ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту технічних каналів об’єкту інформаційної діяльності від несанкціонованого витоку конфіденційної інформації»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Ілля ДОВБНЯ

Виконав: здобувач вищої освіти групи СЗДМ 61
Ілля ДОВБНЯ

Керівник: АВЕРІЧЕВ Ігорь
к.е.н., (ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім’я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти магістр
Спеціальність Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСК
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Довбні Іллі Владиславовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система захисту технічних каналів об'єкту інформаційної діяльності від несанкціонованого витоку конфіденційної інформації»
керівник кваліфікаційної роботи Ігорь АВЕРІЧЕВ к.е.н.,
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій
від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: опорний об'єкт інформаційної діяльності, мережевий канал витоку інформації, вимоги до захисту інформації з обмеженим доступом, сучасні засоби захисту інформації від витоку мережевими каналами, технічні засоби мережевого захисту та технічної системи охорони.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Аналіз основних мережевих загроз несанкціонованого витоку конфіденційних даних на об'єкті інформаційної діяльності;
4.2. Дослідження напрямків удосконалення технічної системи охорони об'єкта інформаційної діяльності від мережевого доступу до інформації з обмеженим доступом;
4.3. Розробка комплексної систему захисту інформації від мережевого доступу на об'єкті інформаційної діяльності.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах.

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Ілля ДОВБНЯ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Ігорь АВЕРІЧЕВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 74 сторінок, має 9 рисунків, 5 таблиць. Список використаних джерел містить 26 найменувань і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності захисту технічних каналів об’єкту інформаційної діяльності від несанкціонованого витоку конфіденційної інформації.

В кваліфікаційній роботі вирішено наступні завдання. Проведено огляд основних мережевих загроз несанкціонованого витоку конфіденційних даних на об’єкті інформаційної діяльності. Дослідження напрямки удосконалення технічної системи охорони об’єкта інформаційної діяльності від мережевого доступу до інформації з обмеженим доступом. Проведено розробку комплексну систему захисту інформації від мережевого доступу на об’єкті інформаційної діяльності. Проведено огляд питань забруднення літосфери в межах проблем охорони природнього середовища.

Апробація:

Ю.В. Жеребок, І.В. Довбня, О.І. Лихогод, Особливості функціонування та завдання системи захисту технічних каналів передачі інформації об’єктів банківської діяльності. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.32-33. https://duikt.edu.ua/uploads/p_2779_72486260.pdf.

Ключові слова: ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, КОМПЛЕКСНА СИСТЕМИ ЗАХИСТУ ІНОФРМАЦІЇ, МЕРЕЖЕВИЙ ЗАХИСТ ІНФОРМАЦІЇ. МЕРЕЖЕВІ ЗАГРОЗИ

ABSTRACT

The qualification work consists of an introduction, four sections, general conclusions, a list of sources used, the total volume of the work is 74 pages, has 9 figures, 5 tables. The list of sources used contains 26 items and takes up 3 pages.

The purpose of the qualification work is to increase the efficiency of the functioning of the technical system for protecting the object of information activity from network threats.

The following tasks are solved in the qualification work. A review of the main network threats of unauthorized leakage of confidential data at the object of information activity was conducted. Research on the direction of improving the technical system for protecting the object of information activity from network access to information with limited access was conducted. A comprehensive system for protecting information from network access at the object of information activity was developed. A review of the issues of lithosphere pollution within the framework of environmental protection problems was conducted.

Approbation:

Yu.V. Zherebok, I.V. Dovbnya, O.I. Lykhogod, Features of the functioning and tasks of the system for protecting technical channels of information transmission of banking objects. All-Ukrainian scientific and practical conference: Current problems of information and telecommunication systems security. Kyiv, November 5, 2025, Kyiv: DUIKT Research Center. – 2025. P.32-33. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: OBJECT OF INFORMATION ACTIVITY, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, NETWORK INFORMATION PROTECTION. NETWORK THREATS

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІзОД	–	Інформація з обмеженим доступом
ОІД	–	Об’єкт інформаційної діяльності
СТЗІ	–	Система технічного захисту інформації
ТКВІ	–	Технічний канал витоку інформації
ОТЗС	–	Основні технічні засоби і системи
ТЗПІ	–	Технічний засіб перетворення інформації
ДТЗС	–	Допоміжні технічні засоби системи
ПЕМВ	–	Побічні електромагнітні випромінювання
ТЗОС	–	Технічні засоби охоронної сигналізації
АС	–	Автоматизована система
КЗЗ	–	Комплекс засобів захисту
КСЗІ	–	Комплексна система захисту інформації
НСД		Несанкціонований доступ
ОС		Обчислювальна система
ДТЗС		Допоміжні технічні засоби та системи
ІТС		Інформаційно-телекомунікаційна система
КС		Комп’ютерна система
НД		Нормативний документ
НД ТЗІ		Нормативний документ системи технічного захисту інформації

ВСТУП

Одним із найвагоміших та найхарактерніших питань сьогодення є турбота про забезпечення безпеки функціонування державних установ, підприємств, національних систем та мереж, що стосуються життя населення, і всі вони вважаються об'єктами інформаційної діяльності. Тобто, об'єкти, що є неналежними або не виконують необхідних функцій, можуть суттєво впливати на якість життя населення цілих регіонів. Виходячи зі значного прогресу в науково-технічному розвитку, ускладнення економічних процесів та соціальних відносин, а також розвитку різних технологій, що базуються на цих принципах, можна зробити висновок, що одним із факторів, що впливає на якість функціонування, є різноманітність інформації. Частина цієї інформації підлягає різним обмеженням на передачу, зберігання та захист і вважається інформацією з обмеженим доступом (RAI). Запобігання ефективному функціонуванню технічної системи, призначеної для захисту об'єктів інформаційної діяльності, з метою запобігання витоку інформації через мережу, є серйозним завданням, яке потребує вирішення.

Метою кваліфікаційної роботи підвищення ефективності захисту технічних каналів об’єкту інформаційної діяльності від несанкціонованого витоку конфіденційної інформації.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

– здійснено аналіз основних мережевих загроз несанкціонованого витоку конфіденційних даних на об’єкті інформаційної діяльності;

– проведено дослідження напрямків удосконалення системи мережевого захисту об’єктів критичної інфраструктури від несанкціонованого доступу до інформації з обмеженим доступом;

– розроблена та подана комплексна системи захисту інформації від мережевого доступу на об’єкті інформаційної діяльності.

Об’єкт дослідження. Система охорони об’єкта інформаційної діяльності.

Предмет дослідження. Технічна системи охорони об’єкта інформаційної діяльності від мережевих загроз.

РОЗДІЛ 1.
АНАЛІЗ ОСНОВНИХ МЕРЕЖЕВИХ ЗАГРОЗ НЕСАНКЦІОНОВАНОГО ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2.1. Шкідливе програмне забезпечення, його функції та класифікація

Термін «шкідливе програмне забезпечення» використовується для опису програмного забезпечення, яке встановлюється на комп'ютер без дозволу та може порушувати протоколи безпеки, завдавати шкоди інформаційним ресурсам, а в деяких випадках негативно впливати на апаратні ресурси комп'ютера. Деякі програми також здатні виконувати шкідливу функцію, тому їх називають деструктивним програмним забезпеченням. Однак шкідливе програмне забезпечення, яке не має вбудованого деструктивного механізму, не може вважатися безпечним для комп'ютерної системи. По-перше, воно шкідливо використовує системні ресурси, а по-друге, порушує її політику безпеки. Однією зі спільних рис шкідливого програмного забезпечення є те, що воно призначене для порушення правил безпеки.[14] Змагальне програмне забезпечення класифікується за різними правилами. Наприклад, у монографії воно поділяється на два класи: ті, що служать деструктивним цілям, і ті, що не служать. Інші автори визначають термін «програмний баг» як окремий клас шкідливого програмного забезпечення. Термін «програмні баги» (рос. программные забрасы, англ. program bug) іноді застосовується до всього, крім комп'ютерних вірусів. Для нас різниця між вірусами та шкідливим програмним забезпеченням є незначною. Будь-яке шкідливе програмне забезпечення може або створювати програмну ваду, або ні. Помилка програми залишатиметься активною на комп'ютері протягом певного часу, перш ніж буде виявлена або почне виконувати інструкції алгоритму. З іншого боку, деяке програмне забезпечення, таке як троянські коні, може виконувати шкідливі дії, які мають

значний вплив (наприклад, форматування диска під час активації), не намагаючись видалити свої компоненти із системи.[10,14]

Чи виконуватиме шкідливе програмне забезпечення насильницькі функції, незрозуміло. По-перше, як уже згадувалося, вони порушують політику безпеки в будь-якому випадку. По-друге, навіть якщо творець шкідливого інструменту не попередив про його руйнівний характер, такий інструмент може призвести до значних збитків. Перші втрати спричинені необхідністю спрямувати зусилля висококваліфікованих (і високооплачуваних) спеціалістів на розпізнавання, ідентифікацію та видалення шкідливого програмного інструменту, а другі втрати спричинені відсутністю доступності систем. Яскравим прикладом є черв'як Морріса, який не мав жодних руйнівних здібностей, але лише за один день в Інтернеті (17 грудня 2007 року) він завдав збитків на суму приблизно 98 мільйонів доларів.[10,14]

В результаті ми вважаємо доречним класифікувати шкідливе програмне забезпечення за одним із двох основних типів:

Спосіб розповсюдження інструменту важливий з точки зору того, як інструмент потрапляє на комп'ютер і активується.

Мета роботи інструменту - які саме шкідливі дії він виконує.

Шкідливе програмне забезпечення вважається шкідливим для комп'ютера, коли виконується його код. Як результат, шкідливе програмне забезпечення використовує такий тип розповсюдження, який дозволяє йому працювати без допомоги користувача або виявлення.

Кілька шкідливих програмних застосунків відрізняються методами розповсюдження.[14]

♣ традиційні комп'ютерні віруси:

♣ розповсюдження вірусів;

♣ комп'ютерні віруси;

Макровіруси;

Скрипт-кідді.

Інтернет-черви;

Поштові черв'яки

Черви, що використовують Інтернет як основний засіб комунікації.

Черви та боти в мережах IRC.

Черви, призначені для зараження мереж обміну файлами (Peer-to-Peer Network, P2P).

♣ інші мережеві черви;

«Троянські коні»;

Спеціальні інструменти для злому.

Наведений вище опис походить з класифікації, запропонованої Лабораторією Касперського.[15]

Класичні комп'ютери заражені вірусами, які самовідтворюються, що означає, що після розмноження код вірусу доповнюється власною версією, а модифікований код потім використовується для зараження інших комп'ютерів. Таким чином, код програми, яку користувач запускає для виконання, замість цього виконується. Більше інформації про комп'ютерні віруси заплановано на наступний розділ.

Класичні мережеві черви поширюються самостійно, без допомоги користувача, по комп'ютерній мережі, виконуючи дві функції: передачу свого коду на інший комп'ютер та запуск свого коду на віддаленому комп'ютері. Для цього черви використовують вразливі системи в комп'ютерах. На відміну від традиційних вірусів, черви зазвичай не використовують коди інших програм як засіб передачі, оскільки вони не хочуть змушувати користувача робити це. В інших випадках черв'яків також називають програмами, які не можуть запускатися на віддаленій комп'ютерній системі, що робиться за допомогою концепції "троянського коня".[14]

Категорія "троянських коней" не має поділу за способом їх поширення. Вони класифікуються за діями, які вони виконують на зараженому комп'ютері (ця категоризація в основному відображає класифікацію цифрових книг). Для тих, хто знає метод зараження комп'ютера, термін "троянський кінь" безумовно асоціюється з ним. Ці програми, використовуючи різні методи соціальної

інженерії, спокушають довірливого користувача, який інтерпретує їх так, що результати відрізняються від очікуваних (у деяких випадках, Шкідливі функції приховані, тому користувач може навіть не усвідомлювати, що його комп'ютер вже скомпрометовано).[14]

Спеціальні інструменти включають надзвичайно небезпечні інструменти, які не мають механізму розповсюдження та призначені для регулярного використання. Ці інструменти використовуються зловмисниками, оскільки вони мають привілеї в системі, які не є авторизованими. Деякі з цих інструментів називаються експлойтами, що підкреслює той факт, що вони використовують (експлуатують) атрибут вразливої системи. Часто ці інструменти призначені не для самого комп'ютера, а для інших комп'ютерів у мережі. Іноді зловмисники використовують ці інструменти як засіб здійснення атак, а не безпосереднього виконання атак. Класифікація спеціальних інструментів буде відповідати функціям, які вони виконують.

