних, проведення конкурентної розвідки;
- **хакінг** – зламування та використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Основна мета сучасної інформаційної війни полягає не у фізичному знищенні суперника та ліквідації його збройних сил, а у широкомасштабному порушенні роботи фінансових, транспортних і комунікаційних мереж і систем, у руйнуванні економічної інфраструктури і підкоренні населення країни, що зазнала атаки, волі країни-переможця.

Основним інструментом ведення інформаційної війни є інформаційна зброя, тобто пристрої та засоби, які призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби.

Основними елементами інформаційної боротьби є:

- засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів;
- інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи таким чином на суспільну думку, на життя суспільства, держави або групи держав загалом.

Інформаційна війна має наступальні та оборонні складові, починаючи з цільового проектування та розроблення своєї структури командування, управління, комунікацій комп'ютерів і розвідки. Вона може бути спрямована проти трьох елементів інфраструктури: комп'ютерів; програмного забезпечення; людини. Однією з головних цілей та завдань інформаційної війни є придушення в людині морального творчого початку, зміна світогляду.

3. Інформаційний тероризм. Інформаційна злочинність

Тероризм - загроза або використання насильства в політичних цілях окремими особами або групами, які можуть діяти як на стороні, так і проти існуючого уряду, коли такі дії, спрямовані на те, щоб уплинути на більше число людей, ніж безпосередні жертви. Об'єктом тероризму є не ті, хто став жертвою,

а ті, хто залишився живими. Його мета не убивство, а залякування і деморалізація живих, тобто, жертви - інструмент, убивство - метод.

На відміну від війни для тероризму характерне початкова нерівність конфронтуючих сторін, що обумовлює прагнення більш слабкої сторони задіяти ті методи і способи, які наносять найбільші збитки противникові при витраті мінімуму своїх сил і засобів, а також здійснюють сильний психологічний вплив. Дана сторона намагається розширити межі конфлікту, залучити в нього нові соціальні групи та інститути, що мають свої цілі й світоглядні установки, щоб звести нанівець переваги більш сильної сторони. При цьому закриваються очі на те, що шкода найчастіше наноситься особистостям і групам, що не беруть участі та не бажають брати участі у конфлікті.

Часто ставиться питання про можливість здійснення **інформаційної диверсії,** яка за об'єктивними ознаками схожа з тероризмом, проте за мету диверсія має підрив економічної безпеки та обороноздатності держави.

Питання про **злочинність в інформаційній сфері** також має кримінально-правовий характер, так як будь-який злочин - це суспільно-небезпечне діяння, заборонене кримінальним законом під загрозою покарання. У той же час **злочин** - це спосіб розв'язання певного соціального конфлікту, що полягає у здійсненні впливу на опонента. Необхідно відзначити, що питання віднесення діянь до розряду злочинних залежить від національного законодавства, тому підходи до нього в різних державах можуть суттєво відрізнятися.

Інформаційні злочини можуть здійснюватися як із використанням інформаційно комп'ютерних, так і інформаційно психологічних методів впливу. Так прикладом складу інформаційно-психологічних злочинів можна назвати наклеп та образу.

4. Інформаційне протиборство як форма забезпечення інформаційної безпеки

У зв'язку з усе більш активним використанням інформаційної сфери для розв'язання соціальних конфліктів стає все більш актуальною мета інформаційного протиборства - **забезпечення ІБ.** Заходи, що приймаються для забезпечення інформаційної безпеки повинні бути адекватними наявним і прогнозованим загрозам, причому вони можуть бути як активними, так і пасивними.

Пасивне забезпечення ІБ передбачає реагування на вже наявні загрози, воно спрямоване на безпосередню протидію акціям, що є деструктивними по відношенню до до соціальної системи. З цією метою створюється певна система захисту, яка складається з ряду адміністративно-режимних, правових, фізичних,

апаратно-технічних, програмних та інших заходів, які утворюють якби безперервну оболонку навкруги системи, що підлягає захисту.

На відміну від пасивного, **активне забезпечення ІБ** спрямоване на завчасне виявлення та попередження загроз. Це може досягатися шляхом проведення заходів, спрямованих на з'ясування планів, цілей, сил та засобів конфронтуючої соціальної системи, а також на протидію деструктивним акціям на етапі їхньої підготовки.

5. Концепція інформаційної війни. Органи інформаційної війни

Концепція інформаційної війни [information warfare conception] - система поглядів на інформаційну війну та шляхи її ведення. Інформаційна війна розглядається як комплекс заходів і операцій, спрямованих на забезпечення інформаційної переваги по відношенню до потенційного або реального противника.

Інформаційна перевага є одним із центральних понять у сфері інформаційного протиборства. Вона представляє собою здатність складної саморегулюючої системи управління та інформаційного забезпечення держави або воєнного відомства забезпечити стійкий безперервний процес своєчасного одержання достовірної інформації та доведення її до відповідних споживачів, при одночасному отриманні можливості використання у своїх інтересах такої ж системи ймовірного противника або пониження ефективності роботи (виведення з ладу) останньої.

Органи інформаційної війни - це органи керування інформаційною війною та люди (фахівці, офіцери, підрозділи) для її ведення.

6. Основні форми інформаційної війни на державному рівні

Ведення інформаційної війни відбувається на державному та воєнному рівнях.

На державному рівні інформаційна війна ведеться з використанням політичних, дипломатичних, економічних, інформаційно-психологічних, інформаційно-технічних і воєнних способів.

Основною формою інформаційної війни на державному рівні **є спеціальна інформаційна операція,** яка може носити одночасно і наступальний і оборонний характер, відповідає передбаченій мірі ризику та очікуваному потенційному ефекту, спрямована на забезпечення національних інтересів і національної безпеки держави.

