Міністерство освіти і науки України
Національний технічний університет «Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента Романюка Едуарда Олександровича

академічної групи 125м-22-2

спеціальності 125 Кібербезпека

за освітньо-професійною програмою Кібербезпека

на тему ***Організація управління доступом в інформаційно-комунікаційній системі підприємства FullNet***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., професор Корнієнко В.І.			
розділів:				
спеціальний	д.т.н., професор Корнієнко В.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викладач Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Романюку Едуарду Олександровичу* **академічної групи** *125м-22-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

за освітньо-професійною програмою *Кібербезпека*

на тему *Організація управління доступом в інформаційно-комунікаційній системі підприємства FullNet*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.23 № 1227-с

Розділ	Зміст	Термін виконання
Розділ 1	Характеристика об'єкта інформаційної діяльності. Огляд та актуальність проблеми а також розгляд методів захисту інформації, що використовуються у DRM.	05.11.2023
Розділ 2	Впровадження методу доступу до відеоінформації підприємства заснованого на використанні цифрових сертифікатів і ЦВК.	20.11.2023
Розділ 3	Визначення економічної доцільності та ефекту від провадження методу доступу до відеоінформації підприємства заснованого на використанні цифрових сертифікатів і ЦВК.	01.12.2023

Завдання видано _____ Олександр ГУСЄВ
(підпис керівника) (прізвище, ініціали)

Дата видачі: 01.09.2023

Дата подання до екзаменаційної комісії: 06.12.2023

Прийнято до виконання _____ Едуард Романюк
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 72 с., 2 рис., 12 табл., 3 додатків, 24 джерел.

Мета магістерської дипломної роботи: підвищення рівня захисту відеоінформації, яка циркулює на підприємстві .

Об`єкт дослідження: приватне підприємство, що займається розробкою ПЗ та консультаціями з приводу розробки ПЗ та комп'ютерних технологій.

У першій частині проаналізовані існуючі DRM технології. Розглянуто методи захисту інформації, що використовуються у DRM. В результаті була обрана модель аналізу ризиків.

У спеціальній частині був розроблений метод доступу до відеоінформаціїї підприємства заснованого на використанні цифрових сертифікатів і ЦВК.

У економічній частині виконано розрахунок вартості запропонованих мір з захисту інформації. Надано оцінку економічної ефективності впровадження системи управління ризиками інформаційної безпеки.

В ході роботи розроблені типова модель загроз та приведений приклад впровадження методу доступу до відеоінформаціїї підприємства заснованого на використанні цифрових сертифікатів і ЦВК.

ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ, МОДЕЛЬ ЗАГРОЗ, ВИКОРИСТАННЯ ЦИФРОІИХ СЕРТИФІКАТІВ, ІНФОРМАЦІЙНИЙ РИЗИК

THE ABSTRACT

Explanatory note: 72 pages, 2 figures, 12 tables, 3 appendices, 24 sources.

The purpose of the master's thesis: increasing the level of protection of video information circulating in the enterprise.

The object of the study: a private enterprise engaged in the development of software and consulting on the development of software and computer technologies.

In the first part, existing DRM technologies are analyzed. The information protection methods used in DRM are considered. As a result, a risk analysis model was chosen.

In a special part, a method of accessing video information of the enterprise based on the use of digital certificates and CA was developed.

In the economic part, the cost of the proposed information protection measures was calculated. An assessment of the economic efficiency of the implementation of the information security risk management system is provided.

In the course of the work, a typical model of threats was developed and an example of the implementation of the method of access to video information of the enterprise based on the use of digital certificates and CA was given.

INFORMATION SECURITY, RISK MANAGEMENT, THREAT MODEL, USE OF DIGITAL CERTIFICATES, INFORMATION RISK

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ТОВ – товариство з обмеженою відповідальністю

ІТС – інформаційна система

ОІД – об'єкт інформаційної діяльності.

АС – автоматизована система

ІБ – інформаційна безпека;

ІТ – інформаційні технології;

ПЗ – програмне забезпечення;

DRM – Digital Rights Management

ЕЦП – Електронний цифровий підпис

ЦВК – Центри видачі ключів

ЗМІСТ

ВСТУП

Сучасний світ інформаційних технологій та інтернету переживає бурхливий розвиток, що призводить до значного збільшення обсягів інформаційних потоків і їх доступності. Однак разом з цим зростає і загроза безпеці інформації, зокрема, відеоданих. Організація управління доступом до відеоінформації стає актуальною та критично важливою задачею для забезпечення конфіденційності, цілісності та доступності цих даних.

Актуальність даної роботи обумовлена зростаючим обсягом відеоінформації, її цінністю для підприємств та організацій, а також зростаючими загрозами її безпеці. Забезпечення конфіденційності відеоданих стає важливим завданням у контексті збереження ділових та особистих секретів.

Метою даної роботи є дослідження та аналіз організації управління доступом до відеоінформації в інформаційно-комунікаційній системі підприємства FullNet. Головною метою є підвищення рівня захисту підприємства через розробку ефективних стратегій та методів захисту відеоданих від несанкціонованого доступу, витоку та пошкодження.

Об'єктом дослідження є інформаційно-комунікаційна система підприємства FullNet та відеоінформація, що в ній обробляється.

Предметом дослідження є організація управління доступом до відеоінформації, включаючи використання криптографії, стеганографії, DRM-технологій, ЕЦП та моделей управління доступом.

Для досягнення поставленої мети використовуються методи аналізу, моделювання, дослідження систем безпеки, а також аналіз сучасних підходів до управління доступом та захисту відеоінформації.

Науковою новизною даної роботи є розробка комплексних підходів до організації управління доступом до відеоінформації, що враховують сучасні вимоги до безпеки даних та використовують передові технології криптографії,

стеганографії та DRM-технологій. Робота спрямована на розробку практичних рекомендацій щодо захисту відеоінформації на підприємствах та організаціях.

РОЗДІЛ 1
СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ.

1.1 Характеристика об’єкта інформаційної діяльності

Об’єктом інформаційної діяльності (далі ОІД) є ТОВ «FullNet».

ТОВ «FullNet» - приватне підприємство, що займається розробкою ПЗ та консультаціями з приводу розробки ПЗ та комп’ютерних технологій.

За формою власності ТОВ «FullNet» комерційна організація, зареєстрована як товариство з обмеженою відповідальністю, на основі приватної власності статутний капітал якої 25663624,50 грн. Підприємство було зареєстровано 30.03.2004.

ТОВ «FullNet» має такі види діяльності:

- 62.01 Діяльність у галузі комп'ютерного програмування
- 62.02 Консультаційні послуги у галузі комп'ютерних технологій
- 62.09 Інші види діяльності в галузі інформаційних технологій та комп'ютерних систем
- 74.90 Інша професійна, наукова та технічна діяльність, не включена до інших категорій

Підприємство функціонує 5 днів на тиждень (з понеділка по п'ятницю). Графік роботи з 9:00 до 18:00, з перервою на обід з 13:00 до 14:00. У період обідньої перерви організація не займається основною діяльністю, служба охорони, яка пропускає людей на територію фірми, обідає по черзі.

Працівники являють собою ключовий ресурс продуктивності підприємства для реалізації проектів та ідей компанії. Кількість працівників на досліджуваному підприємстві складає 6 осіб.

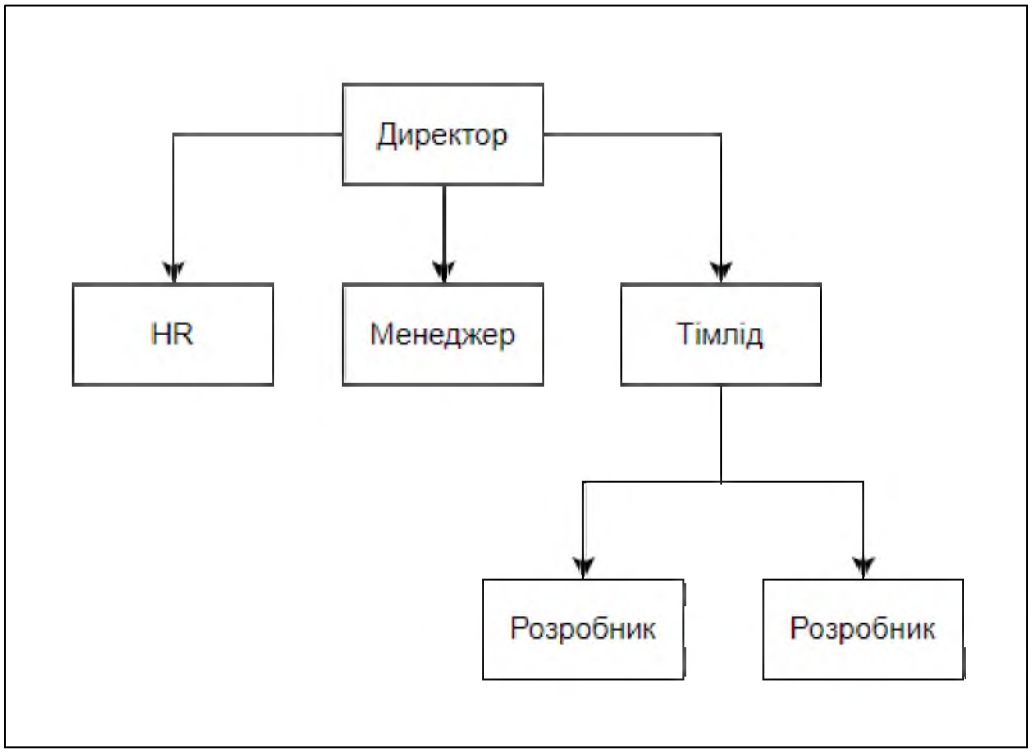

Рисунок 1.1 Організаційна структура підприємства

1.2 Аналіз DRM. Огляд та актуальність проблеми.

Digital Rights Management (DRM) - це набір технологій, що використовуються для контролювання використання цифрових медіа та пристроїв. Поява DRM тісно пов'язана з розвитком цифрових технологій та потребою захисту інтелектуальної власності в онлайн-середовищі. З часом DRM еволюціонував, адаптуючись до зростаючих вимог забезпечення безпеки та приватності.

Основним завданням DRM є запобігання несанкціонованому копіюванню та розповсюдженню цифрового контенту. Це досягається за допомогою впровадження різних технологій шифрування, контролю доступу та управління цифровими ключами. DRM дозволяє власникам контенту встановлювати обмеження на копіювання, друк, передачу або зміну цифрових файлів.

Актуальність DRM у сучасному світі обумовлена зростаючою цифровізацією контенту та необхідністю захисту авторських прав. Однак використання DRM не обмежується лише захистом інтелектуальної власності. Воно також відіграє ключову роль у забезпеченні конфіденційності та інтегрітету даних, особливо у сферах, де обробка та передача інформації відбувається в цифровому форматі.

Однак DRM не позбавлений недоліків. Критики вказують на те, що DRM може обмежувати законні права користувачів на використання придбаного контенту, створюючи бар'єри для доступу та обміну знаннями. Існують також технічні та юридичні виклики, пов'язані з DRM, особливо в контексті міжнародних стандартів та законодавства.

В останні роки спостерігається тенденція до пошуку балансу між захистом прав власників контенту та забезпеченням свободи доступу до інформації для користувачів. Це призводить до розвитку нових підходів та альтернативних рішень в сфері DRM, які прагнуть знайти компроміс між захистом прав та свободою користування цифровим контентом.

