МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Безпека комп'ютерних систем і мереж»

Група: 4КБ-01

Дипломний проект

здобувача освіти денної форми навчання
КБ.01.16.000.ДП

САПОЖНІКОВ
ВАЛЕРІЙ РОМАНОВИЧ

м. Одеса
2024 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Безпека комп'ютерних систем і мереж»**

Група: **4КБ-01**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту на тему:

Розробка онлайн-рішення з оцінки захищеності систем відеоспостереження.

Проектний матеріал складається з пояснювальної записки на 87 сторінках та графічного (презентаційного) матеріалу на 9 аркушах (слайдах).

Дипломник _____ (Сапожніков В.Р.)

Керівник _____ (Стайкуца С.В.)

Консультанти:

з економічного розділу _____ (Іванченков В.С.)

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «20» 06 2024 р. Протокол ЕК № 4

Оцінка ЕК 3 (задовільно) 70 б.

Секретар ЕК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Комісія *КТ та ІП*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Безпека комп'ютерних систем і мереж»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"11" 01 2024 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві (здобувачці) освіти Сапожнікову Валерію Романовичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)) Розробка онлайн-рішення з оцінки захищеності систем відеоспостереження

затверджена наказом по коледжу від "02" листопада 2023 р. № 224

2. Термін здачі закінченого проекту (роботи) 10.06.2024 р

3. Вихідні данні до проекту (роботи):

Об'єкт аналізу – сучасні системи відеоспостереження

Загрози СОТ – мережеві, інфраструктури, ПЗ, обладнання, з боку персоналу

Показник, відповідальний за ризик - карта ризиків (радар ризиків)

Елементи реалізації - HTML5, CCS3, JavaScript, Chartjs

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Дослідити технології та параметри систем відеоспостереження. Дослідити екосистему загроз та ризиків систем відеоспостереження. Розробити опитувальні анкети як основу для Подальшої програмної реалізації. Навести механізми захисту систем відеоспостереження Розробити радар ризиків для оцінки СОТ. Навести економічну частину та охорону праці.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Технології систем відеоспостереження; Загрози сучасним системам відеоспостереження; Дослідження екосистеми загроз безпроводових мереж систем відеоспостереження; "Людський фактор" в фокусі інформаційної безпеки систем відеоспостереження; Комплексний підхід до вивчення загроз сучасних систем відеоспостереження; Механізми та інструменти захисту систем відеоспостереження; Алгоритм програмної реалізації; Інструменти програмної реалізації; Заповнення анкети та побудова радару загроз; Інтерактивні таблиці з обраними механізмами захисту; Висновки

6. Консультанти по проекту, із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	*Стайкуца С.В.*		
Економічний розділ	*Іванченков В.С.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 15 січня 2024 р.

Керівник *Стайкуца С.В.* _____
(підпис)

Завдання прийняв до виконання *Сапожніков В.Р.* _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітк. викон.
1.	*Вступ. Постановка задачі проектування*	*29.04.24-2.05.24*	
2.	*Аналіз технічного завдання та пошук літератури*	*2.05.24-4.05.24*	
3.	*Дослідження систем відеоспостереження*	*4.05.24-10.05.24*	
4.	*Аналіз екосистеми загроз та ризиків*	*10.05.24-15.05.24*	
5.	*Дослідження мережевих вразливостей систем*	*15.05.24-19.05.24*	
6.	*Дослідження екосистеми загроз безпроводових мереж*	*19.05.24-23.05.24*	
7.	*Аналіз механізмів захисту систем відеоспостереження*	*19.05.22-25.05.24*	
8.	*Розробка ТЗ на систему. Дослідження архітектури системи та інструментів реалізації*		
9.	*Програмна реалізація системи радару загроз*	*25.05.24-29.05.24*	
10.	*Виконання економічних розрахунків*	*29.05.24-2.06.24*	
11.	*Розробка питань з охорони праці та техніки безпеки*	*2.06.24-6.06.24*	
12.	*Підготовка мультимедійної презентації проекту*	*06.06.24-09.06.24*	