На воєнному рівні інформаційна війна планується вестись всебічно забезпеченими силами та засобами, що виділяються для боротьби з силами бойового управління противника.

Основними формами інформаційної війни на воєнному рівні (ведення боротьби із системами бойового управління противника) є:

- **Наступальна інформаційна операція** має за мету завоювання інформаційної переваги над противником. У цій операції головні зусилля спрямовуються на дезорганізацію його систем управління військами і зброєю, а частина сил та засобів забезпечують стійкість власного управління. При цьому всі заходи, які проводяться в межах інформаційної боротьби, повинні забезпечувати сприятливі умови для бойових дій своїх військ (сил).
- **Оборонна інформаційна операція** проводиться в умовах великої інформаційної переваги противника і має за мету зниження цієї переваги. В такій операції головні зусилля сил і засобів спрямовуються на забезпечення інформаційної безпеки органів управління об'єднань і з'єднань, на захист інформації у системах керування. Частина сил і засобів спрямовуються на дезорганізацію управління військами і зброєю противника.

Наступальні та оборонні операції можуть вестися одночасно або послідовно, як у мирний, так і у воєнний час.

7. Інформаційна зброя в інформаційній війні

До інформаційної зброї відноситься широкий клас засобів і способів інформаційного впливу на противника від дезінформації і пропаганди до засобів радіоелектронної боротьби.

Сфера застосування інформаційної зброї включає як воєнну галузь, так і економічну, банківську, соціальну та інші галузі потенційного використання з метою:

- дезорганізації діяльності управлінських структур, транспортних потоків та засобів комунікації;
- блокування діяльності окремих підприємств та банків, а також цільових галузей промисловості шляхом порушення багатоланкових технологічних зв'язків та системи взаєморозрахунків, проведення валютно-фінансових махінацій і т.ін.;
- ініціювання великих техногенних катастроф на території противника в результаті порушення штатного управління технологічними процесами та об'єктами, які мають справу із значними кількостями небезпечних речовин та високими концентраціями енергії;
- масового розповсюдження та впровадження у свідомість людей певних уявлень, звичок та поведінкових стереотипів;
- виклику невдоволення або паніки серед населення, а також провокування деструктивних дій різноманітних соціальних груп.

За галузями застосування інформаційну зброю можна підрозділити на інформаційну зброю **воєнного та невоєнного призначення**. До інформаційної зброї, застосування якої можливе, як у воєнний, так і у мирний час, можуть бути віднесені засоби ураження інформаційних комп'ютерних систем та засоби

ураження людей (їхньої психіки).

Інформаційна зброя атаки це інформаційна зброя, за допомогою якої здійснюється вплив на інформацію, що зберігається, оброблюється і передається в інформаційно-обчислювальних мережах (ІОМ) і (або) порушуються інформаційні технології, що застосовуються в ІОМ. Застосування інформаційної зброї атаки спрямоване на зрив виконання ЮМ цільових завдань.

Інформаційна зброя забезпечення - це інформаційна зброя, за допомогою якої здійснюється вплив на засоби захисту інформації об'єкта атаки, наприклад, інформаційно-обчислювальну систему. До складу інформаційної зброї забезпечення входять засоби комп'ютерної розвідки та засоби подолання системи захисту інформаційно-обчислювальної системи.

Успішне застосування інформаційної зброї забезпечення дозволяє здійснювати деструктивні впливи на інформацію, що зберігається, обробляється й передається в мережах обміну інформацією, з використанням інформаційної зброї атаки.

УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Кібербезпека.
2. Рівняння ризику.
3. Управління ризиками.
4. Схильність до ризику.
5. Методи аналізу ризиків.
6. Вплив ризиків.
7. Оцінка ризиків.

1. Кібербезпека

З швидким зростанням ІТ неминуче поширюються і загрози інформації. Кібербезпека стосується захисту особистої чи організаційної інформації або інформаційних ресурсів від несанкціонованого доступу, атак, крадіжки або пошкодження даних.

Актив: будь-яка цінність, яка може бути скомпрометована, викрадена або заподіяна шкода, включаючи інформацію, фізичні ресурси та репутацію.

Загроза: будь-яка подія чи дія, яка потенційно може спричинити пошкодження активу або переривання послуг.

Загроза: навмисна спроба обійти одну або декілька служб безпеки чи засобів керування інформаційною системою.

Вразливість: стан, який робить систему та її активи відкритими для шкоди, включаючи такі речі, як помилки ПЗ, ненадійні паролі, недостатній

фізичний захист і погано спроектовані мережі.

Експлойт: техніка, яка використовує вразливість для здійснення атаки.

Контроль: контрзахід, який ви застосовуєте, щоб уникнути, зменшити або протидіяти ризикам безпеки через загрози чи атаки.

2. Рівняння ризику

Ризик - це міра вашої схильності до ймовірності пошкодження або втрати. Це означає ймовірність виникнення небезпеки або небезпечної загрози. Ризик часто пов'язаний із втратою системи, живлення чи мережі та іншими фізичними втратами. Однак ризик також впливає на людей, практику та процеси.

Щоб ефективно управляти ризиком, необхідно враховувати фактори, властиві ризикам, з якими ви маєте справу. Часто вважається, що ризик складається з трьох факторів, що виражається виразом:

Ризик = Загрози × Вразливі місця × Наслідки

Загроза - це щось або хтось, хто може скористатися вразливими місцями.

Вразливість - це слабке місце або недолік, який дозволяє зловмиснику порушити цілісність системи.

Наслідком є збиток, який виникає через те, що загроза скористалася вразливістю.

3. Управління ризиками

Оцінивши ступінь трьох факторів, що складають ризик, можна визначити ступінь ризику, який керуватиме вашим рішенням щодо того, як з ним боротися.