Цей список був би неповним без іншого типу програмного забезпечення, використання якого може призвести як до порушення протоколів безпеки, так і до знищення програмного та/або апаратного забезпечення, пов'язаного з комп'ютерною системою. Це технологічні програми, що використовуються системними адміністраторами або персоналом технічної служби, які включають: засоби резервного копіювання та відновлення, форматування диска, дефрагментацію файлової системи, перепрограмування BIOS, перевірку та редагування реєстру Windows. Такі програми не вважаються шкідливими або деструктивними, тому ми не будемо їх обговорювати в цьому розділі. Однак, оскільки неправильне використання цих програм зловмисниками або просто некомпетентними користувачами може мати серйозні наслідки, під час розробки політики безпеки системи слід враховувати наявність цих програм і вживати відповідних заходів для запобігання їх неправильному використанню неавторизованими користувачами.[14]

1.2. Мережеві програмні застосунки несанкціонованого витоку інформації

Програмні закладки – це програми, які служать засобом тривалої роботи в комп'ютерній системі та вживають заходів для приховування своєї природи від користувача. Програмні закладки можуть бути запущені вірусами, троянськими кіньми, мережевими черв'яками або безпосередньо зловмисними користувачами. Іноді програмні закладки створюються адміністраторами з метою розпізнавання злочинної поведінки користувачів або для регулювання комп'ютерів користувачів. У цьому випадку програмна закладка не повинна вважатися шкідливою, незважаючи на її функціональну ідентичність шкідливій програмі. Це ще один приклад програмних інструментів в інформаційному середовищі, які часто вважаються зброєю, користь чи шкода якої залежить виключно від того, хто нею володіє (і хто оцінюватиме наслідки її використання).

Програмне забезпечення, що сприяє додаванню веб-сайтів до закладок.

Було створено кілька різних, але пов'язаних класифікацій програмного забезпечення, що сприяє додаванню закладок. Нижче наведено категоризацію, яка враховує нові можливості розробників "троянських коней".

Захоплення та передача інформації – це:

Крадіжка паролів;

Шпигунське програмне забезпечення.

Порушення принципів функціональності системи ("логічні бомби"):

Знищення знань;

Зміна інформації вважається зловмисною.

Блокування системи.

Зміна програмного забезпечення

Інструменти віддаленого адміністрування (люки);

Клікери з онлайн-рекламою;

Проксі-сервери;

Запити на витрачені кошти;

Організація DoS та DDoS-атак.

Психологічний тиск на користувача:

Зловмисні жарти та неправда.

З класифікації видно, що програмні закладки першої групи порушують конфіденційність, тоді як друга стосується цілісності або доступності інформації. Можливості програмних закладок з третьої групи типові для «троянських коней», вірусів та черв'яків. Цим закладкам бракує спостережуваності та керованості комп'ютерної системи. Зрештою, дії програмних закладок четвертої групи в першу чергу призначені для користувача системи. Поширені програмні закладки будуть розглянуті більш детально нижче.

Шпигунське програмне забезпечення

Програми, які прагнуть заразити комп'ютери певною інформацією, а потім передати її зловмиснику, розрізняються за типом інформації, яку вони шукають, способом та технологією її передачі.

Окремий тип програм призначений для збору та надсилання кодів доступу до локальної системи та комп'ютерних ресурсів, зокрема грошових програм, а також банківських та електронних платіжних систем.

Шпигунське програмне забезпечення – це ширший термін, який охоплює різні програмні додатки. Деякі з них спостерігають за діями користувача на зараженому комп'ютері, збираючи інформацію з клавіатури, копії екрана, інформацію про активні програми та їх використання користувачем. Інші люди шукають інформацію в досьє користувача, дотримуючись певних правил (наприклад, використовуючи ключові слова). Існує окремий тип шкідливого програмного забезпечення, який зосереджується на конфігурації апаратного та програмного забезпечення, пов'язаного з комп'ютером користувача, зокрема на серійних номерах ліцензованих програм.[15]

Зловмисник також може отримати доступ до інформації, зібраної таким чином, кількома способами: інформація зберігається на диску та іноді

надсилається зловмиснику або передається в режимі реального часу після її накопичення, використовуючи для цього повноцінні приховані канали, або просто надсилаючи анонімні повідомлення електронною поштою, ICQ. Окрім цього, існує кілька інших каналів.

Цей тип програмного забезпечення зазвичай містить віруси, а також «троянських коней», але зазвичай встановлює інші програми, типові для безкоштовних або умовно-безкоштовних програм. Розробник цих програм вважає це формою компенсації за привілей використовувати їх безкоштовно. Вони обіцяють, що не отримають жодної конфіденційної інформації та не намагатимуться отримати паролі. Основною проблемою є апаратне та програмне забезпечення комп'ютера, а також його конкретне місцезнаходження (країна, мова, часовий пояс). Це сприяє збору статистичної інформації про використання функціональності програми, яку потім можна використовувати для розробки нової версії. Фактично, мова продукту, необхідне обладнання та сумісність з іншим програмним забезпеченням сприяють якості продукту та його популярності серед користувачів.

Різні люди мають різні думки щодо компонентів шпигунського програмного забезпечення. Якщо користувач не знає про попередження, пов'язане з встановленням цього модуля, він не має можливості відмовитися від встановлення, програма вважає це «троянським конем». Якщо ж це вказує на попередження, виникає питання про важливість інформації, яка надсилається через цю програму. Зрештою, конфіденційність інформації вирішує її творець.

Microsoft неодноразово звинувачували у наявності шпигунських компонентів у системі. Звичайно, ці модулі легко додати до операційної системи, яка підтримує мережеві функції та включає поштовий клієнт, браузер, програми обміну повідомленнями та модулі для завантаження нових версій і патчів. Однак, компанія не змогла приписати Microsoft той факт, що ці продукти мають властивості програмних закладок, натомість збирала конфіденційну інформацію від користувачів. У найновіших версіях операційної

системи Microsoft Windows, якщо програмне забезпечення виходить з ладу, можна повідомити розробнику про помилку, що виникла, та конфігурацію програмного та апаратного забезпечення. Система зробить це за вас, а також дозволить переглянути згенерований звіт і відмовитися від його надсилання.

«Логічні бомби»

Клас «логічних бомб» включає програмні закладки, які за певних умов виконають одну з найпоширеніших руйнівних дій. Іноді розпізнається певний тип майнінгу – це приклад «логічних бомб», умовою запуску яких є наявність певного моменту часу. Наприклад, вірус під назвою SIN мав часову міну, яка спрацювала 26 квітня, що є датою Чорнобильської катастрофи (яка була більш відома в країні як «Чорнобиль»). Ця катастрофа отримала назву хвороби, тому в нашій країні вона більш відома як «Чорнобиль». Результат цієї ініціативи був руйнівним для комп’ютера: вона змінила Flash-BIOS, що призвело до повної неможливості функціонування комп’ютера. Як правило, для ремонту такого комп’ютера доводилося замінювати материнську плату.[14]

«Хетчбеки» – утиліти, що керуються дистанційно.

Програмні закладки цієї категорії призначені для використання у віддаленому адмініструванні комп’ютерів через Інтернет. Функціонально вони схожі на відомих виробників програмного забезпечення, які розробили та розповсюдили власні системи адміністрування. Інші спеціалізовані програми та компоненти операційної системи мають таку функціональність, наприклад, віддалений помічник у Windows XP Home Edition.[15]

Єдина відмінність між закладками шкідливого програмного забезпечення та подібними програмами полягає у відсутності попереджувальних повідомлень про їх встановлення або запуск. Користувач не знає про дії закладки програмного забезпечення в системі. Крім того, закладка програмного забезпечення може бути прихована та не відображатися у списку активних програм або процесів. І хоча користувач не знає про наявність цієї програми в системі, його комп'ютер тепер доступний для віддаленого керування.

Приховані утиліти, що керують ураженим комп'ютером, дозволяють робити все, що задумали автори, включаючи: отримання та надсилання файлів, їх запуск та видалення, відображення повідомлень, знищення та зміну інформації, зупинку або відновлення роботи комп'ютера тощо. Як наслідок, ці закладки можуть бути використані хакерами для розпізнавання та передачі секретної інформації, передачі вірусів, знищення даних та здійснення інших шкідливих дій.

Можна стверджувати, що програмні закладки такого типу є одними з найнебезпечніших, оскільки вони дозволяють здійснювати будь-які злочинні дії. Процедури, що використовують ці програмні закладки, також є одними з найшкідливіших. Також важливо розуміти, що «легальні» інструменти віддаленого адміністрування можуть становити загрозу, оскільки вони роблять комп'ютер вразливим до будь-яких зовнішніх дій. Єдиною перешкодою для їх використання є автентифікація вузла та користувача, від якого виходять команди керування. Однак ніхто не може гарантувати відсутність помилок, які дозволяють третім сторонам (зловмисникам) отримати доступ до системи без авторизації (відкритий доступ).

Окрім «агента», встановленого на віддалених комп’ютерах, дотепної назви та зручного графічного інтерфейсу, BackOrifice мав ефективний та результативний менеджер.

Після BackOrifice були створені інші програми, такі як NetBus, Phase, які мали значний вплив на перетворення Інтернету на небезпечне та агресивне середовище.

Сьогодні популярність закладок програмного забезпечення для віддаленого керування поширилася по всьому світу. Додавання цих закладок здійснюється спеціалізованими мережевими паразитами. В результаті їхніх дій генерується велика армія комп’ютерів, на яких використовується спеціальна утиліта віддаленого керування (термін «бот»). Ці мережі контролюються зловмисником централізовано, тому їх називають ботнетами (або мережами ботів). Управління здійснюється переважно через IRC-канал, призначений для

цієї мети, іноді використовується веб-сайт, який направляє команди на уражені комп’ютери, а в деяких випадках спеціальна мережа, організована як P2P. Перші мережі ботів були сформовані у 2002 році, після чого відбулося швидке зростання їх розвитку. Критичні вразливості в системах Windows значною мірою сприяли цьому: у 2003 році було виявлено вразливість у службі RPC DCOM Windows 2000/XP (яку використовував черв'як Lovesan), а у 2004 році... у службі LSASS (використовується черв'яком Sasser). Крім того, значний вплив мав поштовий черв'як Mydoom, виявлений у 2004 році. Згадані черв'яки впроваджували програми дистанційного керування або інші програми, які маніпулювали мережею, а деякі з них мали недоліки, які використовували наступні покоління черв'яків. Усі ці люки використовувалися зловмисниками для розміщення своїх ботів на машинах. Битва між різними групами зловмисників призвела до війни за зомбі-машини, яка буквально закінчилася; комп'ютери, які можна зламати, могли переходити з рук в руки кілька разів на день, як частина ботнету, так і окремо.[14]

1.3 Спеціальні програмні засоби та комп’ютерні віруси несанкціонованого доступу до інформації

Улюблені програми

Програмні закладки – це програми, які служать засобом тривалої роботи в комп'ютерній системі та вживають заходів для приховування своєї природи від користувача. Програмні закладки можуть бути запущені вірусами, троянськими кіньми, мережевими черв'яками або безпосередньо зловмисними користувачами. Іноді програмні закладки створюються адміністраторами з метою розпізнавання злочинної поведінки користувачів або для регулювання комп'ютерів користувачів. У цьому випадку програмна закладка не повинна вважатися шкідливою, незважаючи на її функціональну ідентичність шкідливій програмі. Це ще один приклад програмних інструментів в інформаційному середовищі, які часто вважаються зброєю, користь чи шкода якої залежить

виключно від того, хто нею володіє (і хто оцінюватиме наслідки її використання).

Програмне забезпечення, що сприяє додаванню веб-сайтів до закладок.

Було створено кілька різних, але пов'язаних класифікацій програмного забезпечення, що сприяє додаванню закладок. Нижче наведено категоризацію, яка враховує нові можливості розробників "троянських коней".

Захоплення та передача інформації – це

Крадіжка паролів;

Шпигунське програмне забезпечення.

Порушення принципів функціональності системи ("логічні бомби"):

Знищення знань;

Зміна інформації вважається зловмисною.