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КБ 01. 16 000. 00 ДП	Дипломний проект		
А4			КБ 01. 16 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КБ 01. 16 000. 00 ДП		
Розробив		Сапожніков В.Р.		10.06	Розробка онлайн-рішення з оцінки захищеності систем відеоспостереження	Літ.	Аркуш 4 / Аркушів 83
Перевірив		Стайкуца С.В.		10.06		НДП	
Н. Контр.		Петрашова В.І.		10.06	ВСП "ОТФК ОНТУ" гр.4КБ-01		
Затверд.		Кривченко Ю.В.		10.06			

ЗМІСТ

ВСТУП

Системи відеоспостереження постійно змінювалися, адаптуючись під технологічну "еволюцію", яка відбулася у сфері телекомунікацій. Разом із новими можливостями у процесі розвинення та укріплення зв’язку з іншими системами, сучасні системи відеоспостереження отримали і нові вразливості, раніше їм не притаманні.

Такі системи стоять на заваді у дуже великої кількості правопорушників і злочинців, тому закономірно, що вони самі нерідко стають об’єктами нападу. Камери та інше обладнання постійно підвергається не тільки фізичному впливу, а й спробам перехоплення відеосигналу чи отримання доступу до відеоархіву. Системи відеоспостереження постійно змінювалися, адаптуючись під технологічну "еволюцію", яка відбулася у сфері телекомунікацій. Разом із новими можливостями у процесі розвинення та укріплення зв’язку з іншими системами, сучасні системи відеоспостереження отримали і нові вразливості раніше їм не притаманні. Розвиток і розповсюдження систем відеоспостереження на базі IP призвели не тільки до покращення якості зображення, спрощенню монтажу та масштабування систем відеоспостереження, а і до появи великої кількості нових уразливостей. Більшість із них спільні із стандартними мережевими вразливостями, отже і способи їх ліквідації будуть спільними.

Метою роботи є дослідження сучасних систем відеоспостереження, виявлення їх вразливостей та пошук оптимальних методів захисту цих систем. Фінальним етапом є розробка онлайн-рішення з оцінки рівня захисту будь-якої системи відеоспостереження.

1 ОСНОВНА ЧАСТИНА

1.1 Аналіз загроз та вразливостей сучасних систем відеоспостереження

1.1.1 Методи фізичного впливу

Блокування об'єктива. Найпростіший спосіб вивести телекамеру з ладу - заліпити чим-небудь об'єктив. Його можна замазати клеєм або фарбою, заліпити скотчем або стікером, пластиліном чи іншим речовиною подібної консистенції.

Дальність дії цього способу невелика - до того ж, якщо до камери легко дотягнутися, це швидше за все результат грубої помилки інсталятора. Мова, зрозуміло, не йде про приміщення і проходах з низькою стелею.

Пошкодження кабельної інфраструктури. Припустимо, мета зловмисника полягає в тому, щоб насильно перервати передачу зображення на монітор чергового. Самий простий і ефективний спосіб здійснити це - просто перерізати кабель.

Для цієї мети підійде будь-який гострий предмет, з тих, що прийнято ховати від дітей. Досвідчені люди радять застосовувати інструмент з ізольованими ручками на випадок, якщо в пучку проводів, провідних до камери, виявиться живильний кабель на напругу понад 36 вольт.

У випадку з бездротовими системами відеоспостереження сигнал від камери можна просто заглушити, не вдаючись до псування майна.

Вандалізм. Затвердження виробників про те, що їх камери є антивандальними, з технічної точки зору досить розмиті. Оскільки вага, форма і властивості матеріалу, передбачуваного ними знаряддя замаху на відеоспостереження не регламентуються, ми маємо право припустити найгірше. А народна мудрість стверджує: проти лому немає прийому.

При застосуванні такого жорстокого методу питанням критичної важливості стає траєкторія важкого предмета. Від неї залежить, вдасться чи

пошкодити об'єктив, згорнути камеру з кронштейна, сколупнути купол і т. д. Методика прицілювання відома з часів полювання на мамонтів і гов описах, напевно, не потребує.