1.3 Розгляд методів захисту інформації, що використовуються у DRM

1.3.1 Використання засобів криптографії в DRM

Криптографія є ключовим елементом в системах Digital Rights Management (DRM). Її використання дозволяє ефективно захищати цифровий контент від несанкціонованого доступу та копіювання, а також забезпечує контроль над розповсюдженням та використанням цифрових медіа. Цей розділ детально розглядає роль та механізми застосування криптографії у системах DRM.

Основні криптографічні технології у DRM

1. Шифрування контенту: основою DRM є шифрування контенту, яке перешкоджає доступу до медіа без відповідного ключа дешифрування. Це забезпечує, що лише авторизовані користувачі можуть отримати доступ до

захищеного контенту. Часто використовуються алгоритми симетричного шифрування, такі як AES (Advanced Encryption Standard), через їх швидкість та ефективність.

2. Керування ключами: ключовим аспектом DRM є управління ключами шифрування. Це включає генерацію, зберігання, розподіл та анулювання ключів. Ефективне управління ключами гарантує, що лише уповноважені особи можуть отримати доступ до захищеного контенту та що ключі не можуть бути легко скомпрометовані або вкрадені.
3. Цифровий підпис: для забезпечення автентичності та цілісності цифрового контенту використовуються цифрові підписи. Це дозволяє визначити, чи було контент змінено після його шифрування та чи є він справжнім. Цифрові підписи є важливими для забезпечення довіри до системи DRM.
4. Сертифікація та аутентифікація: криптографічні сертифікати використовуються для аутентифікації користувачів та пристроїв у системах DRM. Це гарантує, що доступ до контенту отримують лише ті користувачі, які мають відповідні права.

Виклики та проблеми криптографії у DRM

1. Баланс між безпекою та зручністю: одним з головних викликів є знаходження балансу між захистом контенту та забезпеченням зручності для кінцевих користувачів. Надмірні обмеження можуть призводити до незручностей та невдоволення користувачів.
2. Управління ключами: ефективне управління ключами – це складний та витратний процес. Існує ризик втрати або компрометації ключів, що може призвести до втрати доступу до контенту або його несанкціонованому розповсюдженню.
3. Сумісність та стандартизація: проблема сумісності різних систем DRM створює виклики для користувачів та розробників. Відсутність

уніфікованих стандартів може призводити до конфліктів між різними DRM-системами.

Перспективи розвитку

Розвиток технологій, таких як блокчейн та розподілені леджери, відкриває нові можливості для вдосконалення систем DRM. Ці технології можуть забезпечити більш прозоре та ефективне управління правами та ліцензіями, а також підвищити безпеку управління ключами. Крім того, розвиток квантових комп'ютерів ставить під сумнів надійність сучасних методів шифрування, що може вимагати розробки нових криптографічних рішень у майбутньому.

1.3.2 Опис схеми роботи DRM-технології на основі шифрування

Digital Rights Management (DRM) - це комплексний підхід до захисту цифрового контенту, який в значній мірі заснований на принципах шифрування. Цей розділ описує детально, як працює DRM-технологія на основі шифрування, включаючи ключові компоненти та етапи її функціонування.

Етапи роботи DRM-технології

1. Шифрування контенту: Першим кроком в DRM є шифрування цифрового контенту. Контент (може бути відео, аудіо, текст тощо) шифрується за допомогою сильних криптографічних алгоритмів. Це гарантує, що контент залишається недоступним без відповідного ключа для дешифрування.
2. Управління ключами: Після шифрування контенту генерується ключ шифрування. Цей ключ зберігається в захищеному середовищі та видається лише авторизованим користувачам. Управління ключами включає їх генерацію, розподіл, зберігання та відкликання.
3. Ліцензування та правила використання: DRM включає механізми ліцензування, які визначають правила використання контенту. Ці правила можуть включати обмеження на кількість переглядів, часові обмеження, обмеження на копіювання тощо.

4. Доставка ключів та ліцензій: Ключі шифрування та ліцензії доставляються до користувача через захищені канали. Це забезпечує, що лише уповноважені користувачі отримують доступ до контенту та інформації про його використання.
5. Дешифрування та перегляд контенту: Коли користувач хоче отримати доступ до контенту, DRM-система перевіряє ліцензію та права користувача. Якщо вони підтверджені, система надає ключ для дешифрування, і користувач може переглядати або використовувати контент відповідно до встановлених правил.

Ключові компоненти DRM-системи

1. Сервер ліцензування: Центральний компонент DRM, що керує видачею ліцензій та ключів шифрування.
2. Сервер шифрування: Відповідає за шифрування контенту та генерацію ключів.
3. Клієнтська DRM-система: Встановлена на пристрої користувача, забезпечує дешифрування контенту та контроль за дотриманням ліцензійних умов.

Виклики та проблеми

1. Безпека ключів: Один з головних викликів - забезпечення безпеки ключів шифрування. Їх витік може призвести до несанкціонованого доступу до контенту.
2. Компроміс між захистом та зручністю: Занадто строгі обмеження можуть відштовхувати користувачів, тоді як слабкі - не забезпечують належного захисту контенту.
3. Сумісність: Різні DRM-системи можуть мати проблеми з сумісністю, що ускладнює використання контенту на різних пристроях.

Перспективи

З огляду на швидкий розвиток технологій, таких як штучний інтелект і блокчейн, очікується, що майбутнє DRM буде спрямоване на підвищення гнучкості, ефективності та безпеки систем. Це може включати розробку більш адаптивних та інтелектуальних механізмів управління правами та ліцензіями.

1.3.3 Використання засобів стеганографії в DRM

Стеганографія, техніка приховування інформації всередині іншої інформації, відіграє важливу роль у розробці та вдосконаленні систем Digital Rights Management (DRM). У цьому контексті стеганографія використовується для приховування інформації про авторські права, ліцензування та ідентифікацію власника всередині цифрового контенту, що дозволяє збільшити захист від несанкціонованого використання та копіювання.

Основні принципи стеганографії в DRM

1. Приховування метаданих: Стеганографія дозволяє вбудовувати метадані, такі як інформація про авторські права, в сам цифровий контент (наприклад, зображення, аудіо чи відео). Ці метадані стають невидимими для звичайного користувача, але можуть бути виявлені та прочитані за допомогою спеціалізованого програмного забезпечення.
2. Ідентифікація та відстеження: Через вбудовані метадані, стеганографія дозволяє ідентифікувати первісного власника та відстежувати історію розповсюдження контенту. Це особливо корисно для виявлення та боротьби з несанкціонованим розповсюдженням та піратством.
3. Захист від маніпуляцій: Стеганографічні методи можуть використовуватися для перевірки цілісності контенту, дозволяючи виявити будь-які спроби зміни або маніпуляції з оригінальним файлом.

Технології та методи стеганографії в DRM

1. Водяні знаки: Найбільш поширена форма стеганографії у DRM - це використання цифрових водяних знаків. Вони можуть бути візуальними

або аудіальними та вбудовуються в контент таким чином, що їх важко виявити або видалити без пошкодження самого контенту.

2. LSB (Least Significant Bit) модифікація: Цей метод полягає у зміні найменш значущих бітів у файлі, що дозволяє приховувати інформацію всередині аудіо, відео або зображень з мінімальним впливом на якість.
3. Спектральні методи: В аудіофайлах стеганографія може бути реалізована шляхом внесення змін у спектральні характеристики звуку, що не впливає на його сприйняття людиною.

Виклики та обмеження

1. Виявлення та видалення: Одним з основних викликів є створення стійких до виявлення стеганографічних методів. Також існує ризик, що спроби видалення водяних знаків можуть пошкодити сам контент.
2. Баланс між невидимістю та стійкістю: Існує потреба знайти оптимальний баланс між невидимістю водяного знака та його стійкістю до спроб видалення.
3. Сумісність та ефективність: Часто виникає потреба в сумісності стеганографічних методів з різноманітними форматами файлів та забезпечення їх ефективності без значного збільшення розміру файлу.

Перспективи розвитку

Майбутнє використання стеганографії в DRM може включати розробку нових, більш стійких та ефективних методів приховування інформації. Це може включати поєднання стеганографії з іншими технологіями, такими як штучний інтелект та машинне навчання, для підвищення її ефективності та безпеки.

1.4 Огляд існуючих DRM-технологій

DRM-технології розвиваються, намагаючись знайти баланс між захистом авторських прав та забезпеченням зручного доступу для користувачів.

1. Adobe Digital Editions Adobe Digital Editions використовується переважно для захисту електронних книг. Ця технологія дозволяє видавцям контролювати копіювання та друк текстів, а також обмежувати кількість пристроїв, на яких можна читати електронну книгу.

2. Apple FairPlay Використовується в продуктах Apple, включаючи iTunes та Apple Music. FairPlay шифрує аудіо та відео контент, вимагаючи авторизації через Apple ID для доступу та відтворення контенту на обмеженій кількості пристроїв.

3. Microsoft PlayReady PlayReady широко використовується у сфері цифрового телебачення та стрімінгових сервісів. Ця технологія підтримує широкий спектр форматів контенту та пристроїв, пропонуючи гнучкі можливості управління правами.

4. Google Widevine Widevine використовується багатьма популярними онлайн-платформами, такими як YouTube та Netflix. Вона надає підтримку різноманітних рівнів безпеки, дозволяючи розповсюджувати контент у високій якості з належними обмеженнями доступу.

5. Marlin DRM Marlin є відкритим стандартом DRM, розробленим для широкого спектра пристроїв та форматів. Ця технологія забезпечує гнучкість управління правами, а також можливість взаємодії з іншими DRM-системами.

6. Amazon DRM Використовується для захисту контенту, придбаного через Amazon, включаючи Kindle eBooks та Prime Video. Ця система обмежує копіювання та перенесення контенту, забезпечуючи контроль над його використанням.

Виклики та тенденції

1. Сумісність: Один з великих викликів для DRM-технологій - це забезпечення сумісності між різними пристроями та платформами. Користувачі часто стикаються з проблемами, коли один і той же контент не можна відтворити на різних пристроях.

2. Користувацький досвід: Забезпечення ефективного захисту авторських прав, не порушуючи при цьому користувацький досвід, залишається ключовою проблемою. Надмірні обмеження можуть відштовхнути користувачів та спонукати їх до пошуку альтернативних способів доступу до контенту.
3. Піратство: Незважаючи на застосування DRM, піратство залишається значною проблемою. Найчастіше це пов'язано з можливістю обходу DRM-обмежень через різні технічні методи.
4. Тенденції розвитку: Сучасні тенденції в DRM включають інтеграцію з хмарними технологіями, штучним інтелектом та машинним навчанням для підвищення ефективності та адаптивності систем.

1.5 Використання ЕЦП

Електронний цифровий підпис (ЕЦП) є важливим компонентом у системах Digital Rights Management (DRM), забезпечуючи автентичність, цілісність та невід'ємність цифрового контенту. ЕЦП дозволяє однозначно ідентифікувати джерело цифрового контенту та перевіряти, що контент не був змінений після його підписання. Цей розділ розглядає роль та застосування ЕЦП у контексті DRM.

Принципи роботи ЕЦП у DRM

1. Автентифікація: ЕЦП забезпечує доведення автентичності джерела контенту. Це означає, що користувачі можуть бути впевнені в тому, що контент походить від законного власника або розробника.
2. Цілісність: За допомогою ЕЦП можна перевірити, що контент не був змінений або пошкоджений після його створення та підписання. Це особливо важливо для захисту прав на інтелектуальну власність та запобігання несанкціонованому редагуванню чи копіюванню.

3. Невід'ємність: ЕЦП гарантує, що після підписання контент не може бути відокремлений від підпису, а підпис - від контенту. Це означає, що власник контенту завжди зможе підтвердити свої права на нього.