Причина, **чому ризиком керують, а не повністю усувають його,** полягає в тому, що ризик не завжди суперечить цілям організації. Насправді, якщо спробувати повністю усунути ризик, організація перестане функціонувати. Тому управління ризиками - це процес розуміння того, на які ризики ви можете піти, якщо винагорода варта ризику.

Управління ризиками зазвичай визначається як циклічний процес, що наведено на рисунку 1.

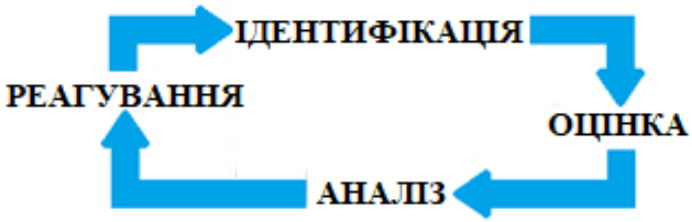

Рисунок 1 - Один із способів представлення циклу управління ризиками

Цей процес не закінчується - поки інформація існує, вона потребуватиме захисту. Таким чином, управління ризиками повторюється безстроково, щоб завжди зберігати інформацію якомога безпечніше. Без управління ризиками

безпека буде пасивною; і якщо пасивно захищати інформацію, вона буде залежати від швидких змін технологічного прогресу.

Комплексний процес оцінювання, вимірювання та пом'якшення багатьох ризиків, які пронизують організацію, називається управлінням ризиками підприємства **Enterprise Risk Management (ERM)**. Процес ERM є важливою частиною будь-якої організації, яка прагне досягти своїх цілей.

4. Схильність до ризику

Властивість, яка визначає, наскільки організація вразлива до втрат називають **схильність до ризику**. Кількісна оцініка показника визначається як добуток ймовірності того, що інцидент станеться, і очікуваного впливу або збитку, якщо він відбудеться.

Організація наражає себе на ризик у кожній своїй дії. Ці дії відбуваються в процесі ведення бізнесу організацією, і постійна потреба в оцінці цих ризиків породила індустрію безпеки в цілому. Без ризику не було б потреби в безпеці, оскільки не було б наслідків для погано виконаних бізнес-процесів. Оскільки підприємства дедалі більше залежать від технологій, зростаюча кількість ризиків пов'язана з професіоналами з комп'ютерної безпеки як основним засобом керування цими ризиками.

Завдяки ERM організація може підтримувати низький рівень ризику, але ніколи не може його повністю уникнути. Ось чому фахівцям із безпеки так важливо постійно стежити за елементами ризику (включаючи загрози, атаки та вразливі місця), які потенційно можуть завдати шкоди активам підприємства. Ігнорування ризику вашої організації обмежить її здатність виживати в будь-якій галузі.

5. Методи аналізу ризиків

При визначенні того, як захистити комп'ютерні мережі, комп'ютерні установки та інформацію, **аналіз ризиків** – це процес безпеки, який використовується для оцінки збитків від ризиків, які можуть вплинути на організацію. Зміст та результат будь-якого аналізу ризиків має відображати рамки та юрисдикцію, в межах якої працює організація.

Методи аналізу ризику, які використовуються для розрахунку ризику, можна розділити на одну з трьох категорій**:**

Якісний: Методи якісного аналізу використовують описи та слова для вимірювання ймовірності та впливу ризику. Наприклад, оцінки впливу можуть бути серйозними/високими, помірними/середніми або низькими. Подібним чином рейтинги ймовірності можуть бути ймовірними, малоймовірними або рідкісними. Якісний аналіз зазвичай базується на сценаріях. Слабкість якісного аналізу ризику полягає в його методології, яка іноді є суб'єктивною та не піддається перевірці. Ви також можете призначити числа від 0 до 9 для

опромінення та потенціалу пошкодження. Однак ви не виконуєте розрахунки за числами, присвоєними ризикам. Метою якісної оцінки є, наприклад, ранжування ризиків за шкалою від 1 до 25.

Кількісний: кількісний аналіз повністю базується на числових значеннях. Дані аналізуються з використанням історичних записів, досвіду, найкращих галузевих практик і записів, статистичних теорій, тестування та експериментів. Ця методологія може бути слабкою в ситуаціях, коли ризик важко визначити кількісно. Метою кількісного аналізу є обчислення ймовірних втрат для кожного ризику.

Напівкількісний: метод напівкількісного аналізу існує, оскільки неможливо провести суто кількісну оцінку ризику, враховуючи, що деякі проблеми не піддаються цифрам. Наприклад, скільки моральний стан вашого працівника коштує в доларах? Чого варта ваша корпоративна репутація? Напівкількісний аналіз намагається знайти золоту середину між двома попередніми типами аналізу ризику, щоб створити гібридний метод.

6. Вплив ризиків на підприємство

Існують різні типи ризиків, з якими може зіткнутися організація. Кіберризики впливають на всі сфери та типи корпоративних ризиків і вони не обов'язково є технічними, але можуть бути сформульовані в термінах бізнесу.

Юридичний: кожне підприємство, незалежно від галузі, повинно дотримуватися певних законів і правил, щоб залишатися в рамках закону.

Фінансовий: організація очікуваний дохід і прибуток на основі ряду розрахунків, і багато різних загроз можуть призвести до того, що бізнес не зможе відповідати грошовим очікуванням.

Фізичні активи: залежно від розміру підприємства, воно можете мати багато цінної фізичної власності: комп'ютери, промислове обладнання та офісна техніка, також ризикує бути викраденою чи іншим чином пошкодженою.

Інтелектуальна власність: організації, які створюють та володіють інтелектуальною власністю, такою як розважальні засоби масової інформації, ПЗ, комерційні таємниці та дизайн продуктів, ризикують знищити ці концепції або використати їх у несанкціонований спосіб.