♣ блокування системи.

Зміна програмного забезпечення

Інструменти віддаленого адміністрування (люки);

Клікери з онлайн-рекламою;

Проксі-сервери;

Запити на витрачені кошти;

Організація DoS та DDoS-атак.

Психологічний тиск на користувача:

Маркетинг;

Зловмисні жарти та неправда.

З класифікації видно, що програмні закладки першої групи порушують конфіденційність, тоді як друга стосується цілісності або доступності інформації. Можливості програмних закладок з третьої групи типові для «троянських коней», вірусів та черв'яків. Цим закладкам бракує спостережуваності та керованості комп'ютерної системи. Зрештою, дії програмних закладок четвертої групи в першу чергу призначені для користувача системи. Поширені програмні закладки будуть розглянуті більш детально нижче.

Шпигунське програмне забезпечення

Програми, які прагнуть заразити комп'ютери певною інформацією, а потім передати її зловмиснику, розрізняються за типом інформації, яку вони шукають, способом та технологією її передачі.

Окремий тип програм призначений для збору та надсилання кодів доступу до локальної системи та комп'ютерних ресурсів, зокрема грошових програм, а також банківських та електронних платіжних систем.

Шпигунське програмне забезпечення – це ширший термін, який охоплює різні програмні додатки. Деякі з них спостерігають за діями користувача на зараженому комп'ютері, збираючи інформацію з клавіатури, копії екрана, інформацію про активні програми та їх використання користувачем. Інші люди шукають інформацію в досьє користувача, дотримуючись певних правил (наприклад, використовуючи ключові слова). Існує окремий тип шкідливого програмного забезпечення, який зосереджується на конфігурації апаратного та програмного забезпечення, пов'язаного з комп'ютером користувача, зокрема на серійних номерах ліцензованих програм.[15]

Зловмисник також може отримати доступ до інформації, зібраної таким чином, кількома способами: інформація зберігається на диску та іноді надсилається зловмиснику або передається в режимі реального часу після її накопичення, використовуючи для цього повноцінні приховані канали, або просто надсилаючи анонімні повідомлення електронною поштою, ICQ. Окрім цього, існує кілька інших каналів.

Цей тип програмного забезпечення зазвичай містить віруси, а також «троянських коней», але зазвичай встановлює інші програми, типові для безкоштовних або умовно-безкоштовних програм. Розробник цих програм вважає це формою компенсації за привілей використовувати їх безкоштовно. Вони обіцяють, що не отримають жодної конфіденційної інформації та не намагатимуться отримати паролі. Основною проблемою є апаратне та програмне забезпечення комп’ютера, а також його конкретне місцезнаходження (країна, мова, часовий пояс). Це сприяє збору статистичної інформації про

використання функціональності програми, яку потім можна використовувати для розробки нової версії. Фактично, мова продукту, необхідне обладнання та сумісність з іншим програмним забезпеченням сприяють якості продукту та його популярності серед користувачів.

Різні люди мають різні думки щодо компонентів шпигунського програмного забезпечення. Якщо користувач не знає про попередження, пов'язане з встановленням цього модуля, він не має можливості відмовитися від встановлення, програма вважає це «троянським конем». Якщо ж це вказує на попередження, виникає питання про важливість інформації, яка надсилається через цю програму. Зрештою, конфіденційність інформації вирішує її творець.

Microsoft неодноразово звинувачували у наявності шпигунських компонентів у системі. Звичайно, ці модулі легко додати до операційної системи, яка підтримує мережеві функції та включає поштовий клієнт, браузер, програми обміну повідомленнями та модулі для завантаження нових версій і патчів. Однак, компанія не змогла приписати Microsoft той факт, що ці продукти мають властивості програмних закладок, натомість збирала конфіденційну інформацію від користувачів. У найновіших версіях операційної системи Microsoft Windows, якщо програмне забезпечення виходить з ладу, можна повідомити розробнику про помилку, що виникла, та конфігурацію програмного та апаратного забезпечення. Система зробить це за вас, а також дозволить переглянути згенерований звіт і відмовитися від його надсилання.

«Логічні бомби»

Клас «логічних бомб» включає програмні закладки, які за певних умов виконають одну з найпоширеніших руйнівних дій. Іноді розпізнається певний тип майнінгу – це приклад «логічних бомб», умовою запуску яких є наявність певного моменту часу. Наприклад, вірус під назвою SIN мав часову міну, яка спрацювала 26 квітня, що є датою Чорнобильської катастрофи (яка була більш відома в країні як «Чорнобиль»). Ця катастрофа отримала назву хвороби, тому в нашій країні вона більш відома як «Чорнобиль». Результат цієї ініціативи був

руйнівним для комп’ютера: вона змінила Flash-BIOS, що призвело до повної неможливості функціонування комп’ютера. Як правило, для ремонту такого комп’ютера доводилося замінювати материнську плату.[14]

«Хетчбеки» – утиліти, що керуються дистанційно.

Програмні закладки цієї категорії призначені для використання у віддаленому адмініструванні комп’ютерів через Інтернет. Функціонально вони схожі на відомих виробників програмного забезпечення, які розробили та розповсюдили власні системи адміністрування. Інші спеціалізовані програми та компоненти операційної системи мають таку функціональність, наприклад, віддалений помічник у Windows XP Home Edition.[15]

Єдина відмінність між закладками шкідливого програмного забезпечення та подібними програмами полягає у відсутності попереджувальних повідомлень про їх встановлення або запуск. Користувач не знає про дії закладки програмного забезпечення в системі. Крім того, закладка програмного забезпечення може бути прихована та не відображатися у списку активних програм або процесів. І хоча користувач не знає про наявність цієї програми в системі, його комп'ютер тепер доступний для віддаленого керування.

Приховані утиліти, що керують ураженим комп'ютером, дозволяють робити все, що задумали автори, включаючи: отримання та надсилання файлів, їх запуск та видалення, відображення повідомлень, знищення та зміну інформації, зупинку або відновлення роботи комп'ютера тощо. Як наслідок, ці закладки можуть бути використані хакерами для розпізнавання та передачі секретної інформації, передачі вірусів, знищення даних та здійснення інших шкідливих дій.

Можна стверджувати, що програмні закладки такого типу є одними з найнебезпечніших, оскільки вони дозволяють здійснювати будь-які злочинні дії. Процедури, що використовують ці програмні закладки, також є одними з найшкідливіших. Також важливо розуміти, що «легальні» інструменти віддаленого адміністрування можуть становити загрозу, оскільки вони роблять комп'ютер вразливим до будь-яких зовнішніх дій. Єдиною перешкодою для їх

використання є автентифікація вузла та користувача, від якого виходять команди керування. Однак ніхто не може гарантувати відсутність помилок, які дозволяють третім сторонам (зловмисникам) отримати доступ до системи без авторизації (відкритий доступ).

Окрім «агента», встановленого на віддалених комп'ютерах, дотепної назви та зручного графічного інтерфейсу, BackOrifice мав ефективний та результативний менеджер.

Після BackOrifice були створені інші програми, такі як NetBus, Phase, які мали значний вплив на перетворення Інтернету на небезпечне та агресивне середовище.

Сьогодні популярність закладок програмного забезпечення для віддаленого керування поширилася по всьому світу. Додавання цих закладок здійснюється спеціалізованими мережевими паразитами. В результаті їхніх дій генерується велика армія комп'ютерів, на яких використовується спеціальна утиліта віддаленого керування (термін «бот»). Ці мережі контролюються зловмисником централізовано, тому їх називають ботнетами (або мережами ботів). Управління здійснюється переважно через IRC-канал, призначений для цієї мети, іноді використовується веб-сайт, який направляє команди на уражені комп'ютери, а в деяких випадках спеціальна мережа, організована як P2P. Перші мережі ботів були сформовані у 2002 році, після чого відбулося швидке зростання їх розвитку. Критичні вразливості в системах Windows значною мірою сприяли цьому: у 2003 році було виявлено вразливість у службі RPC DCOM Windows 2000/XP (яку використовував черв'як Lovesan), а у 2004 році... у службі LSASS (використовується черв'яком Sasser). Крім того, значний вплив мав поштовий черв'як Mydoom, виявлений у 2004 році. Згадані черв'яки впроваджували програми дистанційного керування або інші програми, які маніпулювали мережею, а деякі з них мали недоліки, які використовували наступні покоління черв'яків. Усі ці люки використовувалися зловмисниками для розміщення своїх ботів на машинах. Битва між різними групами зловмисників призвела до війни за зомбі-машини, яка буквально закінчилася;

комп'ютери, які можна зламати, могли переходити з рук в руки кілька разів на день, як частина ботнету, так і окремо.[14]

1.4 Висновки по розділу

У розділі розглядаються основні небезпеки несанкціонованого витоку даних у центрі інформаційної діяльності. Проаналізовано шкідливе програмне забезпечення, його можливості та класифікацію.

Обговорено програмні додатки, що використовуються для незаконного витоку інформації.

Досліджено властивості та обмеження спеціальних програмних засобів та комп'ютерних вірусів, які мають несанкціонований доступ до інформації.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ ТЕХНІЧНОЇ СИСТЕМИ ОХОРОНИ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД МЕРЕЖЕВОГО ДОСТУПУ ДО ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

2.1. Політика безпеки та модель мережевих загроз на об'єкті інформаційної діяльності

На етапі розробки політики безпеки розробник ЗБІ проводить комплексне дослідження об'єкта, призначеного для ЗБІ, дотримуючись моделі загроз, моделі потенційного злочину та результатів аналізу можливих небезпек. Результати розслідування базуються на розробці політики безпеки як для ІТС, так і для ІЗІ.

Додатково, на цьому етапі виконується наступне:

- вибір фундаментальних рішень для усунення всіх суттєвих небезпек, створення загальних вимог, правил, обмежень, рекомендацій тощо, пов'язаних з використанням безпечних технологій обробки інформації в транспортній системі, діями користувачів усіх класів та окремими заходами та методами захисту інформації, що розглядається у статті.

- документування політики безпеки щодо інформації.[13]

Політика безпеки повинна бути доповнена для всього захищеного ноутбука під час виробництва та покращена службою інформаційної безпеки під час його першого випуску на робочому місці.

Створенню політики безпеки передує огляд призначення інформаційного об'єкта.

Після обстеження всіх середовищ ІТС важливо визначити всі можливі небезпеки для ІТС. Причини небезпек можуть бути випадковими або запланованими.

Випадкове призначення спричинене випадковими та незалежними від бажання людини ситуаціями, що виникають під час функціонування ІТС. Найпоширенішими випадковими небезпеками є стихійні катастрофи, збої, несправності, помилки та їх побічні наслідки.

Суть цих небезпек (за винятком стихійних катастроф, суть яких невідома) описується наступним чином:

- відмова - порушення функціональності системи, яке призводить до неможливості виконання її основних обов'язків;

- збій - тимчасове відхилення від функції системи, причиною якого є неправильне виконання нею своїх обов'язків у цьому місці;

- помилка - неправильне виконання функцій системи в результаті її певного стану.

- побічний ефект - негативний вплив на систему, що спричинений будь-якими внутрішніми або зовнішніми подіями, що відбуваються в системі або її середовищі.

Навмисним джерелом шкоди є дії злочинців.

Умови, необхідні для виникнення небезпек, можуть бути об'єктивними або суб'єктивними. Суб'єктивні передумови можуть бути спричинені кількісним або якісним дефіцитом компонентів системи тощо. До суб'єктивних вимог належать: злочинна поведінка, низька якість роботи, виконаної її персоналом, та зовнішня розвідка.

Типи перелічених тут передумов розглядаються наступним чином:

- кількісний дефіцит - фізична відсутність одного або кількох компонентів системи, що погіршує технологічний процес обробки даних або перевантаження існуючих компонентів.

- якісний дефіцит - недоліки в конструкції (організації) компонентів системи, що можуть призвести до випадкового або запланованого негативного впливу на інформацію, що обробляється або зберігається.

Джерело небезпеки - це її первинний творець або вектор. Цим джерелом можуть бути окремі особи, технологічні процеси, моделі (алгоритми), а також програми, фактори навколишнього середовища, технічні засоби та моделі.