Технології та процедури

1. Генерація ключів: Для створення ЕЦП використовуються криптографічні ключі. Зазвичай, це пара ключів: приватний (для створення підпису) та публічний (для його перевірки).
2. Підписання контенту: Власник контенту використовує свій приватний ключ для створення ЕЦП. Цей підпис потім вбудовується в контент або додається до нього як окремий файл.
3. Перевірка підпису: Коли контент розповсюджується або використовується, користувачі можуть перевірити ЕЦП за допомогою публічного ключа власника. Якщо перевірка успішна, це підтверджує автентичність та цілісність контенту.

Виклики та перспективи

1. Збереження ключів: Зберігання та захист приватних ключів є важливими, оскільки їх втрата або компрометація може призвести до серйозних проблем з безпекою.
2. Складність управління: Управління ЕЦП вимагає ретельної організації та впровадження надійних процесів для підтримки цілісності та конфіденційності.
3. Широке застосування: З розвитком цифрових технологій очікується зростання використання ЕЦП у різних сферах, не лише в DRM, а й у цифровому ідентифікуванні, електронному документообігу тощо.

ЕЦП відіграє ключову роль у DRM, надаючи засоби для захисту, автентифікації та підтвердження прав на цифровий контент. Його використання допомагає збільшити довіру між сторонами та захищає від незаконного розповсюдження та зміни контенту.

1.6 Класифікація моделей управління доступом

1.6.1 Дискреційна модель управління доступом

Дискреційна модель управління доступом (Discretionary Access Control, DAC) є однією з основних методологій в регулюванні доступу до інформаційних ресурсів в контексті управління інформаційною безпекою, включаючи системи DRM. В цій моделі права доступу надаються на основі ідентифікації суб'єктів та об'єктів, і власник ресурсу або системи має дискрецію в присвоєнні цих прав.

Основні принципи DAC

1. Власник ресурсу: В DAC, власник ресурсу (наприклад, файлу, програми або системи) має право визначати, хто може отримати доступ до цього ресурсу та яким чином. Власник може надавати, забороняти або обмежувати доступ іншим користувачам.
2. Контроль на рівні суб'єкта: Управління доступом здійснюється шляхом надання прав доступу окремим суб'єктам (наприклад, користувачам, групам користувачів або процесам). Суб'єкти отримують різні рівні доступу в залежності від їх ролі та потреб.
3. Гнучкість та делегування: DAC дозволяє власникам ресурсів делегувати управління правами доступу, що сприяє гнучкості в управлінні та розподілі прав.

Переваги DAC

1. Гнучкість: Одна з ключових переваг DAC - висока гнучкість в управлінні доступом, що дозволяє власникам ресурсів швидко адаптуватися до змін у бізнес-процесах або політиках безпеки.
2. Легкість керування: У порівнянні з більш жорсткими моделями, такими як мандатна модель управління доступом (MAC), DAC забезпечує більш просте та інтуїтивне управління правами доступу.

Недоліки DAC

1. Ризик неправильного управління: Через високу ступінь дискреції та гнучкості існує ризик, що права доступу можуть бути неправильно налаштовані або зловжито ними.
2. Проблеми скалабельності: У великих системах зі складною структурою доступу управління DAC може стати складним і важким для підтримки.

Застосування DAC в DRM

У контексті DRM, DAC може використовуватися для управління доступом до цифрового контенту. Наприклад, власник цифрового медіа (наприклад, електронної книги або музичного файлу) може контролювати, хто має право читати, копіювати або редагувати цей контент. Це дає можливість реалізувати індивідуальні політики доступу, враховуючи конкретні потреби та вимоги.

Майбутнє DAC в DRM

З постійним розвитком цифрових технологій та збільшенням обсягів цифрового контенту, роль DAC в системах DRM буде продовжувати еволюціонувати. Очікується, що інновації у галузі криптографії, блокчейна та штучного інтелекту принесуть нові можливості для підвищення ефективності та безпеки управління доступом.

1.6.2 Мандатна модель управління доступом

Мандатна модель управління доступом (Mandatory Access Control, MAC) є однією з ключових методологій у системах управління інформаційною безпекою, включаючи DRM. Відмінною особливістю MAC є централізоване управління політиками доступу, яке не дозволяє кінцевим користувачам або власникам ресурсів змінювати права доступу на свій розсуд.

Основні принципи MAC

1. Централізоване управління: В MAC, політики доступу визначаються на централізованому рівні, зазвичай організацією або системним

адміністратором. Ці політики встановлюють строгі правила, які регулюють доступ до ресурсів.

2. Класифікація та мітки: Ресурси (наприклад, документи, файли, програми) та користувачі класифікуються згідно з рівнями безпеки. Кожному об'єкту та суб'єкту присвоюється мітка безпеки, яка визначає рівень доступу.
3. Правила доступу: Доступ до ресурсів регулюється на основі порівняння міток безпеки користувачів та ресурсів. Суб'єкти можуть отримувати доступ лише до тих об'єктів, рівень безпеки яких відповідає або нижчий за їх власний.

Переваги MAC

1. Підвищена безпека: MAC забезпечує високий рівень безпеки, оскільки доступ контролюється на основі строгих правил, що знижує ризик несанкціонованого доступу.
2. Контрольований доступ: Ця модель ефективно запобігає випадковому або навмисному розголошенню конфіденційної інформації, оскільки доступ обмежується відповідно до встановлених політик.

Недоліки MAC

1. Негнучкість: MAC може бути занадто негнучкою, особливо в швидко мінливих або динамічних середовищах, де потреби доступу часто змінюються.
2. Складність управління: Встановлення та підтримка MAC може бути складним і витратним, особливо у великих організаціях зі складними ієрархіями та політиками доступу.

Застосування MAC в DRM

У контексті DRM, MAC може бути використана для строгого контролю доступу до цифрового контенту. Наприклад, доступ до певних видів контенту, таких як конфіденційні документи або відео високої якості, може бути обмежений для певних груп користувачів або визначених умов. Це дозволяє

забезпечити, що лише уповноважені особи мають доступ до високоцінного чи чутливого контенту.

Майбутнє MAC в DRM

Очікується, що майбутнє MAC у сфері DRM буде включати інтеграцію з розширеними технологіями, такими як штучний інтелект та машинне навчання, для більш гнучкого та адаптивного управління доступом. Це може підвищити ефективність MAC, зберігаючи при цьому високий рівень безпеки.

1.6.3 Рольова модель управління доступом

Рольова модель управління доступом (Role-Based Access Control, RBAC) є популярною методологією управління доступом, особливо великої значущості вона набуває в контексті систем DRM. В RBAC права доступу призначаються на основі ролей користувачів у системі, а не на основі ідентифікації окремих суб'єктів або об'єктів.

Основні принципи RBAC

1. Визначення ролей: В RBAC, доступ до ресурсів керується через ролі, які представляють певний набір обов'язків і відповідальностей у системі. Кожна роль має визначені права доступу до ресурсів.
2. Призначення ролей: Користувачам або групам користувачів призначаються специфічні ролі, які визначають їхні права доступу. Це спрощує управління доступом, оскільки права можуть бути змінені на рівні ролі, а не для окремих користувачів.
3. Сегрегація обов'язків: RBAC дозволяє ефективно розділити обов'язки між різними ролями, забезпечуючи, щоб жоден користувач або група не мала занадто широких повноважень.

Переваги RBAC

1. Ефективність управління: RBAC дозволяє легко керувати правами доступу великої кількості користувачів, оскільки зміни можна вносити на рівні ролей.
2. Гнучкість та масштабованість: Модель є гнучкою та легко масштабується, що дозволяє її ефективно використовувати в різних організаційних структурах.

Недоліки RBAC

1. Складність конфігурації: Налаштування ролей та визначення відповідних прав доступу може бути складним і потребує глибокого розуміння бізнес-процесів та вимог безпеки.
2. Жорсткість ролей: У деяких випадках, ролі можуть бути занадто жорстко визначені, що може обмежувати гнучкість у роботі користувачів.

Застосування RBAC в DRM

У контексті DRM, RBAC може бути використана для управління доступом до цифрового контенту. Наприклад, в медіа-індустрії, різні ролі (наприклад, редактор, дизайнер, маркетолог) можуть мати різні рівні доступу до цифрових ресурсів, таких як графічні файли, відео або аудіозаписи.

Майбутнє RBAC в DRM

RBAC продовжує еволюціонувати, інтегруючись з передовими технологіями, такими як штучний інтелект та автоматизовані системи управління. Це може включати адаптивні ролі, які можуть змінюватися відповідно до контексту або поведінки користувача, забезпечуючи більшу гнучкість та безпеку.

1.7 Розробка моделі порушника

До зовнішніх порушників відносяться особи, які знаходяться за поза підприємством. Це можуть бути конкуруючі підприємства та крадії або персонал з обслуговування приміщення, особи, яким не передбачено доступ до ІзОД, але

які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД, наприклад, прибиральники, електрики тощо.

До внутрішніх порушників відносяться особи, що мають можливість фізичного підключення до каналів зв'язку або інших складових мережі передачі даних, користувачі АС, персонал, який безпосередньо пов'язаний із забезпеченням функціонування ІТС.

В таблиці 1.2 наведені категорії порушників, що використовуються при створенні моделі. Модель порушника наведена зі специфікаціями за різними показниками:

за мотивами здійснення порушень;

за рівнем кваліфікації та обізнаності щодо ІТС;

за показником можливостей використання засобів ІТС для реалізації загроз;

за часом та місцем дії.

Профіль порушника визначає сукупність цих характеристик.

Таблиця 1.1

Рейтингова оцінка

Рейтингова оцінка	Опис
1	незначний
2	нижчий за середній
3	середній
4	вищий за середній
5	значний

Спираючись на отримані результати аналізу характеристик оброблюваної інформації, категорій порушників, що мають потенційну можливість порушення конфіденційності та цілісності інформації, вважаються найбільш небезпечними, доступності - менш небезпечними, а уважності - найменш небезпечними.

Таблиця 1.2

Категорії порушників. Внутрішні по відношенню до ІТС.