Інфраструктура: організація повинна залежати від своєї структури, щоб функціонувати з максимальною ефективністю. Незалежно від того, фізичні чи абстрактні, структури, які утримують організацію, вразливі до ряду загроз.

Операції: щоденні операції - це те, що забезпечує роботу підприємства та виконання не лише його грошових очікувань, але й його бачення. Особливо шкідливими є ризики, які впливають на операційну спроможність організації (тобто на її здатність виконувати багато бізнес-процесів одночасно).

Репутація: сприйняття організації громадськістю може сильно вплинути на її успіх, а в деяких випадках може приректи її на поразку.

Здоров'я: співробітники чи клієнти, з якими працює організацію ризикують отримати шкоду в результаті її діяльності.

7. Оцінка ризику

Оцінка використовується для ідентифікації будь-яких інформаційних активів, які можуть стати ціллю кібератаки. Вона може включати апаратне чи програмне забезпечення, дані клієнтів та інтелектуальну власність. Після визначення типів даних оцінка ризику дозволить визначитт типи ризиків, пов'язані з кожним типом ідентифікованого ризику.

Після оцінки ризику запроваджуються засоби контролю, щоб запобігти виникненню будь-якого із зазначених ризиків. Цей процес є постійним циклом, який слід виконувати регулярно, оскільки система та активи організації постійно змінюватимуться.

Під час проведення оцінки ризику необхідно враховувати такі речі:

- Яка загроза?
- Чи вразлива система до цієї загрози?
- Як цей ризик вплине на організацію? Репутаційні/фінансові збитки?

Використовуючи цю просту структуру, можна розробити високорівневий розрахунок кіберризику:

Кіберризик = Загроза х Вразливість х Цінність інформації

Види аналізу оцінки ризиків. Після того, як всю цю інформацію, буде зібрано, розпочинається розробка плану оцінки ризиків. Існує кілька різних типів кутів оцінки ризику, які залежатимуть від типу організації та її цілей.

Ризик відповідності ґрунтується на порушеннях законодавства, зокрема законів, правил і нормативних актів, або, з іншого боку, на внутрішніх політиках або бізнес-стандартах певної організації.

Репутаційний ризик - це будь-який вид негативної реклами, суспільного сприйняття або будь-яка неконтрольована подія, яка може вплинути на репутацію організації.

Трансакційний ризик – це будь-який ризик, пов'язаний із наданням послуг або продукту.

Стратегічний ризик - це все, що може статися внаслідок бізнес-рішень, прийнятих працівниками на основі бізнес-цілей. Це можна розглядати як ризик недосягнення цих цілей.

Операційний ризик - це будь-яка зміна в бізнес-процесах, людях, системах або зовнішніх подіях, які можуть завдати збитків організації.

Крім цього, існує два типи методів оцінки ризиків, які можна виконати:

Кількісний: це аналіз найпріоритетніших ризиків, у якому

використовується система чисельних оцінок для визначення їхньої ймовірності.

Якісний: це найпоширеніший тип оцінки ризику. Він базується на судженні оцінювача. Оцінювачем зазвичай є людина з досвідом у цій галузі, яка зможе використовувати власні судження та знання для оцінки та аналізу ризиків.

Оцінка ризиків буде основою стратегії управління ризиками для організації, тому це фундаментальна частина процесу.

Розрахунок рейтинг ризику здійснюється наступним чином:

Вплив * Ймовірність = Рейтинг ризику

Реєстр ризиків використовується для документування ризиків і дій, необхідних для управління ними. Це важлива частина успішного управління ризиками в організації яка допомагає вести облік усіх виявлених ризиків разом із способами їхнього керування, пом’якшення чи реагування на них.

Реєстр ризиків зазвичай міститиме такі відомості: дата виявлення ризику; сам ризик; власник ризику; дія на ризик; опис ризику; ймовірність виникнення ризику; потенційний вплив; рейтинг ризику.

РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Вирішення інцидентів і планування реагування.
2. Планування аварійного відновлення.
3. Процес реагування на інциденти.
4. Плани внутрішніх і зовнішніх комунікацій.
5. Ідентифікація інциденту.
6. Вплив і масштаб інцидентів.
7. Оцінка та аналіз інцидентів.
8. Стримування інциденту.
9. Пом'якшення та ліквідація інциденту.

1. Вирішення інцидентів і планування реагування

Ефективно реагувати на інцидент можливо лише за наявності відповідних процесів, персоналу та інструментів. До того, як станеться інцидент безпеки, організація повинна спланувати та запровадити можливості обробки інцидентів, які включають навички, ролі, процедури, процеси та інструменти для реагування на інциденти безпеки. **Метою є розробка плану реагування на інциденти, який дозволить:**

- виявлення компромісів якомога швидше та ефективніше;
- реагування на інциденти якнайшвидше;
- визначеня причини якомога ефективніше.

У відповідь на інцидент безпеки організація повинна зробити наступне:

- Захистити дані, одночасно обмежуючи безпосередній вплив на клієнтів і ділових партнерів.
- Стримати інцидент, щоб запобігти подальшій ескалації.
- Виправити наслідки інциденту, щоб якомога швидше повернутися до нормальної роботи.
- Визначити, як стався інцидент.
- Визначити, як запобігти подальшому використанню тієї самої вразливості.
- Оцінити вплив і шкоду системам, репутації, фінансам тощо.
- За потреби оновити політику та процеси безпеки організації на основі уроків, отриманих з інциденту.

