ЗАТВЕРДЖЕНО

Науково-методичною радою
Державного університету
«Житомирська політехніка»

протокол від 24 червня 2026 р.
№ 5

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для проведення практичних (лабораторних) занять з навчальної дисципліни «Захист інформації в галузі»

для здобувачів вищої освіти освітнього ступеня «назва»
спеціальності 163 «Біомедична інженерія»
освітньо-професійна програма «Біомедичний комп'ютинг»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерних технологій у медицині та телекомунікаціях

Рекомендовано на засіданні кафедри комп'ютерних технологій у медицині та телекомунікаціях
___ _____ 20__ р.,
протокол № ___

Розробник: старший викладач ГЕРАЙМОВИЧ Олександр, старший викладач НІКІТЧУК Сергій, доцент ДУБИНА Олександр

Житомир
2026

ЗМІСТ

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій та інтелектуалізації охорони здоров’я інформаційна безпека стала критичним елементом функціонування будь-якого медичного підприємства, клініки чи науково-дослідного центру. Впровадження інноваційних систем на кшталт Інтернету медичних речей (IoMT), цифрових платформ охорони здоров'я, телемедицини та комп'ютеризованих комплексів біометричної діагностики вимагає від майбутніх інженерів глибоких знань із захисту даних. Особливої актуальності ці питання набувають у галузі біомедичної інженерії, де об'єктами захисту є не лише стандартна корпоративна документація, а й високочутлива персональна медична інформація пацієнтів, результати фізіологічного моніторингу та параметри критично важливого медичного обладнання.

Основною метою виконання циклу практичних робіт із дисципліни «Захист інформації в галузі» є оволодіння сучасними методами, технологіями та засобами комплексного захисту інформації та технічних систем у сфері біомедичної інженерії.

Представлені практичні заняття адаптовані до специфіки галузі та охоплюють ключові аспекти безпеки у сфері медичних і дослідницьких технологій:

Аналіз загроз та протидія атакам: дослідження методів соціальної інженерії, спрямованих на персонал медичних закладів та дослідницьких лабораторій, а також складання ймовірнісних прогнозів і побудова моделей потенційних порушників для об'єктів медичного приладобудування.

Технічний та фізичний захист: вивчення стандартів проектування захищених серверних та апаратних кімнат, де обробляються бази даних медичних пацієнтів, а також аналіз і блокування технічних каналів витоку інформації в кабінетах керівників та закритих дослідницьких лабораторіях.

Криптографічний захист та автентифікація: практичне застосування електронних цифрових підписів для підтвердження автентичності медичної електронної документації та результатів аналізів, використання класичних

шифрів заміни й перестановки, а також оцінка стійкості паролів доступу до лікарняних інформаційних систем.

Розвідка та аналіз вразливостей: ознайомлення з інструментами OSINT-розвідки, принципами безпеки збору відкритих даних та методами тестування на проникнення задля запобігання витоку інтелектуальної власності та конфіденційних розробок у галузі медтехнологій.

Виконання цих завдань сприяє формуванню у студентів спеціальності «Біомедична інженерія» професійних компетенцій, необхідних для проєктування захищених медичних систем, забезпечення конфіденційності даних пацієнтів, запобігання несанкціонованому втручанню в роботу лікувально-діагностичного обладнання та розробки надійної політики безпеки на медичних підприємствах.

Практичне заняття №1

ДОСЛІДЖЕННЯ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Мета:

- *Дослідження методів соціальної інженерії*
- *Створення інформаційного плаката про кібербезпеку*

Необхідні ресурси

ПК або мобільний пристрій з доступом до Інтернету

ТЕОРЕТИЧНА ЧАСТИНА

Останні дослідження свідчать про те, що кібератаки найпоширеніших типів стають все складнішими, а цілі атак зростають. Метою атаки є викрадення інформації, відключення систем або критичних служб, порушення роботи систем, призупинення діяльності та поточних операцій. Одні атаки призначені для повного знищення інформації чи інформаційних систем, інші − для отримання зловмисником контролю над обчислювальним середовищем чи його інфраструктурою, ще інші − для порушення цілісності даних та/або інформаційних систем. Одним з найефективніших способів отримання доступу до мережі організації є звичайний обман. У світі кібербезпеки він має назву соціальна інженерія.

Атаки соціальної інженерії

Атаки соціальної інженерії дуже ефективні, бо люди хочуть довіряти іншим людям, а атаки соціальної інженерії не є тим типом атак, від яких захищається пересічний користувач; користувачів турбують ботнети, крадіжка особистих даних або програми-вимагачі. Це великі зовнішні загрози, тому користувачі не ставлять під сумнів ті повідомлення, які здаються їм легальними.

Приманювання (Baiting)

Приманювання базується на цікавості або жадібності жертви. Відмінністю приманювання від інших видів соціальної інженерії є використання зловмисниками обіцянок про надання жертві певного предмета або товару. Бейтери (Baiters) можуть запропонувати користувачам безкоштовне завантаження музики або відео за умови, якщо користувачі передадуть свої облікові дані входу на певний сайт. Атаки-приманювання не обмежуються лише онлайн-схемами. Зловмисники можуть використовувати людську цікавість до фізичних носіїв, наприклад USB-накопичувачів.

Підглядання з-за плеча (Shoulder Surfing)

Підглядання з-за плеча (Shoulder Surfing) – дослівно «серфінг через плече» для отримання інформації. Підглядання з-за плеча – це ефективний спосіб отримати інформацію у людних місцях, оскільки досить легко стати поруч із кимось та

непомітно спостерігати за процесом заповнення форми або введення PIN-коду у банкоматі. Підглядання з-за плеча можна також здійснювати з великої відстані за допомогою сучасних мобільних телефонів, біноклів або інших пристроїв поліпшення зору. Для запобігання підглядуванню з-за плеча експерти рекомендують захищати документи або клавіатуру, закриваючи поле зору тілом або рукою. Існують спеціальні екранні щитки, які значно ускладнюють підглядування з-за плеча.

Вигаданий привід (Pretexting)

Вигаданий привід (Pretexting) – це використання обману для створення сценарію, за яким проводяться дії, щоб переконати жертв розголосити ту інформацію, яку вони не повинні розголошувати. Вигаданий привід часто використовується проти організацій, які зберігають дані клієнтів, зокрема, фінансові дані, номери кредитних карток, номери рахунків комунальних послуг та іншу конфіденційну інформацію. Зловмисники, що користуються таким різновидом атак, часто надсилають інформаційні запити певним співробітникам організації, видаючи себе за керівника, співробітника служби підтримки або клієнта, як правило, звертаючись телефоном, електронною поштою або за допомогою текстового повідомлення.

Фішинг (Phishing), Спрямований фішинг (Spear Phishing) та Уелінг (Whaling)

Під час фішингових атак зловмисники, маскуючись під легальних осіб, намагаються отримати особисту інформацію або дані, зокрема, імена користувачів, паролі, дані кредитних карток. Фішинг (Phishing), як правило, здійснюється за допомогою електронної пошти та телефонних дзвінків. Спрямований фішинг (Spear Phishing) – це більш цілеспрямована версія фішингу, у якій зловмисник вибирає як жертву конкретну особу або підприємство, а потім якомога непомітніше провадить атаку. Уелінг (Whaling), дослівно полювання на китів − це фішингова атака ціллю якої є високопоставлена особа, наприклад, генеральний директор (CEO) або фінансовий директор (CFO).

Програми-залякувачі та програми-вимагачі

Атаки програм-вимагачів (Ransomware attacks) передбачають впровадження зловмисного програмного забезпечення, яке виконує шифрування важливих даних жертви. Відповідно кіберзлочинці вимагають викуп за розшифрування даних. Однак, навіть якщо викуп буде сплачено, немає жодної гарантії, що кіберзлочинці виконають розшифрування інформації. Програми-вимагачі є одним із найбільш швидкозростаючих типів кібератак, вони вже вразили тисячі фінансових організацій, державних установ, медичних установ, навіть шкіл та освітніх систем.

Програми-залякувачі (Scareware) використовують страх користувачів, змушуючи їх встановлювати підробне антивірусне програмне забезпечення.

Несанкціоноване проникнення «на хвості» (Tailgating)

Несанкціоноване проникнення «на хвості» (Tailgating) спрямоване на обман жертви, щоб допомогти зловмисникові отримати несанкціонований доступ до фізичних об'єктів організації. Зловмисник намагається проникнути в зону з обмеженим доступом, доступ до якої контролюється програмними електронними пристроями або людьми-охоронцями. Несанкціоноване проникнення «на хвості» (Tailgating) також може виникати тоді, коли зловмисник намагається пройти через двері відразу за легальним співробітником, перш ніж ці двері закриються.

Пошук у смітнику (Dumpster Diving)

У світі соціальної інженерії пошук у смітнику – це техніка, в якій використовується пошук та аналіз даних з викинутої у смітник інформації, з метою подальшого атакування певної особи чи організації. Пошук у смітнику не обмежується пошуком у сміттєвому кошику очевидних «скарбів» як-от коди доступу чи записані на липучках паролі, а також поширюється на електронну інформацію, залишену на настільних комп'ютерах чи збережену на USB-накопичувачах.

ЗАВДАННЯ ДО ВИКОНАННЯ (ХІД РОБОТИ)

Частина 1. Дослідження методів соціальної інженерії.

Крок 1: Ознайомлення з методами Приманювання (Baiting), Підглядування з-за плеча (Shoulder Surfing) та Вигаданий привід (Pretexting).

Національний центр підтримки безпеки систем та забезпечення інформації (CSSIA, National Support Center for Systems Security and Information Assurance) проводить захід **Інтерактивна соціальна інженерія**. Поточне посилання на сайт https://www.caeepnc.org/social_engineering/. Якщо посилання змінилося, спробуйте виконати пошук за ключовою фразою «CSSIA Social Engineering Interactive».

Натисніть **Next** у завданні, а потім скористайтеся вмістом для відповідей на такі запитання.

Що таке Приманювання (Baiting)? Ви натиснули на USB-накопичувач? Що сталося з системою жертви?

_____

_____

_____

_____

Що таке Підглядування з-за плеча (Shoulder Surfing)? Який пристрій було використано для виконання підглядування з-за плеча? Яку інформацію було отримано?

_____
_____
_____
_____

Що таке Вигаданий привід (Pretexting)? Інформацію якого типу запитав кіберзлочинець? Ви б стали жертвою?

_____
_____
_____
_____

Крок 2. Дослідження методів Фішинг (Phishing), Спрямований фішинг (Spear Phishing) та Уелінг (Whaling)

Фішинг призначений для того, щоб змусити жертв виконувати такі дії: натискати посилання на шкідливі веб-сайти; відкривати вкладення, які містять шкідливе програмне забезпечення; розкривати конфіденційну інформацію. Використайте інтерактивне завдання, щоб вивчити різні методи фішингу.

Який трюк у наведеному прикладі фішингу використовує зловмисник для обману жертви, що спонукає до відвідування веб-сайту-пастки? Для чого використовується веб-сайт-пастка?

Який трюк у наведеному прикладі фішингу використовує зловмисник для обману жертви, що спонукає до відвідування веб-сайту-пастки? Для чого використовується веб-сайт-пастка?

_____
_____
_____
_____

У чому відмінність між такими методами як Фішинг (Phishing), Спрямований фішинг (Spear Phishing) та Уелінг (Whaling)?

_____
_____
_____
_____

Крок 3. Ознайомлення з програмами-залякувачами (Scareware) та програмами-вимагачами (Ransomware)

Програма-залякувач (Scareware) – це програма, яка надсилає користувачеві-жертві фальшиві сигнали тривоги та формує у нього думку, що його система інфікована зловмисним програмним забезпеченням, та спонукає користувача до встановлення непотрібного або зловмисного програмного забезпечення. Програма-вимагач (Ransomware) – це тип зловмисного програмного забезпечення, яке загрожує опублікувати або шифрує дані жертви, перешкоджаючи доступу до цих даних чи можливості їх використання. Жертві блокується доступ до її системи або до особистих файлів, допоки вона для відновлення доступу не внесе викуп.

Які дані, як стверджує, має зловмисник у цьому прикладі? Чи піддалися б ви такому обману?