Позначення	Визначення категорії	Рівень загроз
ПВО	Директор	4
ПВ1	HR	1
ПВ2	Розробники	3
ПВ3	Тімлід	3
ПВ4	Менеджер	5

Таблиця 1.3

Категорії порушників. Зовнішні по відношенню до ІТС

Позначення	Визначення категорії	Рівень загроз
П30	Кандидати на вакансію	2
П31	Вахтери, сантехнік, електрик, прибиральниці	3

Таблиця 1.4

Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність(ненавмисне порушення	1
М2	Самоствердження	2
М3	Корисний інтерес	4

Таблиця 1.5

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Рівень кваліфікації	Рівень загроз
К1	Володіє низьким рівнем знань; може використовувати ІС на	1

	рівні користувача	
К2	Володіє середнім рівнем знань, має впевнені навики використання ІС та їх обслуговування	3
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІС	5

Таблиця 1.6

Специфікація моделі порушника за показником можливостей

Позначення	Характеристика можливостей порушника	Рівень загроз
30	Може підслуховувати розмови у приміщеннях та читати документи на чужих робочих місцях	1
31	Використовує пасивні технічні засоби перехвату без можливості модифікації інформації та компонентів ІС.	2
32	Використовує лише штатні засоби та недоліки системи захисту інформації для її подолання (несанкціоновані дії з використанням дозволених та доступних засобів), а також компактні носії інформації, які можливо приховано	4

	пронести повз пост охорони офісу.	
З3	Використовує просунуті технічні засоби активного впливу з метою модифікації інформації та компонентів ІС, дезорганізації систем обробки інформації.	5

Таблиця 1.7

Специфікація моделі порушника за часом дії

Позначення	Час дії	Рівень загроз
Ч1	Під час бездіяльності компонентів системи (неробочий час)	3
Ч2	Під час функціонування системи	5
Ч3	Під час обслуговування компонентів, їх ремонту	4

Таблиця 1.8

Специфікація моделі порушника за місцем дії

Позначення	Час дії	Рівень загроз
Д1	Ззовні приміщень офісу; всередині приміщень, але без	2

	доступу до технічних засобів ІТС.	
Д2	З робочих місць користувачів ІТС.	3
Д3	З доступом у зону зберігання баз даних, архівів, тощо	4

Профілі порушників всіх категорій наведено у таблиці 1.9, у колонці «Сума загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 1.9

Профілі порушників

Позначення	Визначення категорії	Характер дій порушника					Ефективний рівень загроз
		Мотив порушення	Кваліфікація	Можливості	Час дії	Місце Дії	
1	Директор	М1-М3	К3	З0-З2	Ч1-Ч3	Д1-Д3	44
2	HR-менеджер	М1-М2	К2	З0,З2	Ч1-Ч2	Д1-Д2	25
3	Розробник	М1-М3	К3	З0-З2	Ч1-Ч2	Д1-Д2	35
4	Тімлід	М1-М3	К3	З0-З2	Ч1-Ч2	Д1-Д3	39
5	Менеджер	М1-М3	К3	З0-З2	Ч1-Ч3	Д1-Д3	45
6	Кандидати на вакансію	М3	К1-К3	З0-З3	Ч2	Д1	34
7	Вахтери, сантехніки, електрики, прибиральни-ці	М1-М2	К1	З0	Ч1-Ч3	Д1-Д3	29

Досліджені в роботі категорії порушників безпеки інформації, засвідчують, що теоретично найбільш велику небезпеку будуть становити:

Менеджер(він же системний адмін) і директор, оскільки вони мають безпосередній доступ до системи ІТС та працюють з її компонентами, та мають достатню компетенцію і мотиви.

Тому до найму на підприємство співробітників на ці посади потрібно відноситися з великою обережністю та встановити великій поріг проходження або встановити додаткові правила, обмеження на їх роботу в підприємстві, завжди робити перевірку, як вони виконують свою роботу.

1.8 Профіль захищеності для інформаційної системи

При створенні КСЗІ визначається спроможність системи забезпечувати захист інформації. Розглядається захист оброблюваної інформації як від НСД так і від витоку технічними каналами. Критерії комп'ютерної системи набір функціональних послуг і функцій, що забезпечують захист від певних загроз.

АС організаційно-технічна система, що включаючи в себе персонал, оброблювану інформацію, ОС та фізичне середовище.

Для нашого ОІД вибрана АС «3» класу. Відповідно до ND ТЗІ 2.5-005-99: «Відповідний багатомашинний багатоклієнтський комплекс, який обробляє дані різного рівня обмеження доступу. Величезним контрастом від попереднього класу є необхідність передачі даних через нестабільний клімат або, у У загальному випадку, наявність концентраторів, які виконують різні стратегії безпеки.

Вибрані стандартні утилітарні профілі безпеки в КС, необхідні для АС класу «3», з розширеними передумовами для секретності, надійності та доступності оброблюваних даних:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НН-

2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД-2. базова довірча конфіденційність. Реалізована. Політика довірчої конфіденційності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. [НН-1].

КА-2. базова адміністративна конфіденційність. Реалізована. Політика адміністративної конфіденційності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства, інформація про клієнтів та співробітників, рекламні данні, бухгалтерська та фінансова звітності. КЗЗ надає можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. [НИ-1, НО-1].

КО-1. Повторне використання об'єктів. Наявна. До того як користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкту скасовуються, а також вся інформація, що міститься в даному об'єкті, стає недосяжною. [НИ-1, НО-1].

КК-1. Аналіз прихованих каналів - виявлення. Наявна. Канал по пам'яті може бути реалізований, якщо не буде реалізоване повторне використання об'єктів. Канал по часу може бути реалізований, оскільки з високою вірогідністю користувачі не будуть перевіряти схеми закриття і відкриття файлів, однак це можна попередити використовуючи наприклад «port knocking», який вимагае дотримання певних заданих послідовностей для відкриття портів. [КО-1].

КВ-2. базова конфіденційність при обміні. Наявна. Множина об'єктів та інтерфейсних процесів сервер документів, драйвер файлової системи, захищенні документи. Наявні протоколи захисту інформації при обміні (HTTPS —

використовує додатковий шар шифрування/автентифікації, WPA2 - посилена безпека даних і посилений контроль доступу до бездротових мереж - підтримує шифрування відповідно до стандарту AES,...), оновлення НО. [НО-1].

ЦД-1. Мінімальна довірча цілісність. Наявна. КЗЗ надає користувачу можливість для кожного захищеного об'єкта (продукти роботи підприємства), що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. [НИ-1].

ЦА-2. базова адміністративна цілісність. Наявна. Політика адміністративної цілісності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства, інформація про клієнтів та співробітників, рекламні данні, бухгалтерська та фінансова звітності. КЗЗ розмежовує доступ на підставі атрибутів доступу — процесу і захищеного об'єкту. [НИ-1, НО-1].

ЦО-1. Обмежений відкат. Реалізовано. Множина об'єктів захищенні документи, файли, технологічна інформація. Існують автоматизовані засоби, яш дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій - редагування інформації, наприклад в WORD Ctrl+Z, видаленні файли можна відновити, система контролю версії, резервне копіювання..., виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-2. базова цілісність при обміні. Наявна. Об'єкти - документи, файли, технологічна інформація (оновлення НО, антивірусу). Хеш функція (функція, що здійснює перетворення масиву вхідних даних довільної довжини в (вихідну) бітову послідовність встановленої довжини, що виконується певним алгоритмом; не зворотний процес, фіксована довжина на виході, не значні зміни даних повинні значно змінювати результат функції, для різних вхідних даних може створитися один хеш; один з видів алгоритмів — MD5), наявні протоколи передачі по мережі та комутаційні пристрої. [НО-1].

ДР-1. Використання ресурсів - квоти. Наявна. Відносяться до таких ресурсів системи: об’єм пам'яті, дисковий простір, пропускна спроможність каналів зв'язку... [НО-1].

ДС-1. Стійкість при обмежених відмовах. Наявна. Об’єкт оперативна пам'ять. [НО-1].

ДЗ-1. Гаряча заміна модернізація. Наявна. Відноситься не тільки до конструкції, а й до апаратного і програмного забезпечення. Оновлення антивірусу, системних файлів. [НО-1].

ДВ-1. Відновлення після збоїв ручне відновлення. Наявна. (тільки після збоїв системи, а не інформації). Точки відновлення, резервне копіювання. [НО-1].

НР-2. Реєстрація Зовнішній аналіз, захищений журнал. Наявна. [НН-1, НО-1].

НИ-2. Зовнішня ідентифікація і автентифікація, одиночна. Наявна. Вхід до локального запису відбувається з використанням пароля. Також е можливість скористатися фізичним ключом безпеки [НК-1].

НК-1. Одно-направлений достовірний канал. Реалізовано. З’єднання з системою проводить тільки людина(користувач) — введення паролю тільки з клавіатури.

НО-2. Розподіл обов'язків адміністраторів. Наявна. Політика розподілу обов'язків, що реалізується КЗЗ, визначае ролі адміністраторів і звичайного користувача і притаманні їм функції, визначае дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Однак на нашому об’єкті одна людина наділена функціями адміністратора безпеки та системного адміністратора. [НИ-1]

НЦ-2. Цілісність комплексу засобів захисту КЗЗ з гарантованою цілісністю. Наявна. Політика цілісності КЗЗ визначає домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

КЗЗ підтримує домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Політика цілісності КЗЗ визначає склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ: антивірус, вбудовані механізми у системі, хеш функція...

НТ-2. Самотестування за запитом - Самотестування при старті. Наявна. Система та антивірус автоматично починають перевірку при ініціалізації. [НО-1].

НВ-1. Автентифікація вузла. Наявна. Обмін даними може відбуватися через блютуз з'єднання, через USB...

НА-1. базова автентифікація відправника. Наявна. Наявний цифровий підпис. [НН-1].

НП-1. базова автентифікація отримувача. Наявна. Наявний цифровий підпис. [НН-1].

1.9 Постановка задачі

Метою даної дипломної роботи є аналіз, проектування та розробка ефективних методів і механізмів управління доступом до інформаційно-комунікаційних ресурсів підприємства FullNet з використанням сучасних принципів і технологій Digital Rights Management (DRM).

Завдання дослідження:

1. Теоретичний аналіз:
    - Огляд та аналіз існуючих методологій управління доступом, включаючи DRM, та їх застосування в корпоративних інформаційних системах.
    - Дослідження різних моделей управління доступом (дискреційної, мандатної, рольової) та оцінка їх придатності для впровадження на підприємстві FullNet.

2. Аналіз потреб підприємства:
    - Вивчення специфіки роботи та потреб підприємства FullNet у контексті управління доступом до інформаційних ресурсів.
    - Ідентифікація основних вимог до системи управління доступом на підприємстві.
3. Проектування системи:
    - Розробка концептуальної моделі системи управління доступом для підприємства FullNet, виходячи з виявлених потреб та вимог.
    - Визначення ключових компонентів системи, включаючи архітектуру, функціональні можливості та механізми безпеки.
4. Аналіз результатів та висновки:
    - Оцінка ефективності розробленої системи управління доступом в контексті потреб підприємства FullNet.
    - Формулювання висновків та рекомендацій для подальшого вдосконалення системи.

Очікувані результати: Очікується, що в результаті виконання дипломної роботи буде розроблено комплексну систему управління доступом, яка відповідатиме специфічним потребам підприємства FullNet, забезпечуючи ефективний захист інформаційних ресурсів та оптимізацію процесів доступу до них. Система повинна бути гнучкою, масштабованою та легко інтегрованою в існуючу інфраструктуру підприємства.

1.10 Висновки до розділу 1

У першому розділі даної дипломної роботи було проведено всебічний аналіз ключових аспектів управління доступом в інформаційно-комунікаційній системі підприємства FullNet. Були розглянуті та оцінені різні моделі управління доступом, включаючи дискреційну, мандатну та рольову моделі, які надають цінні інсайти для розробки ефективної системи управління доступом.

Окрім цього, була розроблена модель потенційного порушника, що допомогла визначити потенційні загрози та слабкі місця в системі безпеки FullNet. Це дозволило більш точно сформулювати вимоги до системи захисту та розробити стратегії протидії різним формам несанкціонованого доступу.

Далі, було створено профіль захищеності інформаційної системи, який включає детальну оцінку ризиків та рекомендації щодо заходів безпеки. Цей профіль став основою для визначення оптимальних політик і механізмів захисту, які будуть використані в системі.

У сукупності, проведені аналізи та розробки створюють міцну основу для подальшого проектування та впровадження комплексної системи управління доступом на підприємстві FullNet. Отримані результати свідчать про важливість інтеграції різних підходів та методологій для забезпечення високого рівня захисту інформаційних ресурсів та ефективного управління доступом у відповідності з сучасними вимогами та загрозами в галузі інформаційної безпеки.

РОЗДІЛ 2
СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз інформаці, яка циркулює на підприємстві

В автоматизованій системі відсутня інформація, що е власністю держави чи відомості, які становлять державну таємницю. Правила доступу до інформації розподілено директором. Доступ до ІзОД мають тільки зареєстровані в системі користувачі. В організації циркулює велика кількість персональних даних, як клієнтів так і співробітників.