Тепер, спираючись на вищезазначену методологію категоризації ризиків інформаційної безпеки, можна спробувати визначити весь спектр можливих небезпек у сучасних транспортних інформаційних системах. При цьому необхідно враховувати не лише всі раніше невідомі загрози, але й потенційні нові загрози, що виникають внаслідок застосування нових концепцій архітектурного проектування та технологічної обробки інформації.

Усі можливі канали витоку інформації (КВИ) класифікуються за двома критеріями:

- наявність доступу до ІТС;

- стан функціонування системи.

Згідно з першим правилом, КВИ складається з трьох категорій:

- не потребують доступу, тобто інформацію можна отримати дистанційно (наприклад, спостерігаючи за інформаційною системою через вікна приміщення ІТС).

- потребують доступу до будівлі ІТС. Через ці канали може передаватися інформація, яка не залишає сліду на ІТС (наприклад, візуальне представлення зображень на моніторах або документів на папері). Крім того, може передаватися інформація, яка залишає певний слід (наприклад, крадіжка документів або машинних даних).

Друге правило стверджує, що КВИ можна класифікувати на:

- можливо існуючі незалежно від стану ІТС (наприклад, можливо взяти носії інформації незалежно від стану засобів повітряного сполучення);

- присутні лише в робочому стані ІТС (наприклад, бічне випромінювання та наведення).

Як наслідок цієї класифікації, ми виведемо 6 класів IPV, які приблизно схожі:

1-й клас – IPV, які демонструють свою поведінку незалежно від обробки інформації без доступу до компонентів ITS (підслуховування розмов, а також ініціювання розмов осіб, пов'язаних з ІТС, та використання зловмисником візуальних, оптичних та акустичних методів).

2-й клас – ІПВ, що проявляються в процесі обробки інформації без доступу до компонентів ІТС (електромагнітне випромінювання від різних пристроїв, обладнання та ліній зв'язку, паразитне наведення в ланцюгах живлення, телефонних мережах, системах теплопостачання, вентиляції тощо);

3-й клас – ІПВ, що демонструють поведінку, незалежну від обробки інформації, що здійснюється з доступом до компонентів ІТС, але не змінює останні (усі форми відтворення інформаційних активів, а також крадіжка виробничого сміття).

4-й клас – ІПВ, що проявляється в процесі обробки інформації з доступом до компонентів ІТС, але без зміни останніх (зберігання та відтворення інформації під час обробки, використання закладок програми тощо); 5-й клас – IPV, які демонструють відсутність занепокоєння щодо обробки інформації, незважаючи на доступ до компонентів ІТС та зміну останніх (крадіжка інформації у людей або нецільове використання обладнання, наприклад, віруси тощо, перетворені на комп'ютерне програмне забезпечення); та

- 6-й клас – CVI, які проявляються в процесі обробки інформації з доступом до компонентів ІТС та шляхом зміни останніх (незаконне підключення до обладнання та ліній зв'язку, а також видалення інформації з ліній електропередач різних компонентів ІТС).

На основі Звіту про перевірку та Моделі порушника політики безпеки, ДІІ розробляє «Модель загроз для інформації в ІТС», яка затверджується керівником організації (власником) ІТС та включається, за необхідності, до розділів Плану захисту та Технічного завдання на створення КСІІ. Модель загроз повинна включати формалізований або неформальний опис методів та засобів реалізації загроз інформації, яку необхідно захистити.

Модель загроз повинна виводити:

- перелік потенційних загроз, які класифікуються за впливом на інформацію, тобто за порушенням якої властивості вони спрямовані (конфіденційність, цілісність або доступність інформації).

- перелік потенційних підходів до реалізації загроз, пов'язаних з певним типом атаки (методів атаки) проти різних інформаційних об'єктів у різних станах, класифікується, наприклад, за компонентом комп'ютерної системи або програмного забезпечення ІТС, до вразливих областей якого отримує доступ зловмисник, причинами виникнення пов'язаної з цим вразливості тощо.

Загроза втрати інформації в ІТС базується на атрибутах ОС, апаратного забезпечення, програмного забезпечення, фізичного середовища, співробітників, технології обробки та інших компонентів, які можуть бути об'єктивними або суб'єктними.

Загрози особистого характеру класифікуються як випадкові або навмисні. Найпоширеніші типи небезпек для інформаційної безпеки, які можуть бути застосовані проти ІТС, слід визначити та включити до моделі загроз, це:

- зміни фізичного середовища (стихійні катастрофи та аварії, такі як землетруси, повені, пожежі або інші випадкові події);

- технічні або програмні помилки, що виникають під час роботи технічних або програмних засобів, пов'язаних з ІТС;

- наслідки помилок під час проектування або розробки компонентів ІТС (технічних засобів, технологій обробки інформації, програмного забезпечення, засобів захисту, структур даних тощо);

- помилки персоналу (користувачів) ІТС під час експлуатації.

- навмисні дії (спроби) потенційних злочинців.

Суб'єктивні загрози, що мають випадковий характер, є результатом недбалих, неефективних або помилкових дій персоналу, але без навмисного наміру.

До них належать:

- - дії, що призводять до виходу з ладу ІТС (окремо), знищення апаратного, програмного забезпечення, інформаційних ресурсів (пристроїв, каналів зв'язку, видалення даних тощо);

- Випадкове пошкодження сховища інформації;

- несанкціонована зміна принципів роботи ІТС (персональних компонентів, пристроїв, програмного забезпечення тощо), або процесу технологічного чи тестового виконання, що є незворотним (наприклад, форматування носіїв інформації).

- Ненавмисне зараження комп'ютерів вірусами;

- недотримання вимог щодо формального захисту нормативних документів ІТС;

- Помилки під час введення даних у систему, виведення даних на неправильні адреси пристроїв, внутрішніх та зовнішніх абонентів тощо;

- Будь-які дії, що можуть призвести до розголошення конфіденційної інформації, доступу до інформації з обмеженим доступом, втрати атрибутів тощо;

- Забороняється порушення політики безпеки та незаконне використання та впровадження програмного забезпечення.);

- наслідки неефективного використання засобів безпеки тощо.

Суб'єктивні загрози, що є навмисними, – це дії злочинця, спрямовані на проникнення в систему та отримання можливості доступу до її ресурсів або порушення роботи ІТС та запобігання її функціонуванню.

До них належать:

- порушення фізичної природи ІТС (особи, пристрої, обладнання, носії інформації);

- порушення режимів роботи (відмова) системи життєзабезпечення ІТС (живлення, заземлення, охоронна сигналізація, кондиціонування тощо);

- ігнорування принципів роботи ІТС (апаратного та програмного забезпечення).

- впровадження та впровадження комп'ютерних вірусів, вбудованих (апаратних та програмних) та підслуховуючих пристроїв, а також інших форм розвідки;

- шантаж, вимагання тощо з метою використання її ресурсів у особистих цілях.

- крадіжка носіїв інформації, виробничих відходів (роздруківок, записів тощо);

- несанкціоноване відтворення матеріалів, що містять інформацію;

- зчитування залишкових даних з оперативної пам'яті ЕОТ, зовнішніх накопичувачів; - отримання атрибутів, що дозволяють їм отримувати доступ до контенту та використовувати його для приховування своєї справжньої особи як зареєстрованого користувача.

Несанкціонований доступ до каналів зв'язку, перехоплення даних, аналіз трафіку тощо;

- Впровадження та нецільове використання програмного забезпечення заборонено політикою безпеки або заборонено несанкціоноване використання програмного забезпечення, яке має доступ до критичної інформації (наприклад, аналітики мережевої безпеки).

Інше.

Перелік серйозних небезпек має бути якомога більшим та складним. Для кожної з небезпек важливо визначити їхню спрямованість, походження, механізм реалізації та можливі наслідки.

По-перше, які аспекти інформації чи технології намагаються порушити зловмисники:

- секретність - несанкціонований доступ до інформації;

- цілісність - порушення заборони на зміну інформації (деформація, фальсифікація, перекручування);

- доступність - порушення можливості використання ІТС або обробленої інформації (відмова користувачеві в доступі);

- її спостережуваність - нездатність розпізнати, перевірити та задокументувати небезпечну поведінку.

По-друге, джерела небезпеки (які учасники ІТС або інші можуть спровокувати небезпеку):

- персонал та зацікавлені сторони;

- технічні ресурси;

- моделі, процедури, програми.

- Операційні технології.

- Зовнішнє середовище.

- По-третє, можливі методи боротьби із загрозами (механізм боротьби із загрозами):

- шляхом підключення до комп'ютерів та телефонів,

- видаючи себе за активного користувача,

- обхід заходів безпеки з метою використання інформації або поширення неправдивої інформації.

Ризики безпеки, пов'язані з вбудованими пристроями або програмами, є значними. Крім того, існують ризики впровадження шкідливого коду та вірусів.

- По-четверте, опис моделі загрози (щодо потенційних способів реалізації загроз та їх класифікації) має бути максимально детальним, щоб дозволити (на етапі вивчення ризиків, пов'язаних з реалізацією загроз) однозначно визначити як потенційні наслідки загрози, так і ймовірність її реалізації певним чином.

2.2. Зміст та порядок розробки комплексної системи мережевого захисту інформації на об’єкті інформаційної діяльності

Процес розробки комплексної системи безпеки інформаційних технологій на інформаційному об'єкті включає такі кроки:

Етап 1. Його дослідження та збір вхідної інформації для створення вимог до KSIZ. На цьому етапі зазвичай відбувається наступне:

− аналіз правових та нормативних актів, що регулюють доступ до певної інформації або забороняють доступ до такої інформації, визначається необхідність захисту інформації за іншими критеріями.

− Перераховується інформація, яка підлягає автоматизованій обробці, а її класифікація базується на ступені обмеження доступу до неї, необхідності збереження її цілісності та вимозі доступу до неї законними засобами.

При обстеженні ІТС розглядається як організаційно-технічна система, що поєднує комп'ютер, фізичне середовище, середовище користувача, інформацію, що обробляється в системі, та її технологію (яка називається операційним середовищем ІТС).

Метою опитування є опис специфіки операційного середовища кожної ІТС та визначення елементів у цих середовищах, які можуть прямо чи опосередковано впливати на інформаційну безпеку, елементів, спільних для різних середовищ, та документування результатів опитування для їх використання на наступних етапах проекту.

Етап 2. Створення політики безпеки. На цьому етапі виконується наступне:

− оцінка ризиків (вивчення моделі загрози та моделі злочину, потенційних наслідків потенційної загрози);

− визначення того, що необхідно для захисту інформації, які методи та засоби необхідні.

− вибір фундаментальних рішень для усунення всіх суттєвих небезпек, створення вимог, правил, обмежень та рекомендацій, що регулюють використання безпечних методів обробки інформації в транспортних системах, окремі дії та методи захисту інформації, а також регулюють діяльність користувачів усіх класів;

− документування політики безпеки щодо інформації.

Політика безпеки повинна враховувати індивідуальні особливості ЗБІ та може бути розроблена для всієї ІТС, для окремих компонентів компонента, для

функціонального завдання, для технології обробки інформації. Політика безпеки складається з окремого письмового документа, який називається Планом захисту.[11]

Етап 3. Розробка технічних специфікацій (далі – ТЗ), необхідних для створення ЗБІ. Технічні специфікації, що стосуються створення ЗБІ в ІТС, – це початкова письмова робота, яка описує вимоги до захисту інформації, що обробляється в ІТС, процес створення ЗБІ, процес проведення всіх типів тестів ЗБІ в рамках ІТС та процедуру введення інформації у використання в рамках ІТС.

Технічні специфікації на створення ЗБІ розроблені з урахуванням цілісного підходу до створення ЗБІ, який передбачає поєднання всієї необхідної інформації та методів захисту ЗБІ від різних ризиків інформаційної безпеки на всіх етапах життєвого циклу ІТС. ТЗ для КСЗІ може бути впроваджено як на нових ІТС, так і під час модернізації існуючих ІТС.

ТЗ для КСЗЗ дійсні:

− як окрема частина більшого технічного проекту, який відповідає за створення ІТС.

як окреме (часткове) ТЗ.

Як доповнення до загального процесу ТЗ для створення ІТП.

Для інтегрованих ІТС (які включають кілька окремих інформаційних або комунікаційних систем, що можуть як функціонувати автономно, так і взаємодіяти одна з одною) рекомендується створити окреме ТЗ для кожної зі складових частин ІТС та формалізувати вимоги як окреме ТЗ. Можливо створити одне ТЗ для кількох ідентичних частин ІТС, це продемонструє розбіжності або особливості кожного компонента.[11]

Етап 4. Створення та реалізація проекту ТЗ в ІТС.