_____
_____
_____
_____

Що зловмисник вимагає від жертви для повернення даних?

_____
_____
_____
_____

Що таке несанкціоноване проникнення «на хвості» (Tailgating)?

_____
_____
_____
_____

Назвіть три способи запобігання атакам соціальної інженерії?

_____
_____
_____
_____

Частина 2. Створення інформаційного плаката про кібербезпеку

Використайте PowerPoint для створення плакату, що інформуватиме інших користувачів про різні методи соціальної інженерії, які використовуються для

отримання несанкціонованого доступу до організації або доступу до даних організації.

Тематику плакату виберіть з переліку: Приманювання (Baiting), Підглядування з-за плеча (Shoulder Surfing), Вигаданий привід (Pretexting), Фішинг (Phishing), Програми-залякувачі (Scareware), Програми-вимагачі (Ransomware), Несанкціоноване проникнення «на хвості» (Tailgating), Пошук у смітнику (Dumpster Diving).

На плакаті має бути зображено використовувані методи та рекомендації щодо уникнення цих атак соціальної інженерії. Також додайте вказівки щодо того, де слід розмістити плакат.

Частина 3. Додаткові завдання:

1. Навести скріншот для підтвердження проходження Розділу 1 (1.0-1.6) курсу «Основи кібербезпеки» Академії Cisco:

https://www.netacad.com/courses/cybersecurity-essentials?courseLang=uk-UA&instance_id=4cc770bf-9b5f-4480-9c81-66d06d602368

2. Оформити звіт на надіслати на пошту викладача.

Практичне заняття 2

Вивчення світу спеціалістів з кібербезпеки

Цілі та задачі

Проаналізуйте можливості функцій безпеки, які використовують такі організації, як Google та Cisco, для захисту ваших даних.

Частина 1: Захист ваших даних

Частина 2: Підвищення безпеки облікового запису Google

Довідкова інформація / Сценарій

Цей розділ знайомить слухача з кібер-світом. Кібер-світ є великим царством даних,з великою кількістю сховищ даних, які обробляють неймовірні обсяги особистої інформації та інформації організацій. Фахівцям з кібербезпеки, важливо розуміти типи захисних механізмів, які організація повинна реалізувати, щоб захистити дані, які вони зберігає та обробляє. У цій лабораторії ви ознайрмитесь з компанією Google, як з одним із світових лідерів об'єму обробки даних. Переглянувши ці відео, ви зможете дати відповідь на ряд запитань. Кожне відео представляє окремий з аспектів кіберзахисту в Google. Після завершення ви краще зрозумієте заходи безпеки та сервіси, які такі організації, як Google, здійсняють для захисту інформації та інформаційних систем.

Відео:

Як Google захищає Ваші дані (How Google Protects Your Data) Секретний ключ (Security Key)

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Part 1: Захист даних

Як одне з найбільших у світі сховищ персональних даних, Google зберігає величезну кількість даних. Google нараховує майже 50% усіх пошукових запитів в Інтернеті. Ще більше ускладнює задачу та обставина, що Google володіє та забезпечує підтримку YouTube, операційної системи Android та багатьма іншими платформами для збирання даних. У цій роботі ви переглянете коротке відео та спробуєте визначити деякі з заходів, які фахівці з кібербезпеки Google здійснюють, щоб захистити Ваші дані.

Step 1: Відкрийте веб-переглядач і перегляньте відео, як Google захищає ваші дані: How Google Protects Your Data

a. Як Google гарантує, що сервери, які вони встановлюють у своїх центрах обробки даних (ЦОД), не заражені зловмисним програмним забезпеченням виробниками обладнання?

_____

_____

b. Як Google здійснює захист від фізичного доступу до серверів, розташованих у центрах обробки даних Google?

_____

_____

c. Як Google захищає дані клієнта, що знаходяться на серверах?

_____

_____

Step 2: Визначення вразливостей даних.

a. Як видно з цього відео, дані в центрах обробки даних Google добре захищені, проте під час використання Google не всі ваші дані розміщуються в центрі обробки даних Google. Де ще можна знайти ваші дані під час використання пошукової системи Google?

_____

_____

b. Чи можете ви вжити заходів для захисту даних під час використання пошукової системи Google? Які декілька заходів можна використовувати для захисту ваших даних?

_____

_____

Part 2: Підвищення безпеки облікового запису Google

Найбільшою з загроз при використанні веб-сервісів, таких як Google є захист вашої персональної інформації облікового запису (ім'я користувача та пароль). Ситуацію ускладнює те, що ці облікові записи загальнодоступні та використовуються для автентифікації вас на інших веб-сервісах, таких як Facebook, Amazon або LinkedIn. У вас є кілька варіантів для покращення керування вашою реєстраційною інформацією для входу в Google. Ці заходи включають створення двоетапної перевірки або коду доступу для вашого імені користувача та пароля. Google також підтримує використання ключів безпеки (security keys). У цій роботі ви переглянете коротке відео та спробуєте визначити заходи, які можна використовувати для захисту ваших облікових даних під час використання облікових записів, що базуються на web.

Step 1: Відкрийте веб-переглядач і перегляньте відео: Ваш ключ простіше, швидше і безпечніше

a. Що таке двоетапна аутентифікація? Як ким чином вона захищає ваш обліковий запис Google?

_____

_____

b. Що таке ключ безпеки і яку функцію він виконує? Чи можна ви використовувати ключ безпеки у кількох системах?

_____

_____

c. Натисніть тут для перегляду поширених запитань про ключ безпеки. Якщо ви налаштували свій обліковий запис, щоб використовувати ключ безпеки, чи можете ви все ще входити в цей обліковий запис не маючи ключа безпеки?

_____

_____

Step 2: Захистіть доступ до облікового запису Gmail.

a. Використання облікового запису Gmail стало надзвичайно популярним. У Google зараз більше 1 мільярда активних облікових записів Gmail. Одна з зручних функцій облікових записів Gmail - це можливість надавати доступ іншим користувачам до вашого облікового запису. Ця функція спільного доступу створює спільну електронну адресу. Хакери можуть використовувати цю функцію для доступу до вашого облікового запису Gmail. Щоб перевірити свій обліковий запис, увійдіть до свого облікового запису Gmail і натисніть значок шестірні у верхньому правому куті (налаштування). Коли відкриється екран налаштувань, під заголовком екрана налаштувань з'явиться рядок меню. (Загальні - Мітки - Вхідні - Облікові записи та імпорт - Фільтри та заблоковані адреси ...)

b. Натисніть **Облікові записи та імпорт** у меню Натисніть опцію **Надати доступ до свого облікового запису** Видаліть будь-які неавторизованих користувачів вашого облікового запису.

Step 3: Перевірте активність облікового запису Gmail

a. Користувачі Gmail також можуть перевіряти активність в обліковому записі, щоб переконатися, що жоден інший користувач не має доступу до їх особистого облікового запису Gmail. Ця функція може визначити, хто мав доступ до облікового запису та з яких місць. Використовуючи опцію **Остання активність облікового запису** можна визначити, чи хтось ще має доступ до вашого облікового запису. Для доступу до опції **Остання активність облікового запису** необхідно зробити три кроки.

   1) Увійдіть у свій обліковий запис Gmail

   2) Виберіть **Остання активність облікового запису** (знайдіть внизу сторінки). Вона відобразить останній раз, коли неавторизований користувач отримав доступ до облікового запису та звідки.

   3) Саме під цим повідомленням є гіперпосилання «Деталі». Клацніть гіперпосилання «Деталі».

b. Переглянути журнал активності облікового запису. Якщо ви виявили неавторизованого користувача, ви можете від'єднати неавторизованого користувача, натиснувши кнопку вгорі ліворуч **Вийдіть з усіх інших сеансів**. Тепер змініть пароль, щоб неавторизований користувач не мав доступу до цього облікового запису.

Практичне заняття 3
Використання цифрових підписів

Цілі та задачі

Зрозуміти концепції цифрового підпису.

Частина 1: Продемонструвати використання цифрових підписів.

Частина 2: Продемонструвати перевірку цифрового підпису.

Довідкова інформація / Сценарій

Цифровий підпис - це математичний метод, який використовується для перевірки автентичності та цілісності цифрового повідомлення. Цифровий підпис є еквівалентом рукописного підпису. Цифрові підписи можуть бути набагато більш безпечними. Мета цифрового підпису полягає в тому, щоб запобігти підробці та інперсоніфікації цифрових повідомлень. У багатьох країнах, включаючи Сполучені
Штати, цифрові підписи мають таке ж юридичне значення, як і традиційні форми підписаних документів. Уряд Сполучених Штатів тепер публікує електронні версії бюджетів, законів і законопроектів Конгресу з цифровими підписами.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Part 1: Використання цифрових підписів

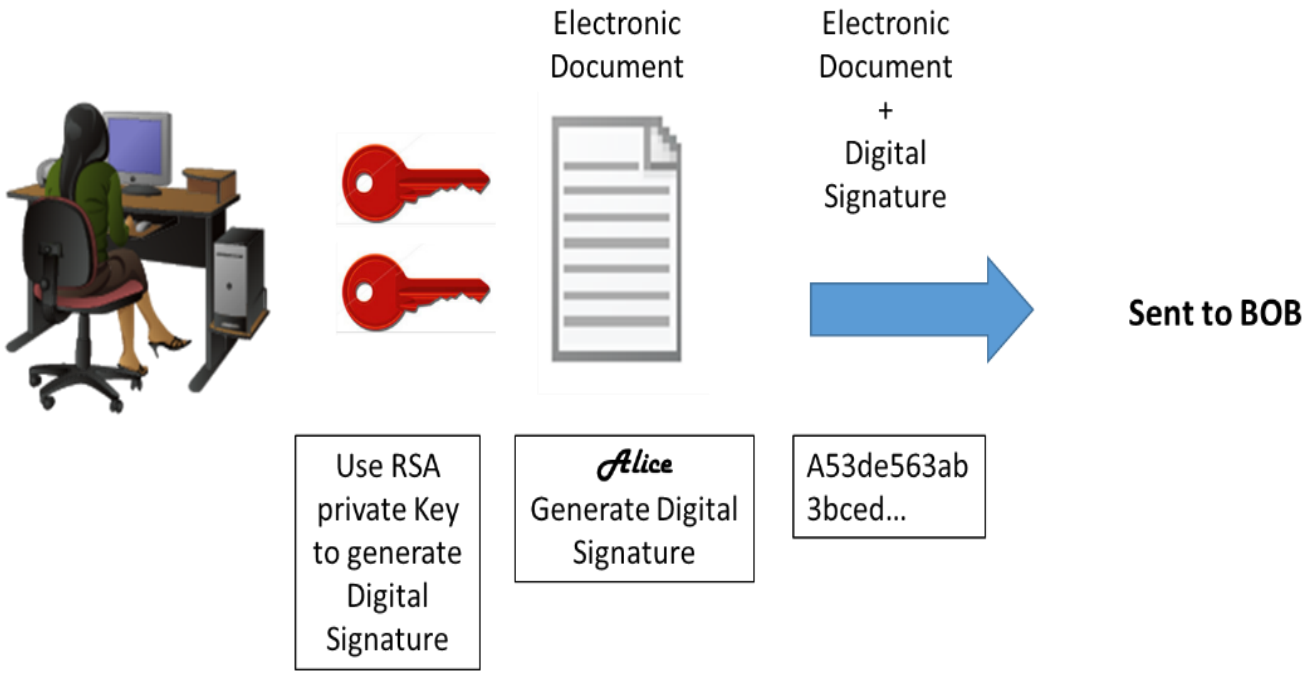
У цій частині ви будете використовувати веб-сайт для перевірки підпису документа між Алісою і Бобом. Аліса і Боб використовують одну пару закритих і відкритих ключів RSA. Кожен з них використовує свій закритий ключ для підписання юридичного документа. Потім вони відправляють документи один одному. І Аліса, і Боб можуть перевірити підпис один одного відкритим ключем. Вони також повинні домовитися про спільну відкриту експоненту для розрахунку.

Таблиця 1 - Відкритий і закритий ключі RSA

Відкритий ключ RSA	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Закритий ключ RSA	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Відкрита експонента	10001

Step 1: Підпишіть документ.