Таблиця 2.1

Класифікація інформації, яка циркулює на ІТС

№	Вид інформації		Режим доступу	Правовий режим	Вид представ-лення в ІТС	Вимоги до захисту		
						К	Ц	Д
1	Інформація про клієнтів (персональна)		ІзОД	Конфіден-ційна інформація	ТекстовийЕлектрон-ний	3	2	3
2	Інформація про працівників (персональна)		ІзОД	Конфіден-ційна інформація	ТекстовийЕлектрон-ний	4	4	4
3	Продукти роботи підприємства	Вхід./Вихід. документи	ІзОД	Конфіден-ційна інформація	Текстовий Електрон-ний	4		4
		Матеріали про проект				4	5	4
		Дизайн				4	5	4

4	Фінансова звітність (банківські рахунки, виручка)	ІзОД	Службова інформація	Електрон-ний	3	4	4

Рівні конфіденційності:

– К1 - рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не е конфіденційною;

– К2 - рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К3 - рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К4 - рівень конфіденційності інформації, що може призвести до значних;

– матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

– К5 - критичний рівень конфіденційності інформації, що може призвести до краху

– компанії у разі втрати конфіденційності інформації. Рівні цілісності:

– Ц1 - рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

– Ц2 - рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

– Ц3 - рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

– Ц4 - рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

– Ц5 - критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

– Д1 - рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

– Д2 - рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

– Д3 - рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

– Д4 - рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

– Д5 - критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Всі ресурси обробляються працівниками підприємства - 1 менеджер, 2 розробника, 1 тімлід, 1 HR, 1 директор.

Вся текстова документація прибирається на склад під ключ, до якого тільки має доступ лише директор. Електронні дані записуються на жорсткі диски ємністю 2 ТБ і розміщуються на 5 різних стійках (закритих). Усі дані щодня підтримуються на цих дисках, а також щодо розподіленого сховища OneDrive.

Дані про клієнтів (фізичну особу) менеджер узгоджує з клієнтом зобов'язання (запит), потім, у цей момент, вводить їх у інформацію у системи (CRM, ERP, Printofбce24) і надсилає дані керівнику, як правило, друковані. Зберігаються їх на стелажі в закритому сейфі.

Дані працівника (індивідуальні) обробляються директором і можуть бути роздруковані. Зберігаються на стелажі в закритому сейфі.

Результати діяльності – інформація та звіти про результати (зміни, розрахунки, експертиза тощо), матеріали про проекти, планування архітектури та покращень – під час виконання завдання група та інженери постійно зберігають

результати на певному етапі та подають для директора звіти. Після розгортання кожного з проектів, завершений проект переміщується до клієнта та зберігається в електронному вигляді на стійках у закритому закритому сейфі.

Клієнти самі звертаються до компанії (реклама) або менеджери самі знаходять потенційних клієнтів (спеціальні платформи, аналіз та опрацювання нових компаній та підприємств); клієнт звертається до компанії з своїм проектом/ідеєю до менеджера компанії з яким ведуться переговори з приводу проекту (мета, ціль, розвиток, потенціал та прибуток) та його можливостей. Клієнта вносять в програми (CRM, ERP, Printofбce24). Усі супровідні дані про підприємство та власну інформацію клієнти надсилають на корпоративну пошту. Після ознайомлення з завданням директор набирає його, розробляє план роботи та встановлює терміни виконання період вивчення ринку, період створення моделі проекту, корективи, графічна робота, корективи, побудова фінальної моделі та виведення результатів на ринок). 3 клієнтом також зв'язуються директор та менеджер та створюють договір, після якого клієнт вносить повну оплату проекту (під час проекту можуть виникати додаткові витрати, про які інформують клієнтів). Менеджери працюють над проектом, використовуючи певне ПЗ. При кожному етапі відтворення проекту, директор та тімлід вносять корективи. Для конкретного проекту створюють свої терміни для кожного етапу, під час яких з клієнтом підтримується зв'язок (інформується по виконанню певного етапу та його результатів) через sales-менеджера (Google Meet). Клієнти також можуть вносити свої корективи. Для коректівів проекту на кожній стадії він може друкуватися принтерами, які локально підключені до кожного директор та HR. Після завершення проекту директор тримає зв’язок із клієнтом для підтвердження результатів та у ролі допомоги для правильного просування проекту у ринок.

Схема інформаційних потоків надана на рисунку 2.1.

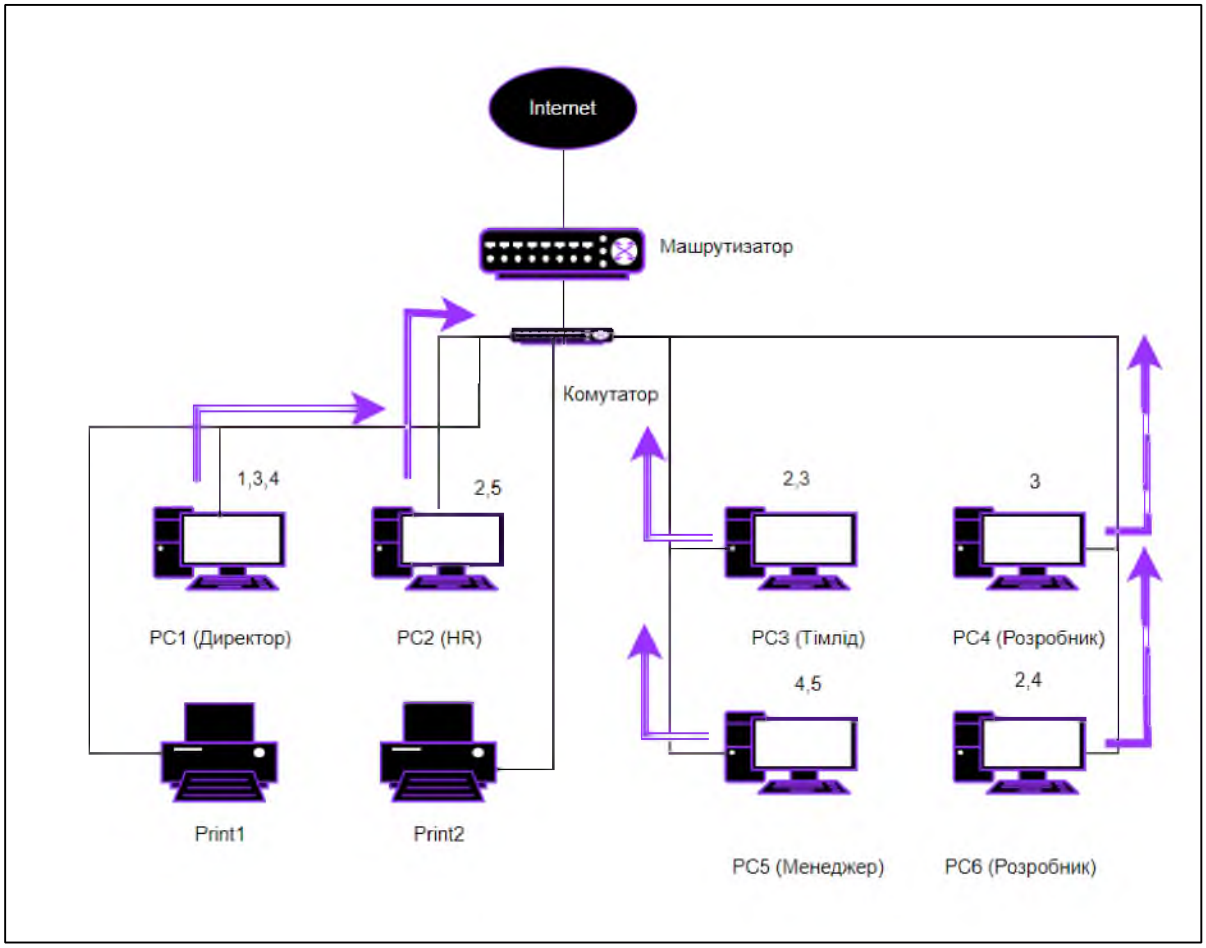

Рисунок 2.1 — Схема інформаційних потоків

Інформаційні потоки:

1. Обробка інформації про клієнтів
2. Обробка інформація про працівників
3. Обробка продуктів роботи підприємства
4. Обробка договорів

2.2 Аналіз існуючої системи відеонагляду

У цьому розділі проводиться детальний аналіз існуючої системи відеонагляду на підприємстві FullNet. Система відеонагляду є ключовим компонентом загальної системи безпеки, забезпечуючи візуальний контроль над територією та внутрішніми просторами підприємства.

Опис системи

Існуюча система відеонагляду складається з наступних елементів:

1. Камери спостереження: Підприємство оснащене 40 камерами відеонагляду, які розміщені на стратегічних точках, включаючи входи/виходи, коридори, зони виробництва та складські приміщення. Камери включають в себе як стандартні, так і камери з підтримкою інфрачервоного освітлення для нічного спостереження.
2. Сервери запису: Відеозаписи зберігаються на локальних серверах з обмеженим доступом. Відеоархів містить записи за останні 30 днів.
3. Система управління: Для контролю та управління системою використовується централізоване програмне забезпечення, яке дозволяє переглядати живий відеопотік, а також доступ до архівних записів.

Аналіз ефективності

1. Покриття території: Більшість ключових зон на підприємстві покриваються системою відеонагляду, проте існують "сліпі зони", де спостереження відсутнє, що може становити потенційний ризик безпеки.
2. Якість зображення: В цілому, якість зображення задовільна, але деякі камери, особливо ті, що працюють у нічний час, мають низьку роздільну здатність, що ускладнює ідентифікацію осіб або предметів.
3. Система зберігання та доступу: Хоча сервери запису є надійними, відсутність хмарного зберігання або віддаленого доступу обмежує можливості оперативного реагування на інциденти поза місцем.

Проблеми та рекомендації

1. Оновлення обладнання: Рекомендується оновити застарілі камери, особливо ті, що працюють в нічний час, до моделей з вищою роздільною здатністю та кращими можливостями нічного бачення.

2. Вдосконалення покриття: Необхідно збільшити кількість камер для усунення "сліпих зон" та забезпечення повного візуального контролю над територією підприємства.
3. Інтеграція з хмарними технологіями: Впровадження хмарного зберігання та віддаленого доступу дозволить оперативно реагувати на безпекові інциденти та забезпечити більш ефективне управління відеоархівами.

Загальний висновок

Існуюча система відеонагляду на підприємстві FullNet відіграє важливу роль у забезпеченні безпеки, проте потребує ряду удосконалень. Оновлення обладнання, покращення покриття та впровадження сучасних технологій збільшать ефективність системи та забезпечать вищий рівень захисту інформаційних ресурсів підприємства.

2.3 Аналіз і розгляд відеопотоків підприємства

Цей розділ присвячений аналізу та оцінці відеопотоків на підприємстві FullNet. Відеопотоки є критичною частиною системи безпеки, оскільки вони забезпечують візуальне спостереження та контроль за діяльністю на території підприємства.

Опис відеопотоків

Відеопотоки підприємства включають:

1. Живі трансляції: Камери надають живі відеопотоки з критичних локацій на території підприємства, що дозволяє оперативно відстежувати поточну ситуацію та швидко реагувати на нестандартні ситуації.
2. Записи: Відеозаписи зберігаються на серверах для подальшого перегляду та аналізу. Записи можуть використовуватися для розслідування інцидентів, аналізу робочих процесів тощо.