2. Планування аварійного відновлення

Однвєю їх основних частин процесу планування має бути зосередження на відновленні після інциденту. Після переходу до фази відновлення може виявитися особливо складним, а в деяких випадках і неможливим, є повне відновлення системи без належної підготовки. Під час великомасштабних інцидентів, які завдають шкоди багатьом активам, організація може використовувати резервне копіювання всіх даних і систем за межами підприємства. В ідеальному випвдку це зовнішнє резервне копіювання має бути достатньо відокремлене від основних операцій, щоб на нього не вплинуло порушення чи катастрофа. Замість відновлення з нуля, відновлення буде швидшим і легшим за допомогою цієї резервної копії.

3. Процес реагування на інциденти

Процес реагування на інцидент складається з наступних кроків:

- Планування і визначення інциденту.
- Ініціювання протоколиівобробки інцидентів.
- Запис інциденту.
- Оцінка і аналіз події.
- Опис наслідків інциденту.
- Пом’якшення та ліквідація негативних наслідків інциденту.
- Передача проблемм відповідному члену команди, якщо це можливо.
- Відновлення після інциденту.
- Розгляд та повідомлення подробиць інциденту.
- Складання звіту про завершення дії.

Операційний центр безпеки (SOC) - це місце, де фахівці з безпеки контролюють і захищають критично важливі інформаційні активи в організації. SOC є життєво важливими для управління безпекою, оскільки вони централізують і оптимізують зусилля організації з безпеки, щоб максимізувати

її ефективність. Оскільки SOC може бути складно встановити, підтримувати та фінансувати, їх зазвичай використовують великі корпорації, які мають захищати вразливу інформацію, як-от урядові установи чи медичні компанії, які працюють з особистою інформацією (PII).

Організація CSIRT. Організації часто створюють групу реагування на інциденти кібербезпеки (CSIRT), щоб допомогти ідентифікувати інциденти інформаційної безпеки та керувати ними. Особи, які входять до складу CSIRT, навчаються належним методам збору та збереження для розслідування інцидентів безпеки.

4. Плани внутрішніх і зовнішніх комунікацій

Є багато різних осіб з різними ролями, які можуть бути залучені в інцидент, на який реагує CSIRT. Тому **слід розробити плани внутрішньої та зовнішньої комунікації,** спрямовані на цих осіб.

Приклади внутрішніх і зовнішніх зацікавлених сторін, які можуть мати відношення до заходів реагування:

- Будь-які окремі жертви (крім самої компанії), які постраждали внаслідок інциденту.
- Внутрішні відділи, яким може знадобитися повідомити про інцидент співробітників і клієнтів.
- Акціонери.
- Засоби масової інформації.
- Потенційні винуватці інциденту.
- Місцеві правоохоронні органи.
- Системні адміністратори.
- Менеджери та керівники.
- Постачальники, з якими ведуться ділові відносини.
- Інші групи CSIRT і комп’ютерні групи реагування на надзвичайні ситуації (CERT), які можуть надати цінну інформацію, що може вплинути на ваш процес реагування.

5. Ідентифікація інциденту

Визначення того, що стався інцидент, а потім з’ясування його наслідків може бути найскладнішим кроком у процесі обробки та реагування. Це пояснюється кількома причинами, зокрема тим, що різні механізми виявлення, як ручні, так і автоматичні, мають різні рівні чутливості та точності. Успіх цих механізмів також залежатиме від того, відома чи невідома загроза - атаку, яка не мала прецедентів, буде важко вчасно ідентифікувати, або вона може повністю обійти виявлення.

Іншою важливою проблемою є те, що залежно від розміру організації та характеру її активів кількість сповіщень, які отримує персонал служби безпеки,

може бути настільки великою, що її неможливо легко проаналізувати. Нарешті, для людини, що надає першу допомогу, може бути важливо мати глибокі знання про певні системи та контекст, у якому ці системи впроваджуються в організації. Може просто не вистачити кадрів з необхідним фахом.

Тому, завдання служби реагування полягає в тому, щоб визначити, коли сталося порушення. Для цього вони повинні шукати **індикатори компромісу** indicators of compromise (**IOCs**) на основі зібраних даних. IOCs бувають у багатьох формах і надходять із багатьох джерел, тому важливо знати про кожен актив безпеки, який використовує організація, як технічні, так і нетехнічні.

ПЗ для захисту від зловмисного ПЗ: сповіщення, яке створюється, коли в системі хоста виявлено сигнатуру вірусу.

Система виявлення вторгнень у мережу/система запобігання вторгнень у мережу (NIDS/NIPS): сповіщення, що створюється після виявлення автоматичного сканування портів.

Система виявлення вторгнень на хост/система запобігання вторгнень на хост (HIDS/HIPS): сповіщення, створене після того, як криптографічний хеш важливого файлу більше не відповідає його відомому, прийнятому значенню.

Системні журнали: запис у журналі подій Windows вказує, коли користувач увійшов на хост.

Журнали мережевого пристрою: запис у журналі брандмауера вказує на розірване з'єднання, призначене для заблокованого порту.

Інформація про безпеку та керування подіями (SIEM): сповіщення генерується, якщо в будь-яких відповідних журналах виявляється аномальна поведінка.

Пристрій контролю потоку: незвичайно великий обсяг трафіку в мережі вказує на стан спроби відмови в обслуговуванні (DoS).

Внутрішній персонал: свідчення співробітників вказують на те, що вони могли бути свідками порушення.

Люди за межами організації: зовнішня сторона, яка стверджує, що несе відповідальність за атаку, означає, що це так.

Дослідження: сторонні дослідження та інформація з бази даних уразливостей вказують на нову загрозу, яка може бути націлена на вашу організацію.