Аліса підписує юридичний документ і відправляє його Бобу з використанням відкритих і закритих ключів RSA, показаних в таблиці вище. Тепер Бобу доведеться перевірити цифровий підпис Аліси, щоб довіряти справжності електронного документа.



Step 2: Перевірте цифровий підпис.

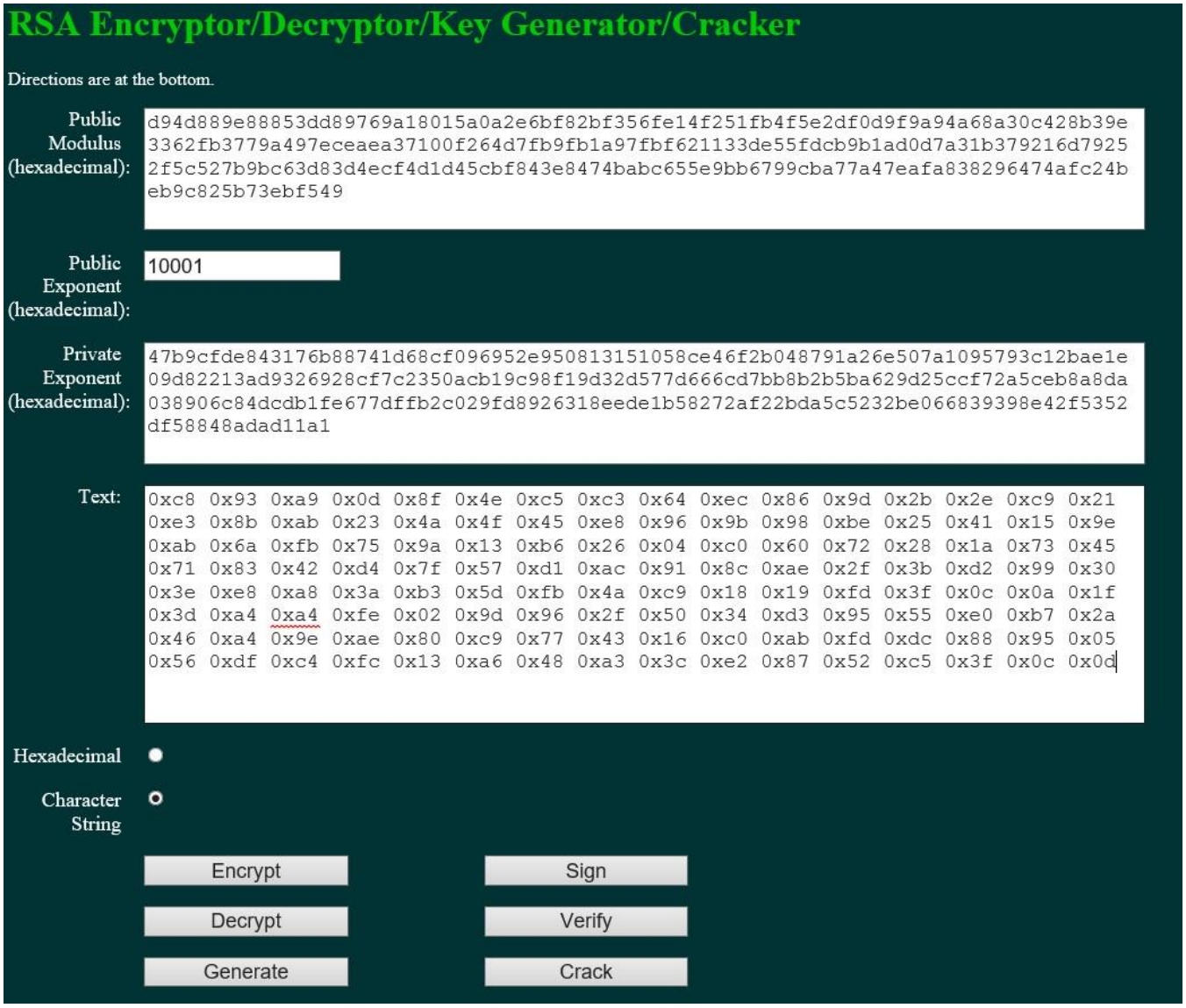
Боб отримує документ з цифровим підписом, показаним в таблиці нижче.

Таблиця 2 - Цифровий підпис Аліси

Цифровий підпис Аліси
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d

Натисніть тут, щоб використати онлайн-інструмент RSA для перевірки справжності цифрового підпису Аліси.

Таблиця 3 Онлайн інструмент цифрового підпису



a. Скопіюйте і вставте **відкриті** і **закриті** ключі з Таблиці 1 вище у поля **Public Modulus** і **Private Exponent** на сайті, як показано на рисунку вище.

b. Переконайтеся, що значення Public Exponent дорівнює 10001.

c. Вставте цифровий підпис Аліси з Таблиці 2 в поле з написом на веб-сайті, як показано вище.

d. Тепер Боб може перевірити цифровий підпис, натиснувши кнопку **Verify** знизу веб-сайту. Чий підпис ідентифіковано?

_____

Step 3: Створіть підпис для відповіді.

Боб отримує і перевіряє електронний документ і цифровий підпис Аліси. Тепер Боб створює електронний документ і генерує свій власний цифровий підпис, використовуючи закритий ключ RSA в Таблиці 1 (Примітка: ім'я Боба великими літерами).

-

Таблиця 4 Цифровий підпис Боба

Цифровий підпис Боба
0x6c 0x99 0xd6 0xa8 0x42 0x53 0xee 0xb5 0x2d 0x7f 0x0b 0x27 0x17 0xf1 0x1b 0x62 0x92 0x7f 0x92 0x6d 0x42 0xbd 0xc6 0xd5 0x3e 0x5c 0xe9 0xb5 0xd2 0x96 0xad 0x22 0x5d 0x18 0x64 0xf3 0x89 0x52 0x08 0x62 0xe2 0xa2 0x91 0x47 0x94 0xe8 0x75 0xce 0x02 0xf8 0xe9 0xf8 0x49 0x72 0x20 0x12 0xe2 0xac 0x99 0x25 0x9a 0x27 0xe0 0x99 0x38 0x54 0x54 0x93 0x06 0x97 0x71 0x69 0xb1 0xb6 0x24 0xed 0x1c 0x89 0x62 0x3d 0xd2 0xdf 0xda 0x7a 0x0b 0xd3 0x36 0x37 0xa3 0xcb 0x32 0xbb 0x1d 0x5e 0x13 0xbc 0xca 0x78 0x3e 0xe6 0xfc 0x5a 0x81 0x66 0x4e 0xa0 0x66 0xce 0xb3 0x1b 0x93 0x32 0x2c 0x91 0x4c 0x58 0xbf 0xff 0xd8 0x97 0x2f 0xa8 0x57 0xd7 0x49 0x93 0xb1 0x62

Боб посилає Алісі електронний документ і цифровий підпис.

Step 4: Перевірте цифровий підпис.

a. Скопіюйте і вставте **відкриті** і **закриті** ключі з Таблиці 1 вище у поля **Public Modulus** і **Private Exponent** на сайті, як показано на рисунку вище.

b. Переконайтеся, що значення Public Exponent дорівнює 10001.

c. Вставте цифровий підпис Боба з Таблиці 4 в поле з написом на веб-сайті, як показано вище.

d. Тепер Аліса може перевірити цифровий підпис, натиснувши кнопку **Verify** знизу веб-сайту. Чий підпис ідентифіковано?

_____

Part 2: Створіть свій власний цифровий підпис

Тепер, коли ви бачите, як працюють цифрові підписи, ви можете створити свій власний цифровий підпис.

Step 1: Створіть нову пару RSA-ключів.

Перейдіть на інструмент веб-сайту і створіть новий набір відкритих і закритих ключів RSA.

a. Видаліть вміст полів з написами **Public Modulus**, **Private Modulus** і **Text**. Просто використовуйте мишу, щоб виділити текст і натисніть клавішу delete на клавіатурі.

b. Переконайтеся, що поле «Public Exponent» має значення **10001**.

c. Створіть новий набір ключів RSA, натиснувши кнопку **Generate** в правому нижньому кутку вебсайту.

d. Скопіюйте нові ключі в Таблицю 5.

Таблиця 5 - Нові ключі RSA

Відкритий ключ	
Закритий ключ	

e. Тепер введіть своє повне ім'я в поле з написом **Text** і натисніть **Sign**.

Таблиця 6 Персональний цифровий підпис

Персональний цифровий підпис	

Part 3: Обміняйтеся і перевірте цифрові підписи

Тепер ви можете використовувати цей цифровий підпис.

Step 1: Обміняйтеся вашими новими відкритими і закритими ключами в Таблиці 5 з вашим партнером по лабораторній роботі.

a. Запишіть відкриті і закриті ключі RSA свого партнера з його Таблиці 5.

b. Запишіть обидва ключа в таблиці нижче.

Таблиця 7 - Ключі RSA партнера по лабораторній роботі

Відкритий ключ	
Закритий ключ	

c. Тепер обміняйтеся цифровими підписами з Таблиці 6. Запишіть цифровий підпис в таблиці нижче.

Цифровий підпис партнера по лабораторній роботі	

Step 2: Перевірте цифровий підпис партнера по лабораторній роботі

a. Щоб підтвердити цифровий підпис свого партнера, вставте його або її відкриті і закриті ключі до відповідних полів, помічених **Public and Private modulus** на веб-сайті.

b. Тепер вставте цифровий підпис в поле з написом **Text**.

c. Тепер перевірте його або її цифровий підпис, натиснувши кнопку verify.

d. Що відображається в текстовому полі?

_____

Практичне заняття № 4

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СЕРВЕРНИХ КІМНАТАХ

Мета заняття: дослідження процесів фізичних аспектів захисту інформації та здобуття професійних компетенцій проектування серверної кімнати підприємства у відповідності до вимог міжнародних стандартів ANSI/EIA/TIA 568A, 569, 570, 606, 607

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Основні положення міжнародних стандартів ANSI/EIA/TIA 568A, 569, 570, 606, 607 щодо вимог до проектування серверної кімнати

Приміщення з обмеженим доступом – приміщення, у яких розташовані робочі місця з комп'ютерною технікою, обробляються електронні документи, та інша електронна інформація, доступ до якої обмежений;

Комутаційні кімнати – приміщення, у яких розташовано телекомунікаційне обладнання, що забезпечує функціонування локальних і корпоративних мереж організації, а також зв'язок з іншими установами та мережами загального користування, рис.13.1;

Рисунок 13.1 – Вигляд комунікаційної кімнати

Серверні приміщення – приміщення, у яких розташовані сервери баз даних, сервери прикладних програм, файлові сервери тощо, на яких обробляються та зберігаються електронні документи і бази даних, рис.13.2.

Рисунок 13.2 – Вигляд апаратної серверної кімнати

1.1. Розміщення в будівлі

Приміщення серверної не має бути прохідним. Бажано, щоб воно не мало вікон і не примикало впритул до зовнішніх стін будівлі. Якщо ж в технічному приміщенні передбачені вікна, то розташовувати апаратну рекомендується на північній або північно-східній стороні будівлі. Украй небажано розміщувати серверну поряд з тими внутрішніми конструкціями будівлі, які обмежують її можливе розширення в майбутньому: ліфтові шахти, сходові марші, вентиляційні камери і так далі.

Забороняється розташовувати серверну поряд з приміщеннями для зберігання пожежонебезпечних або агресивних хімічних матеріалів. Не рекомендується виділяти приміщення для серверної на верхніх поверхах будівлі, оскільки вони найбільш схильні до ушкоджень на випадок пожежі і можуть заливатися при протіканні даху. Не допускається розміщення серверної під приміщеннями, пов'язаними із споживанням води (туалети, душові, столові, буфети і так далі). При розміщенні серверної в підвалі, потрібні додаткова гідроізоляція і ретельний вибір трас прокладення трубопроводів. Через серверну не повинні прокладатися транзитом трубопроводи інженерних систем будівлі. Забороняється розташовувати серверну в приміщенні, суміжному з приміщенням виробництв з мокрими технологічними процесами.