Аналіз ефективності

1. Якість відеопотоку: Якість відеопотоку є задовільною в більшості випадків, однак в деяких зонах, особливо в умовах низької освітленості, якість знижується, що може ускладнювати ідентифікацію осіб або предметів.
2. Час зберігання записів: Поточний період зберігання відеозаписів становить 30 днів. Для деяких сценаріїв безпеки та аналізу цей термін може бути недостатнім.
3. Доступність та управління: Система управління відеопотоками є ефективною для перегляду живих трансляцій та архівних записів, але має обмежену функціональність щодо швидкого пошуку та аналізу відеоматеріалів.

Проблеми та рекомендації

1. Оновлення камер: Рекомендується замінити застарілі камери на більш сучасні моделі з вищою роздільною здатністю, особливо для зон з низьким рівнем освітленості.
2. Покращення системи зберігання: Розглянути можливість збільшення терміну зберігання відеозаписів або впровадження хмарних технологій для гнучкого зберігання та архівування даних.
3. Розширення функціоналу управління: Вдосконалення системи управління відеопотоками з використанням технологій штучного інтелекту для розширеного аналізу відеоданих, таких як автоматичне розпізнавання облич або інших важливих об'єктів.

Загальний висновок

Аналіз існуючої системи відеонагляду виявив ключові аспекти, які потребують удосконалення для забезпечення більш високого рівня безпеки на підприємстві FullNet. Оновлення обладнання, покращення систем зберігання та управління відеопотоками дозволять забезпечити ефективний моніторинг, швидке реагування на інциденти та краще розуміння повсякденних операцій на підприємстві.

2.4 Аналіз існуючих та можливих загроз, побудова моделі загроз

За результатами впливу на інформацію та систему її обробки, загрози поділяються на чотири класи:

1 Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування доступу до інформації.

2 Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.

3 Порушення доступності інформації (Д) - часткова або повна втрата працездатності системи, блокування доступу до інформації в результаті некоректних дій адміністраторів, технічного обслуговуючого персоналу.

4 Втрата уважності (керованості системою) (С) - порушення процедур ідентифікації та автентифікації адміністраторів або процесів і надання їм повноважень, втрата контролю за їх діяльністю, можливість відмови від отримання або пересилання повідомлень.

Потенційно загрози можуть завдати шкоди оброблюваної інформації, працівникам, клієнтам, технічним засобам і процесам. Загрози також можна поділити на:

- навмисні (Н);
- випадкові (В);
- природні (П).

Потрібно ідентифікувати як випадкові, так і навмисні джерела загроз. Загрози можуть бути ідентифіковані в загальному вигляді або за типами.

Таблиця 2.2

Модель загроз

№ з/п	Вид загрози	Можливий механізм реалізації	Джерело загрози	Наслідки	Ймовірність	Збитки
1	Катастрофа	Пожежа, повінь, землетрус, техногенні аварії	Зовнішнє середовище	Ц, Д	Середня	Високі
2	Хакінг	Виконання несанкціонованих дій(спроба ddos-атаки, фішинг тощо)	Зловмисник	К, Ц	Середня	Високі
3	Крадіжка	Крадіжка носія з ключовою інформацією	Зловмисник, співробітник.	К, Ц, Д	Висока	Високі
4	Вірусне зараження	Зараження кінцевого пристрою шкідливим програмним	Зловмисник співробітник	Ц	Висока	Середні

		забезпеченням				
5	Соціальна інженерія	Незаконне отримання конфіденційних даних	Зловмисник	К, Ц	Середня	Високі
6	Відмова в обслуговуванні	Виведення з ладу/пошкодження/перехід в нештатний режим роботи інформаційно-телекомунікаційної системи	Персонал, зловмисник, програма	Д	Середня	Низькі
7	Відмова в обслуговуванні	Виведення з ладу/пошкодження/ перехід в нештатний режим роботи апаратно-програмного	Персонал, зловмисник, програма	Д	Середня	Низькі

		забезпечення				
8	Недоліки	Помилки під час конфігурації, використання та підключення засобів захисті (міжмережеві екрани, системи попередження атак)	Апаратно-програмні комплекси	К, Д, Ц	Середня	Низькі
9	Комп'ютерна неграмотність	Помилкові дії персоналу	Персонал	К, Ц, Д	Висока	Низькі
10	Зловживання можливостями адміністраторів	Порушення правил, встановлених ролями користувачів	Персонал	К,Ц,Д,С	Середня	Середні
11	Відсутність	Використан	Зловмисн	К,Ц,Д,С	Висока	Середн

	антивірусів, наявність вільних каналів руху інформації.	ня вірусів для отримання або пошкодження даних	ик			і
12	Погано підібраний персонал; Низька заробітна плата та мотивації співробітників	Доступ до конфіденційних даних через співробітників	Зловмисник, персонал	К,Ц,Д,С	Низька	Високі
13	Використання системи в корисних цілях	Відсутність правил використання системи	Персонал	С	Середня	Середні
14	Використання системи в корисних цілях	Порушення правил розмежування доступу	Персонал	К,Д,Ц	Середня	Низькі

Якщо ідентифіковані загрози використають відповідні до них вразливості інформаційної безпеки, негативними наслідками для підприємства стануть порушення конфіденційності інформації, її цілісність та доступність. Подібні інциденти негативно вплинуть на ресурси підприємства та на всю роботу.

Через що будуть падіння репутації підприємства, старі клієнти відмовлятимуться від послуг , а нових залучати буду усе складніше.

2.5 Дослідження можливих методів захисту відеоінформації

У цьому розділі проводиться детальний аналіз та дослідження різних методів захисту відеоінформації на підприємстві FullNet. З огляду на зростаючу важливість відеоданих в комерційній та операційній діяльності, забезпечення їх безпеки є критичним аспектом загальної стратегії захисту інформації.

Методи захисту відеоінформації

1. Шифрування даних: Це один з найефективніших способів захисту відеоінформації. Шифрування забезпечує, що навіть у випадку несанкціонованого доступу до відеоданих, їх не можна буде використовувати або зрозуміти без відповідного ключа дешифрування.
2. Водяні знаки: Використання цифрових водяних знаків дозволяє вбудовувати в відео непомітну маркування, яка може використовуватися для ідентифікації джерела відео та запобігання його незаконному використанню.
3. Обмеження доступу та контроль: Встановлення строгих політик доступу до відеоархівів і регулювання прав на перегляд та копіювання відео є важливими для запобігання неавторизованому розповсюдженню.
4. Хмарне зберігання з шифруванням: Зберігання відеоданих у хмарі з використанням шифрування допомагає забезпечити їх безпеку та доступність, одночасно знижуючи ризики, пов'язані з фізичним зберіганням даних.
5. Регулярні бекапи та відновлення даних: Створення регулярних резервних копій допомагає запобігти втраті відеоданих у випадку технічних збоїв або кібератак.

Аналіз ефективності методів

1. Оцінка ризиків: Кожен із зазначених методів має свої сильні та слабкі сторони. Наприклад, шифрування є ефективним проти зовнішніх загроз, але може бути менш ефективним проти внутрішніх загроз.

2. Технічна впровадження: Використання сучасних технологій шифрування та хмарних рішень потребує значних технічних зусиль та інвестицій.
3. Вартість та ресурси: Реалізація цих заходів захисту може вимагати значних фінансових та ресурсних інвестицій з боку підприємства FullNet.

Рекомендації та напрямки розвитку

1. Комплексний підхід: Застосування комбінації різних методів захисту може забезпечити більш ефективний захист відеоінформації.
2. Інноваційні технології: Підприємству FullNet рекомендується розглянути впровадження інноваційних технологій, таких як штучний інтелект для автоматичного аналізу відеоданих та виявлення аномалій.
3. Постійне оновлення та навчання: Важливо постійно оновлювати системи безпеки відповідно до новітніх стандартів та забезпечувати регулярне навчання персоналу з питань кібербезпеки та захисту даних.

Загальний висновок

Аналіз можливих методів захисту відеоінформації виявив, що комплексний підхід, який включає шифрування, використання водяних знаків, обмеження доступу, хмарне зберігання та регулярні бекапи, може значно підвищити рівень захисту відеоданих на підприємстві FullNet. Залучення сучасних технологій та методів може забезпечити більш ефективне управління ризиками, пов'язаними з безпекою відеоінформації.

2.6 Впровадження методу доступу до відеоінформаціїї підприємства заснованого на використанні цифрових сертифікатів і ЦВК

Цей розділ присвячений впровадженню методу доступу до відеоінформації на підприємстві FullNet, який базується на використанні цифрових сертифікатів та центрів видачі ключів (ЦВК). Цей підхід має на меті підвищити безпеку відеоданих, обмеживши доступ до них через надійну систему аутентифікації та авторизації.

Принципи роботи методу

1. Цифрові сертифікати: Цифровий сертифікат - це електронний документ, який використовується для підтвердження володіння публічним ключем і ідентифікації власника сертифіката. В контексті відеоінформації, цифрові сертифікати забезпечують, що тільки авторизовані користувачі мають доступ до відеоданих.
2. Центри видачі ключів (ЦВК): ЦВК відповідають за видачу, управління та анулювання цифрових сертифікатів. Вони гарантують, що кожен цифровий сертифікат є унікальним і дійсним, та відповідає певному користувачу або пристрою.
3. Процес аутентифікації та авторизації: Коли користувач або система намагається отримати доступ до відеоданих, вони повинні пройти процес аутентифікації за допомогою свого цифрового сертифіката. Після успішної аутентифікації, система перевіряє права доступу користувача перед наданням доступу до відеоінформації.

Кроки впровадження

1. Вибір та налаштування ЦВК: Першим кроком є вибір надійного постачальника ЦВК та налаштування процесів видачі та управління цифровими сертифікатами.
2. Реєстрація користувачів і пристроїв: Всі користувачі та пристрої, які будуть мати доступ до відеоінформації, повинні бути зареєстровані в ЦВК для отримання відповідних цифрових сертифікатів.
3. Інтеграція з існуючою системою відеонагляду: Необхідно інтегрувати нову систему аутентифікації та авторизації з існуючою системою відеонагляду.
4. Тестування та оцінка системи: Перед впровадженням системи в експлуатацію, важливо провести ретельне тестування для переконання у її надійності та ефективності.

Переваги методу

1. Збільшення безпеки: Використання цифрових сертифікатів та ЦВК значно підвищує безпеку доступу до відеоданих, знижуючи ризик несанкціонованого доступу.
2. Контроль та відстеження: Цей метод дозволяє точно контролювати та відстежувати, хто має доступ до відеоінформації, та як вона використовується.
3. Гнучкість та масштабованість: Система може бути легко масштабована та адаптована до змін у структурі підприємства або його безпекових потреб.

Виклики та обмеження

1. Технічна складність: Впровадження такої системи може бути технічно складним та вимагати спеціалізованих знань.
2. Вартість: Розробка, налаштування та підтримка системи може бути фінансово витратною.
3. Залежність від постачальників: Існує залежність від зовнішніх постачальників ЦВК та потенційні ризики, пов'язані з безпекою та надійністю їх послуг.

Деталізація процесу впровадження

1. Розробка політик безпеки: Важливим аспектом впровадження є розробка та імплементація чітких політик безпеки, які включають процедури видачі, використання, анулювання та оновлення цифрових сертифікатів.
2. Навчання персоналу: Проведення навчальних сесій для співробітників щодо нової системи аутентифікації та безпеки відеоінформації є критично важливим для її ефективного використання.
3. Моніторинг та аудит: Система повинна включати засоби для моніторингу та аудиту доступу до відеоінформації, щоб забезпечити постійний контроль за дотриманням політик безпеки.