6. Вплив і масштаб інцидентів

Збитки, завдані в результаті інциденту, можуть мати широкомасштабні наслідки. Крім того, **вплив інциденту** може бути як матеріальним, так і нематеріальним. Відчутними наслідками можуть бути пошкоджені дані на жорсткому диску, видалений список клієнтів або вкрадені паролі. Однак

інциденти можуть мати більш нематеріальні наслідки, наприклад, організація може зазнати економічної шкоди через втрату потенційних клієнтів через недоступність веб-сайту після DoS-атаки. Репутація компанії може бути заплямована, якщо конфіденційні дані клієнтів і співробітників будуть викрадені.

Важливо не недооцінювати масштаб впливу інциденту на організацію. Щоб визначити ступінь збитку, слід поспілкуватися з членами CSIRT, а також іншими співробітниками, щоб визначити всі аспекти організації, на які може вплинути інцидент.

7. Оцінка та аналіз інцидентів

Зусилля з виявлення та аналізу інцидентів можуть бути складними. Навіть окрім величезної кількості сповіщень, які генеруються щодня, багато з цих сповіщень можуть виявитися помилковими. На етапі аналізу необхідно вміти відокремити помилкові спрацьовування від реального показника інциденту.

Навіть якщо сповіщення або запис у журналі не є хибно позитивним і фактично вказує на щось несприятливе, це не обов’язково означає, що це результат інциденту. Сервери виходять з ладу, робочі станції виходять з ладу, а файли змінюються через помилки, спричинені як машинами, так і людьми. Однак вони не повідомляють автоматично, чи ваша організація щойно зазнала значної атаки чи нещасного випадку.

8. Стримування інциденту

Методи стримування збитків під час реагування на інцидент безпеки є унікальними для інциденту та організації, проте можна визначити деякі загальні підходи.

- Забезпечення безпеки персоналу.
- Видалення пристроїв із мережі.
- Вимкнення зв’язку між мережевими пристроями.
- Вимкнення мережевих облікових записів користувачів.
- Вимкнення облікових записів електронної пошти.
- Обмеження доступу до уражених підмереж.
- Ізоляція скомпрометованої системи.

9. Пом'якшення та ліквідація інциденту

Після того, як інцидент було виявлено, проаналізовано та локалізовано, можна перейти до його пом’якшення та ліквідації

Заходи, які вживаються для **відновлення після інциденту**, значною мірою залежатимуть від характеру інциденту, а також від того, як підготувалися саме до такого інциденту.

Останню фазу процесу реагування на інцидент часто називають фазою

після інциденту post-incident phase, оскільки вона відбувається після того, як організація успішно відновилася після інциденту. Звіт про завершення дії **after-action report** (AAR) або звіт про отримані уроки **lessons learned report** (LLR) - це документація після інциденту, яка містить аналіз подій та інцидентів у сфері безпеки, що може надати розуміння напрямків, які ви можете зробити для підвищення безпеки в майбутньому.

Важливим компонентом документації після інциденту буде узагальнення та надання опису того, що сталося під час інциденту. Іншим компонентом AAR є **аналіз першопричини** або спроба визначити каталізатор інциденту. Найпростіший спосіб знайти першопричину - це продовжувати задавати питання: «Що було першочерговим, що дозволило цьому статися?» Як правило, першопричину можна розкрити приблизно у шести питаннях. І, як правило, буде більше однієї першопричини.

УПРАВЛІННЯ НАСЛІДКАМИ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Зміцнення системи
2. Управління мобільними пристроями
3. Безпечне видалення та утилізація
4. Стримування та пом’якшення наслідків

1. Зміцнення системи

Стримування та пом’якшення наслідків мають бути основною частиною плану **реагування на інциденти** Incident Response (IR) будь-якої організації. Захист системи – це процес, за допомогою якого хост або будь-який інший пристрій стає більш безпечним шляхом зменшення поверхні атаки цього пристрою.

Зміцнення системи є ефективним як профілактичний захід під час проектування безпеки системи, але це не завжди можливо через обмеження часу, грошей і потребу в зручності. Однією з найважливіших стратегій пом’якшення, яку можна застосувати для майже всіх типів інцидентів, є **ізоляція**, що передбачає видалення ураженого компонента з середовища, частиною якого він є.

Медові горщики Honeypot - це практика, яка затримує зловмисників в ізольованому середовищі, де за ними можна стежити та утримуватися від компрометації систем у виробництві.

Чорний список - це процес блокування відомих програм, служб, трафіку та інших передач до та з систем.

Білий список - це відповідь на проблему чорного списку щодо того, що

невідомо. У білому списку все інше, крім того, що є надійним, блокується.

Одним із механізмів залучення до чорного та білого списків є **DNS фільтрація.** Фільтрація системи доменних імен (DNS), яка також називається веб-фільтрацією, - це процес обмеження запитів на пошук, які перевіряються в організації.

Маршрутизація чорної діри. У мережевій архітектурі **чорна діра** пропускає трафік до того, як він досягне свого призначення та не попереджає про джерело.

2. Управління мобільними пристроями

Оскільки мобільні пристрої стають все більш поширеними на робочому місці, вони неминуче будуть фактором інцидентів кібербезпеки. Практика **управління мобільними пристроями** (MDM) відстежує, контролює та захищає мобільну інфраструктуру організації. Рішення MDM часто є веб-платформами, які дозволяють адміністраторам працювати з централізованої консолі.

Якщо організація встановлює MDM перед інцидентом, служби швидкого реагування можуть використовувати адміністративну консоль кількома способами для пом’якшення інцидентів, які впливають на мобільні пристрої. Якщо зловмисне ПЗ, націлене на мобільні ОС, потрапляє на пристрої співробітників, CSIRT може швидко надіслати виправлення на кожен пристрій, щойно постачальник надасть виправлення. Це лише деякі приклади того, як процес MDM може посилити безпеку мобільних пристроїв, про яку часто не звертають уваги, під час інциденту.