Проект KSIZ ініціюється на основі Технічного технічного завдання на створення ІТС, після чого йдуть етапи попереднього проектування, технічного проектування та робочої документації створення ІТС.

Під час розробки проекту KSIZ обґрунтовуються та впроваджуються проектні рішення, що дозволяють усім компонентам KSIZ взаємодіяти один з одним та мати сумісне середовище, а також мати доступ до інформації.

Спільно приймаються рішення, які не є необхідними для виконання вимог ТЗ щодо КСІЗ, щодо організаційної структури КСІЗ, структури технічних та програмних засобів, принципів функціонування та умов використання засобів захисту, а також реалізації послуг інформаційної безпеки, визначених функціональним профілем безпеки.

Етап 5. Функціонування КСІЗ.

На цьому етапі розробка КСІЗ мала бути завершена, а документи Плану захисту мали бути санкціоновані.

Його користувачі всіх рівнів (персонал технічної служби, звичайні люди) навчаються фундаментальним принципам та процедурам документів Плану захисту, які необхідні для дотримання ними правил політики інформаційної безпеки, експлуатації засобів інформаційної безпеки.

Побудований комплекс технічного захисту інформації щодо витоку через технічні засоби визнано легітимним, результати якого свідчать про видачу документа: «Свідоцтво про визнання комплексу технічного захисту інформації».

Встановлення, початкове налаштування та перевірка функціональності комплексу засобів захисту інформації від НРЗ проводиться згідно з документованим робочим проектом. Під час встановлення мають бути враховані всі методи сегментації доступу до інформаційних та апаратних ресурсів, пов'язаних з ІТС, а також методи контролю цілісності програмного забезпечення та захисту бази даних.

До бази даних захисту вноситься інформація про користувачів ІТС, визначаються їх права доступу до захищених ресурсів ІТС, їх створення, зміна, зберігання, експорт/імпорт із системи.

Етап 6. Початкові випробування.

Метою початкових випробувань є оцінка ефективності КСЗІ, її відповідності технічним характеристикам та визначення придатності КСЗІ для регулярної експлуатації. Попередні випробування проводяться згідно з протоколом та методами тестування. Вони структуруються замовником ІТС та проводяться розробником КСЗІ спільно із замовником.

Етап 7. Практична експлуатація. Під час тестування КСЗІ:

− Розробляються технології захисту оброблюваної інформації, передачі машинної інформації, обмеження доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів.

− Співробітники інформаційної системи та її користувачі отримують практичні знання щодо використання технічних та інформаційних засобів, а також опановують вимоги формальних документів щодо режиму доступу.

Процедура включає: програмування, тестування та налаштування КПП з НСД.

− Переглядається документація, що використовується для робочих та експлуатаційних цілей.

Експлуатація ІТС повинна здійснюватися без використання інформації, що вважається державною таємницею. У разі використання комплексу методів захисту інформації від НСЗ у складі КСІЗ, щодо якого відсутнє експертне рішення щодо відповідності цього комплексу вимогам НД ТЗІ, необхідно здійснити комплекс заходів щодо підготовки до оцінки відповідності цього комплексу вимогам НД ТЗІ під час оцінки стану КСІЗ.

Етап 8. Державна експертиза КСІЗ. Комплексна система захисту інформації, що є власністю держави, або інформація, до якої є обмежений доступ, чи інша інформація, що охороняється державою, повинна мати сертифікат відповідності вимогам інформаційної безпеки, який видається Державною службою безпеки та захисту інформації України на основі результатів оцінки стану сучасних технологій. Державна експертиза КСІЗ проводиться з метою визначення відповідності КСІЗ технічному завданню,

вимогам правових норм щодо захисту інформації, а також можливості активації КСІЗ у складі ІТС. Знання стану є складовою приймальних випробувань KSIZ та проводиться відповідно до нормативних актів щодо державної експертизи у сфері технічного захисту інформації. Якщо ІТС обробляє інформацію, що є державною власністю, або інформацію, що охороняється державою, то керівник організації може наказати експлуатацію ІТС за наявності сертифікації відповідності KSIZ.[12]

Етап 9. Підтримка KSIZ. На цьому етапі докладаються зусилля для підвищення ефективності організації щодо запланованої модернізації KSIZ та управління методами захисту інформації відповідно до Плану захисту та експлуатаційної документації для компонентів KSIZ.[10]

Етапи створення комплексної системи захисту інформації для мереж.

Формування комплексу TZI складається з трьох етапів.

- створення комплексу TZI (етап I);
- впровадження комплексу TZI (етап II);
- сертифікація комплексу TZI (етап III).

Зміст та порядок етапів створення комплексу TZI диктуються правилами системи TZI.[10]

Вимоги до захисту інформації від технічних каналів витоку та стандарти інформаційної безпеки регулюються як статутами, так і нормативними актами системи TZI.

Виходячи з вищезазначеного опису процедури створення KSIZ, можна зробити висновок, що процес створення KSIZ є подібним для кожного об'єкта інформаційна діяльність. Незважаючи на схожість, кожен об'єкт повинен створювати власну модель та окремий повний перелік документів. Весь процес є повільним, що погіршує можливості компанії працювати. Для бізнесу час – це гроші. Крім того, під час побудови KSIZ зазвичай використовуються активні методи захисту, які можуть негативно впливати на організм людини. Зокрема, на цьому етапі можна визнати такі проблеми під час побудови KSIZ:

Давно настав час створювати та розгортати KSIZ.

Використання шкідливих методів захисту, які є активними.

- Дефіцит інформації щодо SID.

- Низький рівень знань співробітників щодо обробки SID.

Я вважаю важливим вирішити вищезазначені проблеми та спростити процес побудови SIS, зокрема зосередитися на розробці системи побудови ACS та розробці політик інформаційної безпеки. Крім того, я вважаю важливим підвищити обізнаність та сприяти особистій відповідальності щодо захисту інформації про співробітників.

2.3 Вимоги до програмного захисту інформації

Програмний компонент повинен забезпечувати інформаційну безпеку відповідно до методу STRIDE. Крім того, програмне забезпечення повинно включати інструменти для обробки цифрового контенту (MS Office, Adobe Reader).

Метод класифікації загроз, що використовується STRIDE.

Метод STRIDE був розроблений, продемонстрований та активно просувається експертами корпорації Microsoft. Фактично, це ще один метод категоризації небезпек за їх наслідками. Методологія використовується для створення моделі загроз під час розробки програмного забезпечення. Назва методу походить від перших літер назв потенційних класів загроз.

• Обманні об'єкти [підроблена особистість]. Окрім вищезгаданих небезпек, що виникають через збої протоколу в мережі, цей клас також включає загрозу, спричинену зміною особи користувача. Це досягається шляхом використання слабких місць системи автентифікації або отримання інформації для автентифікації шляхом крадіжки чи шахрайства (так звана соціальна інженерія).

• Деструктивна обробка даних. Цей клас охоплює небезпеки, які навмисно впливають на дані (наприклад, атаки можуть бути зосереджені на інформаційних об'єктах, що зберігаються на диску (файли, бази даних), а також на тих, що передаються через Інтернет).

Відмова від оригіналу. Ці загрози дозволяють зловмиснику заперечувати дії або бездіяльність, які він здійснив. Причиною цієї небезпеки є відсутність методів реєстрації подій або автентифікації відповідно.

Обмін інформацією. Ці небезпеки не потребують пояснень.

Відмова в обслуговуванні. Ми раніше обговорювали небезпеки цього типу. Атаки, що призводять до відмови в обслуговуванні, зазвичай прості у виконанні в розподілених системах і надзвичайно складні для захисту. Розподілені атаки відмови в обслуговуванні особливо шкідливі, ці атаки відбуваються на одному об'єкті серед кількох мережевих компонентів одночасно.

Збільшення привілеїв. Цей клас включає небезпеки, які дозволяють зловмиснику збільшити свої привілеї в системі. Наприклад, типовий користувач отримує адміністративні привілеї, або зловмисник, який підключається до мережевої служби без перевірки, виконує дії як авторизований користувач.[18]

2.4. Висновки по розділу

У розділі містяться результати досліджень щодо вжитих заходів щодо захисту інформації та нових методів удосконалення технічної системи захисту інформації від несанкціонованого доступу.

Під час інформаційного заходу було розроблено політику безпеки та представлено модель загрози.

Розкрито процес та зміст розробки комплексної системи захисту інформації для об'єктів інформаційної діяльності.

Обговорюються вимоги до програмного забезпечення, призначеного для захисту інформації під час її передачі.

РОЗДІЛ 3
КОМПЛЕКСНА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1 Нормативно-правове забезпечення створення комплексної системи захисту інформації на об'єкті інформаційної діяльності

Створення КСЗІ проводиться відповідно до НД ТЗІ 3.7-003-05 «Метод створення комплексної системи захисту інформації в телекомунікаційній та інформаційній системі».

Процес створення КСЗІ в ІТС є ідентичним незалежно від створення КСЗІ в існуючій чи новій ІТС. Якщо є необхідність захисту інформації або вдосконалення вже створеної КСЗІ, то процедура ідентична.[13]

Процедура створення комплексних систем захисту інформації передбачає реалізацію низки узгоджених заходів, що сприяють розвитку та впровадженню інформаційних технологій, що полегшують обробку інформації в ІТС, відповідно до вимог нормативно-правових актів та НД у сфері захисту інформації. Процес створення комплексної системи захисту інформації в ІТС розглядається цією НД як низка окремих, пов'язаних та комбінованих етапів, які необхідно реалізувати для створення КСЗІ.

Порядок, у якому етапи виконання та типовий зміст кожного з цих етапів пов'язані зі створенням КСЗІ, повинні відповідати пов'язаним етапам та роботі зі створення ІТС, як визначено в ГОСТ 34.601.

Етапи роботи під час створення КСЗІ в конкретній ІТС, їх результати та зміст, а також терміни виконання визначаються ТЗ на створення КСЗІ.[13]

Допускається виключення певних частин роботи або об'єднання кількох етапів, крім того, можливо додавання нових етапів до процесу. За необхідності дозволяється змінювати порядок виконання окремих етапів - дозволяючи виконувати кілька етапів роботи одночасно, дозволяючи виконувати окремі етапи до завершення попередніх тощо, якщо це не впливає негативно на якість роботи або не має суперечливої мети.

Якщо галузь традиційно впроваджує цей метод і має НД ТЗІ на відомчому рівні, або існують відповідні закони, що регулюють ІТС, дія яких поширюється на власника організації або саму ІТС, тоді сила дії збільшується.

Якщо певний тип роботи не охоплюється національними законами про захист технічної інформації жодного з вищезазначених рівнів, тоді дозволяється використання рекомендацій міжнародних стандартів, якщо вони не відхиляються від правових норм та стандартів України.[13]

3.2 Зміст та порядок реалізації заходів функціонування комплексної системи захисту інформації на об’єкті інформаційної діяльності

ЗБІ містить процедури та методи зберігання, обробки та захисту інформації.

- Потік інформації через технічні засоби, включаючи канали, що створюють побічні електронні випромінювання та перешкоди, акустоелектричні та інші канали;

- Порушення системи безпеки, включаючи несанкціоновані дії та доступ до інформації, що може бути здійснено шляхом підключення до обладнання та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів безпеки з метою використання інформації або нав'язування неправдивості, використання вбудованих пристроїв або програм, використання комп'ютерних вірусів тощо;

-- унікальний вплив на інформацію, який може бути здійснений шляхом формування полів та сигналів з метою порушення легітимності інформації або знищення системи безпеки.[13]

Для кожної конкретної ІТС склад, структура та вимоги ЗБІ випливають з властивостей інформації, що обробляється, типу автоматизованої системи та умов, за яких ІТС експлуатується.

У випадках, коли законодавство спеціально вимагає проведення робіт з проектування, створення, тестування та експлуатації ІТС, це має здійснюватися разом із заходами щодо забезпечення секретності інформації, протидії технічній розвідці, а також з організаційними заходами щодо збереження інформації з обмеженим доступом, яка не є секретною.[13]

Згідно з пунктом 5.8 НД ТЗІ 3.7-003-2005, створення комплексів технічного захисту інформації щодо витоку через технічні канали ініціюється, якщо інформаційні процеси потребують секретної інформації, або коли власник інформації визначає, що це необхідно. У цьому пункті слід окремо звернути увагу на власників інформації. Можливо, комплекс формального захисту інформації не є необхідним, але увага до формального захисту має бути приділена.