4. Підтримка та технічне обслуговування: Належне технічне обслуговування та підтримка системи є необхідними для забезпечення її стабільної та безперебійної роботи.

Оцінка ризиків та заходи їх мінімізації

1. Ризик компрометації ключів: Потрібно розробити ефективну систему управління ключами для запобігання їх втрати або компрометації.
2. Залежність від ЦВК: Підприємству необхідно мати план дій на випадок збоїв у роботі ЦВК або припинення їх послуг.
3. Адаптація до змін у технологіях: Система має бути гнучкою, щоб адаптуватися до швидких змін в технологіях та забезпечити довгострокову стійкість.

Переваги та потенційний вплив на бізнес

1. Підвищення довіри клієнтів та партнерів: Впровадження такої системи збільшить довіру клієнтів та бізнес-партнерів до підприємства, підкреслюючи його відданість захисту інформації.
2. Зниження юридичних ризиків: Ефективний захист відеоінформації допомагає знижувати ризик юридичних наслідків, пов'язаних з витоком або зловживанням даних.
3. Підвищення ефективності внутрішніх процесів: Захищений доступ до відеоінформації сприяє підвищенню ефективності операційних та управлінських процесів на підприємстві.

Заключення

Впровадження методу доступу до відеоінформації з використанням цифрових сертифікатів та ЦВК на підприємстві FullNet має потенціал значно підвищити рівень безпеки відеоданих. Це не тільки захистить важливу інформацію від несанкціонованого доступу, але й підсилить загальну стратегію безпеки підприємства. Втім, для успішного впровадження цього методу необхідно врахувати ряд технічних, організаційних та фінансових факторів.

2.7 Обов‘язки, права та рекомендації по роботі з системою відеоспостереження підприємства і по дотриманню правил доступу до відеоінформації, заснованого на використанні ЕЦП і ЦВК

2.7.1 Обов‘язки та права директора по роботі з відео інформацією, яка циркулює на підприємстві

У цьому розділі розглядаються ключові обов'язки та права директора, відповідального за роботу з відеоінформацією на підприємстві FullNet. Ця роль є важливою для ефективного управління, захисту та використання відеоданих, які мають велике значення для безпеки та операційної діяльності підприємства.

Основні обов'язки

1. Керування та нагляд: Директор несе відповідальність за керування всіма аспектами роботи з відеоінформацією. Це включає нагляд за збором, зберіганням, обробкою та передачею відеоданих.
2. Забезпечення захисту даних: Важливо забезпечити відповідність всіх процесів роботи з відеоінформацією стандартам безпеки, у тому числі шляхом впровадження відповідних методів захисту.
3. Розробка політик та процедур: Розробка та імплементація політик і процедур, що регулюють використання відеоінформації, включаючи доступ, архівацію, а також відповіді на інциденти безпеки.
4. Координація з іншими відділами: Взаємодія з іншими відділами та службами підприємства для забезпечення ефективної координації у роботі з відеоінформацією.

Права

1. Доступ до відеоінформації: Директор має право доступу до всіх відеоданих, що циркулюють на підприємстві, з метою нагляду та адміністрування.

2. Прийняття рішень: Має повноваження приймати рішення щодо використання, зберігання та захисту відеоінформації.
3. Делегування обов'язків: Можливість делегувати певні обов'язки пов'язані з відеоінформацією іншим співробітникам або відділам.
4. Вимога звітності: Право вимагати звітність від підлеглих або відповідальних осіб щодо стану відеоінформації та її обробки.

Проблеми та виклики

1. Збалансування конфіденційності та безпеки: Необхідно знайти баланс між забезпеченням безпеки даних та дотриманням норм конфіденційності та приватності.
2. Адаптація до змін у технологіях: Швидкий розвиток технологічного ландшафту вимагає постійної адаптації та оновлення знань та навичок у сфері захисту відеоінформації.
3. Координація з внешніми регуляторами: Потрібно враховувати законодавчі та регуляторні вимоги при роботі з відеоданими, забезпечуючи їх відповідність зовнішнім стандартам.

Заключення

Роль директора по роботі з відеоінформацією є вирішальною у забезпеченні безпеки та ефективності обробки відеоданих на підприємстві FullNet. Відповідальність, права та обов'язки цієї посади охоплюють широкий спектр діяльності, від технічного управління до розробки стратегій безпеки та політик. Ефективне виконання цих завдань вимагає не тільки технічних знань, але й управлінських та комунікативних навичок.

2.7.2 Обов‘язки та права адміністратора інформаційної безпеки по роботі з відео інформацією, яка ціркулює на оброном підприємстві

Адміністратор інформаційної безпеки грає ключову роль у захисті відеоінформації на оборонному підприємстві, такому як FullNet. Ця роль вимагає

високого рівня компетентності та відповідальності, оскільки вона зосереджена на забезпеченні конфіденційності, цілісності та доступності відеоданих.

Основні Обов'язки

1. Забезпечення Захисту Відеоданих: Встановлення та підтримка належних заходів безпеки для захисту відеоінформації від несанкціонованого доступу, витоку, зміни, знищення або втрати.
2. Моніторинг та Відповідь на Інциденти: Постійний моніторинг системи відеонагляду для виявлення та своєчасного реагування на інциденти безпеки.
3. Оновлення Політик Безпеки: Розробка та оновлення внутрішніх політик і процедур, пов'язаних з обробкою та зберіганням відеоінформації, забезпечуючи їх відповідність сучасним стандартам безпеки та законодавчим вимогам.
4. Координація з Іншими Відділами: Тісна співпраця з іншими відділами, зокрема з IT-департаментом та службою безпеки, для забезпечення інтегрованого підходу до захисту відеоінформації.

Права

1. Доступ до Відеоінформації: Адміністратор має повний доступ до всіх відеоданих, що обробляються на підприємстві, для виконання своїх обов'язків з моніторингу та аудиту.
2. Прийняття Рішень щодо Заходів Безпеки: Має право ініціювати та затверджувати заходи безпеки, необхідні для захисту відеоінформації.
3. Проведення Аудитів та Інспекцій: Може ініціювати аудити та інспекції системи відеонагляду для оцінки її ефективності та відповідності стандартам безпеки.

Виклики та Ризики

1. Комплексність Технологій: Робота з відеоінформацією на оборонному підприємстві часто включає у себе складні технологічні системи, що вимагають постійного оновлення знань та навичок.
2. Забезпечення Приватності: Необхідно дотримуватися законодавчих та етичних норм щодо приватності, особливо при обробці відеоданих, що можуть містити особисту інформацію.
3. Відповідальність за Інциденти Безпеки: Висока відповідальність за наслідки будь-яких інцидентів безпеки, пов'язаних з відеоінформацією.

Заключення

Посада адміністратора інформаційної безпеки є критично важливою для забезпечення захисту відеоінформації на оборонному підприємстві. Ефективне виконання цієї ролі вимагає не тільки технічних знань, але й розуміння правових та етичних аспектів, а також вміння швидко реагувати на зміни в технологіях та загрозах безпеки.

2.7.3 Обов'язки та права охоронця по роботі з відео інформацією підприємства

Охоронець, відповідальний за безпеку відеоінформації на підприємстві FullNet, відіграє важливу роль у забезпеченні фізичної та технічної безпеки відеоданих та системи відеонагляду. У цьому розділі розглядаються його основні обов'язки та права.

Основні обов'язки

1. Фізична безпека: Забезпечення фізичної безпеки систем відеонагляду та зберігання відеоінформації. Це включає в себе контроль доступу до обладнання та місць зберігання відеоданих.
2. Моніторинг та реагування на інциденти: Постійний моніторинг відеопотоків та реагування на події, які можуть загрожувати безпеці об'єктів або відеоінформації.

3. Співпраця з охороною: Взаємодія з охоронною службою підприємства для забезпечення загальної безпеки та координації заходів у разі інцидентів.
4. Запобігання саботажу та витоку даних: Запобігання можливим актам саботажу системи відеонагляду та витоку конфіденційної відеоінформації.

Права

1. Доступ до відеоінформації: Охоронець має право доступу до відеоданих та систем відеонагляду для виконання своїх обов'язків.
2. Прийняття рішень щодо заходів безпеки: Має право приймати рішення щодо заходів безпеки, включаючи евакуацію або блокування доступу до об'єктів у разі загрози.
3. Проведення перевірок: Може здійснювати перевірки на дотримання правил безпеки та внутрішніх процедур у сфері відеонагляду.

Виклики та ризики

1. Навчання та компетентність: Охоронець повинен мати необхідні знання та навички для ефективного виконання завдань забезпечення безпеки відеоданих.
2. Взаємодія з персоналом: Важливо підтримувати взаємодію та співпрацю з іншими співробітниками підприємства для досягнення спільних цілей безпеки.
3. Ефективність реакції: Реагування на інциденти безпеки повинно бути швидким і ефективним, оскільки від цього залежить мінімізація можливих збитків.

Заключення

Охоронець, відповідальний за безпеку відеоінформації на підприємстві FullNet, виконує важливу місію забезпечення захисту відеоданих та системи відеонагляду. Його обов'язки та права націлені на забезпечення безпеки об'єктів, протидію саботажу та витоку даних, а також на оперативну реакцію на будь-які загрози безпеці підприємства.

2.8 Висновки до розділу 2

У цьому розділі був проведений аналіз існуючої системи відеонагляду підприємства FullNet, розглянуті основні аспекти роботи з відеопотоками, виявлені можливі загрози та розглянуті методи захисту відеоінформації. Отримані результати дозволяють зрозуміти важливість впровадження ефективних заходів безпеки в цій сфері.

Аналіз існуючої системи відеонагляду показав, що вона є важливою складовою інфраструктури підприємства, забезпечуючи безпеку та контроль за подіями на об'єктах. Однак існують певні недоліки, такі як обмежена можливість обробки великих обсягів відеоданих та вразливість до потенційних загроз.

Аналіз і розгляд відеопотоків підприємства дозволив визначити різноманітність відеоданих та їх значення для різних підрозділів підприємства. Це підкреслює важливість забезпечення конфіденційності та цілісності цих даних.

Аналіз існуючих та можливих загроз показав, що відеоінформація підприємства піддається різноманітним загрозам, включаючи несанкціонований доступ, виток даних та саботаж. Важливо приділити належну увагу заходам безпеки для запобігання цим загрозам.

Дослідження можливих методів захисту відеоінформації вказує на необхідність використання комплексного підходу, який включає в себе використання криптографії, стеганографії, DRM-технологій, ЕЦП та моделей управління доступом. Ці методи дозволять забезпечити конфіденційність, цілісність та доступність відеоінформації.

Усі ці аспекти демонструють важливість впровадження ефективних заходів безпеки в сфері відеонагляду підприємства FullNet. Досягнення цієї мети вимагатиме спільних зусиль технічних та адміністративних підрозділів підприємства та розробки комплексної системи захисту відеоінформації.

РОЗДІЛ 3
ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ РОЗРОБКИ ПОЛІТИКИ БЕЗПЕКИ

3.1 Економічне обгрунтування доцільності впровадження політики безпеки інформації

Для економічного обгрунтування доцільності розробки політики безпеки інформації ТОВ «FullNet» потрібно провести розрахунки, щоб визначити економічну ефективність використання основних результатів, які будуть отримані після розрахунків.

Економічна доцільність визначається:

- розрахунками капітальних витрат, що потребує розроблена політика безпеки;
- розрахунками експлуатаційних витрат;
- розрахунками річного економічного ефекту від розробки інформаційної політики безпеки.