Оптичний вплив. Найбільш технологічний із способів боротьби з охоронними камерами. Інтенсивний пучок світла, спрямований об'єктив, викликає надмірну засвічення чутливого елемента - яскравість досягає граничного значення, і зображення виявляється повністю або частково «залито» однорідною плямою. Навіть при досить широкому динамічному діапазоні з потрапили в кадр прожектором впораються далеко не всі камери. Сам прожектор, швидше за все, буде видно непогано. А ось розгледіти під ним постать людини, а тим більш риси обличчя, вкрай важко. Замість видимого світла, який видно неозброєним оком, можна використовувати невидимий інфрачервоний діапазон.

Справа в тому, що майже всі фото - і відеокамери (а особливо чорно-білі) бачать в інфрачервоному діапазоні. Це робиться спеціально, щоб поліпшити якість зйомки в умовах слабкого освітлення: всередині приміщень, у сутінках, в темряві. Використовуючи цей принцип, можна зробити пристрій, який надійно засвітить ваше обличчя від фото - і відеокамер старих моделей. Достатньо купити дешевих інфрачервоних світлодіодів і батарейку на 9 вольт – і непомітно закріпити це на кепці або іншому головному уборі.

Однак даний метод працює тільки з бюджетними моделями камер. Більш дорогі моделі швидко адаптуються до такого роду засліпленням.

У мережі є безліч прикладів пристроїв, сконструйованих різними умільцями, для засвічування об'єктивів камер спостереження. Бюджет складання таких пристроїв часто не перевищує 150-200 доларів.

На рис. 2.1 представлено всі розглянуті методи фізичного впливу на системи відеоспостереження

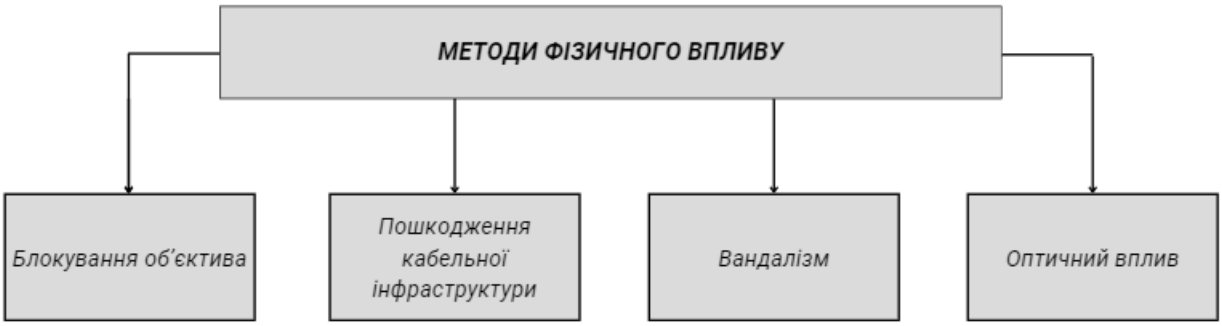


Рисунок 1.1. Методи фізичного впливу

1.1.2 Мережеві вразливості систем відеоспостереження

Причин масових вразливостей систем відеоспостереження на базі IP багато, проте головна причина одна: при впровадженні нових систем фізичної безпеки і відеоспостереження з використанням IP-протоколу часто не враховуються мережеві та IT-загрози. Це ж явище спостерігається при переході з традиційних аналогово-цифрових систем на сучасне IP- відеоспостереження.

Ситуація із вразливостями фізичної безпеки нагадує відому багатьом ситуацію з безпекою IP- телефонії: систему телефонії переводили з TDM на IP, але про супутні IT-ризики досить часто забували. Як наслідок, могло мати місце шахрайство з дзвінками або порушення доступності телефонії.

Системи відеоспостереження вибираються, проектуються та впроваджуються департаментами фізичної безпеки, які зазвичай, досить далекі від аналізу сучасних IT-загроз. IT та IT-безпека у кращому разі притягуються на етапах підключення систем в мережу підприємства. Іноді навіть для відеоспостереження будуються окремі канали зв'язку і окремий вихід в Інтернет, які також рідко захищають за стандартами підприємства. Експлуатація цих систем теж здійснюється незалежно від IT- процесів.