3. Безпечне видалення та утилізація

У деяких випадках захищати хост або ізолювати його від інших пристроїв буде недостатньо, щоб повністю знищити зловмисне ПЗ або іншу точку компрометації. Часто важко перевірити, чи використані методи неруйнівного видалення справді очистили руткіти та інші механізми збереження з пристрою. У подібних ситуаціях може знадобитися **безпечне видалення** за допомогою процесу, відомого як санітарна обробка.

Дезінфекція - це ретельне й повне видалення всіх даних із пристрою зберігання, щоб їх неможливо було відновити. Ця ретельність є важливою, оскільки на пристрої не повинно бути залишків даних, які можуть призвести до подальшого зламу.

Дезінфекція руйнівна для віртуальних даних, а не для самого носія. Це дає змогу реконструювати та повторно створювати образ диска після його дезінфекції за допомогою відомої чистої резервної копії, створеної до інциденту. Однак у деяких випадках немає гарантії, що інфекцію вдалося знищити, доки не буде знищено сам носій даних. Утилізація зламаного

обладнання зазвичай передбачає фізичне знищення пристрою.

4. Стримування та пом’якшення наслідків

Стримування та пом’якшення наслідків мають бути основною частиною плану реагування на інциденти будь-якої організації. Пристрої та інструменти, що використовуються для стримування та пом’якшення є наступними:

Брандмауери - можуть виконувати деякі з найпростіших процесів фільтрації трафіку у вашій мережі..

IDS/IPS - система виявлення вторгнень/система запобігання вторгненням (IDS/IPS) допоможе гарантувати, що тривалі або постійні атаки легше ідентифікувати та охарактеризувати.

Рішення для безпеки кінцевих точок - включають надійні функції захисту від зловмисного ПЗ, можуть допомогти виявити й усунути руткіти, бекдори й інші ознаки розширеної постійної загрози (APT).

Маршрутизатори та комутатори - маршрутизатори можуть бути корисними для створення чорних дір для відкидання трафіку DoS. Комутатори також є звичайним компонентом для створення підмереж. Ці підмережі можуть ізолювати скомпрометовані пристрої, забезпечуючи їм підключення до мережі.

Проксі - веб-проксі-сервери можна використовувати як метод фільтрації вмісту.

Віртуальні машини - коли справа доходить до пом’якшення зараження зловмисним ПЗ, можна виділити та проаналізувати його у віртуальному середовищі.

Настільні комп’ютери - це платформа, на якій будуть використовуватися професійні інструменти реагування на інциденти.

Сервери - забезпечують балансування навантаження та резервне копіювання даних під час DDoS-атак і знищення даних.

Мобільні пристрої - портативність смартфонів, планшетів та інших мобільних пристроїв може пришвидшити зусилля з пом’якшення, оскільки вони не прив’язані до одного фізичного розташування, як настільний комп’ютер.

РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ

1. Група розслідування інцидентів.
2. Процедури для захисту доказів.
3. Моделі судових розслідувань.
4. Етапи криміналістичного дослідження.
5. Автентифікація та зберігання доказів.
6. Інструментарій розслідування івнцидентів.
7. Робота з доказами.

1. Група розслідування інцидентів

Коли трапляється інцидент, аналітикам може знадобитися виконати різних експертних дій, наприклад зібрати дані та виявити докази. Під час і після інциденту спеціалісти з реагування на інциденти повинні виконувати різні завдання, щоб переконатися, що аналітики-криміналісти зможуть ефективно виконувати свою роботу.

Комп'ютерні аналітики-експерти можуть бути залучені до розслідувань, зосереджених на широкому спектрі вторгнень або порушень, таких як хакерство; тероризм; політичне, промислове або комерційне шпигунство; викрадення співробітниками конфіденційної інформації компанії; онлайн-шахрайство; і нелегальна порнографія. Групи IT-технологій або безпеки також можуть звернутися до судових аналітиків для допомоги в плануванні IT-систем і процесів, щоб переконатися, що докази будуть належним чином оброблені під час інциденту кібербезпеки.

Комунікація з експертами аналітиками-криміналістами. Після інциденту члени CSIRT можуть бути запрошені тісно співпрацювати з судово криміналістичними аналітиками.

Після інциденту кібербезпеки організація може провести аналіз, наприклад, зібрати докази та визначити, як і чому стався інцидент і хто його спричинив. Для цього потрібно:

- створити план проведення судово-криміналістичних розслідувань після інцидентів;
- зібрати та проаналізувати електронні докази безпечним способом, щоб запобігти підробці або компрометації;
- вжити заходів щодо подальшого розслідування.

2. Процедури для захисту доказів

Організація може мати юридичні зобов'язання під час розслідування інциденту кібербезпеки. Важливо мати план, який гарантує, що організація проводить криміналістичну експертизу належним чином, ефективно та відповідно до чинних норм. У будь-якому випадку судовий криміналіст аналітик повинен **дотримуватися процедур для захисту доказів:**

- Переконатися, що вся розслідувальна діяльність виконується згідно із законами, правилами безпеки та стандартами конфіденційності, а також відповідно до політики компанії.
- Захистити докази, заповнивши форму ланцюга зберігання.
- Під час інциденту або після нього захистити IT-системи та апаратне забезпечення, щоб їх неможливо було втручати.
- Навчити інших належним процедурам захисту доказів.

3. Моделі судових розслідувань

Більшість цифрових криміналістичних моделей і фреймворків просто пропонуються і не широко прийняті як галузевий стандарт. Багато з цих моделей і структур успадковано від традиційних криміналістичних процедур, які десятиліттями використовувалися в кримінальних розслідуваннях. Ці моделі потім перетворюються, щоб бути більш придатними для ІТ, а деякі націлені на більш специфічні контексти.

