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 *Колєснік Марини Олександрівни*

академічної групи *125м-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз ризиків кібербезпеки в IP-системах корпоративного відеоспостереження*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. д. ф-м. н. Кагадій Т.С.			
розділів:				
спеціальний	ас. Мілінчук Ю.А..			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Колєснік М.О.* **академічної групи** *125м-19-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*
спеціалізації[1] _____
за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз ризиків кібербезпеки в IP-системах корпоративного відеоспостереження*

Затверджено наказом ректора НТУ «Дніпровська політехніка» від 22.10.2020 № 888-с

Розділ	**Найменування етапів робіт**	**Строки виконання робіт** (початок-кінець)
1	Виконання аналізу систем відеоспостереження	01.09.20-01.10.20
2	Виконання аналізу проблем систем	02.10.20-31.10.20
2	Розробка контрзаходів	01.11.20-14.11.20
3	Виконання економічного розділу	15.11.20-30.11.20
	Оформлення пояснювальної записки	01.12.20-05.12.20

Завдання видано _____ проф. д.ф. – м.н. Кагадій Т.С..
(підпис керівника) (прізвище, ініціали)

Дата видачі: 01.09.20р.

Дата подання до екзаменаційної комісії:

Прийнято до виконання _____ Колєснік М.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 62с., 7рис., 9 табл., 20 джерел.

Об’єкт дослідження: IP-системи відеоспостереження.

Предмет дослідження: методи та заходи захисту IP-систем від кіберзагроз.

Мета дипломної роботи: дослідження та удосконалення захисту інформації у IP-системах відеоспостереження.

У першому розділі дипломної роботи проаналізовано види систем відеонагляду, наведена їх класифікація, представлені способи збереження інформації, а також наведено основні проблеми захисту даних у систем відеонагляду.

У спеціальній частині дипломної роботи проаналізовані основні проблеми захисту даних, наведені види атак та їх класифікація, розроблена модель порушника системи, розроблені контрзаходи та методика протидії виділеним атакам, надані рекомендації для безпечного користування IP-системами відеонагляду.

У економічній частині були розраховані витрати на реалізацію методики, щодо безпечного зберігання та передачі інформації у IP-системах.

IP-СИСТЕМ ВІДЕОНАГЛЯДУ, АТАКА, ВРАЗЛИВІСТЬ, ЗАГРОЗИ, ХМАРНІ НОСІЇ, КАНАЛИ ПЕРЕДАЧІ ІНФОРМАЦІЇ.

РЕФЕРАТ

Пояснительная записка: 62с., 7рис., 9 табл., 20 источников.

Объект исследования: IP-системы видеонаблюдения.

Предмет исследования: методы и способы защиты IP-систем от киберугроз.

Цель дипломной работы: исследования и усовершенствования защиты информации в IP-системах видеонаблюдения.

В первой главе дипломной работы проанализированы виды систем видеонаблюдения, приведена их классификация, представлены способы хранения информации, а также приведены основные проблемы защиты данных в систем видеонаблюдения.

В специальной части дипломной работы проанализированы основные проблемы защиты данных, приведены виды атак и их классификация, разработанная модель нарушителя системы, разработанные контрмеры, разработаны методики противодействия выделенным атакам, даны рекомендации для безопасного пользования IP-системами видеонаблюдения.

В экономической части были рассчитаны затраты на реализацию методик, по безопасному хранению и передаче информации в IP-системах.

IP-СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ, УЯЗВИМОСТЬ, АТАКА, УГРОЗА, КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ.

ABSTRACT

Explanatory note: 62p., 7pic., 9 tab., 20 sources.

Object of research: IP video surveillance systems.

Subject of research: methods and ways to protect IP systems from cyber threats.

The purpose of the thesis: research and improvement of information security in IP-video surveillance systems.

In the first chapter of the thesis, the types of video surveillance systems are analyzed, their classification is given, methods of storing information are presented, and the main problems of data protection in video surveillance systems are presented.

In the special part of the thesis, the main problems of data protection are analyzed, the types of attacks and their classification, the developed model of the system intruder, the developed countermeasures, the methods of countering selected attacks are developed, and the recommendations for the safe use of IP video surveillance systems are given.

In the economic part, the costs were calculated for the implementation of techniques for the safe storage and transmission of information in IP systems.

SECURITY OF OPERATION OF IP-VIDEO SURVEILLANCE SYSTEMS, INFORMATION TRANSMISSION CHANNELS.

ЗМІСТ

ВСТУП

На даний момент системи відеоспостереження стали невід'ємною частиною життя і широко поширені в усьому світі. Найголовніша причина використання систем відеоспостереження - це прагнення підвищити рівень безпеки і захищеності людей і об'єктів приватної власності. Слід сказати, що камери досягли великого успіху в забезпеченні безпеки: тільки факт присутності камер відеоспостереження на об'єкті може відлякати злочинця. Але якщо злочин все ж мало місце бути, то наявні записи з камер допоможуть надати допомогу в затриманні і впізнання зловмисника. Бажання захистити приватну власність і свою сім'ю вимагає застосування найсучасніших систем безпеки.

Але забезпечення безпеки не єдина область застосування систем відеоспостереження. Велика і мала промисловість все більше потребує надійних і автоматизованих засобах контролю і управління технологічними процесами і людьми. За допомогою системи відеоспостереження стає можливим контролювати і управляти багатьма технологічними та виробничими процесами, особливо тими, де немає прямого контролю людиною.

В останні 3 роки системи відеоспостереження все більше використовуються в різних галузях. Вони застосовуються лікарнями для постійного спостереження за тяжкохворими пацієнтами, освітніми установами для контролю студентів і учнів, магазинами для спостереження за покупцями і припинення спроб крадіжок, муніципальними властями і УВС для спостереження в громадських місцях, в транспорті, місцях відпочинку і розваг, банківськими структурами та т.д.

РОЗДІЛ 1. АНАЛІЗ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

1.1 Історія виникнення систем відеоспостереження

Відео, як таке та, взагалі, поєднання декількох сталих зображень на послідовність кадрів — винахід сучасний, початку XX століття. У 1907 році було видано першу у світі заявку на патент у сфері відео, а саме «Спосіб електричної передачі зображення». А 1911 року фізик Борис Розінг в своїй лабораторії прийняв зображення найпростіших фігур з конструйованою ним, електронно-променевою трубкою (кінескопом). Однак, найважливішим винаходом, який допоміг перейти від механічного телебачення до електронного, став іконоскоп, який було винайдено 1931 року інженером Володимиром Зворикіним, коли він керував лабораторією електроніки Radio Corporation of America в еміграції у Сполучені Штати Америки.

1932 року, за допомогою іконоскопа з передавача потужністю 2,5 кВт, встановленого на хмарочосі Empire State Building, почалися перші пробні передачі електронного телебачення. Іконоскоп Зворикіна складався з вакуумної скляної колби, усередині якої закріплені світлочутлива мішень, на яку об'єктивом проектується зображення, і електронна гармата, розміщена збоку або знизу від об'єктива. Зображення в іконоскопі потрапляє на пластину з мозаїкою фотоелементів, ізольованих один від одного. В ті часи, цю мозаїку створювали зі слюди з фоточутливим шаром цезію. Володимир Кузьмович під час досліджень удосконалив метод. Тонку срібну плівку, під його керівництвом обпекли на слюді, щоб вона згорнулася в безліч дрібних крапель. В пластині іконоскопа (6х10 см) використовується 1 200 000 таких крапель. Кожна крапля представляє собою своєрідний фотоелемент. При освітленні мішені, під дією фотоефекту краплі срібла набувають позитивний заряд, пропорційний освітленості.

Зворикін, окрім наукових досліджень для бізнесу, також намагався розвивати власний військовий проект, так звану «повітряну торпеду з електронним оком», тобто керовану зброю. Для демонстрації концепції, він у 1937 році поставив великий іконоскоп на літак і пустив його літати навколо статуї

Свободи. Експеримент, загалом, видався вдалим і вдалося зняти відео статуї Свободи згори, але проект, у підсумку, був визнаний провальним — відеосигнал легко глушився противником, зате попутно Повітряні та Військово-морські сили США отримали кілька систем телевізійної розвідки.

1.2 Система відеоспостереження

Система відеоспостере ження — система передачі інформації з відеокамер, телевізійних камер на обмежену кількість моніторів та/або записувальних пристроїв (рис 1.1).

Відмінність систем відеоспостереження від телевізійного мовлення полягає у тому, що сигнал не передається у відкритому режимі. Системи відеоспостереження часто використовуються для спостереження у місцях, які потребують постійного нагляду, таких як банки, банкомати, казино, вокзали, аеропорти, військові об'єкти та звичайні крамниці тощо.