3.1.1 Розрахунок суми витрат на розробку політики безпеки інформації

Спочатку розраховуеться трудомістшсть розробки політики безпеки інформації, для цього потрібно скласти час, який знадобиться для кожної робочої операції:

$t = tmз + tв + ta + tвз + tозб + tовр + tд$, годин, де

- tmз - тривалість складання ТЗ на розробку ПБІ = 40 годин;
- tв - тривалість розробки концепції безпеки інформації у організації = 20 годин;
- ta - тривалість процесу аналізу ризиків = 26 годин;

- tак - тривалість визначення вимог заходів, методів та засобів захисту = 8 годин;
- tозб - тривалість виробу основних рішень з забезпечення БІ = 46 годин;
- tовр - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 110 години;
- tд - тривалість документального оформлення політики безпеки = 10 годин.

t = 40 + 20 + 26 + 8 + 46 + 110 + 10 = 270 годин.

3.1.2 Розрахунок суми витрат на реалізацію політики безпеки інформації.

Сума витрат на розробку політики безпеки {Kpn) складається з витрат на:

- Заробітну плату спеціаліста з кібербезпеки — Ззп, грн;
- Вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації — Змч.

Kpn = Ззп + Змч = 22911 грн

Заробітна плата спеціаліста складається з основної та додаткової заробітної плати, соціальних виплат та визначається за формулою:

Ззп = t * Зіб = 20250,00 грн

де t — загальна тривалість розробки політики безпеки інформації = 270 годин;

Зіб — середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями = 12000 / 160 = 75, грн/годину

Вартість машинного часу для розробки політики безпеки інформації на ІТК визначається за формулою:

Змч = t * Смч = 2661 грн

де t — трудомістшсть підготовки документації на ІТК =4 години;

Смч — вартість 1 години машинного часу ПК, грн./година (5,6 грн).

Відповідно до розроблених рекомендацій, планується використання ліцензійних програмних засобів, як вже встановлених, так і нових.

Розрахована вартість розробки політики безпеки інформації Крп ь складовою одноразових капітальних витрат разом з витратами на придбання програмних засобів, як рекомендовані для використання.

Отже фіксована сума капітальних витрат на розробку політики безпеки інформації складае:

К = Крп + Кзпз + Каз + Кнавч + Кн = 56911 грн.

К = 22911 + 11150 + 7850 + 9400 + 5600 = 56911 грн

де *К* — вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх спеціалістів, тис. грн;

Кзпз — вартість закупівлі ліцензійного основного і додаткового програмного забезпечення (ПЗ), тис. грн;

Крп — вартість розробки політики безпеки інформації, тис. грн;

Каз — вартість закупівлі апаратного забезпечення та допоміжних матеріалів,

Кнавч вартість витрати на навчання технічних фахівців і обслуговуючого персоналу = 5600 грн;

Кн — витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

3.2 Оцінка можливого збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

tn — час простою вузла або сегмента корпоративної мережі внаслідок атаки, 1 година;

tв — час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

tви — час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі 2 години;

Зо — заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 5500 грн./міс.;

Зс — заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 11000 грн./міс.;

Чо — чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

Чс — чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 7 осіб.;

О — обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 2 млн грн. у рік;

Пзч — вартість заміни устаткування або запасних частин, грн; I — число атакованих сегментів корпоративної мережі, 1;

N — середнє число атак на рік, 10.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

U=Пп +Пв +V=11740,4,

де Пп — оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

Пв — вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V — втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} * t_n,$$

Пп = ((11000 *7)/176)*3 = 1312,5 грн,

де F — місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:

Пви = ((11000 *7)/176)*4 = 1750 грн,

Витрати на заміни устаткування або запасних частин можуть скласти 3200

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

Пв = 1312,5 + 1750 + 125 = 1875 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

В = 1 * 14 * 13764,4 = 192700 грн.

3.3 Розрахунок економічного ефекту

Економічний ефект в сфері проектування рішення:

$$Е_{пр}=Ц_а-Ц_п \qquad (3.21)$$

$Е_{пр}$ = 65000,0 – 56911,6 = 8089,4 грн.

Річний економічний ефект в сфері експлуатації:

$Е_{кс}=В_{еа}-В_{еп}$

$Е_{кс}$ = 24544,8 - 16354,8 = 8190 грн.

Додатковий економічний ефект у сфері експлуатації:

$$\Delta E_{ekc} = \sum_{t=1}^{T} E_{ekc}(1+R)^{T-t}$$

$$\Delta E_{ekc} = \sum_{t=1}^{5} 8190 * (1+0{,}16)^{5-t} = 56323.7 \text{ грн.}$$

Сумарний ефект складає:

$$E = E_{пр} + \Delta E_{ekc} = 414{,}4 + 56323.7 = 56738{,}1 \text{ грн}$$

Таблиця 3.1.

Показники економічної ефективності проектного рішення

№	Найменування	Одиниці вимірювання	Значення показників	
			Базовий варіант	Новий варіант

1	Капітальні вкладення	Грн.	-	3527,38
2	Ціна придбання	Грн.	5000,0	4585,6
3	Річні експлуатаційні витрати	Грн.	5922,0	3956,4
4	Ціна споживання	Грн.	24544,8	16354,8
5	Економічний ефект в сфері проектування	Грн.	-	3588,4
6	Річний економічний ефект в сфері експлуатації	Грн.	-	8190
7	Додатковий ефект в сфері експлуатації	Грн.	-	56738,1
8	Сумарний ефект	Грн.	60362,5	

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

ROSI = E / K, частки одиниці

де — Е загальний ефект від впровадження системи інформаційної безпеки грн.; К — капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

56911,4 / 58911,4 = 0,97

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

Розрахункове значення коефіцієнта повернення інвестицій:

0,97 > 0,95

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

Т = 1/0,97 = 1.03 років.

Висновки до розділу 3

Розробка політики інформаційної безпеки для ТОВ «FullNet» є економічно доцільною, оскільки коефіцієнт повернення інвестицій ROSI складає 0,97, що означає отримання 0,97 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів.

ВИСНОВКИ

У даній роботі було проведено детальний аналіз та розгляд питань організації управління доступом до відеоінформації в інформаційно-комунікаційній системі підприємства FullNet. Робота охоплює важливі аспекти забезпечення безпеки відеоданих та розробки стратегій їх захисту.

Актуальність даної роботи визначається зростаючим обсягом відеоінформації, її цінністю для підприємств та організацій, а також зростаючими загрозами її безпеці. Забезпечення конфіденційності, цілісності та доступності відеоінформації стає важливою задачею в умовах сучасного інформаційного середовища.

Метою дослідження було розробити комплексні підходи до організації управління доступом до відеоінформації, включаючи використання криптографії, стеганографії, DRM-технологій, ЕЦП та моделей управління доступом. Отримані результати дозволяють зрозуміти важливість цих методів для забезпечення безпеки відеоданих.

В ході роботи було проведено аналіз існуючої системи відеонагляду підприємства FullNet, розглянуті аспекти роботи з відеопотоками та виявлені можливі загрози. Це дало змогу визначити необхідність вдосконалення системи відеонагляду та її захисту.

Дослідження можливих методів захисту відеоінформації вказує на необхідність комплексного підходу до розв'язання цієї проблеми. Використання криптографії, стеганографії, DRM-технологій, ЕЦП та моделей управління доступом дозволить забезпечити високий рівень захисту відеоінформації.

Усі ці аспекти демонструють важливість впровадження ефективних заходів безпеки в сфері відеонагляду підприємства FullNet. Досягнення цієї мети вимагатиме спільних зусиль технічних та адміністративних підрозділів підприємства та розробки комплексної системи захисту відеоінформації.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Статистика кібератак на підприємства [Електронний ресурс]. - Режим доступу https://techexpert.ua/cyber-attacks-number-statistics/

2. Статистика кібератак на малі підприємства за 2021 рік [Електронний ресурс]. - Режим доступу https://www.fundera.com/resources/small-business-cyber-security-statistics#

3. Інформація щодо IT компаній, які ведуть бізнес на території України [Електронний ресурс]. - Режим доступу https://jobs.dou.ua/ratings/

4. Закон України «Про інформацію» від 02.10.1992 No 2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація “інформації в законодавстві України”.

5. Закон України “Про захист персональних даних” від 01.06.2010 No 2297-VI// Відомості Верховної Ради України. - 2010. - No 5. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2297-17.

6. Закон України “Про доступ до публічної інформації” від 13.01.2011 No 2939- VI // Відомості Верховної Ради Україии. - 2011. - No 32. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2939-17.

7. Закон Україии “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 No80-VI // Відомості Верховної Ради України. -

8. 1994. - No 80. [Електронний ресурс]. - Режим доступу http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

9. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id doc=66911.

10. ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. - 2017. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id doc=66912.

11. НД ТЗІ 3.7-003 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. - [Чинний від 08.11.2005] - К. ДССЗЗІ, 2005. - No125 - (Нормативний документ системи технічного захисту інформації).

12. НД ТЗІ 1.4-001 - Типове положення про службу захисту інформації в автоматизованій системі. - [Чинний від 04.12.2000] - К. : ДСТСЗІ СБУ, 2000. - No53 - (Нормативний документ системи технічного захисту інформації).

13. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).

14. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).

15. НД ТЗІ 1.6-005 - Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної темниці. - [Чинний від 15.04.2013] - К. : ДССЗЗІ, 2013. - No125 - (Нормативний документ системи технічного захисту інформації).

16. Етапистворення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу:http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive- zavdannya-sogodennya/.

17. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/Упоряд. Д. П. Пілова. Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.

18. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека / О.В. Герасіна, Д.С.Тимофеев, О.В. Кручинін, Ю.А.Мілінчук Дніпро: НТУ "ДП", 2020. 47 с.

19. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).

20. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).

21. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2-004-99. — Київ: ДСТСЗІ СБ України, 1999. — 55 с.

22. Інформація щодо середньої заробітної плати спеціаліста з кібербезпеки. [Електронний ресурс]. - Режим доступу https://ua.trud.com/ua/salary/2/67683.html

23. Актуальні ціни на електроенергію [Електронний ресурс]. - Режим доступу https://yasno.com.ua/b2c-tariffs

24. Середня заробітна плата спеціаліста з кібербезпеки [Електронний ресурс]. - Режим доступу https://ua.trud.com/ua/salary/2/67682.html

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	1 Розділ	25	
5	А4	2 Розділ	22	
6	А4	3 Розділ	9	
7	А4	Висновки	1	
8	А4	Перелік посилань	3	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	

ДОДАТОК Б. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

Романюк_Е.О._125м-22-2.docx

Романюк_Е.О._125м-22-2.pptx

Романюк_Е.О._125м-22-2.pdf

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 74 б. («добре»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

Відгук

на кваліфікаційну роботу студента групи 125м-22-2 Романюк Едуарда Олександровича на тему: «Організація управління доступом в інформаційно-комунікаційній системі підприємства FullNet»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 64 сторінці.

Метою кваліфікаційної роботи є підвищення рівня захисту відеоінформації, яка циркулює на підприємстві .

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз відеоінформації, яка циркулює на підприємстві, а також впровадження методу доступу до відеоінформації підприємства заснованого на використанні цифрових сертифікатів і ЦВК.

Розроблені комплексні підходи до організації управління доступом до відеоінформації.

Практичне значення результатів кваліфікаційної роботи полягає у розробці методів захисту відеоінформації для підприємства галузі розробки ПЗ та консультації з приводу розробки ПЗ та комп'ютерних технологій.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Романюк Е.О. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему запобігання та виявлення плагіату НТУ «Дніпровська політехніка»".

Кваліфікаційна робота заслуговує оцінки «74»(добре).

Керівник роботи _____ _____

(підпис) (ініціали, прізвище)