Переважно розміщувати серверну недалеко від вантажних або вантажопасажирських ліфтів, використовуваних для транспортування важкого устаткування. У той же час, слід уникати близького розміщення потужних джерел електричних і магнітних полів, а також устаткування, яке може викликати підвищену вібрацію.

Багато джерел рекомендують розташовувати серверну в геометричному центрі будівлі хоч би тому, що це дозволяє істотно заощадити на прокладенні кабелю.

1.2. Приміщення серверної

Мінімальний допустимий розмір серверної – 14 квадратних метрів.

Розміри серверної повинні відповідати вимогам до устаткування, що розташовується в ній, або (за відсутності даних) складати 0,7 квадратних метра на кожні 10 квадратних метрів площі обслуговуваних робочих місць.

У будівлях з низькою щільністю робочих місць площа апаратної повинна складати не менше 37 $м^2$, але до 400 робочих місць, не менше 74 $м^2$ до 800 робочих місць і не менше 111 $м^2$ до 1200 робочих місць.

Мінімальна висота стелі апаратною повинна складати 2,44 м.

Підлога в серверній згідно вимог стандартів має бути рівною і мати антистатичне покриття з опором 106 Ом, забезпечуючи стікання і відведення статичної електрики. Настил підлоги повинен бути стійким до пожежі, дозволяти виконувати очистку пилососом і вологе прибирання.

Максимально допустиме навантаження на підлогу в серверній повинне складати: розподілене навантаження не більше 12 кПа; зосереджене навантаження не більше 4,4 кН.

Вхідні двері в апаратну повинні виготовлятися з стійкого до пожежі матеріалу, мати протизнімні засоби і відкриватися назовні з кутом 180 градусів. Двері повинні мати розмір не менше 2,0х0,9 метра, з ущільнювачем і закриватися на внутрішній замок. При необхідності монтажу великогабаритного устаткування встановлюються двостулкові двері. Поріг в дверному отворі не передбачається.

Серверна має бути забезпечена підсистемами:

- Охоронній сигналізації.
- Пожежній сигналізації.
- Пожежогасіння.
- Контролю доступу.
- Кондиціонування.
- Освітлення.
- Аварійного освітлення (для роботи при відключенні робочого освітлення).
- Захисного і телекомунікаційного заземлення, причому з серверної має бути забезпечена можливість підключення безпосередньо до головної пластини заземлення.

1.3. Основні вимоги до підсистем

Рівень освітленості в серверній має бути не менше 500 лк при вимірі на висоті 1 метр від рівня підлоги на вільному від устаткування просторі. Рекомендована мінімальна висота установки світильників 2,6 метри від рівня підлоги.

Рекомендується використовувати для освітлення серверної лампи розжарювання або галогенні лампи, оскільки люмінесцентні лампи випромінюють електромагнітні завади. При використанні люмінесцентних ламп рекомендується поміщати їх в екрануючу сітку, а між лампою і силовим щитком прокладати екранований кабель і встановлювати фільтр. Вимикач системи загального освітлення рекомендується розташовувати поряд з вхідними дверима на висоті 1,5 метра від рівня підлоги.

Система кондиціонування повинна забезпечувати підтримку температури в діапазоні від 18 до 24 градусів за Цельсієм при вимірах на висоті 1,5 метра від рівня підлоги. Відносна вологість повітря повинна підтримуватися в діапазоні від 30 до 55 відсотків при вимірах на висоті 1,5 метра від рівня підлоги. Швидкість зміни вологості повітря обмежується величиною 6% в годину. Конденсація вологи має бути виключена за будь-яких умов. Рекомендується розміщувати датчики на висоті 1,5 метра від рівня підлоги.

Система вентиляції повинна створювати в приміщенні серверної надлишковий тиск, а її продуктивність повинна забезпечувати мінімум одноразову повну зміну повітря в годину. Перевищення припливу над витягом по нормах складає 20%.

У серверній вимагається наявність не менше двох подвійних електричних розеток із заземленням, розрахованих на максимальний струм не менше 13А. Живлення цих розеток повинне здійснюватися від двох незалежних фідерів. Рекомендується встановлення подвійних електричних розеток по усьому периметру приміщення серверної. Мінімальна висота установки розеток 150 мм від рівня підлоги, а відстань між розетковими модулями не повинна перевищувати 1,8 метра. Забороняється застосування розеток з вимикачами. Живлення розеток для технологічного устаткування і системи освітлення апаратною повинно здійснюватися від різних панелей силового щита.

При використанні джерела безперебійного живлення (ДБЖ), рекомендується мати два незалежні підключення ДБЖ до міської електромережі.

Серверна має бути сполучена з головним електродом системи заземлення будівлі кондуїтом розміром 1+1/2" (38,1 мм). Безперервні сегменти кондуїту не повинні перевищувати по довжині 30 метрів або містити більше двох вигинів з кутом в 90° без застосування протяжних боксів відповідного розміру.

Згідно із стандартом ANSI/TIA/EIA - 607 головна шина заземлення має бути мідною шиною необхідної довжини з мінімальними розмірами 6 мм (товщина) х 100 мм (ширина) із заздалегідь просвердленими отворами, розміри і відстань між якими повинні відповідати вимогам до типів конвекторів, що використовуються. Бажано, щоб шина мала гальванічне покриття для зниження контактного опору. Шина має бути ізольована від своїх засобів підтримки/кріплення.

Рекомендується в серверній мати підйомну підлогу (настил) або підвісну систему підтримки кабелю під стелею (так звані сходи).

Рекомендується, принаймні, дві стіни серверної покрити панелями (фанера або ДСП) для настінного монтажу устаткування.

У серверній розміщують пересувні або переносні вуглекислотні вогнегасники з розрахунку не менше два на кожні 20 квадратних метрів площі.

1.4. Розміщення устаткування в серверній

Устаткування в робочому положенні повинне встановлюватися горизонтально, вертикально і співвісне. Відхилення не повинні перевищувати значень, вказаних в технічній документації і керівництві по монтажу компанії-виробника. Для вирівнювання устаткування і конструктивів, виконаних в підлоговому виконанні і не оснащених регульованими опорами, дозволяється застосовувати підкладки з листової сталі. Загальна товщина пакету підкладок не повинна перевищувати 5 мм, площу кожної підкладки не менше 40 квадратних сантиметрів.

При розміщенні устаткування в 19-дюймових шафах/стійках необхідно розміщувати 19-дюймові конструктиви так, щоб був доступ не лише до їх передньої, але і задньої частинам. Стандарт ANSI/NECA/BICSI 568-2001 визначає мінімальну вільну відстань перед передньою і задньою частинами шафи або стійки рівним 914 мм при мінімальній ширині бічного проходу 762 мм. Встановлювані в одному ряду шафи мають бути скріплені в єдину конструкцію з'єднанням болтами бічних сторін каркаса. Скріплення стійок здійснюється по верхній частині каркаса. Шафи і стійки згідно п. 3.3.2 ANSI/NECA/BICSI 568-2001 мають бути заземлені мідним провідником перерізом не менше 5 AWG (4,621 мм).

Не рекомендується розміщення в межах шафи/стійки розподільних пристроїв електроживлення, за винятком тих, які потрібні для роботи змонтованих в цій шафі/стійці телекомунікаційного і/або серверного устаткування.

При кріпленні устаткування серверної до вертикальних стін дюбелями або функціонально аналогічними ним елементами, навантаження на кожен верхній дюбель не повинне перевищувати для цегляних і бетонних/залізобетонних (марка 200) стін – 150 Н, а для бетонних/залізобетонних стін (марка 400) – 350 Н.

Обслуговуване настінне устаткування повинне розташовуватися так, щоб органи управління і індикатори знаходилися на висоті 1,6+/-0,1 метра від рівня підлоги. Максимальна висота розміщення настінного устаткування, що не обслуговує, не більше 2,4+/-0,1 метра від рівня підлоги. При цьому величина проміжку між верхньою поверхнею корпусу монтованого устаткування і стелею має бути не менше 150 мм. Вільний простір поряд з бічною поверхнею корпусу настінного устаткування повинен складати не менше 300 мм.

ЗАВДАННЯ ДО ВИКОНАННЯ:

1. Розробити план серверної кімнати міжнародних стандартів ANSI/EIA/TIA 568A, 569, 570, 606, 607. Розміри серверної визначити виходячи з площі робочих місць організації за варіантом (номер студента за списком).

№ варіанту	1	2	3	4	5	6	7	8	9
Площа робочих місць організації, $м^2$	150	100	125	140	180	200	250	260	270
№ варіанту	10	11	12	13	14	15	16	17	18
Площа робочих місць організації, $м^2$	110	120	130	160	220	300	290	280	240
№ варіанту	19	20	21	22	23	24	25	26	27
Площа робочих місць організації, $м^2$	310	320	340	350	360	370	380	390	400
№ варіанту	28	29	30	31	32	33	34	35	36
Площа робочих місць організації, $м^2$	155	165	175	185	195	205	215	225	230

Визначення площі серверної проводися з врахуванням вимог міжнародних стандартів і становить 0,7 $м^2$ на 10 $м^2$ площі робочих місць організації.

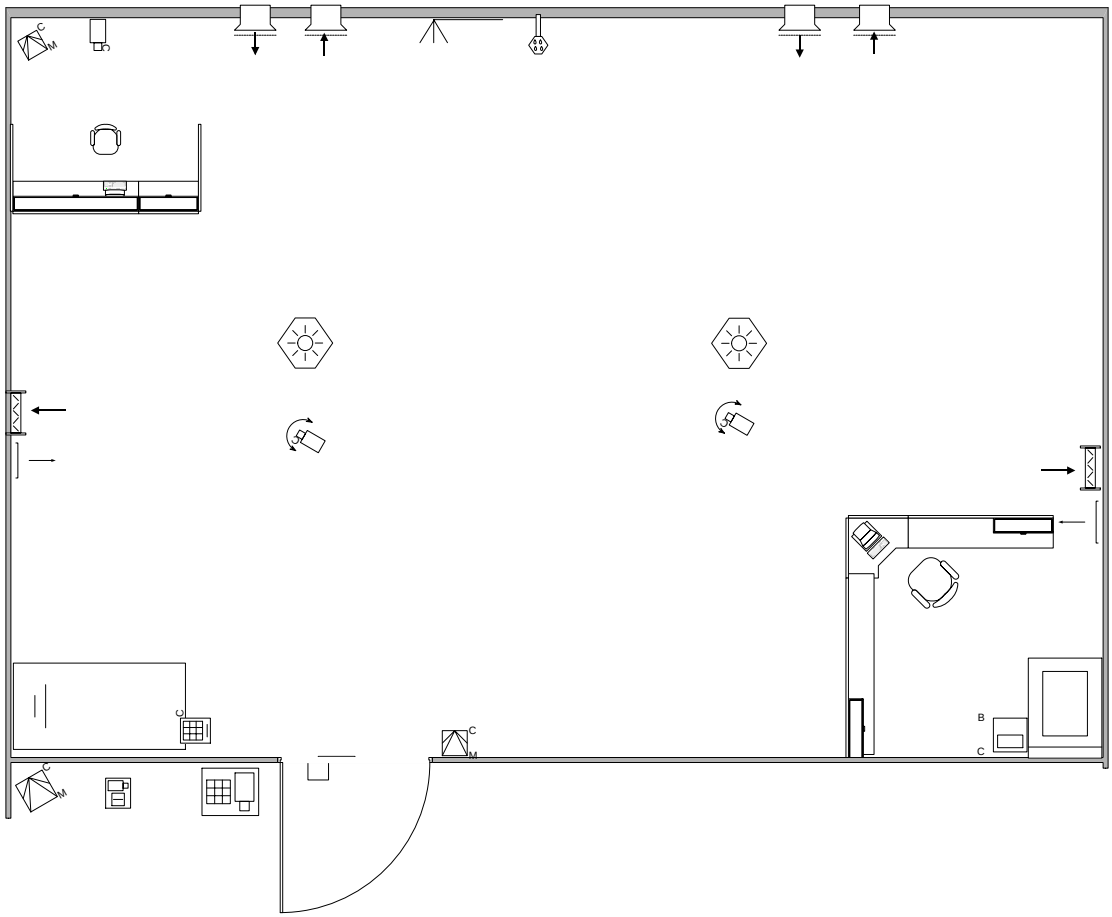
2. Визначити розміри та нанести на план приміщення дверні отвори та вікна, визначити та описати системи захисту даних отворів від несанкціонованого доступу (замки, відеокамери, грати, герконові датчики, датчики руху та інші засоби). Всі засоби нанести на план приміщення серверної кімнати.