На промислових об'єктах камери спостереження можуть використовуватись для централізованого стеження за виробничим процесом, або, у разі наявності середовища, небезпечного для людини . Системи відеоспостереження можуть знімати безперервно, або вмикатись лише за заданою подією. Досконаліші системи стеження, з використанням відеореєстраторів, дозволяють створювати записи, які зберігатимуться роками, з різною якістю та з додатковими можливостями (такими як виявлення рухів та оповіщення через електронну пошту).

Відеоспостереження за громадськими місцями, особливо поширене у Великій Британії, де оцінна кількість камер до населення, найбільша серед країн світу. Використання відеоспостереження підсилило дебати про баланс між захистом приватності та безпекою.

Водночас, системи відеоспостереження поділяються на дротові та бездротові.

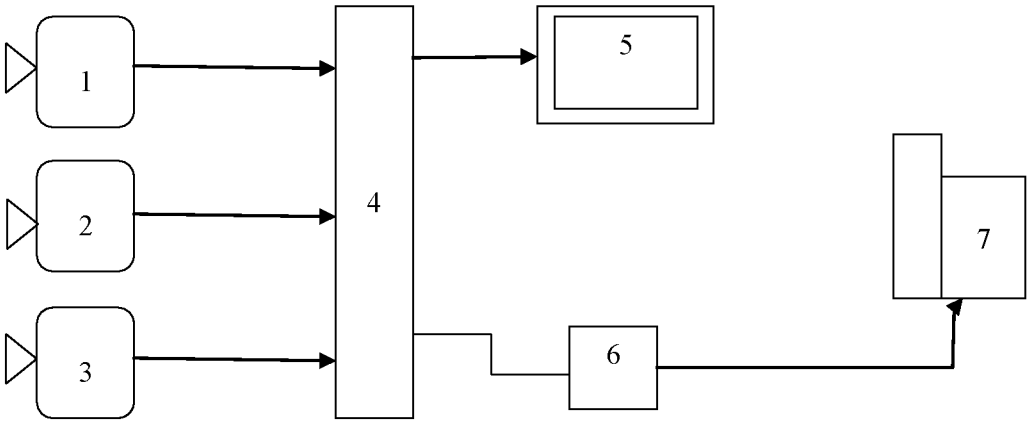

Рисунок 1.2 – Схема системи відеонагляду

Данна схема складається з:

1- Камера;

2- Камера;

3- Камера;

4- Відеорегістратор;

5- Монітор;

6- Комутатор;

7- Компьютер;

1.3 Класифікація систем відеонагляду

1.3.1 Аналогове відеоспостереження

Аналогові камери відеоспостереження (рисунок 1.2) - це пристрої, які через коаксіальний кабель передають відео в форматі аналогового сигналу в відеореєстратор. Після отримання відеореєстратором аналогового сигналу, відео оцифровується і записується в архів.

Переваги:

- Вартість: аналогові відеокамери спостереження, як правило, коштують дешевше, ніж IP-камери.
- Простота використання: установка, налаштування і експлуатація аналогових систем досить прості для розуміння і використання професіоналами.

- Обсяг даних: оскільки аналогові камери відправляють файли за коаксіальним кабелем, вони зазвичай займають меншу ємність.
- Широкий вибір продукції: оскільки аналогові камери вже давно є галузевим стандартом, випущено безліч варіантів для різних завдань і різного бюджету.

Недоліки:

- Додаткові кабелі: оскільки всі аналогові пристрої мають отримувати живлення за окремим кабелем, а підключатися до цифрового відеореєстратора за допомогою іншого, кабельної продукції знадобиться значно більше. Коаксіальні кабелі також, як правило, коштують дорожче, ніж кабелі для IP-систем відеоспостереження.
- Якість відео: навіть найкраща аналогова камера не може конкурувати з IP-камерою найнижчої якості. При збільшенні зображення може виявитися зернистим і непридатним для використання з метою ідентифікації.
- Охоплення: аналогові камери спостереження не забезпечать такого широкого поля огляду, як більш високотехнологічні мережеві відеокамери, тому їх знадобиться більше.
- Обмеження розміщення: чим далі камера відеоспостереження знаходиться від відеореєстратора, тим менш надійним є з'єднання.
- Обмежена кількість портів: відеореєстратор має обмежену кількість відео-входів, тому, можливо, вам доведеться обмежити себе в кількості відеокамер або купити додатковий відеореєстратор.

Рисунок 1.3.1 – Типова схема підключення аналового відеоспостереження

Данна схема складається з:

Таблиця 1.1 – умовні позначення до рисунку 1.3.1

№	Зображення	Назва
1		Камера1
2		Камера2
3		Блок живлення
4		Відеорегістратор
5		Монітор
6		Роутер
7		Ме

1.3.2 Цифровий відео нагляд

Цифрові камери відеоспостереження забезпечують максимальну деталізацію відео картинки, з їх допомогою можна розглядати деталі одягу, обличчя людей і номери машин. Одним з основних плюсів цифрових камер відеоспостереження є простота їхньої установки. Досить підключити камеру в комп'ютерну мережу, будь то офіс або склад, і можна буде відразу переглядати відео картинку в режимі онлайн. А встановивши безкоштовний софт, що йде в комплекті поставки, можна буде організувати запис відео архіва на будь-який стаціонарний комп'ютер в мережі. Цифрові камери відеоспостереження дозволяють встановити контроль над великим числом об'єктів. При застосуванні цифрових камер відеоспостереження досягається висока якість запису. Надається більша кількість можливостей для обробки аудіоінформації. За допомогою цифрової камери відеоспостереження можна

переглядати отримовану інформацію в режимі реального часу. У цифрових камерах записуючими пристроями є реєстратори відеоспостереження (або DVR), що мають функції квадратора (або мультиплексора), а також відеомагнітофона, детектора руху і т.п. Сучасні реєстратори відеоспостереження володіють мережевим інтерфейсом. Мережевий інтерфейс дозволяє реєстраторам відеоспостереження передавати зображення по протоколу IP для подальшої обробки та перегляду конкретним користувачем на ПК. Крім реєстраторів відеоспостереження, записуючим пристроєм може бути комп'ютер з встановленим спеціалізованим програмним забезпеченням і платою відеозахоплення. Обсяг записуваної інформації обмежується в такому випадку об'ємом жорсткого диска.

1.3.3 IP-системи відеонагляду

Перетворення відеосигналу в цифровий файл відбувається всередині самого пристрою - IP-відеокамери спостереження (рисунок 1.3). Цифрові файли відправляються в мережевий відеореєстратор (NVR) за захищеною мережею через Ethernet-з'єднання. Відеореєстратор стискає і записує цифрові файли, роздільна здатність яких набагато вище, ніж роздільна здатність аналогових файлів.

Переваги

- Якість відеозапису: роздільна здатність і загальна якість зображення значно вище, ніж у аналогових систем.
- Охоплення: одна IP-камера може охоплювати територію, для ефективного огляду якої знадобиться чотири аналогові камери.
- Менше кабелів: для функціонування IP-системи потрібно значно менше кабелів.
- Розташування: між мережевим відеореєстратором і камерами може бути набагато більша відстань.
- Бездротові мережі: IP-системи добре працюють в бездротовій мережі і не схильні до перешкод.
- Безпека: шифрування даних підвищує їх безпеку.

Недоліки:

- Первісна вартість: високотехнологічні камери, швидше за все, будуть коштувати дорожче, ніж аналогові. Однак, можливо, вам знадобиться менше камер і обладнання в цілому.
- Пропускна здатність: навіть після стиснення розмір файлів набагато вище, ніж в аналогових системах.
- Місце для зберігання: буде потрібно місце для зберігання великих обсягів цифрових файлів.

Рисунок 1.3.3 – типова схема роботи IP-системи відео нагляду

Данна схема складається з:

Таблиця 1.2 – умовні позначення до рисунку 1.3.3

№	Зображення	Назва
1		Зарядка
2		IP-камера
3		Роутер
4		Монітор
5		Хмарне сховище
6		Телефон

1.3.4 Способи збереження та передачі інформації у IP-системах

Завдяки новим технологіям та розширеної функціональності пристроїв сучасних систем відеоспостереження, можна побудувати практично будь-яку систему безпеки з урахуванням індивідуальних особливостей об'єкту, що охороняється, специфіки спостереження, зберігання і передачі інформації, а також цінової політики моделей і обладнання.

Практично кожна модель сучасних відеокамер спостереження передбачає можливості створення архівів відеоінформації на тому чи іншому пристрої.

Отже, основні способи зберігання відеопотоків з аналогових і цифрових камер:

1. Запис інформації безпосередньо на комп'ютер

Даний спосіб можливий при наявності спеціального програмного забезпечення. Комплектація деяких моделей камер включає в себе таке ПО, але виробники не виключають можливість окремого його придбання, з метою комплектації більш бюджетних або застарілих моделей. Принцип роботи полягає у фіксуванні сигналу з пристрою спостереження на ПК (ноутбук, сервер, інше) в режимі безперервного відеопотоку. За допомогою спеціальної програми цю інформацію можна зберегти, переглядати і редагувати надалі.