Створення КЗЗ ініціюється в усіх інформаційних системах держави, ці інформаційні системи належать державі або мають секретне призначення, або є специфічними для типу інформації, яку потрібно захистити, необхідність захисту визначається законом, а також в інформаційних системах, які є приватними або мають секретне призначення. Вибір щодо вжиття запобіжних заходів проти особливого впливу на інформацію здійснюється окремим власником інформації в кожному окремому випадку.[13]

Повний комплекс захисту інформації як частина об'єкта інформаційної поведінки

Для планування зусиль щодо створення KSIZ в ITS створюється служба, призначена для захисту інформації, процедура її створення, її обов'язки, функції, структура та повноваження визначені в НД 1.4-001-2000.

SIS запускається після прийняття рішення щодо створення SIS. Як виняток, SIS може бути створена після завершення проекту, але не пізніше етапу підготовки SIS до впровадження.[13]

Служба захисту інформації є критично важливою для будь-якої інформаційної системи, яка потребує захисту. Залежно від масштабу вашого підприємства та кількості співробітників, ви повинні подбати про структуру захисту інформації.

Для невеликої компанії може бути достатньо найняти 1-2 співробітників, які відповідають за захист інформації, і їм слід доручити завдання створення відділів інформаційної безпеки, для великих компаній слід створити хоча б один.

3.3. Розробка комплексної системи мережевого захисту інформації на об’єкті інформаційної діяльності

Створення Зони розділення інформації та безпеки знань (ЗЗІЗ) на платформі ноутбука має базуватися на трьох вимірах захисту інформації:

1. Захист технічної інформації

2. Захист інформації програмного забезпечення

3. Організаційно-технічний захист інформації

Кроки створення ЗЗІЗ для захищеного ноутбука

Крок 1: Забезпечення технічного захисту на основі джерела живлення змінного струму ноутбука [8].

На першому етапі слід впровадити базовий технічний захист та провести дослідження для виявлення ПЕВМН. Зокрема, слід впровадити екранування ноутбука, встановити лінійні шумоподавлювачі в блоці живлення ноутбука, а також виявити потенційне випромінювання та перешкоди для подальшого вдосконалення експлуатаційної документації.

Впроваджена комплексна схема технічного захисту для запобігання витоку інформації через технічні канали (на основі пасивних заходів захисту та лінійного шумоподавлення) сертифікована, а за результатами сертифікації видано «Сертифікат сертифікації систем автоматизації». Фаза 2: Початкова підготовка даних для обстеження інтелектуальних транспортних систем (ІТС) та вимоги до Стратегії інформаційної безпеки (КСІЗ)

На цьому етапі зазвичай виконується така робота:

- Аналіз відповідних нормативних актів та правових документів для визначення того, які обмеження або заборони застосовуються до певних типів інформації, та визначення необхідності забезпечення захисту інформації відповідно до інших стандартів;

- Визначення переліку інформації, яка має оброблятися автоматично, та її категоризація відповідно до рівнів обмеження доступу, вимог цілісності та вимог доступності відповідно до нормативних актів та правових документів. [8]

Опитування повинно враховувати такі аспекти:

- Технічні системи;

- Програмні компоненти;

- Оброблювана інформація;

- Користувачі;

- Дозволи на доступ до місцезнаходження. Фаза 3: Розробка стратегії безпеки

На цьому етапі буде виконано таку роботу:

- Аналіз ризиків (вивчення моделей загроз та зловмисників, а також можливих наслідків реалізації потенційної загрози);

- Визначення вимог до заходів, методів та засобів захисту інформації;

- Вибір базових рішень для усунення всіх основних загроз, розробка вимог, правил, обмежень та рекомендацій щодо використання технологій безпечної обробки інформації в інтелектуальних транспортних системах (ІТС), а також конкретних заходів та засобів захисту інформації та регулювання діяльності різних користувачів;

- Документація стратегії інформаційної безпеки. [8]

Стратегія інформаційної безпеки повинна враховувати всі характеристики середовища обробки інформації та може бути повністю змінена відповідальним

за захист інформації в організації клієнта. Стратегія не повинна бути меншою за вимоги, перелічені розробником автоматизованих систем (АС).

Стратегія повинна бути розроблена як окрема система та повинна включати:

- Посібник користувача;
- Посібник системного адміністратора;
- Посібник адміністратора безпеки.

Посібник користувача повинен чітко визначати методи та правила обробки інформації, ігнорування яких може призвести до реалізації загроз та витоку інформації.

Фаза 4: Розробка технічної специфікації (ТЗ) на створення KSIZ

Технічна специфікація на створення KSIZ в ITS визначає вимоги до захисту інформації, що обробляються в ITS, процес створення KSIZ, різні процеси тестування KSIZ, а також початкову організаційну та технічну документацію для її впровадження як частини ITS.

Розробка технічної специфікації на створення KSIZ враховує комплексний підхід до побудови KSIZ, який передбачає інтеграцію всіх необхідних заходів та засобів на кожному етапі життєвого циклу ITS в єдину систему для вирішення різних загроз інформаційній безпеці.

ТЗ KSIZ може бути розроблений як під час початкового створення ITS, так і під час модернізації існуючої ITS.

ТЗ KSIZ може бути розроблений такими способами [8]:

- Як окремий розділ у загальній технічній специфікації на створення ITS;
- Як окреме (часткове) ТЗ;
- Як доповнення до загальної технічної специфікації на інтелектуальні транспортні системи (ITS). Для інтегрованих ІТС (що складаються з кількох незалежно працюючих та інтерактивних інформаційних або комунікаційних систем) рекомендується створити окрему Ключову інформаційну систему та інформаційну систему (КСІЗ) для кожного компонента ІТС та офіційно

визначити її вимоги в окремій технічній специфікації. Як варіант, можна розробити єдину технічну специфікацію для кількох ідентичних компонентів ІТС, в якій будуть окреслені їхні відмінності або характеристики. [6]

Фаза 5: Розробка та впровадження проекту КСІЗ в ІТС

Розробка проекту КСІЗ базується та здійснюється відповідно до технічних специфікацій, створених ІТС, і проводиться в таких фазах, створених ІТС: попередній проект, технічний проект та робоча документація.

Під час розробки проекту КСІЗ необхідно перевірити та сформулювати проектні рішення, щоб забезпечити сумісність та взаємодію між різними компонентами КСІЗ, а також різні заходи та засоби захисту інформації.

Для реалізації вимог технічного завдання KSSI розробляються необхідні спільні рішення, включаючи організаційну структуру KSSI, архітектуру апаратного та програмного забезпечення, алгоритми роботи та умови використання засобів захисту, а також реалізацію послуг інформаційної безпеки, визначених у профілі функціональної безпеки. Фаза 6: Робота KSSI на основі захищених ноутбуків

На цьому етапі розробка KSSI має бути завершена, система адаптована до операційного середовища, а документація, що входить до плану захисту, має бути затверджена.

Усі категорії користувачів ITS (персонал технічної служби, звичайні користувачі) повинні пройти навчання з основних умов та процедур документації плану захисту, щоб забезпечити дотримання ними правил політики інформаційної безпеки та правильну експлуатацію засобів захисту інформації. [13]

Програмні продукти, необхідні для обробки інформації, та засоби захисту інформації встановлюються та тестуються відповідно до методів обробки та передачі інформації.

Під час встановлення вмикаються всі механізми обмеження доступу користувачів до інформації. Апаратні ресурси, механізми контролю поведінки

користувачів та база даних контролю цілісності програмного забезпечення та захисту інформаційно-технологічної системи (ІТС). [12]

Інформація про користувачів АС вводиться до засобу захисту, а також визначаються їхні права доступу до захищених ресурсів та середовищ обробки/передачі інформації.

Фаза 7: Попереднє тестування АС

Під час попереднього тестування працездатність системи визначається шляхом обробки інформації користувачем. Розробник системи намагатиметься вплинути на систему, здійснивши атаку на комп'ютерну систему. Оцінка системи стосуватиметься центральної системи захисту даних. Виявлені дефекти та висновки будуть усунені.

Фаза 8: Національний огляд АС

Комплексна система, що використовується для захисту всієї національної інформації, інформації з обмеженим доступом або іншої інформації, захищеної національними гарантіями, повинна отримати сертифікат відповідності вимогам захисту інформації. Цей сертифікат видається Державною службою захисту інформаційно-комунікаційних технологій України за результатами національного огляду. [19]

Національна оцінка КСІЗ проводиться для визначення відповідності її вимогам технічних завдань, нормативних актів та документів, пов'язаних із захистом інформації, а також для визначення доцільності введення КСІЗ в експлуатацію як частини ІТС. Національна сертифікація КСІЗ є етапом приймальних випробувань ІТС та проводиться відповідно до Національного регламенту сертифікації у сфері захисту технічної інформації. [12]

Етап 9: Підтримка КСІЗ

На цьому етапі будуть проводитися роботи з організаційної підтримки функціонування КСІЗ, її планової модернізації та управління заходами захисту інформації відповідно до планів захисту та експлуатаційних документів компонентів КСІЗ. [8]

Усі дії, пов'язані з модернізацією та обслуговуванням АС, не повинні порушувати специфікації, зазначені в експлуатаційних документах, та повинні відповідати політиці захисту інформації.

Вимоги до технічних каналів для запобігання несанкціонованому доступу до мережевої інформації

Потенційні технічні канали витоку інформації для портативних ноутбуків:

1. Канал бокового електромагнітного випромінювання (СЕМ) ОТЗС;

2. Бічний канал електромагнітного випромінювання ДТЗС;

3. Бічний канал електромагнітних перешкод на лінії електропередач ОТЗС (земля);

4. Бічний канал електромагнітних перешкод на зв'язку ДТЗС;

5. Канал радіочастотних перешкод;

6. Оптичний канал витоку інформації;

7. Встановлення вбудованих пристроїв.

3.4. Вимоги до системи контролю доступу на об’єкті інформаційної діяльності

Захист від витоку технічної інформації має бути забезпечений через такі канали [8]:

- Запобігання боковому електромагнітному випромінюванню від OTZS шляхом екранування OTZS або часткового екранування електронних компонентів.

- Запобігання боковому електромагнітному випромінюванню від DTZS шляхом визначення зони випромінювання R1 та подальшої рекомендації розміщення ноутбуків поза цією зоною.

- Запобігання боковим електромагнітним перешкодам на лінії електропередач OTZS (землі) шляхом придушення лінійного шуму на лінії електропередач OTZS.

- Усунення бокових електромагнітних перешкод на зв'язку DTZS шляхом використання незалежного джерела живлення (наприклад, електростанції, акумулятора) для живлення DTZS; використання пристроїв технічного захисту, що затримують сигнали низького рівня; та встановлення мережевих фільтрів у лінії електропередач DTZS. Інший підхід полягає у встановленні лінійних шумоподавлювачів у блоці живлення ноутбука.

- Запобігання високочастотним перешкодам шляхом екранування OTZS.

- Світловий канал для витоку інформації повинен оцінюватися самими співробітниками.

Встановлення вбудованих пристроїв слід запобігати організаційними заходами, що запобігають проникненню неавторизованого персоналу до приміщення, або ж використанням пошукового обладнання для огляду приміщення за необхідності.

Приміщення, де обробляється важлива корпоративна інформація, повинні бути оснащені системою контролю доступу (СКУД) [8]. Встановлення системи контролю доступу є однією з найважливіших та найважливіших систем у будь-якій структурі підприємства. Її функції включають автоматизацію виробничих процесів, контроль доступу до підприємства та його будівель, ідентифікацію та управління користувачами, запобігання несанкціонованому доступу та можливість розподілу приміщень відповідно до різних правил доступу. Все це завдяки швидкому розвитку інформаційних технологій, які не лише надають нові можливості для посилення контролю та безпеки будівель, але й для посилення контролю та безпеки інформації підприємства. Сьогодні системи контролю доступу використовуються по-різному залежно від політики конфіденційності, потреб та можливостей підприємства [1-3].