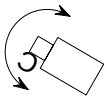
3. Вибрати та описати системи кондиціонування та вентиляції. Нанести на план розміщення даних пристроїв.

4. Вибрати систему автоматичного пожежогасіння та пожежні сповіщувач. Нанести на план приміщення розміщення даних датчиків та схеми комутації.

5. Вибрати освітлення приміщення серверної кімнати та нанести розміщення засобів на план.

Приклад виконання завдання:



 – відеокамера купольна;

 – детектор руху;

 – відеокамера звичайна;

– відеокамера із зчитувачем карт;

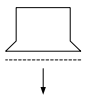
 – лампи (освітлення);

 - камера з клавіатурою;

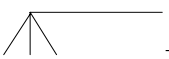
 – повітряний клапан для забору повітря в кондиціонер;

 - дорожній блокіратор ;

 вентиляційна решітка для видачі повітряного потоку з кондиціонера;

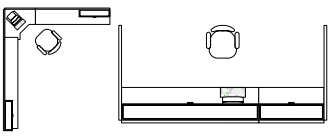
 – вентиляційна решітка;

 – зчитувач карт з клавіатурою;

 – зволожувач повітря;

 - датчик виміру вологості;

 – комбінаційна шафа;

 - робочі місця;

Вигляд пристроїв та засобів:

Екранована комунікаційна шафа

Джерело безперебійного живлення

Дизельна електростанція

Газова система автоматичного пожежогасіння

Сповіщувач пожежний комбінований тепло-димовий

Сповіщувач пожежний ручний

Прецизійний кондиціонер

Кодовий сенсорний замок

Відеокамера

Купольна поворотна відеокамера

Герконовий датчик

Датчик руху

ЗМІСТ ЗВІТУ

1. Тема та мета практичного заняття.
2. План приміщення серверної кімнати, побудований відповідно до варіанту з розміщенням всього необхідного обладнання, меблів, інженерних систем.
3. Вигляд обраних засобів та пристроїв з коротким анатованим описом кожного.
4. Висновок.

Практичне заняття №5

СКЛАДАННЯ ІМОВІРНІСНОГО ПРОГНОЗУ ТА МОДЕЛІ ПОРУШНИКА

Мета – отримання практичних навичок щодо визначення можливих шляхів несанкціонованого доступу до інформації та їх оцінки, складання ймовірнісного прогнозу моделі порушника.

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Оцінка можливостей порушника щодо подолання засобів захисту систем

Для проведення оцінки нам необхідно визначити компетентності порушника. В якості порушника розглядається суб'єкт, який має доступ до роботи зі штатними засобами інформаційно-телекомунікаційних систем (ІТС) і ПК як частини ІТС. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами ІТС, інформаційними систем (ІС). Класифікація є ієрархічною, тобто кожен наступний рівень включає в себе функціональні можливості попереднього.

Виділяється чотири рівні цих можливостей:

Перший рівень визначає найнижчий рівень можливостей ведення діалогу в ІТС (ІС) - запуск програмного забезпечення та задач з визначеного набору, що реалізують, заздалегідь передбачені функції по обробці інформації відповідно до посадових функцій.

Другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації, що передбачені політикою безпеки підприємства (організації).

Третій рівень визначається можливістю управління функціонуванням ІТС (ІС), тобто з можливістю впливу на базове програмне забезпечення системи, її на склад, конфігурацію та устаткування.

Четвертий рівень визначається всім обсягом можливостей осіб, які здійснюють проектування, реалізацію та ремонт технічних засобів ІТС (ІС), аж до включення до складу ІТС власних технічних засобів з новими функціями з обробки інформації.

Вважаємо, що у своєму рівні порушник є фахівцем вищої кваліфікації, знає все про ІТС і, зокрема, про систему і засоби її захисту.

Крім рівня знань порушника, його кваліфікації, підготовленості до реалізації своїх задумів, для формування найбільш повної моделі порушника необхідно визначити категорію осіб, до яких може належати порушник.

В загальному випадку порушників можна розділити на **внутрішніх та зовнішніх**. Отримуємо наступні відкриті класифікаційні угрупування:

$\mathbf{N} = \bigcup_{\gamma} N_{\gamma}$ – множина персоналу, який може бути задіяний у проведенні

або підготовці актів незаконного втручання в діяльність ІТС (ІС);

$\mathbf{Z} = \bigcup_j Z_j$ – множина потоку відвідувачів та контрагентів, який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність ІТС (ІС)

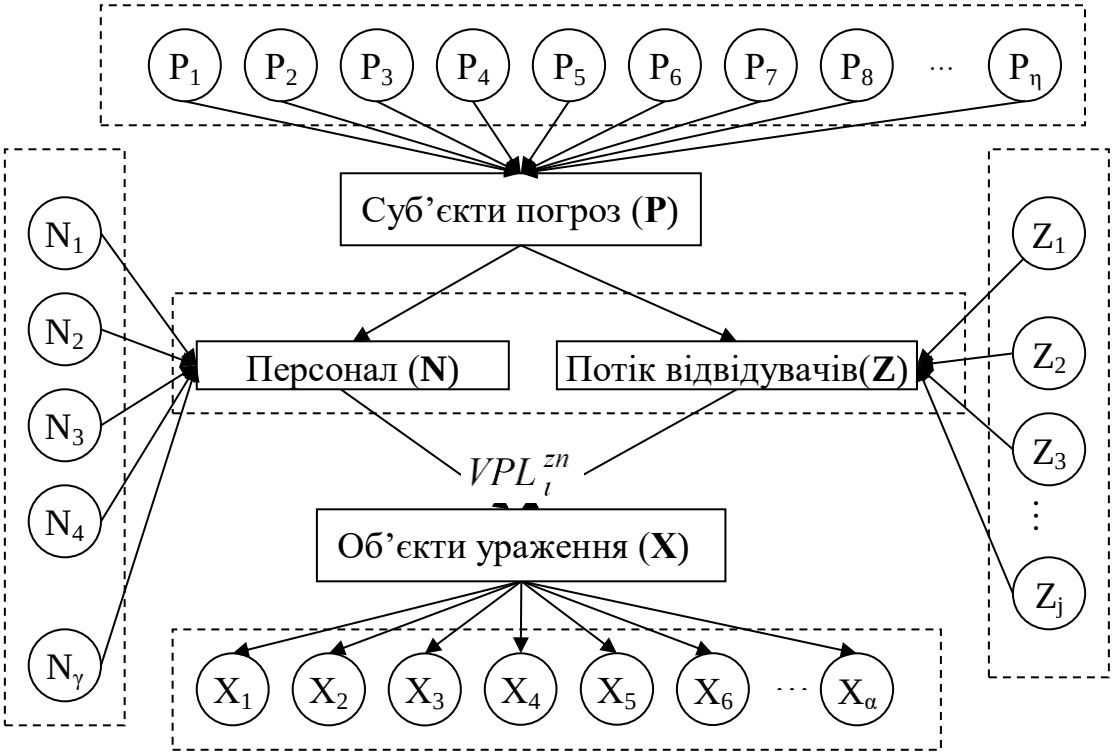


Рисунок 1. Модель прояву суб'єктів погроз виникнення НС на території аеропорту

Виходячи з рис. 1., маємо відкрите класифікаційне угрупування суб'єктів погроз, представлене у вигляді об'єднання множин потенційних учасників (реалізаторів) погроз виникнення загроз безпеки:

$$\mathbf{P} = \mathbf{N} \bigcup \mathbf{Z} = (N \setminus Z) \vee (Z \setminus N) \vee (Z \wedge N) \quad (1)$$

Таким чином, визначено джерела небезпеки у вигляді множини суб'єктів погроз (P), які можуть реалізувати свої погрози через потік відвідувачів (клієнтів, контрагентів) (Z) або (та) персонал (N), які, в свою чергу, можуть здійснити дії (впливи) на об'єкти ураження та спровокувати виникнення загрози кібервтручання. Неважливо, чи є у вашої системи зв'язок із зовнішнім світом, і чи є зовнішній захист, **але захист від внутрішніх порушників повинен бути обов'язково**.

Враховуючи той факт, що кожна організація має свою специфіку діяльності, не може існувати єдиної моделі порушника. Тому, при розробці

заходів безпеки необхідно розглядати всі можливі для даної організації категорії порушників, яких можна класифікувати наступним чином, таблиця 1:

Таблиця 1. Класифікація порушників

Зовнішні порушники	Внутрішні порушники
Конкуренти	Системні адміністратори
Клієнти, контрагенти	Співробітники IT-відділу
Відвідувачі	Користувачі (оператори) системи
Хакери	Керівний склад організації
Злочинні організації	Технічний персонал
Звільнені співробітники	Співробітники служб безпеки

При створенні моделі порушника й оцінці ризику втрат від дій персоналу необхідно диференціювати всіх співробітників по їх можливостям доступу до системи і, отже, по потенційному збитку від кожної категорії користувачів. Наприклад, оператор або програміст ІС може завдати незрівнянно більший збиток, ніж звичайний користувач, тим більше непрофесіонал.

Таким чином, кожен користувач у відповідності зі своєю категорією ризику може завдати більший або менший збиток системі. Крім того, необхідно враховувати, що користувачі різних категорій розрізняються не тільки за ступенем ризику, а й по тому, якого елементу системи вони загрожують найбільше. В результаті можна *оцінити ступінь ризику даної категорії користувачів щодо даного елемента системи* і представити результати аналізу у вигляді таблиці відповідностей.

Одним з варіантів градації ризику може бути наступний:

- Найбільший ризик - 5
- Підвищений ризик - 4
- Середній ризик - 3
- Обмежений ризик - 2
- Низький ризик - 1
- Немає загрози – 0

Нижче наводиться таблиця 1.2, в рядках якої перераховані що наведені вище категорії користувачів, а в стовпцях – найбільш вразливі елементи системи. Таблиця показує, який ступінь ризику даної категорії користувачів щодо даного елемента систем.

Таблиця 2. Ступінь ризику для різних категорій користувачів

	Елементи АС																	
	I			**II**			**III**			**IV**			**V**			**VI**		
Види збитків Категорії користувачів	**A**	B	C	**A**	B	C	**A**	B	C	**A**	B	C	**A**	B	C	**A**	B	C
Інженер системних магнітних носіїв											4	4		3	3		3	3
Користувач-операціоніст	2	2	2		1	1				2	2	2		1	1			
Оператор системи	1	5	5		5	5		5	5	1	3	3						
Оператор периферійного обладнання											3	3		4	4		1	1
Оператор завдань											3	3		4	4			
Оператор вводу та підготовки даних	3	3	3		4	4		5	5	3	3	3		4	4		1	5
Менеджер обробки	1	5	5		5	5		5	5	1	3	3		4	4		1	5
Адміністратор баз даних	3	3	3							3	3	3						
Системний програміст		5	5		5	5	5	5	5							5	1	5
Прикладний програміст	1	1	1	2	2	2							2	2	2			
Користувач- програміст	1	1	1	2	2	2							2	2	2			
Менеджер програмного забезпечення	1	1	1	4	4	4							4	4	4			
Інженер/оператор по зв’язку		5	5															
Інженер системи							2	2	2									
Адміністратор безпеки	5	5	5	5	5	5	5	5	5	3	3	3	4	4	4	5	5	5
Системний адміністратор	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Уразливі компоненти системи:

I - внутрішні дані

II - внутрішні прикладні програми

III - внутрішні системні модулі

IV - зовнішні дані

V - зовнішні системні модулі

VI - елементи комп'ютера та ін апаратура.

Види загроз:

A - модифікація,

B - знищення,

C - компрометація (розкриття) інформації.

Як видно з таблиці 2, різні категорії користувачів можуть по-різному впливати на різні частини ІТС. Ці тонкощі корисно враховувати як при проектуванні системи, так і при її експлуатації.