Так, для аналогових пристроїв запис архівація можлива за допомогою плати відеозахоплення (видеоввода), яка встановлюється безпосередньо в ПК або на цифровий реєстратор (таким чином для зберігання відеопотоку буде потрібно окреме додаткове обладнання) (рисунок 1.4).

Цифрові камери в даному способі найбільш сучасні і адаптовані під пряме підключення до ПК, однак, в тому і в іншому випадку пишуть обладнанням відеокамери виступати не будуть. IP камери мають можливість працювати з ПО, яке входить в комплектацію, а також багато моделей мають власний web-клієнт (встановлюється безпосередньо з камери при первинному підключенні до ПК).

Рисунок 1.3.4.1 – Схема запису інформації на комп’ютер

Дана схема складається з:

Таблиця 1.3 – Умовні позначення до рисунку 1.3.4.1

№	Зображення	Назва
1		Зарядка
2		IP-камера
3		Роутер
4		Монітор

Недоліком цього способу зберігання відеоінформації, можна вважати необхідність постійного зв'язку оператора спостереження з ПК, що значно зменшує відстань спостереження за об'єктом.

2. Запис відеопотоку на IP відеореєстратор

Відеореєстратори - це обладнання, яке спеціально призначене для розширення функціональності пристроїв спостереження, створення якісних архівів і доступу до редагування інформації. При використанні реєстратора окреме ПЗ не потрібно (рисунок 1.5).

Рисунок 1.3.4.2 – спосіб передачі інформації на відео реєстратор

Дана схема складається з:

Таблиця 1.4 – умовні позначення до рисунку 1.3.4.2

№	Зображення	Назва
1		Зарядка
2		IP-камера
3		Роутер
4		IP-відеорегістратор

3. Запис інформації на вбудовану карту пам'яті відеокамери (при наявності такої функції), або на окрему карту пам'яті

При зберіганні інформації даними способом відеокамера працює повністю автономно, без підключення до реєстратора або ПК (рисунок 1.6). Даний спосіб підключення характерний для цифрових моделей, формування архівів визначається:

- можливістю обсягу карти;
- швидкістю відеопотоку, яка обумовлена здатністю, способом архівації, кількістю кадрів в секунду, наявністю функцій датчиків, інше.

Рисунок 1.3.4.3 – передача інформації на карту пам’яті

Дана схема складається з:

Таблиця 1.5 – умовні позначення до рисунку 1.3.4.3

№	Зображення	Назва
1		Зарядка
2		IP-камера
3		Карта пам’яті

Як правило, пристрої даного типу підтримують SD карти пам'яті, об'ємом від 8 до 64 Гб. Фіксація відео відбувається у форматі, який забезпечує до семи діб роботи на карту ємністю в 32 Гб. Зручність даного способу полягає в можливості отримання (або заміни) карти пам'яті в будь-який момент і перегляду відео на будь-якому іншому пристрої.

Камери спостереження з можливістю запису на флеш-накопичувачі, також можна віднести до цього способу формування відеоархівів. Єдине, якщо карта пам'яті розташовується в корпусі камери, то флеш-накопичувач приєднується через USB - роз'єм (як правило, за допомогою гнучкого дроту).

По суті спосіб зберігання інформації за допомогою флеш-накопичувача практично ідентичний з можливостями пристроїв зі слотом для SD карти. Головними і не суттєвими відмінностями можна вважати:

- гранично можливий обсяг пам'яті;
- тип роз'єму підключення.

До недоліку цього способу слід віднести циклічність записи (записуючи відеопотік, при нестачі обсягу карти пам'яті, пристрій автоматично перезаписує початок відео). Для економного використання накопичувачів інформації можна оснастити систему датчиком руху.

4. Хмарний запис

В цьому випадку мова йде про цифрових моделях відеокамер, які за допомогою відповідних налаштувань здатні створювати архіви відеопотоку на спеціальних ресурсах в мережі Інтернет (рисунок 1.7). Можливості таких хмарних

архівів досить широкі, доступ до них забезпечується безпосередньо за допомогою особистого пристрої оператора спостереження (смартфона, планшета), а також слід зазначити широкі можливості і великі обсяги зберігання такої інформації. Доступ до інформаційного потоку обмежений конфіденційними налаштуваннями оператора, а також не прив'язує оператора спостереження до місця розташування об'єкта спостереження.

Рисунок 1.3.4.4 – передача інформації на хмарне сховище

Дана схема складається з:

Таблиця 1.6 – умовні позначення до рисунку 1.3.4.4

№	Зображення	Назва
1		Зарядка
2		IP-камера
3		Хмарне сховище

1.4 Постановка задачі:

Розробити методи протидії типовим атакам на IP-системи відео нагляду.

Для виконня задачі потрібно:

- Проаналізувати вразливості системи;
- Зробити аналіз загроз системи відео нагляду;
- Проаналізувати атаки, виділити найбільш вразливі та розробити методику протидії;
- Розрахувати витрати на реалізацію методик протидії, щоб забезпечити безпечну роботу та передачу інформації у IP-системах

відеоспостереження.

1.5 Висновок

У данному розділі була розглянута історія виникнення систем відеопостереження та наведена класифікація систем відповідно до їх типу. Розглянуті способи передачі та збереження данних під час роботи IP-системвідеонагляду. Виконана постановка задачі.

РОЗДІЛ 2. АНАЛІЗ ПРОБЛЕМ У IP-СИСТЕМАХ ВІДЕОНАГЛЯДУ ТА РОЗРОБКА ЗАХОДІВ БЕЗПЕКИ.

Перед тим як розглянути деталі, важливо розуміти, що ризик є завжди. Немає 100% захищеного пристрою. Зламати можна все що завгодно, питання лише в часі і витрачених ресурсах. Але є можливість знизити ризики і підвищити захищеність. Саме ж поняття «ризик» можна описати як ймовірність негативного впливу від будь-якої загрози. Для ефективного управління ризиками слід доцільно дослідити та проаналізувати потенційні загрози, атаки та вразливості систем відеоспостереження.

2.1 Ідентифікація вразливостей систем відеоспостереження

Вразливість представляє собою слабке місце активу чи засобу управління, яке може бути використано однією та більше загрозою.

Для систем відеоспостереження можна виділити ряд вразливостей, що становить великий ризик атаки на них.

Оцінку вразливостей можна провести за значенням їх критичності. Дана оцінка приведена в таблиці 2.1. При цьому ранжування проводиться за наступними варіантами рівня критичності https://bugcrowd.com/vulnerability-rating-taxonomy:

1 – малий рівень критичності;

2 – середня критичність;

3 – високий рівень критичності;

4 – дуже критична вразливість.

Таблиця 2.1 – Оцінка критичності вразливостей

№	Умовне позначення	Вразливість	Критичність вразливості
1	В1	Неправильне налаштування	3
2	В2	Помилка користувача	3
3	В3	Вразливість ПО	4

Продовження таблиці 2.1 - Оцінка критичності вразливостей

№	Умовне позначення	Вразливість	Критичність вразливості
4	В4	Помилки розмежування прав доступу	3
5	В5	Система приймає слабкі паролі	2
6	В6	Слабке інтернет-з'єднання	2
7	В7	Відсутність систематичного оновлення паролів	1
8	В8	Вразливості пристроїв для зберігання відео	2
9	В9	Відключення шифрування або VPN	3
10	В10	Відсутність шифрування відеопотоку і / або передача облікових даних у відкритому вигляді	4

Таблиця 2.1 – Оцінка критичності вразливостей

2.2 Класифікація загроз систем відеоспостереження

Основною метою створення класифікації загроз було надання найбільш повної, детальної класифікації, яка описує всі існуючі загрози систем відеоспостереження, по якій кожна із загроз потрапляє тільки під одну класифікаційну ознаку, і яка, таким чином, найбільш застосовна для аналізу ризиків реальних систем.

Загрози системи відеоспостереження можна поділити на три великі групи:

1) аварії;

2) диверсії;

3) невірне реагування оператора.

Розглянемо першу групу загроз «аварії». До аварій системи можна віднести масу різних неприємностей, які можуть спіткати відеоспостереження на об'єкті без чийогось злого наміру. Розглянемо деякі з них.

Найбільш уразливі "цеглинки" відеоспостереження - це, звичайно,

телекамери і їх кабельні лінії. Біди, які з ними відбуваються, незчисленні. Деякі - через огріхи монтажу, деякі - через неправильно обраного обладнання та місця установки, а частина - чистої води форс-мажор.