4. Етапи криміналістичного дослідження

Перелік дій, які організація може вжити для підготовки до розслідування інцидентів наступні:

Вивчення апаратного забезпечення, що використовується у організації: це може бути все, від робочих станцій, мережевих пристроїв, мобільних пристроїв, знімних носіїв тощо..

Вивчення операційних систем: різні операційні системи виконують різні цілі, і так само кожна може потребувати іншого підходу до збору та аналізу доказів.

Вивчення програмного забезпечення, яке використовується у організації: чим більше інформації щодо ПЗ, яким щодня користуються персонал, тим легше буде отримувати відповідну інформацію з цих програм.

Вивчення інструментів професії: слідчі не повинні вибирати криміналістичні утиліти після інциденту - краще заздалегідь.

Вивчення віртуалізованих середовищ організації: проведення криміналістичних досліджень на віртуальних машинах (ВМ) є більш складним завданням, ніж дослідження локальної машини через розподілену природу віртуальних середовищ.

Вивчення системи, які мають залишатися активними під час розслідування: бувають випадки, коли слідчі не обов’язково матимуть можливість ізолювати систему, позначену як доказ. Деякі системи мають залишатися активними з комерційних причин, а з технічних причин дослідники можуть не мати змоги відтворити їхній вміст в ізольованому середовищі.

Вивчення відповідних законів та правил: нерозуміння законів може зробити розслідування недоцільним.

5. Автентифікація та зберігання доказів

Автентифікація доказів: Збір доказів не означає автоматично, що докази прийнятні в суді або що вони повністю перевірені під час розслідування. Докази мають бути засвідчені або підтверджені, щоб вони були саме такими, якими стверджує прихильник цих доказів.

Коли створюється план розслідування інциденту, слід розглянути, як можна перевірити автентичність різних типів доказів, які слідчі можуть зібрати.

Це допоможе сформувати розслідування, підкресливши його ключові висновки, усунувши слабші або непереконливі аспекти. Також може знадобитися визнати, що деякі докази просто не можуть бути засвідчені, і тому вони не будуть прийнятними.

Ланцюжок зберігання - це записи обробки доказів від збору до аналізу та зберігання до представлення в суді до знищення. Доказами можуть бути апаратні компоненти, електронні дані, телефонні системи тощо. Ланцюжок доказів зміцнює цілісність і належне зберігання доказів протягом усього процесу розслідування. Кожна особа в ланцюжку, яка працює з доказами, повинна реєструвати методи та інструменти, які вони використовували. Коли порушення безпеки передаються до суду, ланцюжок контролю захищає організацію від звинувачень у тому, що докази або були підроблені, або вони зовсім інші, ніж вони були на момент їх збору.

6. Інструментарій розслідування івнцидентів

Створення інструментарію є важливою частиною підготовки до розслідування інцидентів. Набір інструментів має бути достатньо широким, щоб охоплювати багато різних аспектів аналізу. Один інструмент не обов’язково охопить усі ці параметри.

На додаток до різноманітних доступних програм, також потрібно розглянути можливість зібрати фізичні інструменти, які були б корисними у вашому набір інструментів криміналістики.

7. Робота з доказами

Дані є мінливими, і можливість отримати або перевірити дані після інциденту безпеки залежить від того, де вони зберігаються в розташуванні чи на рівні пам’яті комп’ютера чи зовнішнього пристрою.

Порядок, у якому потрібно відновити дані після інциденту, перш ніж дані погіршаться, будуть стерті або перезаписані, називається порядком нестабільності. Загальний порядок мінливості для носіїв даних від найбільшої до найменшої:

1. Регістри процесора, кеші процесора та оперативна пам'ять.
2. Мережеві кеші та віртуальна пам'ять.
3. Жорсткі диски, флеш-накопичувачі та твердотільні накопичувачі.
4. CD-ROM, DVD-ROM та роздруківки.

Мінливість також може стосуватися непостійності пам’яті, коли її відключено від джерела живлення.

Файлова система комп’ютера може виявити багато корисної інформації про інцидент, зокрема: структура каталогу; розташування файлу; розмір файлу; ім'я файлу; значення дати й часу (останнє змінення, останній доступ тощо); різні атрибути файлів і папок. Аналіз цих метаданих може допомогти слідчим

встановити часову шкалу подій для інциденту, який залишив сліди на хості та його файлах.

Розрізання файлів - це процес вилучення даних із комп’ютера, коли ці дані не мають пов’язаних метаданих файлової системи.

Збереження даних. Кримінальні справи або внутрішні перевірки безпеки можуть тривати місяці чи роки. Необхідно вміти зберігати всі зібрані докази належним чином протягом тривалого періоду часу. Як відомо, апаратне забезпечення комп’ютера схильне до зношування, а такі важливі носії інформації, як жорсткі диски, можуть вийти з ладу, навіть якщо використовуються нормально або не використовуються взагалі. Помилка такого роду може означати корупцію або втрату доказів, що може мати серйозні наслідки для розслідування.

Тому, коли це можливо, необхідно відтворювати докази на кількох носіях інформації з метою резервування.

Підписано до друку 18.04.2023 р.
Формат 60х84/16. Папір офсетний.
Друк офсетний. Зам. № 23-10245
Умов.-друк. арк. 2,9. Обл.-вид. арк. 3,1.
Тираж 30 прим.

Віддруковано ФО-П Шпак В. Б.
Свідоцтво про державну реєстрацію В02 № 924434 від 11.12.2006 р.
м. Тернопіль, бульвар Просвіти, 6/4. тел. 097 299 38 99.
E-mail: tooums@ukr.net

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 7599 від 10.02.2022 р.