1. Помилки у налаштуванні обладнання. Невірні дії з налаштування мережевих параметрів можуть збільшити ризик нападу.

Незахищена архітектура

Неправильно налагоджена мережа - це головна точка входу непрошених гостей. Відкрити, грунтовану на довірі, незахищену локальну мережу для

доступу з небезпечного Інтернету - це те ж саме, що відкрити двері в кримінальному районі - можливо, за якийсь час нічого не станеться, але врешті-решт хтось скористається цим.

Широкомовні мережі

Системні адміністратори часто недооцінюють у своїх схемах захисту важливість мережевого устаткування. Просте устаткування, на зразок концентраторів або маршрутизаторів, використовує принцип широкомовлення, а не комутації; тобто, коли один вузол передає по мережі дані іншому, концентратор або маршрутизатор посилає широкомовні пакети, доки одержуючий вузол не прийме їх і не обробить. Такий спосіб передання є уразливим для атак протоколу arp або підміни MAC- адреси, здійснюваних зловмисними користувачами локальної мережі або ззовні.

Централізовані сервери

Ще однією можливою мережевою уразливістю є централізована комп'ютерна система. Поширеним способом зниження витрат на багатьох підприємствах є перенесення усіх служб на один потужний комп'ютер. З одного боку, це зручно, оскільки в порівнянні з конфігураціями з багатьма серверами це полегшує управління і зменшує витрати. Але з іншого боку, централізований сервер в мережі є поодинокою уразливою точкою. Якщо цей сервер скомпрометований, це може привести до виходу усієї мережі з ладу, або, що ще гірше, до зміни або викрадення даних. У таких випадках головний сервер стає широко розкритими дверима, що відкривають доступ до усієї мережі.

2. Використання стандартних паролів

Різні виробники по-різному відносяться до питань установки захисту в моделях відеокамер, які ними випускаються.

Захист на основі особистого пароля передбачається на більшості моделей IP- камер. Найвідоміші виробники технічним шляхом примушують користувача змінити існуючий пароль за умовчанням на індивідуальний на момент установки. Зробити це можна під час активізації роботи камери після монтажу. У деяких моделях система вимагає певну кількість символів конкретного формату.

Деякі користувачі залишаються невдоволені згаяним часом, але при такому паролі мережевий доступ до роботи камери отримує тільки строго обмежене коло людей.

Деякі виробники IP-камер не досить уважно відносяться до питання несанкціонованого доступу до моделей обладнання, що ними випускаються. В табл. 2.1 наведено деякі базові логіни та паролі до IP-камер.

При перевірці якості різних видів продукції відомих брендів було виявлено, що деякі моделі мають декілька призначених для користувача записів обліку доступу і паролі за умовчанням, які не підлягають заміні або видаленню, оскільки вони наділені правами адміністратора. Чимала кількість компаній – виробників IP-камер не піклуються про те, щоб користувачі змінювали пароль з базового на на власний. Можливо, це залежить від самих користувачів. До того ж, лінь і неуважність - потенційні союзники зловмисників. Якщо ви придбаєте та встановлюєте камери для захисту і спостереження важливих об'єктів, то відсутність гарантії щодо захисту відеоданих незрозуміла. В цьому випадку звичайна неуважність з боку споживача тільки сприятиме досягненню мети із злочинними намірами.

Деякі компанії на своїх сайтах виставляють існуючі паролі за умовчанням на свою продукцію, щоб таким шляхом змусити користувачів змінити парили на індивідуальні, і хоч якось захистити свою продукцію від хакерського посягання. Таким чином компанії прагнуть постійно нагадувати найбільш безвідповідальним користувачам, що, якщо вони не змінили пароль за умовчанням на власний - їх система спостереження є незахищеною від стороннього проникнення.