Відсутність відеосигналу

Найбільш "популярна" проблема - відсутність відеосигналу. Якщо на екрані монітора з'явилося сумне Video Loss, оператор зробить запис в журналі, а потім подзвонить керівнику або відразу людині, що займається обслуговуванням. Завдання останнього - локалізувати і усунути несправність.

Типовий випадок - поганий контакт на сигнальній лінії або в ланцюзі харчування камери. "Улюблені" місця: роз'єми на камері, DVR, блоці живлення, різного роду перехідниках, комутаційних панелях і коробках, а також пайки, скручування, місця натягу або перегину кабелю. У переважній більшості випадків ці проблеми виникають через неохайного монтажу або надмірної економії грошей і часу на пристойному кабелі, роз'єми на пайку, термоусадочної трубці і інших матеріалах.

Але трапляється і форс-мажор:

- обрив кабельної лінії або "знесення" телекамери господарськими органами замовника при ремонті;
- обрив повітряної лінії зв'язку бурулькою або вантажівкою "несанкціонованої" висоти;
- обрив підземної лінії при ремонті теплотраси і т.д.

Кожен інсталятор може продовжити цей список. За великим рахунком такі несправності зрозумілі, і їх усунення - завдання просте, хоча і пов'язана іноді з деякими труднощами (адже кабель може бути прокладений в важкодоступному місці).

Несправність обладнання

Варіант гірше - несправність обладнання, починаючи від камери і закінчуючи реєстратором. Можливі причини:

- заводський брак, сплив в прцессе експлуатації;
- помилки в проектуванні, наприклад перевантаження блоку

живлення або недостатній перетин кабелю живлення;

- "Вигорання" електронної начинки телекамер через грозу, наведень від зварювальних апаратів і ін .;
- перегрів обладнання (іноді може бути віднесений до помилок в монтажі);
- вихід з ладу через заливання водою;
- "Напад" комах, гризунів;
- забруднення понад усіляких розумних меж і т.д.

Зникнення електроживлення

В окрему групу можна віднести випадки, пов'язані зі зникненням електроживлення. Воно відбувається часто-густо і часто викликано випадковими відключеннями відповідних автоматичних вимикачів електриками або іншими співробітниками об'єкта. Рідше відбуваються реальні аварії у вигляді коротких замикань або обривів мережі 220 В. Як не дивно, більшу загрозу збереження обладнання несе не відключення мережі, а її включення після тривалої перерви. За добу телекамера може так охолонути на морозі, що рухомі частини у вигляді механізму автоматичної діафрагми об'єктива або поворотною платформи "спіддомов" цілком можуть примерзнути, і після включення електрики чахлим електромеханічним приводам може прийти кінець. Тому для запуску "особливо ніжного" обладнання при сильному морозі іноді варто переплатити за систему попереднього прогріву кожуха перед включенням електроніки.

Наступна загроза – диверсія. Диверсія - свідоме пошкодження або відключення системи відеоспостереження або її складових частин, вироблене з метою безкарного вчинення протиправних дій. Диверсії можуть здійснюватися як відвідувачами, так і співробітниками об'єкта, включаючи недобросовісних співробітників служби охорони, а також самими операторами відеоспостереження.

Окрему групу проблем, хоча і не пов'язаних з самою системою спостереження, можна назвати "невірні дії оператора" в критичній ситуації.

"Ліками" від цієї "хвороби" є Інструкція оператора. Свідомо пишу це слово з великої літери, тому що без неї система відеоспостереження в кращому випадку перетворюється в систему реєстрації, а в гіршому - в купу непотрібного мотлоху.

Оператор повинен заздалегідь чітко знати свої дії при будь-яких подіях - кому дзвонити, куди бігти, що робити. І чим більше часу буде заздалегідь витрачено на інструктаж і нудну зубріння, тим більш осмисленими і передбачуваними будуть дії людини в найважливіші моменти.

2.3 Види атак на мережу системи відеоспостереження

У ході аналізу загроз та вразливостей систем відео спостереження можна виділити ряд атак на них:

- Сніффер пакетів

Сніффер пакетів це прикладна программа, яка використовує мережеву карту, що працює в режимі promiscuous mode (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки).

При цьому сниффер перехоплює всі мережеві пакети, які передаються через певний домен. В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу трафіку. Однак з огляду на те, що деякі мережеві додатки передають дані в текстовому форматі (Telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніффер можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі).

Перехоплення імен і паролів створює велику небезпеку, так як користувачі часто застосовують один і той же логін і пароль для безлічі додатків і систем. Багато користувачів взагалі мають єдиний пароль для доступу до всіх ресурсів і додатків.

Якщо додаток працює в режимі «клієнт-сервер», а аутентифікаційні дані передаються по мережі в читається текстовому форматі, то цю

інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів. Хакери занадто добре знають і використовують людські слабкості (методи атак часто базуються на методах соціальної інженерії).

Вони чудово уявляють собі, що ми користуємося одним і тим же паролем для доступу до безлічі ресурсів, і тому їм часто вдається, дізнавшись наш пароль, отримати доступ до важливої інформації. У найгіршому випадку хакер отримує доступ до призначеного для користувача ресурсу на системному рівні і з його допомогою створює нового користувача, якого можна в будь-який момент використовувати для доступу в Мережу і до її ресурсів.

- IP-спуфінг – Ddos атака

IP-спуфинг відбувається в тому випадку, коли хакер, що знаходиться всередині корпорації або поза нею, видає себе за санкціонованого користувача. Це можна зробити двома способами: хакер може скористатися або IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або вповноваженим зовнішнім адресою, якому дозволяється доступ до певних мережевих ресурсів.

Атаки IP-спуфінга часто є відправною точкою для інших атак. Класичний приклад - атака DoS, яка починається з чужої адреси, що приховує справжню особистість хакера.

Як правило, IP-спуфинг обмежується вставкою помилкової інформації або шкідливих команд у звичайний потік даних, переданих між клієнтським і серверним додатком або по каналу зв'язку між однорангових пристроями.

Для двостороннього зв'язку хакер повинен змінити все таблиці маршрутизації, щоб направити трафік на помилковий IP-адреса. Деякі хакери, проте, навіть не намагаються отримати відповідь від додатків - якщо головне завдання полягає в отриманні від системи важливого файлу, то відповіді додатків не мають значення.

Якщо ж хакеру вдається поміняти таблиці маршрутизації і направити трафік на помилковий IP-адреса, він отримає все пакети і зможе відповідати

на них так, як ніби є санкціонованим користувачем.

- Відмова в обслуговуванні

Denial of Service (DoS), без сумніву, є найбільш відомою формою хакерських атак. Крім того, проти атак такого типу найважче створити стовідсотковий захист. Серед хакерів атаки DoS вважаються дитячою забавкою, а їх застосування викликає зневажливі усмішки, оскільки для організації DoS потрібно мінімум знань і умінь.

Проте саме простота реалізації і величезні масштаби завданої шкоди залучають до DoS пильну увагу адміністраторів, що відповідають за мережеву безпеку. Найбільш відомі різновиди DoS атак:

- TCP SYN Flood;
- Ping of Death;
- Tribe Flood Network (TFN) і Tribe Flood Network 2000 (TFN2K);
- Trinco;
- Stacheldracht;

Онним з джерел інформації з питань безпеки є група екстреного реагування на комп'ютерні проблеми (Computer Emergency Response Team, CERT).

Атаки DoS відрізняються від атак інших типів. Вони не націлені ні на отримання доступу до вашої мережі, ні на отримання з цієї мережі будь-якої інформації, але атака DoS робить вашу мережу недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми.

У разі використання деяких серверних додатків (таких як Web-сервер або FTP-сервер) атаки DoS можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих додатків, і тримати їх в зайнятому стані, не допускаючи обслуговування рядових користувачів. В ході атак DoS можуть використовуватися звичайні Інтернет-протоколи, такі як TCP і ICMP (Internet Control Message Protocol).

Більшість DoS атак розраховани ні на програмні помилки або проломи в системі безпеки, а на загальні слабкості системної архітектури.

Деякі атаки зводять до нуля продуктивність мережі, переповняючи її небажаними і непотрібними пакетами або повідомляючи помилкову інформацію про поточний стан мережевих ресурсів.

Даному типу атак важко запобігти, так як для цього потрібно координація дій з провайдером. Якщо не зупинити у провайдера трафік, призначений для переповнення мережі, то зробити це на вході в мережу вже буде вже не можливо, оскільки вся смуга пропускання буде зайнята. Коли атака даного типу проводиться одночасно через безліч пристроїв, говорять про розподілені атаки DoS (distributed DoS, DDoS)

- Парольні атаки

Хакери можуть проводити парольні атаки за допомогою цілого ряду методів, таких як простий перебір (brute force attack), троянський кінь, IP-спуфинг і сніффінг пакетів. Хоча логін і пароль часто можна отримати за допомогою IP-спуфинга і сніффінга пакетів, хакери нерідко намагаються підібрати пароль і логін, використовуючи для цього численні спроби доступу. Такий підхід носить назву простого перебору (brute force attack).