Далі кожну групу ймовірних порушників необхідно проаналізувати окремо за наступними параметрами:

- Дані необхідні порушнику і період їх актуальності;

- Технічна оснащеність і використовувані для вчинення порушення методи та засоби;

- Передбачувані місця і час здійснення незаконних дій порушника;

- Обмеження і припущення про характер можливих дій;

- Кількісна оцінка часу, який порушник може витратити для подолання захисту (рисунок 2).

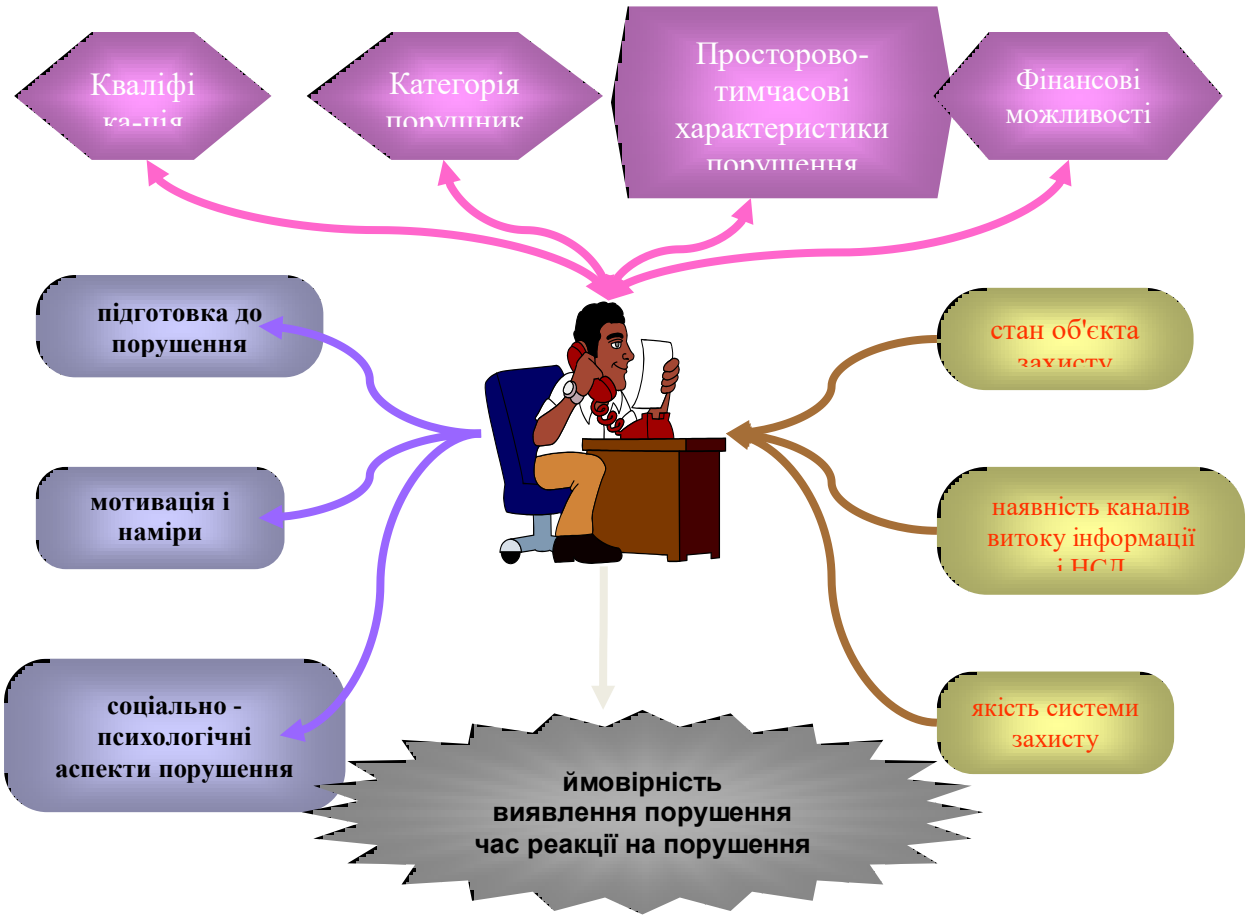


Рисунок 2. Схематична модель дій порушника

За технічної оснащеності та методами і засобами, що використовуються, порушники поділяються на тих, що:

- застосовують пасивні засоби (засоби перехоплення без модифікації компонентів системи);

- використовують тільки штатні засоби і недоліки систем захисту для її подолання (несанкціоновані дії з використанням дозволених засобів);

- застосовують методи і засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).

Наведена класифікація передбачає, перш за все, знання і постійне їх поповнення про характеристики технічних і програмних засобів ведення розвідки і забезпечення доступу до інформації.

Незаконні дії порушник може здійснювати:

- *В різний час* (в процесі функціонування ІС, під час роботи компонентів системи, під час планових перерв у роботі ІС, в неробочий час, в перерви для

обслуговування і ремонту і т.п.);

- *З різних місць* (за меж контрольованої зони ІС; всередині контрольованої зони ІС, але без доступу в виділені для розміщення компонентів ІС приміщення; всередині виділених приміщень, але без доступу до технічних засобів ІС; з доступом до технічних засобів ІС і з робочих місць кінцевих користувачів; з доступом в зону даних, архівів тощо; з доступом в зону управління засобами забезпечення безпеки ІС).

Облік місця і часу дій зловмисника також дозволить конкретизувати його можливості по доступу до інформаційних ресурсів і врахувати їх для підвищення якості системи захисту інформації.

Визначення значень можливих характеристик порушників в значній мірі суб'єктивно. Модель порушника, побудована з урахуванням особливостей конкретної предметної області та технології обробки інформації, може бути представлена перерахуванням декількох варіантів його вигляду.

Для того, щоб розроблена модель порушника приносила користь у вирішенні проблем інформаційної безпеки, а не була простою формальністю, вона повинна бути строго адаптована до конкретного об'єкта інформаційної захисту. Крім того, кожен блок моделі порушника повинен мати продовження як у вигляді причинно-наслідкових зв'язків між окремими блоками, так і у вигляді деталізації інформації, що міститься в кожному блоці. Така деталізація передбачає побудову ланцюжків передбачуваних наслідків настання тих чи інших висновків щодо вигляду порушника.

Наявність сукупності моделей дій порушника може бути корисною з точки зору прогнозування можливих подій у всьому розмаїтті ситуацій, що складаються, запобігання дій порушника, побудови надійної системи захисту інформації, використання сучасних засобів інтелектуальної підтримки для управління системою захисту.

Серед обмеження і припущення про характер дій можливих порушників можуть бути наступні:

- робота з підбору кадрів та спеціальні заходи ускладнюють можливість створення коаліцій порушників, тобто об’єднання (змови) і цілеспрямованих дій щодо подолання підсистеми захисту двох і більше порушників;

- порушник, плануючи спроби НСД, приховує свої несанкціоновані дії від інших співробітників;

- НСД може бути наслідком помилок користувачів, адміністраторів, що експлуатує та обслуговуючого персоналу, а також недоліків прийнятої технології обробки інформації і т.д.

Один зі спрощених варіантів табличного оформлення моделі порушника наведено Таблиці 3-10. Для побудови даної моделі використовується 4-х бальна шкала оцінювання

Таблиця 3. Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
	Внутрішні по відношенню до ІТС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІТС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Побудова причинно - наслідкових зв’язків між елементами моделі і ланцюжків передбачуваних наслідків вимагає знань в області соціально-психологічних аспектів діяльності порушника, в галузі техніки промислового шпигунства, можливостей засобів інформаційного захисту та цілого ряду інших, нерозривно пов'язаних з проблемою захисту інформації.

Таблиця 4. Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок (ПЗ4)	4

Таблиця 5. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 6. Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 7. Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 8. Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Далі виводимо два варіанти сумарного рівня загроз для окремих категорій можливих порушників:

1) внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов’язків;

2) зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

Зведемо все у таблицю 9.

Таблиця 9. Сумарна рівень загроз для окремих категорій порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
прибиральник	ПВ1	М1	К1	З1	Ч4	Д1	9
	1	1	1	1	4	1	
	ПЗ4	М4	К4	З4	Ч4	Д1	21
	4	4	4	4	4	1	
електрик	ПВ1	М1	К1	З1	Ч1	Д1	8
	1	1	1	1	3	1	
	ПЗ4	М4	К4	З4	Ч1	Д1	20
	4	4	4	4	3	1	
технік	ПВ2	М1	К2	З1	Ч4	Д3	12
	2	1	2	1	4	2	
	ПЗ4	М4	К4	З4	Ч4	Д3	22
	4	4	4	4	4	2	
юрист	ПВ3	М1	К2	З1	Ч3	Д2	11
	2	1	2	1	3	2	
	ПЗ4	М4	К4	З4	Ч3	Д2	21
	4	4	4	4	3	2	
адміністратор	ПВ4	М1	К4	З1	Ч4	Д4	17
	3	1	4	1	4	4	
	ПЗ4	М4	К4	З4	Ч4	Д4	24
	4	4	4	4	4	4	
працівник служби безпеки	ПВ5	М1	К1	З1	Ч4	Д3	14
	4	1	1	1	4	3	
	ПЗ4	М4	К4	З4	Ч4	Д3	23
	4	4	4	4	4	3	

Після зведення усіх даних 1-го варіанту в одну таблицю отримаємо таку табличну «Модель внутрішнього порушника політики безпеки інформації», таблиця 10.

Таблиця 10. Модель внутрішнього порушника політики безпеки інформації

Категорія порушника «ПВ»	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Служба безпеки	М1	К1	З1	Ч4	Д3	14
Адміністратор ІТС	М1	К4	З1	Ч4	Д4	17
Користувач	М1	К2	З1	Ч3	Д2	11
Технік ІТС	М1	К2	З1	Ч4	Д3	12
Електрик	М1	К1	З1	Ч1	Д1	8
Прибиральник	М1	К1	З1	Ч4	Д1	9

Аналіз останньої таблиці показує, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор ІТС. Тому організація роботи цієї особи повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

Таким чином представлено побудову моделі порушника та досліджено її особливості формування.

ЗАВДАННЯ НА ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Провести вибір об'єкту захисту та представити короткий опис діяльності.
3. Визначити організаційну структуру об'єкту дослідження та представити її у звіті.
4. Провести оцінку ступеня ризику для різних категорій користувачів відносно елементу системи відповідно до таблиці 2.
5. Побудувати модель порушника відповідно до наведених таблиць 3-10 для вибраного об'єкту дослідження.
6. Зробити висновки та оформити звіт.

КОНТРОЛЬНІ ПИТАННЯ

1. Назвіть основні типи та мотивацію порушень концепції безпеки підприємства.
2. Які категорії порушників Ви знаєте?
3. Назвіть типи конфліктів, які можуть виникати в організації?
4. Назвіть категорії порушників, які є потенційно небезпечними.
5. Назвіть основні заходи та методи захисту інформації від НСД.
6. Яким чином, на вашу думку, можна заохотити персонал до якісного виконання професійних обов'язків?
7. Якою є мотивація до роботи для Вас особисто?
8. Які наслідки можуть бути від розголошення інформації для організації?
9. Які наслідки розголошення інформації можуть бути для працівника?
10. Перерахуйте засоби та технології захисту інформації в кібернетичному просторі, які Ви знаєте?

Практичне заняття №7

ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ШИФРУ ПЕРЕСТАНОВКИ ТА ЗАМІНИ

Мета – отримання практичних навичок захисту інформації за допомогою шифру перестановки та заміни

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Шифрування текстової інформації із використанням криптографічного шифру заміни

Заміна (підстановка) – це метод шифрування, при якому кожен знак вихідного тексту взаємно однозначно заміняється шифропозначенням – одним, або декількома знаками деякого набору символів (алфавіту) [2]. Шифр однобуквеної простої заміни – один з найдавніших шифрів. Шифропозначення для нього застосовувались різні – від букв алфавіту до фігурок «танцюючих чоловічків». У найпростішому вигляді даний шифр полягає в тому, що буква переходить у букву, а вхідний і вихідний алфавіти збігаються як множини, тобто з точністю до перестановки. Для зашифрування чергової букви відкритого тексту визначається її номер у вхідному алфавіті і на відповідне місце формовного шифртексту поміщається буква з тим же номером, але вже з вихідного алфавіту.