Система контролю доступу – це набір апаратних та програмних засобів безпеки, призначених для обмеження та реєстрації входу та виходу об'єктів (персоналу, транспортних засобів) у певній зоні через «точки входу» (такі як двері, ворота, контрольно-пропускні пункти) [3].

Сучасні системи контролю доступу включають такі елементи:

1. Ідентифікатор – це пристрій, який дозволяє системі ідентифікувати персонал. Наразі як ідентифікатори зазвичай використовуються широко використовувані безконтактні картки, контактні картки (з чорними магнітними смугами) та електронні брелоки. Спеціальні коди або біометричні дані (такі як відбитки пальців, відбитки долонь, відбитки сітківки ока, розпізнавання голосу тощо), що вводяться персоналом під час входу до охоронюваної зони, також можуть використовуватися як ідентифікатори.

2. Зчитувач – пристрій, що використовується для ідентифікації особи та передачі даних до блоку керування.

3. Блок керування – «мозок» системи. Він відповідає за визначення того, чи має власник певного посвідчення особи право входити до приміщення. Якщо вхід дозволено, надсилається сигнал для відкриття електронного замка (обертові ворота, шлагбаумні ворота, двері). У мережевих системах контролю доступу блок керування також підключений до комп’ютера [3]. Основні завдання системи контролю доступу включають:

• Контроль доступу до певних зон, включаючи обмеження доступу, ідентифікацію уповноваженого персоналу та облік робочого часу;

• Розрахунок заробітної плати (при інтеграції з системою бухгалтерського обліку);

• Ведення бази даних персоналу/відвідувачів;

• Інтеграція з усіма системами безпеки:

- Інтеграція з системами відеоспостереження для консолідації архівів системних подій, надсилання команд до системи відеоспостереження для

початку запису та налаштування кутів камери для запису подальших подій підозрілих подій;

- Оснащення системою охоронної сигналізації (SOS) для обмеження доступу до приміщення або автоматичного ввімкнення та вимкнення безпеки в приміщенні;

- Обладнаний системою пожежної сигналізації (СПС) для отримання інформації про стан від пожежних сповіщувачів та автоматичного розблокування евакуаційних виходів і закриття протипожежних дверей у разі спрацьовування пожежної тривоги [4].

В особливо чутливих місцях мережа пристроїв СКУД фізично відключена від інших інформаційних мереж.

Таблиця 3.1

Класифікація СКУД	
За технічними характеристиками і функціональними можливостями	• рівень ідентифікації; • кількість контрольованих місць; • пропускна здатність; • кількість користувачів; • умови експлуатації [3]
За рівнем ідентифікації доступу	• одноріневі (ідентифікація здійснюється за однією ознакою, наприклад, з зчитування коду картки); • багаторівневі (ідентифікація здійснюється за кількома ознаками, наприклад, з зчитування коду картки і біометричних даних); [3]
За кількістю контрольованих місць	• малої місткості (до 16 місць); • середньої місткості (від 16 до 64 місць); • великої місткості (понад 64 місць);
За умовами експлуатації	• у закритих приміщеннях; • у закритих неопалюваних приміщеннях; • під навісом на вулиці в умовах помірно-холодного клімату; • на вулиці в умовах помірно-холодного клімату; • в особливих умовах (підвищена вологість,
За основними функціональними можливостями	• можливість оперативного перепрограмування; • схемно-технічний та програмний захист від вандалізму і саботажу; • високий рівень секретності; • автоматична ідентифікація; • розмежування повноважень співробітників і відвідувачів з доступу в приміщення і на об'єкт у цілому; • надійне механічне замикання контрольованих місць з можливістю аварійного ручного відкриття; • автоматичний збір і аналіз даних; • вибіркова роздруківка даних.

3.5 Висновок до розділу

У цьому розділі представлено комплексну систему захисту інформації для цілей інформаційної діяльності, призначену для запобігання несанкціонованому розкриттю інформації через мережу, тим самим протидіючи несанкціонованому доступу.

У цьому розділі аналізуються вимоги до нормативно-правового забезпечення комплексної системи захисту інформації для цілей інформаційної діяльності.

У цьому розділі визначено низку заходів для впровадження комплексної системи захисту інформації для цілей інформаційної діяльності.

У цьому розділі побудовано та продемонстровано архітектуру комплексної системи захисту інформації для цілей інформаційної діяльності, призначеної для запобігання несанкціонованому розкриттю інформації через мережу.

У цьому розділі визначено та продемонстровано вимоги до системи контролю доступу для забезпечення захисту комплексної системи захисту інформації для цілей інформаційної діяльності від несанкціонованого доступу до мережі.

ВИСНОВКИ

Під час підготовки до кваліфікаційного огляду було виконано такі завдання:

– Проведено аналіз основних кіберзагроз, з якими стикається Центр інформаційної діяльності (тобто несанкціоноване розголошення конфіденційних даних).

– Вивчено напрямки вдосконалення технічних систем Центру інформаційної діяльності (запобігання доступу до інформації з обмеженим доступом через мережу).

– Розроблено комплексну систему захисту інформації для Центру інформаційної діяльності (запобігання доступу до інформації з обмеженим доступом через мережу).

– Розглянуто питання охорони навколишнього середовища.

1. У першій частині кваліфікаційного огляду було проаналізовано основні кіберзагрози, з якими стикається Центр інформаційної діяльності (тобто несанкціоноване розголошення конфіденційних даних). Було проаналізовано шкідливе програмне забезпечення та його функції та класифікації. Було представлено мережеві програмні додатки, що використовуються для несанкціонованого розголошення інформації. Було проаналізовано характеристики та потенціал спеціалізованих програмних засобів та комп'ютерних вірусів, що використовуються для несанкціонованого доступу до інформації.

2. У другій частині кваліфікаційного огляду було представлено напрямок розробки стратегій безпеки та результати досліджень нових методів удосконалення системи фізичного захисту критичної інфраструктури (запобігання несанкціонованому доступу до інформації з обмеженим доступом). Центр інформаційної діяльності розробив стратегію безпеки та запропонував модель загроз. Опубліковано зміст та процедури впровадження заходів щодо розвитку комплексної мережі системи захисту інформації Центру

інформаційної діяльності. Запропоновано вимоги до програмного забезпечення для захисту інформації в мережі передачі інформації Центру інформаційної діяльності. 3. У третій частині роботи з акредитації описано інтегровану систему захисту інформації в центрі інформаційної діяльності для запобігання несанкціонованому розкриттю в Інтернеті. Проаналізовано вимоги до нормативного забезпечення інтегрованої системи захисту інформації в центрі інформаційної діяльності для запобігання несанкціонованому розкриттю в Інтернеті. Визначено перелік заходів щодо впровадження функціонування інтегрованої системи захисту інформації в центрі інформаційної діяльності. Розроблено та описано структуру інтегрованої системи захисту інформації в центрі інформаційної діяльності для запобігання несанкціонованому розкриттю в Інтернеті. Визначено та продемонстровано вимоги до системи контролю доступу для забезпечення функціонування інтегрованої системи захисту інформації в центрі інформаційної діяльності для запобігання несанкціонованому розкриттю в Інтернеті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К. : Консум. — 2005. — 576 с.

2. Гинце А. А. Особенности СКУД систем доступа крупных распределенных объектов / А. А. Гинце. ААМ Систем, 2005.

3. Юдін О. Критеріальний аналіз сучасних операційних систем у задачах захисту інформаційних ресурсів / О. Юдін, О. Весельська // Наукоємні технології. — 2012. — Т. 14. — №. 2. — С. 74-79.

4. Волхонский В.В. Системы контроля и управления доступом - СПб: Университет ИТМО, 2015.

5. Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування. Методологія побудови класифікатора / О. К. Юдін, С. С. Бучик // Наукоємні технології. - 2015. - № 2. - С. 188-195

6. Аналіз та класифікація систем контролю та управління доступом на підприємстві О. К. Юдін, д-р техн. наук, проф. Національний авіаційний університет orcid.org/0000-0001-5098-7796; О. М. Весельська Національний авіаційний університет orcid.org/0000-0002-4914-2187.

7. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу – Київ, 1999. – 20 с.

8. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Ю.В. Землянко, О.А. Замула, О.О. Ткач, Н.І. Литвинова, Я.А. Пересічанська.]., 2010.

9. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.]–Вінниця : ВНТУ, 2017.– 120 с.

10. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення – Київ, 2007. – 6 с.

11. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяль-ності. Створення комплексу технічного захисту інформації. Передпроектні роботи – Київ, 2007. – 5 с.

12. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних систем [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://openarchive.nure.ua/bitstream/document/861/1/460-469.pdf.

13. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі – Київ, 2005. – 20 с.

14. Засоби створення шкідливого програмного забезпечення [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://studfile.net/preview/5206321/page:17/.

15. Безпека інформаційно-комунікаційнихсистем. Шкідливе програмне забезпечення [Електронний ресурс] – Режим доступу до ресурсу: http://virt.ldubgd.edu.ua/pluginfile.php/39805/mod_resource/content/3/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%201.4.pdf.

16. ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ Навчальний посібник у 15 частинах Загальна редакціяАндрій Іванович Семенченко, Валерій Михайлович Дрешпак Формат 60×90/16.Папір офс. 80 г/м2. Гарн. Таймс. Друк офс.Ум. друк. арк. 4,5. Авт. арк. 3,0. Наклад 500 прим. Видавець та друк: ФОП Москаленко О. М.

17. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації [Електронний ресурс] : навчальний посібник / С. О. Іванченко, О. В. Гавриленко, О. А. Липський [та ін.] ; НТУУ «КПІ». – Електронні текстові дані (1 файл: 615 Кбайт). – Київ : НТУУ «КПІ», 2016. – 104 с. – Назва з екрана.

18. Безпека систем підтримки прийняття рішень [Текст] : навч. посіб. / Ковтунець В. В., Нестеренко О. В., Савенков О. І. ; Нац. акад. упр. - Київ : Нац. акад. упр., 2016. - 189 с. : рис., табл. - Бібліогр.: с. 183-184. - 300 прим. - ISBN 978-617-7386-00-0

19. ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

20. Білявський Г. О., Падун М. М., Фурдуй Р. С. Основи загальної екології. — К.: Либідь. 1995 — 368 с.

21. Білявський Г. О., Фурдуй Р. С. Практикум із загальної екології. // Навч. посібн.— К.:Либідь, 1997.—160с.

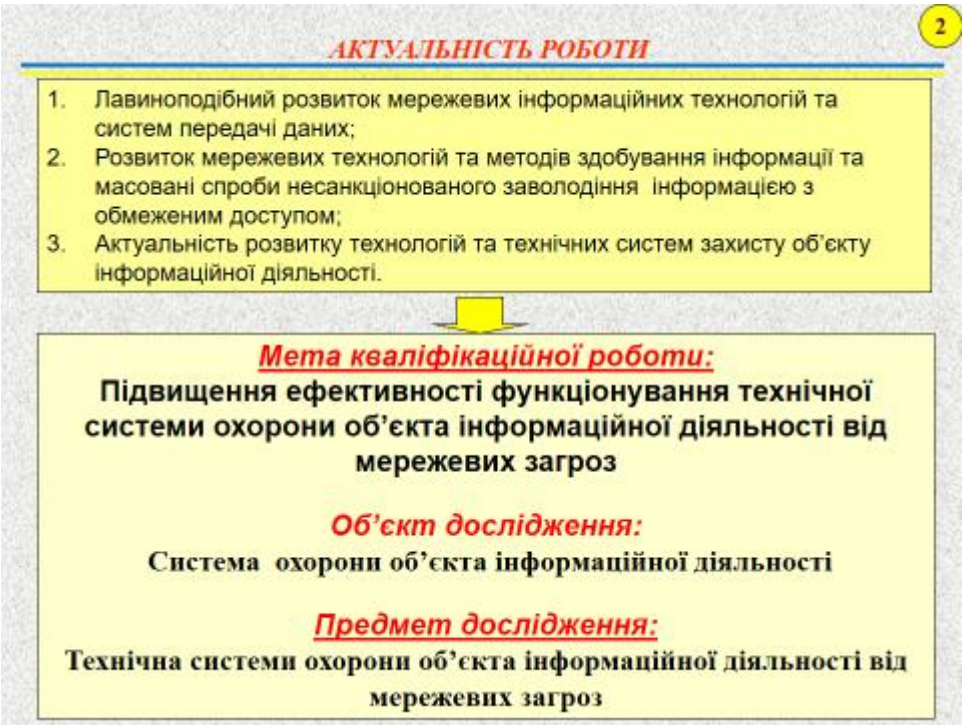
22. Волошин І. М. Методика дослідження проблем природокористування. — Львів: ЛДУ, 1994. — 160 с.