Часто для такої атаки використовується спеціальна програма, яка намагається отримати доступ до ресурсу загального користування (наприклад, до сервера). Якщо в результаті хакеру надається доступ до ресурсів, то він отримує його на правах звичайного користувача, пароль якого був підібраний.

Якщо цей користувач має значні привілеї доступу, хакер може створити собі «прохід» для майбутнього доступу, який буде діяти, навіть якщо користувач змінить свої пароль і логін.

Ще одна проблема виникає, коли користувачі застосовують один і той же (нехай навіть дуже хороший) пароль для доступу до багатьох систем: до корпоративної, персональної і до систем Інтернету. Оскільки стійкість пароля дорівнює стійкості самого слабкого хоста, то хакер, що довідався пароль через цей хост, отримує доступ до всіх інших систем, де використовується той же пароль.

- Перехоплення інформації під час передачі інформації у

відкритому вигляді

Досить часто аби не витрачати багато часу на належне шифрування даних, передачу їх виконують у відкритому вигляді. Тому саме перехоплення інформації під час передачі і є найчастішою атакою на системи відеоспостереження.

- Атаки типу Man-in-the-Middle

Для атаки типу Man-in-the-Middle хакеру потрібен доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера в будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак даного типу часто використовуються сніфери пакетів, транспортні протоколи і протоколи маршрутизації.

Атаки проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережевих ресурсів, для аналізу трафіку і отримання інформації про мережу та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережеві сесії.

- Несанкціонований доступ до відеорхіву

Несанкціонований доступ не може бути виділений в окремий тип атаки, оскільки більшість мережевих атак на системе відеоспостереження проводяться саме заради отримання несанкціонованого доступу до відеоархіву. Щоб підібрати логін Telnet, хакер повинен спочатку отримати підказку Telnet на своїй системі. Після підключення до порту Telnet на екрані з'являється повідомлення «authorization required to use this resource» («Для користування цим ресурсом потрібна авторизація»).

Якщо після цього хакер продовжить спроби доступу, вони будуть вважатися несанкціонованими. Джерело таких атак може перебувати як усередині мережі, так і зовні.

- Віруси і додатки типу «троянський кінь»

Робочі станції кінцевих користувачів дуже уразливі для вірусів і троянських коней. Вірусами називаються шкідливі програми, які

впроваджуються в інші програми для виконання певної небажаної функції на робочій станції кінцевого користувача.

Троянський кінь - це не програмна вставка, а справжня програма, яка на перший погляд здається корисним додатком, а на ділі виконує шкідливу роль.

Проаналізувавши атаки та вразливості на IP- системи відеоспостереження, можна дійти висновків, що найбільш впливовими на роботу системи є перехоплення інформації та Ddos-атака, які будуть розлянуті нижче.

2.3.1 Перехоплення інформації під час передачі у відкритому вигляді

Ця атака не погіршує цілісність системи і строго кажучи не відноситься до категорії загроз. Але негативні наслідки можуть бути і тут. По-перше, по записах нескладно зрозуміти за якими саме об'єктами ведеться спостереження, де знаходяться непроглядаємі камерами ділянки, наскільки деталізовано зображення і т.д. Що, в свою чергу, полегшить нанести запланований умисний шкоду об'єкту, що охороняється. По-друге, може мати місце комерційне шпигунство, особливо якщо камери використовуються для спостереження за робочими процесами (т.зв. промислове або маркетингове відеоспостереження). Прямих збитків (псування або розкрадання) тут може і не бути, а ось факт недоотримання прибутку аж до повної збитковості підприємства - дуже навіть може.

2.3.2 IP-спуфіннг – Ddos атака

Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх

запитів (часто безглуздих або неправильно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється:

- примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу;
- заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам.

Один з найпоширеніших на сьогоднішній день атак – спосіб флуду HTTP-флуд. Заснований на нескінченному посиланні http-повідомлень GET на 80-й порт із метою завантажити web-сервер настільки, щоб він виявився не в змозі обробляти всю решту запитів. Часто, метою флуду стає не корінь web-сервера, а один із скриптів, що виконують ресурсоємні завдання або що працює з базою даних. У будь-якому разі, індикатором атаки, що почалася, служитиме аномально швидке зростання логів web-сервера.

Частіше за все HTTP DDoS атака проводиться за допомогою ботнету, розподіленої роботизованої системи, що об'єднується за допомогою комп'ютерної мережі та віддалено керується зловмисником. Учасниками такої спілки, як правило стають заражені вірусом, або троянською програмою комп'ютери звичайних користувачів, які навіть про це не підозрюють.

Винятком є використання для атаки фреймів (тег frame) або посилань (тег link, або script), що розміщуються на одному або декількох web-ресурсах з великою кількістю користувачів та посилаються на web-сервер, що атакується.

У деяких випадках, атаку проводять користувачі, що усвідомлено формують чисельну групу та об'єднані ціллю нанести шкоду обраному

web-ресурсу. Як правило, група координується організатором за допомогою соціальних мереж або інших засобів зв'язку, що дають змогу передавати повідомлення великій кількості користувачів одночасно.

Розставимо види HTTP DDoS атак в залежності від ступеня складності захисту від них (від найменшого до найбільшого): атака з використанням фреймів та посилань; атака з використанням мережі ботів; атака, що організована чисельною групою користувачів.

Вразливим місцем атаки з використанням фреймів або посилань є обов'язкова наявність в HTTP запиті заголовка referer, що встановлюється браузером користувача і містить URL ресурсу, з котрого перейшов по посиланню користувач. Сформувавши на основі статистики за кількістю переходів перелік і виключивши з нього сайти, на котрих офіційно розміщені рекламні або інші посилання на ресурс (каталоги, прайс агрегатори) можна відфільтрувати та заблоковувати шкідливий трафік.

2.4 Модель порушника функціонування системи

Порушник - це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби, здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Порушники можуть бути: внутрішніми (з числа персоналу або користувачів системи), або зовнішніми (сторонніми особами).

Користувач інформації в системі - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі ІТС, особи, що мають доступ до неї, поділяються на наступні категорії:

– користувачі, яким надано повноваження продивлятися передану інформацію на хмарний носій;

– користувачі, яким надано право доступу зміни чи видалення конфіденційної інформації;

– розробники ПЗ, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючих;

– постачальники обладнання і технічних засобів та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування;

– технічний персонал, що здійснює повсякденне підтримання життєдіяльності систем відео нагляду.

Модель порушника (табл.2.2) – абстрактний формалізований або неформалізований опис порушника. Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

Таблиця 2.2 – Модель порушника функціонування системи

Можливий порушник	Можливий мотив	Обізнаність, які (не) має порушник
Співробітник	Безвідповідальність Самозатвердження Корисливий мотив	Знає функціональні особливості системи Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування Знає структуру, функції й механізми дії засобів захисту, їх недоліки. Знає недоліки та “вади” механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості. Є розробником програмних та програмно-апаратних засобів захисту або системного

		програмного забезпечення. Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення.
Найманий хакер	Корисливий мотив	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації систем відео нагляду. Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування
Хакер	Самозатвердження Корисливий мотив	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації систем відео нагляду.

Таблиця 2.2 - Модель порушника функціонування системи

2.5 Розробка контрзаходів

В ході роботи були представлені різні атаки на системи відео нагляду. У більшості випадків пов'язаних з атаками на системи не вдається виявити шахраїв так як вони використовують шифрування даних.

Встановлене програмне забезпечення має поганий рівень захисту. Досить часто при підключенні систем відео спостереження та під'єднання хмарного носія співробітники нехтують таким важливим фактором як шифрування бездротового з'єднання.

Таким чином на даний час одним з ключових факторів боротьби з атаками на системи відеоспостереження впершу чергу є комплексна система захисту інформації.

Комплексна система захисту забезпечує виконання таких функцій:

1. Захист від незахищених каналів передачі інформації
2. Розробка і відладження порядку обробки інформації
3. Захист від несанкціонованого доступу до хмарного сховища
4. Своєчасна передача інформації для збереження
5. Постійні заходи з проведення навчання обслуговуючого персоналу
6. Своєчасне оновлення програмного забезпечення системи
7. Постійні оновлення кодів доступу до сичтем.

2.6 Розробка методик протидії типовим атакам

В ході проведеної роботи і аналіз типових атак на системи відеоспостереження було виділено дві найбільш вразиві атаки : перехоплення інформації під час передачі у відкритому вигляду та IP-спуфінг, а також були розроблені загальні методики протидії типовим атакам.

Для кожного виду атак можна визначити ряд послідовних дій які в свою чергу підвищать безпеку передачі та збереження інформації.