Створення ключа

Вихідним алфавітом є малі літери українського алфавіту та дефіс:

а б в г ґ д е є ж з и і ї й к л м н о п р с т у ф х ц ч ш щ ь ю я -

Для побудови ключа скористаємось процедурою рандомізації, тобто перемішаємо вихідний алфавіт у випадковому порядку. Отримуємо такий ключ:

б л з а п у х с я н к е ґ і и ю ц ч є й г р ї в м ф щ ж о ш - т д ь

Шифрування

Маємо наступний текст, який необхідно зашифрувати (відкрите повідомлення):

є-люди-які-беруть-у-руки-ціпок-коли-в-них-кульгають-докази

Створюємо таблицю зашифрування: зіставляємо вихідний символ алфавіту відповідному символу ключа.

а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	-
б	л	з	а	п	у	х	с	я	н	к	е	ґ	і	и	ю	ц	ч	є	й	г	р	ї	в	м	ф	щ	ж	о	ш	-	т	д	ь

Використовуючи отриману таблицю зашифровуємо відкрите повідомлення. Перший символ тексту «є» відповідно до таблиці кодується символом «с». Аналогічно, другий символ «-» – «ь» і т. д. В результаті отримуємо наступне зашифроване повідомлення:

сьютукьдиеьлхгвї-ьвьгвикьщейєиьиєюкьзьчкфьивю-абтї-ьуєибнк

Дешифрування

Аналогічно таблиці зашифрування створюємо обернену таблицю розшифрування:

а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	-
г	а	у	р	ї	я	і	о	ч	в	к	й	т	п	и	б	ф	з	ш	ґ	с	є	ю	д	х	е	м	н	щ	ц	-	л	ж	ь

За допомогою цієї таблиці розшифровуємо попередньо отримане повідомлення: знаходимо відповідності зашифрованих символів до відкритих. Так перший символ «с» розшифровується як «є». Другий «ь» — «-». Після розшифрування усіх символів отримуємо:

є-люди-які-беруть-у-руки-ціпок-коли-в-них-кульгають-докази

Розшифроване повідомлення еквівалентне вихідному відкритому повідомленню. Це свідчить про правильність виконання процесів шифрування та дешифрування.

2. Провести шифрування текстової інформації із використанням криптографічного шифру перестановки

Теоретичні відомості

Шифри типу перестановки застосовувались ще у античні часи. Відмінність цього типу шифру від шифрів заміни полягає в тому, що під час зашифрування буква a_i відкритого тексту переходить не у фіксований знак алфавіту, а в іншу букву того ж відкритого тексту, скажемо a_j, у результаті чого букви розташовуються на нових місцях, тобто переставляються. Ключем для даного шифру також служить таблиця заміни, тільки не букв алфавіту, а їхніх індексів (номерів місць) у тексті, який підлягає зашифруванню. У загальному випадку розмір таблиці заміни дорівнює довжині відкритого тексту. Такі таблиці зручно формувати (і записувати) у вигляді так званих підстановок.

Для зашифрування шифром вертикальної перестановки будується прямокутна таблиця, кількість рядків якої визначається довжиною тексту, а кількість колонок дорівнює довжині ключа. Потім кожна буква ключового слова замінюється на число таким чином, щоб буква, яка має менший порядковий номер в алфавіті, замінялася на менше число. Отримані числа проставляються підряд на початку відповідних стовпців таблиці і надалі вважаються номерами цих стовпців. Відкритий текст вписується у таблицю, переходячи звичайним чином з рядка на рядок. Потім виписуються букви зі стовпців таблиці: спочатку весь стовпець, на початку якого стоїть одиниця, потім – стовпець, позначений двійкою і т. д. У підсумку, одержуємо шифротекст.

Створення ключа

Ключем для шифру перестановки буде слугувати гасло – слово «апогей». На основі гасла створюємо таблицю, яка буде використовуватись для шифрування (шкала рознесення). Кількість стовпців у таблиці дорівнює кількості літер у гаслі. Пронумеруємо кожен стовпчик таблиці таким чином, щоб менший порядковий номер літери гасла у алфавіті отримав менше число.

а	п	о	г	е	й
1	6	5	2	3	4

Шифрування

Дано наступний відкритий текст: «Не я належу минулому, а минуле належить мені».

Опускаємо неалфавітні символи тексту і вписуємо його до таблиці послідовно порядково:

а	п	о	г	е	й
1	6	5	2	3	4
н	е	я	н	а	л
е	ж	у	м	и	н
у	л	о	м	у	а
м	и	н	у	л	е
н	а	л	е	ж	и
т	ь	м	е	н	і

Виписуємо літери із стовпців таблиці: у порядку нумерації стовпців, зверху вниз. Отримуємо такий шифротекст (для зручності розбитий на групи по п’ять символів):

неумн тнмму ееаиу лжнлн аеиія уонлм ежлиа ь

Дешифрування

Для розшифрування шифротексту треба виконати обернену послідовність дій: у порядку номерів стовпчиків вписати до таблиці зверху вниз шифротекст і потім виписати послідовно порядково вихідний текст повідомлення.

3. Оцінювання стійкості паролів користувачів до зламу

Оцінимо стійкість U пароля до взлому.

1. Нехай L - довжина пароля.

Якщо довжина пароля $L \leq 4$, то U=0

інакше, якщо $5 \leq L \leq 7$, то U=6

інакше, якщо $8 \leq L \leq 15$, то U=12

інакше, якщо $16 \leq L$, то U=18

2. Якщо в паролі є букви, але тільки в одному (нижньому або верхньому регістрі), то U=U+5

інакше, якщо в паролі є букви і в нижньому і у верхньому регістрах, то U=U+7

3. Хай N - число цифр в паролі.

Якщо число цифр в паролі $1 \leq N \leq 2$, то U=U+5

інакше, якщо $3 \leq N$, то U=U+7

4. Хай S - число спецсимволів (#$%@) у паролі.

Якщо $1 \leq S < 2$, то U=U+5

інакше, якщо $2 \leq S$, то U=U+10.

5. Якщо в паролі є букви в обох регістрах, спецсимволи і цифри, то U=U+6 інакше, якщо тільки чогось одного з цього немає, U=U+4.

6. Оцінювання результатів.

Якщо U < 16 - пароль дуже слабкий

інакше, якщо 15 < U < 25 – слабкий

інакше, якщо 24< U < 35 – середній

інакше, якщо 34< U < 45 – сильний

інакше, якщо 44 < U – дуже сильний

ЗАВДАННЯ НА ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.

2. Провести шифрування текстової інформації із використанням криптографічного шифру заміни, використовуючи гасло-шифр та зсув на кількість літер у гаслі-шифру. У таблиці 1.1 представлено індивідуальні завдання на виконання. Варіант завдання вибирається відповідно до списку академічної групи.

Таблиця 3.1. Індивідуальні завдання із використанням криптографічного шифру заміни

№ варіанту	Гасло-шифр	Текст, який необхідно зашифрувати
1.	Захист	Вимоги безпеки до технологічного обладнання та процесів
2.	Підручник	Інтерфейс прикладного програмування системи
3.	Синема	Для створення шифрованого тексту на вихідний накладається гама.
4.	Зупинка	Атака, що має на меті змусити сервер не відповідати на запити
5.	Порушник	Безліч людей розмовляють в масштабі реального часу шляхом набору повідомлень на клавіатурі
6.	Гроза	Сьогодні є чимало каналів просочування інформації з організації
7.	Модель	У першій частині розглядаються загальні проблеми безпеки інформаційних систем
8.	Форма	У другій частині увага приділяється методам та засобам можливого вирішення цих проблем
9.	Техніка	Роль інформації в сучасному світі та необхідність її захисту
10.	Слова	Разом з поняттям інформація, важливе значення має поняття дані
11.	Ключ	Від інформації дані відділяються конкретною формою подань.
12.	Пароль	Інформація на стадії даних характеризується певною формою подання й додатковою характеристикою
13.	Футляр	Нематеріальність інформації полягає у тому, що не можна виміряти параметри відомими фізичними методами
14.	Вірус	Таким чином, інформація зберігається і передається на

№ варіанту	Гасло-шифр	Текст, який необхідно зашифрувати
		матеріальних носіях
15.	Клей	Все що є матеріальним об’єктом, інформацією бути не може
16.	Користувач	Інформація не може існувати сама по собі, у відриві від матеріального носія
17.	Логін	Матерія ж не може не нести інформації, оскільки завжди перебуває в певному стані
18.	Флешка	Матеріальними носіями інформації можуть бути мозок людини, звукові та електромагнітні хвилі
19.	Тенол	Інформація, якщо вона міститься на матеріальному носієві, доступна людині.
20.	Техніка	Цінність інформації визначається мірою її корисності для власника
21.	Захист	Якщо доступ до інформації обмежується, то така інформація є конфіденційною
22.	Крипто	Для позначення цінності конфіденційної комерційної інформації використовується категорія конфіденційно
23.	Граф	Інформацію правочинно розглядати як товар, що має певну цінність
24.	Модель	Кількість інформації тим більша, чим нижча ймовірність події
25.	Теорія	Підхід ентропії широко використовується при визначенні кількості інформації, переданої по каналах зв’язку
26.	Процес	Тезарусний підхід заснований на розумінні інформації як знань
27.	Директор	У результаті копіювання без зміни інформаційних параметрів носія кількість інформації не змінюється, а ціна зменшується
28.	Завуч	Проблеми захисту інформації непокоїли людство з давніх-давен.
29.	Равлик	Необхідність захисту інформації виникла через потребу таємного передавання інформації (повідомлень)
30.	Таємниця	Створення сучасних комп’ютерних систем і мереж радикально змінили характер і діапазон проблем захисту інформації.
31.	Краб	Античні спартанці шифрували свої військові повідомлення
32.	Шифр	Завдяки персональним комп’ютерам працювати з інформацією дуже просто
33.	Портал	Зловмисникам стало набагато простіше викрадати конфіденційну інформацію
34.	Ложка	Краще вчитися на чужих помилках. Нехай навіть безглуздих
35.	Монстер	Чим безглуздіша помилка, тим передбачливішими треба бути, щоб її передбачити.

3. Провести шифрування текстової інформації із використанням

криптографічного шифру перестановки. У таблиці 1.2 представлено індивідуальні завдання на виконання. Варіант завдання вибирається відповідно списку академічної групи.

Таблиця 3.2. Індивідуальні завдання до виконання завдання із використанням криптографічного шифру перестановки

№ варіанту	Ключове слово	Текст, який потрібно зашифрувати
1.	Файл	Існують різні методи боротьби із фішингом
2.	Засіб	Ніколи не відповідайте на листи, які запитують про вашу конфіденційну інформацію
3.	Фітинг	У разі одержання інформації з джерела, що викликає у вас недовіру, – перевірте його сайт
4.	Фішинг	Регулярно перевіряйте стан своїх електронних рахунків
5.	Рівень	Перевіряйте рівень захисту відвідуваного вами сайту
6.	Метод	Будьте обережними, працюючи з електронними листами й конфіденційними даними
7.	Захист	Забезпечте якісний захист свого комп’ютера
8.	Копія	Завжди повідомляйте по виявлену підозрілу активність
9.	Диск	Алгоритми симетричного шифрування використовують ключі не дуже великої довжини.
10.	Інтер	Алгоритми симетричного шифрування можуть швидко шифрувати великі обсяги даних.
11.	Буква	Ключ шифрування в асиметричних системах називається відкритим ключем
12.	Шифр	Ключ розшифрування потрібно тримати в секреті
13.	Рупор	На противагу тайнопису криптографією з ключем називають сьогодні алгоритми шифрування
14.	Колесо	У криптографічних системах ключ формує людина або він створюється автоматично
15.	Інформація	Усі крипто алгоритми з ключем поділяються на симетричні і асиметричні
16.	Мережа	У симетричних криптоалгоритмах використовуються ідентичні ключі
17.	Літера	Ключ несе у собі всю інформацію про засекречування повідомлення
18.	Коефіцієнт	Електростатичне і магнітостатичне екранування ґрунтується на замиканні екраном
19.	Україна	На високій частоті застосовується виключно електромагнітне екранування
20.	Небо	Двері і вікна приміщення серверної кімнати повинні бути екрановані
21.	Соловей	Усі системи захисту телефонних ліній поділяються на пасивні і активні
22.	Калина	Для контролю стану ліній зв’язку використовуються різні

№ варіанту	Ключове слово	Текст, який потрібно зашифрувати
		індикатори
23.	Сонце	Апаратура пригнічення радіовипромінюючих пристроїв прослуховування являє собою генератор шумових перешкод
24.	Козак	Робоче місце користувача автоматизованої системи має бути обладнане відповідно до рекомендацій
25.	Гетьман	Помилкові операції або дії можуть викликати відмови апаратних і програмних засобів.
26.	Мороз	Деякі помилкові дії можуть привести до порушень цілісності інформації
27.	Загрево	Для блокування помилкових дій використовуються технічні й апаратно-програмні засоби
28.	Цінність	Дублювання інформації є ефективним способом забезпечення цілісності інформації
29.	Конфіденційність	Найбільш простим методом дублювання інформації є використання виділених ділянок на робочому диску
30.	Руйнування	Найбільшого поширення комп'ютерні віруси зазнали з розвитком персональних комп'ютерів
31.	Наклеп	Особливістю пакетного вірусу є розміщення його голови в пакетному файлі
32.	Техніка	Копіювання вірусу в середину файлу може статися в результаті помилки вірусу
33.	Практика	До шкідливого програмного забезпечення відносять також віруси і хробаки
34.	Зошит	Найуразливішими з точки зору безпеки є критичні комп'ютерні системи
35.	Папір	Технічні засоби і системи можуть лише випромінювати в довкілля сигнали

4. Для двох зареєстрованих користувачів інформаційної системи обрахувати стійкість їх паролів. Зробити висновок для чого у великих інформаційних системах зберігають паролі користувачів у вигляді хеш функцій.