23. Екологічний словник: Навч. посібник /В.В.Прежко та ін. – Харків: ХДАМГ, 1999. – 416 с.

24. Екологія і закон: Екологічне законодавство України. У 2-х кн./ Відповідальний редактор док. юрид. наук, професор, акад. Андрейцев В. А. — К.: Юрінком інтер, 1997. — 704 с.

25. Злобін Ю.А. Основи екології.- К.: Лібра, 1998. – 249.

ДОДАТОК А


2
АКТУАЛЬНІСТЬ РОБОТИ
1. Лавиноподібний розвиток мережевих інформаційних технологій та систем передачі даних;
2. Розвиток мережевих технологій та методів здобування інформації та масовані спроби несанкціонованого заволодіння інформацією з обмеженим доступом;
3. Актуальність розвитку технологій та технічних систем захисту об'єкту інформаційної діяльності.
Мета кваліфікаційної роботи:
Підвищення ефективності функціонування технічної системи охорони об'єкта інформаційної діяльності від мережевих загроз
Об'єкт дослідження:
Система охорони об'єкта інформаційної діяльності
Предмет дослідження:
Технічна системи охорони об'єкта інформаційної діяльності від мережевих загроз

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

3

1. РОЗДІЛ 1: **Аналіз основних мережевих загроз несанкціонованого витоку конфіденційних даних на об'єкті інформаційної діяльності**
2. РОЗДІЛ 2: **Дослідження напрямків удосконалення технічної системи охорони об'єкта інформаційної діяльності від мережевого доступу до інформації з обмеженим доступом**
3. РОЗДІЛ 3: **Комплексна системи захисту інформації від мережевого доступу на об'єкті інформаційної діяльності**
4. РОЗДІЛ 4: **Охорона природнього середовища**
5. ВИСНОВКИ: **Узагальнено одержані результати**

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

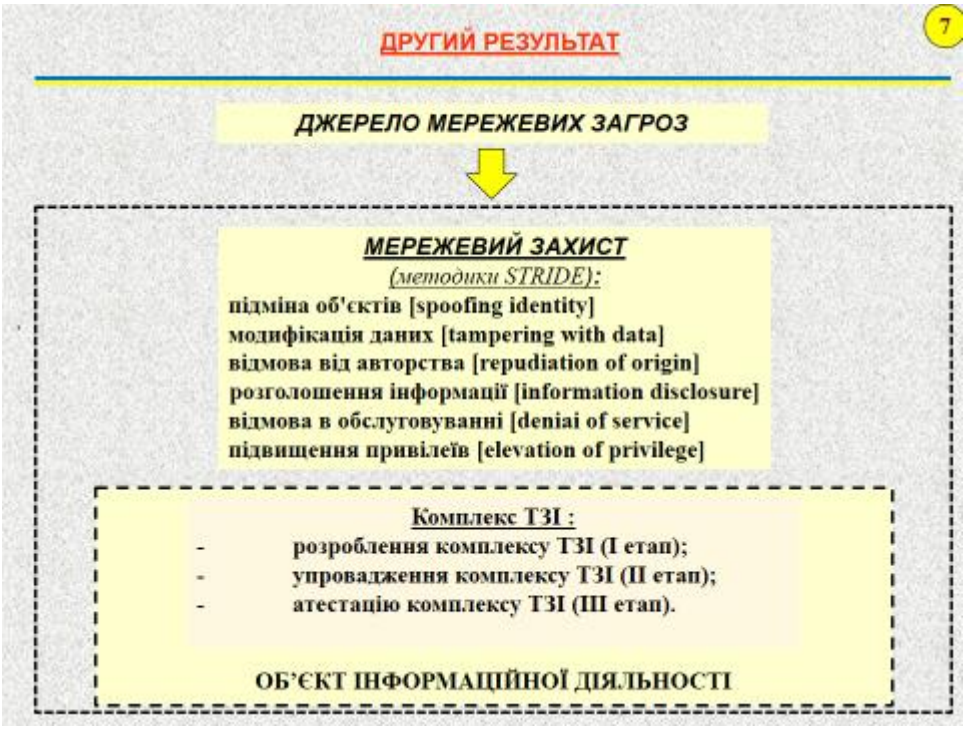
3

1. РОЗДІЛ 1: **Аналіз основних мережевих загроз несанкціонованого витоку конфіденційних даних на об'єкті інформаційної діяльності**
2. РОЗДІЛ 2: **Дослідження напрямків удосконалення технічної системи охорони об'єкта інформаційної діяльності від мережевого доступу до інформації з обмеженим доступом**
3. РОЗДІЛ 3: **Комплексна системи захисту інформації від мережевого доступу на об'єкті інформаційної діяльності**
4. РОЗДІЛ 4: **Охорона природнього середовища**
5. ВИСНОВКИ: **Узагальнено одержані результати**


4
ПЕРШИЙ РЕЗУЛЬТАТ
Аналіз основних мережевих загроз несанкціонованого витоку конфіденційних даних на об'єкті інформаційної діяльності
ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ
ОСНОВНІ МЕРЕЖЕВІ ЗАГРОЗИ
Шкідливе програмне забезпечення:
1. Спеціальні хакерські утиліти
2. Класичні мережні хробаки
3. Програми «Троянський кінь»
4. Засоби віддалених DoS- і DDoS-атак
Мережеві програмні застосунки:
1. Програмні закладки
2. Шпигунські програми
3. «Логічні бомби»
4. «Люки»
Комп'ютерні віруси:
1. Інтернет-клікери
2. Проксі-сервери
3. Платні ресурси
4. Інсталяція з мережі
5. Рекламні модулі
6. «Лихі жарти»


5
ПЕРШИЙ РЕЗУЛЬТАТ
ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ
ВЛАСТИВОСТІ МЕРЕЖЕВИ ЗАГРОЗ
Властивість 1.
Загрози порушення конфіденційності інформації
Властивість 2.
Загрози порушення цілісності інформації
Властивість 3.
Загрози порушення доступності інформації


6
ДРУГИЙ РЕЗУЛЬТАТ
Дослідження напрямків удосконалення технічної системи охорони об'єкта інформаційної діяльності від мережевого доступу до інформації з обмеженим доступом
ДЖЕРЕЛО ЗАГРОЗ
ЗАХИСТ
Кількісна недостатність
Якісна недостатність
МОДЕЛЬ ЗАГРОЗ
- перелік можливих типів загроз
- перелік можливих способів реалізації загроз
ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ


7
ДРУГИЙ РЕЗУЛЬТАТ
ДЖЕРЕЛО МЕРЕЖЕВИХ ЗАГРОЗ
МЕРЕЖЕВИЙ ЗАХИСТ
(методики STRIDE):
підміна об'єктів [spoofing identity]
модифікація даних [tampering with data]
відмова від авторства [repudiation of origin]
розголошення інформації [information disclosure]
відмова в обслуговуванні [deniai of service]
підвищення привілеїв [elevation of privilege]
Комплекс ТЗІ :
- розроблення комплексу ТЗІ (І етап);
- упровадження комплексу ТЗІ (ІІ етап);
- атестацію комплексу ТЗІ (ІІІ етап).
ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

8

ТРЕТІЙ РЕЗУЛЬТАТ

Комплексна системи захисту інформації від мережевого доступу на об'єкті інформаційної діяльності

ТЕХНІЧНА СИСТЕМА ОХОРОНИ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Фізичні засоби захисту

- різноманітні пристрої, конструкції, апарати, вироби, призначені для створення перепон на шляху руху зловмисників:
  - охоронні та охоронно-пожежні системи
  - охоронне телебачення
  - охоронне освітлення
  - засоби фізичного захисту

Апаратні засоби захисту

- різноманітні технічні конструкції, які забезпечують припинення розголошення, захист від витоку та протидію несанкціонованому доступу до джерел конфіденційної інформації:
  - апаратура для проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливого витоку інформації
  - засоби виявлення каналів витоку інформації на об'єктах та у приміщеннях
  - засоби локалізації каналів витоку
  - апаратура для пошуку та виявлення засобів промислового шпигунажу
  - засоби протидії несанкціонованому доступу до джерел конфіденційної інформації

Програмні засоби захисту

- система спеціальних програм, які входять до складу програмного забезпечення:
  - програми для захисту інформації від несанкціонованого доступу
  - програми для захисту інформації від копіювання
  - програмні засоби програм від вірусів
  - програмні засоби для захисту інформації від вірусів
  - засоби програмного захисту каналів за язку

Криптографічні засоби захисту

- апаратні, програмні та програмно-апаратні засоби, що реалізують захист інформації за допомогою криптографічних перетворень

9

ТРЕТІЙ РЕЗУЛЬТАТ

ТЕХНІЧНА СИСТЕМИ ОХОРОНИ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД МЕРЕЖЕВОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

ФІЗИЧНІ ЗАСОБИ ЗАХИСТУ

ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ

10

ТРЕТІЙ РЕЗУЛЬТАТ

НД ТЗІ 3.7-003-05

ЕТАПИ СТВОРЕННЯ КСЗІ ДЛЯ ЗАХИЩЕНОГО НОУТБУКА:

1. Забезпечення технічного захисту АС на базі ноутбука;
2. . Обстеження ІТС та підготовка вихідних даних для формування вимог до КСЗІ
3. Формування політики безпеки КСЗІ в ІТС
4. Розробка технічного завдання КСЗІ в ІТС
5. Розробка і реалізація проекту КСЗІ в ІТС
6. Введення КСЗІ на базі захищеного ноутбука в дію
7. Попередні випробування АС
8. Державна експертиза АС
9. Супровід КСЗІ

11

ТРЕТІЙ РЕЗУЛЬТАТ

Класифікація СКУД

За технічними характеристиками і функціональними можливостями	- рівень ідентифікації; - кількість контрольованих місць; - пропускна здатність; - кількість користувачів; - умови експлуатації
За рівнем ідентифікації доступу	- одноріневі (ідентифікація здійснюється за однією ознакою, наприклад, з зчитування коду картки); - багаторівневі (ідентифікація здійснюється за кількома ознаками, наприклад, з зчитування коду картки і біометричних даних);
За кількістю контрольованих місць	- малої місткості (до 16 місць); - середньої місткості (від 16 до 64 місць); - великої місткості (понад 64 місць);
За умовами експлуатації	- у закритих приміщеннях; - у закритих неопалюваних приміщеннях; - під навісом на вулиці в умовах помірно-холодного клімату; - на вулиці в умовах помірно-холодного клімату; - в особливих умовах (підвищена вологість, запиленість, вібрації і т. п.)
За основними функціональними можливостями	- можливість оперативного перепрограмування; - схемно-технічний та програмний захист від вандалізму і саботажу; - високий рівень секретності; - автоматична ідентифікація; - розмежування повноважень співробітників і відвідувачів з доступу в приміщення і на об'єкт у цілому; - надійне механічне замикання контрольованих місць з можливістю аварійного ручного відкриття; - автоматичний збір і аналіз даних; - вибіркова роздруківка даних. [3]

12

ТРЕТІЙ РЕЗУЛЬТАТ

РЕКОМЕНДАЦІЇ ПО РОЗРОБЦІ ТА ВТІЛЕННЮ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Основні завдання СКУД:

1. Управління доступом на задану територію: пропуск та обмеження доступу;

2. Ідентифікація особи, яка має доступ на задану територію;

3. Ведення бази персоналу/відвідувачів;

4. Планово-фінансовий облік (при інтеграції з системами бухгалтерського обліку);

5. Інтеграція зі всіма системами безпеки:
- з системою відеоспостереження;
- з системою охоронної сигналізації;
- з системою пожежної сигналізації .

13

ВИСНОВКИ:

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

– **Проведено аналіз основних мережевих загроз несанкціонованого витоку конфіденційних даних на об'єкті інформаційної діяльності.**

– **Досліджено напрямки удосконалення технічної системи охорони об'єкта інформаційної діяльності від мережевого доступу до інформації з обмеженим доступом.**

– **Розроблено комплексну систему захисту інформації від мережевого доступу на об'єкті інформаційної діяльності.**

ДЯКУЮ ЗА УВАГУ !