2.6.1 Методи протидії перехопленню інформації під час передачі у відкритому вигляді.

Згідно постанови кабінету міністрів України від 8 серпня 2012 №766:

"Система захисту інформації від несанкціонованого доступу повинна виконувати такі функції:

- ідентифікація користувачів мережі, захист параметрів ідентифікації користувачів і параметрів;
- розмежування доступу до ресурсів і процесів у системі відеоспостереження;
- забезпечення цілісності інформаційних ресурсів;
- захист носіїв інформації від несанкціонованого доступу;
- забезпечення функцій адміністрування в системі захисту інформації від несанкціонованого доступу;
- захист від шкідливих комп'ютерних програм."

Як вже було зазначено вище перехоплення інформації під час передачі є однією з типових атак при використанні систем відеоспостереження.

Тому насамперед найпершою протидією до таких атак є шифрування даних, що не дозволяє переглянути їх або скористатися ними під час передачі по мережі. Цього можна досягти за допомогою кількох різних технологій. Кожна з них має свої переваги і недоліки. Як правило, застосовуються такі рішення:

- фільтрація IP-адрес;
- віртуальна приватна мережа;
- протокол HTTPS;

Фільтрація IP-адрес. Деякі мережеві камери і відеокодери використовують фільтрацію IP-адрес, надаючи доступ до мережевих відеокомпонентів тільки з одного або декількох IP-адрес. За своєю дією фільтрацію IP-адрес можна порівняти з вбудованим брандмауером.

Ця технологія підходить для проектів, де потрібно більш високий рівень безпеки. Як правило, мережеву камеру необхідно налаштувати таким чином, щоб вона приймала команди тільки з IP-адреси сервера, на якому встановлено ПЗ для управління відео.

Безпечний маршрут. Ще більш безпечна альтернатива - віртуальна приватна мережа (VPN), де використовується протокол шифрування для побудови захищеного тунелю між мережами; по ньому дані передаються приховано для

сторонніх спостерігачів, в тому числі через загальну мережу, наприклад Internet, тому що тільки пристрої з правильним «ключем» можуть працювати в мережі VPN.

VPN, як правило, зашифровує пакети на рівнях IP або TCP / UDP і вище. У мережі VPN найбільш часто реалізується протокол шифрування IPSec. У ньому використовуються різні алгоритми шифрування: стандарт потрійного шифрування даних (3DES) або стандарт удосконаленого шифрування (AES). Для останнього характерна наявність 128 і 256-розрядних ключів, що забезпечує більш високу ступінь захисту і вимагає помітно меншої потужності комп'ютера для шифрування і розшифровки даних, ніж стандарт 3DES.

За допомогою мереж VPN часто організовуються з'єднання між кількома офісами однієї організації або здійснюється доступ до мережі віддалених співробітників (див. Рисунок 1). Дистанційні камери включаються в корпоративну систему охоронного відеоспостереження аналогічним чином.

Шифрування даних за протоколом HTTPS**.** Ще більш високого рівня конфіденційності можна домогтися шляхом безпосереднього шифрування даних. Найбільш поширеним протоколом шифрування даних є HTTPS. Він використовується, наприклад, при проведенні банківських операцій через Internet. HTTPS відрізняється від HTTP єдиною ключовою особливістю - шифруванням переданих даних (див. Рисунок 2), яке здійснюється за допомогою протоколу безпечних з'єднань (SSL) або протоколу захисту транспортного рівня (TLS).

Протокол SSL був розроблений компанією Netscape і опублікований в 1994 р Безпека, що забезпечується протоколами SSL / TLS, базується на трьох основних елементах:

- аутентифікація партнера по обміну даними;
- симетричне шифрування даних;
- захист від маніпуляцій з переданими даними.

При здійсненні з'єднання SSL / TLS протокол квітірованія зв'язку визначає, які методи шифрування повинні використовувати одержувач і відправник: алгоритми шифрування, основні настройки, генератори випадкових чисел і т.д. Потім перевіряється справжність партнера по обміну даними: сервер Web

ідентифікується браузером лише після надання сертифіката - свого роду посвідчення особи. Цей документ в довічним форматі зазвичай випускається підтверджуючий центр VeriSign. Користувачі можуть створювати власні сертифікати для закритих груп, таких як Web-сервер локальної мережі, до якого мають доступ тільки співробітники компанії.

На наступному етапі партнери обмінюються попередніми (premaster) секретним кодом, який перед передачею на сервер шифрується за допомогою загального ключа з сертифіката сервера із залученням методу асиметричного шифрування або алгоритму обміну ключами Діффі-Хеллмана. Обидві сторони обчислюють головний (master) код локально і на його основі створюють сеансовий ключ. Якщо сервер здатний розшифрувати ці дані і завершити виконання приписаних протоколом процедур, то клієнт може бути впевнений, що у сервера є правильний приватний ключ. Це найважливіший етап в процесі аутентифікації сервера, оскільки тільки сервер з приватним ключем, відповідним загальному ключу в сертифікаті, в змозі розшифрувати отримані дані і продовжити процедуру узгодження в рамках протоколу.

Багато продуктів мережевого відео мають вбудовану підтримку протоколу HTTPS, що дозволяє безпечно переглядати відеозображення через браузер Web.

На основі вище наведених методів можна розробити методику протидії для збереження даних:

- Фільтрувати IP-адреси
- Використовувати симетричне шифрування данних
- Аутентифіковувати користувачів при обміні данними

2.6.2 Методи протидії DDos-атакам

Небезпека більшості DDoS-атак – в їх абсолютній прозорості і "нормальності". Адже якщо помилка в ПЗ завжди може бути виправлена, то повне зжирання ресурсів - явище майже буденне. З ними стикаються багато адміністраторів, коли ресурсів машини (ширина каналу) стає недостатньо, або web-сайт піддається слешдот-ефекту. І якщо різати трафік і ресурси для всіх

підряд, то врятуєшся від DDoS, но втратиш велику половину клієнтів. Наслідки DDoS-атак і їх ефективність можна істотно понизити за рахунок правильного налаштування маршрутизатора, брандмаузера і постійного аналізу аномалій в мережевому трафіку.

Поради для запобігання атакам:

-Завжди містити ПО для забезпечення безпеки сервера в актуальному стані;

- передбачати можливість резервного копіювання даних і перенесення їх на інший сервер;

- мати можливість віддалено перезавантажити будь-сервер в аварійній ситуації;

- мати в наявності запасний мережевий інтерфейс, за яким можна буде отримати доступ до атакується системі;

- переклад ресурсів в «хмару». Компанії, що спеціалізуються на хмарних технологіях і пропонують перенесення сервера в хмару, мають куди більш потужні засоби протидії хакерам, ніж підприємство малого чи середнього бізнесу;

- інструктувати співробітників, як вести себе в підозрілої ситуації. DDos-атака починається не миттєво і часто її можна перехопити ще на початковій стадії.

Методи протидії

Стовідсоткових методів сьогодні від DDos-атак не існує. До попередження DDos-атак потрібно підходити комплексно: з огляду на програмні аспекти, так і апаратні і організаційні.

1. Передбачення. Часто DDos-атаки здійснюються або економічними конкурентами, або з релігійних, етнічних, політичних причин. Тому, якщо організація знаходиться в зоні ризику - краще заздалегідь передбачити ймовірність атаки.

2. Нарощування обчислювальної потужності. При дійсно серйозною DDos-атаці цей метод може не спрацювати, але, якщо запитів не надто багато або атака

знаходиться на початку реалізації, краще мати потужний сервер, який буде чинити опір як можна довше. Зрештою, за цей час можна буде застосувати інші заходи протидії.

3. Атака. Суть методу в тому, що весь атакуючий трафік перенаправляється в зворотню сторону. Якщо в розпорядженні є досить потужний сервер, атака захлинеться і обернеться проти зловмисників.

4. Спеціальне ПО. Існує маса спеціальних пропозицій з протидії DDos-атакам. Подібного роду ПО коштує недешево, але витрати окупляться при першій же критичної ситуації.

5. Розосередження серверів. Необхідно рознести активні частини сервера з можливістю їх дублювання. Навіть якщо якась частина ресурсів виявиться недоступною, інша частина буде функціонувати.

6. Відведення активної IP-адреси або доменного імені від ресурсів, які можуть бути схильні до DDos-атакам.

7. Фільтрація і блокування трафіку. Часто при цьому важко відокремити «чистий» трафік від «поганого», але можна відсікати тільки другорядні запити. Втім, якщо зловмисник використовує першорядні запити, цей метод виявиться слабким захистом.

8. Ліквідація вразливостей. Відразу після відбиття атаки або навіть під час неї потрібно шукати і усувати вразливі місця в системі.