КОНТРОЛЬНІ ПИТАННЯ

1. Які недоліки мають розглянуті алгоритми?
2. Яким чином можна покращити стійкість криптографічних алгоритмів?
3. Які типи криптографічних алгоритмів Ви знаєте?
4. Дайте визначення поняттю «електронний цифровий підпис».
5. Дайте визначення поняттю «стеганографія».

Практичне заняття №9

Дослідження процесів проникнення та OSINT-розвідки

***Мета**: дослідження процесів проникнення в ІКС підприємства, дослідження інструментів здійснення OSINT-розвідки.*

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. **Тест на проникнення та рекомендації стосовно розробки і впровадження політики безпеки організації (установи)** (І. Вінклер, National computer security association). **Опис експерименту:**

Експеримент провели з дозволу компанії. Про його хід було проінформовано тільки керівництво вищого рівня. Першим кроком експерименту стало використання атакувальниками методів соціального інжинірингу (СІ), за допомогою яких без особливих труднощів і пояснень вони виконали відповідний пошук в мережі Інтернет та сформували для себе уявлення про досліджувану організацію. Вивчення баз даних організації дозволило встановити імена багатьох її співробітників та її керівництва. Пошук у телефонному довіднику дав телефонний номер офісу компанії, розташованого поблизу від атакувальників. Дзвінок в офіс дав змогу отримати копію щорічного звіту компанії, а також безплатний телефонний номер компанії. Об'єднавши дані щорічного звіту з даними, узятими з мережі Інтернет, атакувальники мали вже відомості про імена й посади багатьох осіб із керівництва разом з інформацією про проекти, над якими вони працюють. Наступним кроком було отримання телефонного довідника компанії. Це дозволило встановити імена ще низки співробітників і дістати повне уявлення про організаційну структуру компанії. За безплатним телефонним номером було здійснено дзвінок на основний номер компанії для контакту зі службою розсилання. Той, хто телефонував цього разу, представився як новий співробітник і намагався довідатися, яку інформацію потрібно вказати для пересилання поштою в межах США та за кордон. Отримана відповідь показала, що для цього достатньо лише знати, по-перше, особистий номер співробітника, а по-друге, номер торговельного центру. Дзвінок у відділ графіки підтвердив важливість цих двох чисел. Використовуючи телефонний довідник, атакувальники почали дзвонити десяткам службовців у різних відділах, аби отримати їхні особисті номери, які можна було б використати для подальших атак. Номери отримували в такий спосіб: той, хто телефонував, видавав себе за співробітника відділу кадрів, який помилково подзвонив не тому співробітникові, і при цьому запитував потрібний йому номер. Потім атакувальники вирішили спробувати дізнатися імена нових

співробітників, розраховуючи на їхню недостатню обізнаність із можливими загрозами для компанії. Таким чином, із використанням інформації, роздобутої на першому кроці атаки, зловмисники встановили імена кількох керівників компанії. Телефонний довідник допоміг з'ясувати ім'я тієї особи, яка швидше за все і є керівником. Що ж до встановлення імен нових службовців, то з цією метою було задіяно такий прийом: озвучування від імені керівника побажання особисто познайомитися з новими службовцями компанії. Для цього атакувальники планували спочатку заявити, що вони виконують доручення керівника, а потім, що керівник невдоволений через якість отриманої інформації. Утім суто технічне сприяння супроводжувало їхні дії: на дзвінок у відділ по роботі з новими співробітниками відповів автосекретар. Повідомлення дозволило атакувальникам установити таке: 1) відділ переїхав; 2) ім'я особи, за якою закріплено телефонний номер; 3) новий телефонний номер. Особливу цінність становила інформація про ім'я зазначеної особи, оскільки це дає змогу додзвонювачеві ставити максимально правдоподібні запитання. Зрештою атакувальники мали імена всіх співробітників, що почали працювати протягом поточного тижня, а також назви майже всіх відділів, де вони працюють. Проте, як з'ясувалося, атакувальникам варто уникати контакту зі співробітниками відділу ІС, які, безперечно, усвідомлюють важливість захисту паролів. Саме тому при дзвінках новим співробітникам зловмисники видавали себе за співробітників відділу ІС і проводили з ними короткий інструктаж з комп'ютерної безпеки. У ході цього інструктажу атакувальник отримав базову інформацію, зокрема про типи використовуваних комп'ютерних систем, наявні додатки, номер співробітника, ідентифікатор користувача й пароль.

2. Інструменти OSINT-розвідки

Вивчення OCIHT тулзів є частиною компетенцій аналітика: кожен новий OSINT інструмент збільшує можливості фахівця під час збору даних. Часом з'являються нові інструменти, що надають доступ до раніше закритої чи дуже фрагментарної інформації. Гарний аналітик хоче дізнатися про це одним з перших. Ще одна розповсюджена потреба – заміна старих інструментів на нові. Це роблять з метою оптимізації та покращення роботи, або просто через те, що попередні тулзи перестали працювати.

Усі чи майже всі створені інструменти використовують джерела OSINT, тобто більшість доступних тулзів є агрегаторами відкритої інформації. Проте деякі інструменти OSINT містять унікальні дані, наприклад, FlightRadar24 – інтерактивна мапа з трекінгом геолокації цивільних та деяких військових літаків в режимі реального часу. Або MarineTraffic – аналогічний сайт для трекінгу геолокації кораблів. Ці OSINT інструменти є виключеннями, оскільки вони відображають унікальні дані, фрагменти яких не знаходяться у вільному доступі. Подібні тулзи

створені та підтримуються спеціалізованими командами в рамках програм розвитку доступності даних, їх просто потрібно знати та використовувати.

OSINT інструменти – це сукупність ресурсів, додатків та програмного забезпечення, за допомогою яких аналітик може швидко отримати специфіковану інформацію з відкритих джерел. Всі інструменти OSINT поділяються на дві групи за ступенем розповсюдження: публічні та кастомні.

Публічні OSINT інструменти

Це сервіси, програми та додатки, що доступні всім без винятку користувачам інтернету. Наприклад, сервіс для пошуку людини за нікнеймом WhatsMyName.

Кастомні OSINT інструменти

Це специфічне програмне забезпечення, створене досвідченими аналітиками для власного користування. Кастомні тулзи використовують ті самі відкриті джерела, але зазвичай мають дуже спеціалізовану функцію. Наприклад: аналітики Molfar створили кастомний OSINT інструмент для пошуку інформації про людину за прізвищем серед вакансій та резюме на сайтах з пошуку роботи.

За статистикою, більшість людей мають дуже обмежені можливості у зборі та аналізі інформації з відкритих джерел.

Здебільшого OSINT інструменти використовують розвідники, які працюють з відкритими джерелами інформації. Проте більшість тулзів створені для широкого кола користувачів.

Розглянемо небажаний для використання сервіс Getcontact, який показує як підписані в інших людей номери з переліку ваших контактів. Сервіс створювався для задоволення цікавості простих людей, натомість знайшов широке використання під час дослідження персоналій у розвідці. Getcontact– чудовий приклад OSINT інструмента, який використовує широке коло людей.

Ще один приклад: OSINT інструмент Wayback Machine, створений для вивчення історичних змін вебсторінки. Ресурс не отримав масового поширення серед звичайних користувачів, натомість він активно використовується в розвідці для отримання інсайтів.

Сервіс не тільки дає вам можливість подивитись як підписані номери в контактах у інших людей, але й надає іншим людям доступ до інформації з вашої телефонної книги. Це досить сильна вразливість, на яку добровільно погоджуються користувачі додатка.

Застереження:

Інструменти OSINT можуть зашкодити тим, хто хоче їх використати. Щоб залишатися в безпеці, аналітики Molfar рекомендують використовувати сек’юрний девайс та сек’юрний акаунт.

Сек’юрний девайс

Смартфон, на якому не міститься жодної чутливої інформації. Чутлива інформація – це дані, виток яких може зашкодити вам чи пов’язаним із вами людям. Наприклад: паролі, адреси пошт чи фізичні адреси, персональні фотографії тощо. Деякі OSINT інструменти можуть не збирати чутливу інформацію з девайса безпосередньо, але через внутрішні вразливості бути в зоні потенційного втручання зловмисників.

Сек’юрний акаунт

Це адреса пошти, номер телефону та інші дані, які не розкривають справжньої інформації про вас та пов’язаних із вами людей. У разі отримання доступу до вашого сек’юрного акаунту, зловмисники не можуть встановити ваш вік, стать, ім’я та іншу правдиву інформацію.

Отже, які б інструменти OSINT ви не використовували, перш за все подбайте про власну безпеку. Інакше збір та аналіз інформації може зашкодити вашій приватності.

Завдання до виконання:

1. Проаналізувати наведену інформацію щодо експерименту. Дати оцінку.
2. Розробити комплекс заходів із розробки й упровадження політики безпеки, які дозволять захиститися від подібних втручань.
3. Провести реалізацію окремих аспектів запропонованого експерименту.
4. Провести OSINT-розвідку по власним даним (особистісними). Представити результати у вигляді скріншотів. Дати оцінку.
5. Провести OSINT-розвідку вибраної людини (одногрупника, працюємо в парі). Представити результати проведеної розвідки та дати оцінку.
6. На наступному занятті представити результати одногрупнику та провести сумісну оцінку отриманих даних. Розробити рекомендації щодо покращення захисту інформації.
7. Оформити звіт.

Додаткові матеріали та інструменти:

1. https://chatgpt.com/
2. https://gptgo.ai/uk
3. https://osvita.nakypilo.ua/osint-dlya-zhurnalistiv-iz-chogo-pochaty-ta-chym-korystuvatysya/?gad_source=1&gclid=Cj0KCQiAq-u9BhCjARIsANLj-s26AvfCcdnY0fQHdtf88RIb0ciDZGphs_Thr-EP0eUMcPcD8KOHa5waAmkcEALw_wcB
4. https://itedu.center/ua/blog/war/top-16-platnix-ta-bezplatnix-instrumentiv-dlya-osint/?srsltid=AfmBOopvGitAtaMD0s5-9MA2TDlwzmzJ7StON32XKwZYOP7gTcopH333
5. https://osintflow.com/instruments/
6. https://www.unite.ai/uk/best-open-source-intelligence-osint-tools/
7. https://hackyourmom.com/kibervijna/instrumenty-osint-dlya-analizu-zobrazhen-u-2024-roczi/
8. https://hackyourmom.com/category/kibervijna/zbir-informacziyi-pro-suprotyvnyka/osint-akademiya/