На основі вище наведених методів розроблено методику протидії:

- Оновлення програмного забезпечення проводити раз на 3 місяці
- Розсередити сервери для можливості їх дублювання
- Раз на пів року дублювати данні на хмарні сховище

2.7 Рекомендації щодо безпечного користування IP-системами відеоспостереження

Рекомендації щодо безпечного користування IP-системами відеоспостереження:

- Використовувати засоби захисту інформації сучасних класів та сертифіковані;
- Вчасно встановлювати оновлене програмне забезпечення;
- Робити розмежування доступу між користувачами систем;

2.8 Висновки

У данному розділі було надано ідентифікацію вразливостей систем відео спостереження, класифіковано загрози системи. Також було надано види атак на мережу систем відеоспостереження, на основі котрих було виділено найбільш впливові атаки на системи та надано методи боротьби протидії. У розділі було розглянуто модель порушника системи. Було розроблено контрзаходи, а також надано рекомендації щодо безпечного користування системами відеоспостереження.

РОЗДІЛ 3. ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ СТВОРЕННЯ МЕТОДИК ПРОТИДІЇ ТИПОВИМ АТАКАМ

3.1 Вступ

Метою розділу є обґрунтування економічної доцільності створення методики протидії типовим атакам систем відеонагляду. Для доказу захисту системи відеонагляду було розроблено методику протидії типовим атакам.

Щоб визначити ефективність необхідно розрахувати:

– капітальні витрати на розробку, впровадження та підтримку методик;

– трудомісткість витрати на розробку, впровадження та підтримку методик, а також трудомісткість на підтримку IP-системи відеонагляду;

– річні експлуатаційні витрати на впровадження та підтримку IP-системи;

– показники економічної ефективності захисту.

3.2 Розрахунок фіксованих (капітальних) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на створення програми і методики $К_{пз}$ складаються з витрат на заробітну плату виконавця програми і методики $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання на ПК $З_{мч}$:

$$К_{пз} = З_{зп} + З_{м} \qquad (3.1)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$Ззп = t \times Зпр\ ,\ грн \qquad (3.2)$$

де t – загальна тривалість створення ПЗ, годин;

$З_{пр}$ – середньогодинна заробітна плата.

Розрахуємо час, який буде витрачено на створення програми і методики:

$$t = t_{тз} + t_{втз} + t_{ае} + t_{сп} + t_{вз} + t_{ор},\ годин \qquad (3.3)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку програми та методики;

$t_{втз}$ – тривалість вивчення технічного завдання;

$t_{ае}$ – тривалість аналізу елементів модуля «Проактивний захист»;

$t_{сп}$ – тривалість складання методик проведення аналізу рівня захищеності системи;

$t_{вз}$ – тривалість випробувань захищеності системи;

$t_{ор}$ – тривалість опрацювання результатів;

У таблиці 3.1 представлена трудомісткість процесів.

Таблиця 3.1 – Трудомісткість процесів

Назва процесу	Трудомісткість, год.
Складання технічного завдання на розробку методик	2
Вивчення технічного завдання	1
Аналіз елементів модуля «Проактивний захист» системи	5
Складання методик протидії типовим атакам сайтом»	6
Випробування захищеності системи	2
Опрацювання результатів	3

$$t = 2 + 1 + 5 + 6 + 2 + 3 = 49 \text{ годин.}$$

$З_{пр}$ – середньогодинна заробітна плата фахівця з нарахуваннями, грн/годину.

$$З_{пр} = \frac{З_м}{t_m} = 15000/160 = 93.75, \text{грн/год} \quad (3.4)$$

де – середня заробітна плата фахівця з інформаційної безпеки – 15 000 грн., – робочій час на місяць -160 год.

$$З_{зп} = 49*93.75 = 4593.75, \text{ грн}$$

Вартість машинного часу для впровадження методик визначається за формулою:

$$З\,мч = (\,topp + td\,) \times C\,мч \quad \text{грн} \quad (3.5)$$

де $t_{опр}$ – трудомісткість налагодження всіх необхідних операцій на ПК, годин (80 год);

$t_д$ – трудомісткість підготовки документації на Пк, годин (40 год);

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \times C_e + Ф_{зал} \times H_a, F_p \text{ грн} \quad (3.6)$$

де P – встановлена потужність ПК, 0.5 кВт;

C_e – тариф на електричну енергію, 1,55грн/кВт·година;

$Ф_{зал}$– залишкова вартість ПК на початок року, 7000 грн.; H_a – річна норма амортизації на ПК, 0.1 частки одиниці;

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920 год).

$$Смч = 0,5 \times 1,55 + 7000 \times 0,1 = 1,20 \text{ грн/год}$$

$$Змч = 80 \times 1,20 + 40 = 136 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на створення та впровадження програми та методики складають:

$$K_{пз} = 136+4593.75 = 4729.75, \text{ грн} \quad (3.7)$$

Оскільки в даній роботі розглядається тільки перевірка елементів захисту модуля «Проактивний захист», перевірка повної системи вимагає більше часу, а відповідно більші капітальні витрати. Передбачається, що для повної перевірки капітальні витрати становитимуть у 2 рази більше.

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$C = C_а + C_з + C_{ел} + C_{тос}, \text{ грн}, \quad (3.8)$$

де $C_а$ – річний фонд амортизаційних відрахувань ($C_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ);

$$C_а = K_{пз} /2 =(4729.75)/2=2364.88, \text{ грн}, \quad (3.9)$$

Сз – річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ,складає:

$$C_з = (Зм+ 22\%) \cdot m = 15\,000 \cdot 12 = 180\,000 \text{ грн}, \quad (3.10)$$

де m – кількість місяців.

До річного фонду заробітної плати додається єдиний внесок (22%) на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного

ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою:

$$С_{ел} = Р \cdot Fр \cdot Ц_е \text{ , грн} \qquad (3.11)$$

де Р – встановлена потужність апаратури інформаційної безпеки, 0.5 кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (за 40-годинного робочого тижня $F_р = 2080$ год);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин, 1.68 грн/кВт·година.

$$С_{ел} = 0,5 \cdot 2080 \cdot 1,68 = 1\ 747,2 \text{ грн.}$$

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначається за формулою:

$$С_{тос} = С_{ліц} + С_{хст}, \text{ грн} \qquad (3.12)$$

де $С_{ліц}$ – вартість ліцензії на 1 рік системи;

$С_{хст}$ – вартість послуги хостинга на 1 рік .

$$С_{тос} = 7\ 100 + 1\ 479 = 8\ 579, \text{ грн}$$

Отже, річні поточні (експлуатаційні) витрати складають:

$$С = 2364.88 + 180\ 000 + 1\ 747,2 + 8\ 579 = 192871.08 \text{ грн.}$$

3.4 Оцінка можливого збитку від атаки

Упущена вигода від простою атакованного вузла або сегмента системи становить:

$$U = П_п + П_в + V \quad (3.13)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента системи, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента системи (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента системи, 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:

$$Пп = E\,(Зс)/F*tп \quad (3.14)$$

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

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

$$П = 15000 + 12000 \times 2 = 306{,}82 \text{ , грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв}, \quad \text{грн} \quad (3{,}15)$$

де $П_{ви}$ – витрати на повторне введення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента мережі,

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованного вузла або сегмента системи $З_с$, які зайняті повторним введенням втраченої інформації, з

урахуванням необхідного для цього часу $t_{ви}$:

$$Пви =(E(Зс)*tп)/F \quad (3.16)$$

де $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$$П =(5000 + 5000 +12000)/176 \times 4 = 500 \text{ , грн}$$

Витрати на відновлення вузла або сегмента системи $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньоденної заробітної плати обслуговуючого персоналу (адміністраторів):

$$Ппв = E(Зо)/F*tв \quad (3.17)$$

де Зо – заробітна плата обслуговуючого персоналу (адміністратора), грн на місяць;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин.

$$Ппв= 15000/176 \times 2=170,46 \text{ , грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = 500 + 170,46 = 670,46, \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента системи визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = O/Fг \times (tп + tв + tви) \quad (3.18)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі,

грн у рік.

$$V= 750000 /2080\times(2+4+2)=2884,64 \text{ , грн}$$

Упущена вигода від простою атакованного вузла або сегмента системи становить:

$$U = 306,82 + 670,46 + 2\ 884,64 = 3\ 861,92 \text{ , грн}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі складе

$$B = EiEnU \qquad (3.19)$$

де і – число атакованих вузлів або сегментів системи;

n – середнє число атак на рік.

$$B = 1 \cdot 450 \cdot 3\ 861,92 = 1\ 737\ 864 \text{ грн.}$$

3.5 Загальний ефект від використання засобів безпеки, які дозволено використовувати завдяки програмі та методиці

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \qquad (3.20)$$

де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці(0,4 найбільш ймовірний відсоток);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис.грн.

$$E = 1\ 737\ 864 \cdot 0,4 - 192871.08 = 502274.52 \text{ грн.}$$

3.6 Економічне обгрунтування

Оцінка економічної ефективності системи захисту інформації,

здійснюється на основі визначення та аналізу наступних показників:

– коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій $Т_о$.

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

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = E/K \text{, частки одиниці} \qquad (3.21)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

$$ROSI = 502274.52/4729.75 = 106.19$$

Нормативне значення коефіцієнта повернення інвестицій визначається з наступних міркувань.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань), то в якості $Е_н$ варто приймати бажану норму прибутковості альтернативних варіантів вкладення коштів К (наприклад, у цінні папери, інші проекти, на депозитний рахунок у банку, тощо) з урахуванням інфляції. Визначити бажане значення коефіцієнта ефективності можна також виходячи з прийнятної для підприємства індивідуальної норми прибутковості, яка б, принаймні, не знижувала ринкову вартість фірми.

При цьому проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > (Nдеп – Nінф)/100) \quad (3.22)$$

де Nдеп – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, 18%;

Nінф – річний рівень інфляції, 13,7%.

$$106.19 > (18\text{-}13,7)/100$$

$$106.19 > 0,043$$

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій T_o.

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

$$To=K/E=1/ROSI=0.009\approx 33 \text{ дні.}$$

3.7 Висновок

В економічному розділі у результаті розрахованих витрат потрібних на реалізацію створення основного й додаткового програмного забезпечення, розробки проекту інформаційної безпеки, була доведена економічна ефективність і період окупності витрат.

Розрахунок (фіксованих) капітальних витрат:

1) Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 4 тис.грн

2) Витрати на навчання технічних фахівців і обслуговуючого персоналу, це є підготовчі курси з адміністрування та обслуговування системи виявлення вторгнень складають 3 тис. грн;

3) Вартість машинного часу для налагодження програми на ПК складає - 8.6415,грн.

Експлуатаційні витрати:

Витрати на технічне й організаційне адміністрування та сервіс

системи виявлення вторгнень становлять 66,819 , тис. грн.

Оцінка можливого збитку від атаки (злому) на вузол корпоративної мережі

Загальний збиток від атаки на вузол, або сегмент корпоративної мережі становить 300985.65 грн.

Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить 180524.57 грн,

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Термін окупності: 33 дні.

Проект економічно доцільний та його можно використовувати на підприємстві.

ВИСНОВОК КВАЛІФІКАЦІЙНОЇ РОБОТИ

Проблема захисту інформації у системах відеоспостереження на даний момент є однією з ключових проблем. Як звичайні користувачі не хочуть втратити та оприлюднювати свої дані і не стати жертвою шахрайства, так і підприємства бажають зберегти свою репутацію.

У кваліфікаційній роботі було надано ідентифікацію вразливостей систем відеоспостереження. Було надано класифікацію загроз системи. Також було надано види атак на мережу систем відеоспостереження, на основі котрих було виділено найбільш впливові атаки на системи та надано методи боротьби протидії. Також у розділі було розроблено методики протидії цим типовим атакам. Також було наведено модель порушника системи. Було розроблено контрзаходи, а також надано рекомендації щодо безпечного користування системами відеоспостереження.

В економічному розділі наведено обгрунтування запропонованих методик протидії атакам. Було розраховано капітальні та експлуатаційні витрати на впровадження методик. А також оціно можливий збиток від атаки на вузол мережі.

Практичне значення роботи полягає взменшенні часу та фінансових витрат при впровадженні методик протидії атакам.

Відеоаналітіка в системах відеоспостереження не стоїть на місці, таким функціоналом, як вихід з периметра, пропажа предмета з області, детекция пішоходів та інше, вже нікого не здивувати.

ПЕРЕЛІК ПОСИЛАНЬ

1. Системы видеонаблюдения [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://otherreferats.allbest.ru/radio/00800684_0.html#text.
2. Системи відеоспостереження [Електронний ресурс] – Режим доступу до ресурсу:https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D1%81%D0%BF%D0%BE%D1%81%D1%82%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F.
3. Що краще: аналогове відеоспостереження або IP-система безпеки? [Електронний ресурс] – Режим доступу до ресурсу: http://ipkey.com.ua/uk/partners-6/1171-chto-luchshe-analogovoe-videonablyudenie-ili-ip-sistema-bezopasnosti.html.
4. Сучасні системи безпеки бізнесу [Електронний ресурс] – Режим доступу до ресурсу: https://ssbb.com.ua/uk/systemu-videosposterejenya-v-kievi/vib%D1%96r-v%D1%96deosposterezhennya/cifrovye-kamery-videonabludeniya/.
5. Відеоспостереження із записом: способи зберігання інформації [Електронний ресурс] – Режим доступу до ресурсу: https://worldsecurity.com.ua/ua/blog/videonablyudenie-s-zapisyu-sposoby-hraneniya-informatsii .
6. Информационная безопасность в системах охранного видеонаблюдения [Електронний ресурс] – Режим доступу до ресурсу: https://www.videomax-server.ru/support/articles/informatsionnaya-bezopasnost-v-sistemakh-okhrannogo-videonablyudeniya/.
7. DoS-атака [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/DoS%D0%B0%D1%82%D0%B0%D0%BA%D0%B0#HTTP-%D1%84%D0%BB%D1%83%D0%B4.
8. IP-видеокамеры в DDoS-атаках [Електронний ресурс] – Режим доступу до ресурсу: https://ohrsys.ru/articles/ip-videokamery-v-ddos-atakakh/.
9. Способы защиты от DDos-атак. [Електронний ресурс] – Режим доступу до ресурсу: https://evrohost.com/ddos-protection/.
10. Боротьба з flood-атаками [Електронний ресурс] – Режим доступу до ресурсу:https://wiki.tntu.edu.ua/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%

D0%B8_%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D0%B.

11. ПОСТАНОВА [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/766-2012-%D0%BF#Text.

12. Baldissera D., Franco A., Maio D., Maltoni D. Fake Fingerprint Detection by Odor Analysis//Proceedings of International Conference on Biometric Authentication 2006 — ICBA06, Lecture Notes in Computer Science, 2006. V. 3832. P. 265-272.

13. Результати досліджень систем відеоспостереження [Електронний ресурс] – Режим доступу до ресурсу: https://cyberpolice.gov.ua/results/2018/.

14. Бурячок, В. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно – телекомунікаційних систем [Текст] / В. Л. Бурячок // Захист інформації. НАУ. - К. – 2011. - №3. – С. 1-9.

15. Schuckers S. A. C. Spoofing and Anti-Spoofing Measures//Information Security Technical Report, Elsevier. 2002. V. 7. No 4. P. 56-62.

16. Рейтинг вразливостей OWASP Top – 10 – 2017 Електронний ресурс]. – Режим доступу: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

17. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом[Електронний ресурс]Режимдоступу: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=28807

18. Вимоги до системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/6012701/page:6/.

19. Информационная безопасность в системах охранного видеонаблюдения [Електронний ресурс] – Режим доступу до ресурсу: https://www.videomax-server.ru/support/articles/informatsionnaya-bezopasnost-v-sistemakh-okhrannogo-videonablyudeniya/.

20. Безопасность видеонаблюдения на базе IP [Електронний ресурс] – Режим доступу до ресурсу: https://www.osp.ru/lan/2009/09/10534599.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Зміст	2	
3	А4	Вступ	3	
4	А4	1 Розділ	45	
5	А4	2 Розділ	33	
7	А4	Економічний розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік файлів на електронному носії

1. Пояснювальна Записка.docx
2. Презентація.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник: _____к.е.н, доц. Пілова Д.П.
(підпис)

ДОДАТОК Г.

В І Д Г У К

на кваліфікаційну роботу Колєснік Марини Олександрівни

студентки групи 125м-19-2

на тему: «Аналіз ризиків кібербезпеки у IP-системах корпоративного відеоспостереження»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 62 сторінках.

Метою кваліфікаційної роботи є дослідження та удосконалення захисту інформації у IP-системах відеоспостереження.

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 нормативно-правової бази та класифікація систем відеоспостереження, розглянуто способи передачі та збереження даних під час роботи IP-систем відеоспостереження, проведено оцінку критичності вразливостей та загроз систем відеоспостереження. Також було розглянуто види атак на мережу систем відеоспостереження, виділено найбільш впливові атаки та розроблені методи протидії.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні захисту даних у IP-системах відеоспостереження, за рахунок розробки рекомендацій.

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

Недоліком роботи є недостатньо деталізований аналіз ризиків систем відеоспостереження та не чіткість сформульованих висновків в підрозділах та розділах роботи.

Загалом за час дипломування Колєснік Марина Олександрівна проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістр за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «добре»/78б.

Керівник кваліфікаційної роботи

д.ф-м.н., проф. Т.С. Кагадій

Керівник спеціального розділу

асистент Ю. А. Мілінчук