3. Вразливість відеореєстраторів

В ході тестів, проведених компаніями, що надають послуги оцінки уразливості систем, були виявлені сенсаційні уразливості ряду моделей мережевих відеореєстраторів. Були виявлені "Діри в захисті" які дозволяють видаленому хакерові порушити роботу домашньої системи відеоспостереження шляхом DDoS- атаки, вторгнутися у відеоархіви і процеси адміністрування

системи - не утрудняючи себе підбором пароля, в цих моделях можна без проблем додавати до системи нових користувачів і навіть міняти пароль адміністратора.

Серед знайдених помилок - стандартний пароль суперкористувача, який не можна змінити через особливості його зберігання, відкриті сервісні порти і множинні уразливості в програмному забезпеченні DVR-пристрої, що відкривають зловмисникові доступ до системи.

Також вдалося виявити так званий майстер-пароль, який підходить до облікового запису будь-якого користувача системи і відкриває доступ до пристрою відеоспостереження з максимальними привілеями. Цей пароль однаковий для всіх DVR-пристроїв під управлінням даного програмного забезпечення і не може бути змінений користувачем.

Додати до системи нового користувача означає можливість перегляду живих і архівних відео з IP- відеореєстратора без необхідності злому або зміни адміністраторського пароля. Таким чином хакер може залишатися непоміченим впродовж тривалішого часу, ніж при зміні пароля - адже в останньому випадку хазяїну системи буде відмовлено в доступі, і він може запідозрити недобре.

Також можна " вивідати" у відеореєстратора IP- адреси, підключених до нього камер відеоспостереження, паролі і логіни для доступу до них, а також паролі і логіни будь-яких підключених до облаштування FTP- серверів. Особливо небезпечною може виявитися можливість дистанційного перепрошивання пристрою довільним софтвером - тобто, при необхідності хакер, залишаючись непоміченим, здатний без проблем занести у відеореєстратор шкідливий код.

4. Віруси

Як і усі системи, що мають доступ до глобальної мережі, мережеві системи відеоспостереження схильні до поразки комп'ютерними вірусами.

Комп'ютерний вірус - програма, потайно працююча в системі, з метою завдання шкоди комп'ютеру. Вірус здатний самостійно створювати і поширювати свої копії. Існує велика кількість різних комп'ютерних вірусів. Одні

з них, можуть просто примушувати рухатися курсор миші, інші, можуть вкрасти ваші особисті дані і навіть пошкодити роботу усієї операційної системи.

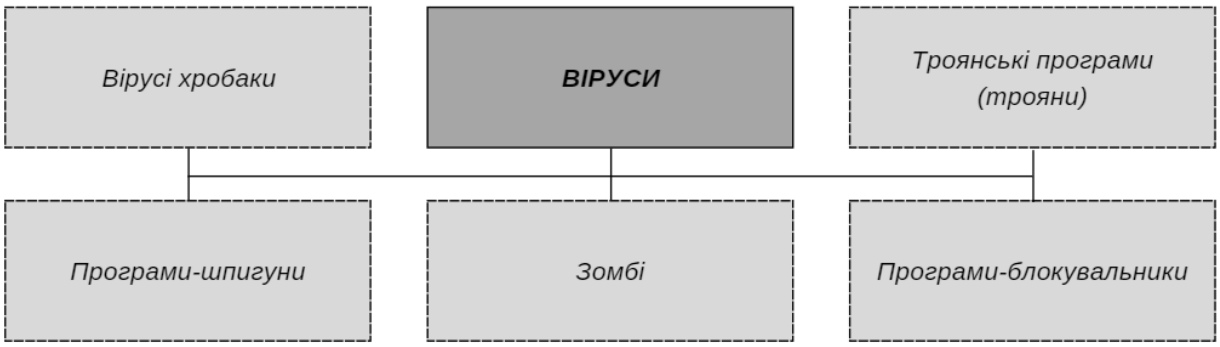


Рисунок 1.2. Основні види вірусів

Основні види комп'ютерних вірусів :

– Черв'як - програма, яка робить копії самій себе. Її шкода полягає в захаращенні комп'ютера, через що він починає працювати повільніше. Відмітною особливістю черв'яка є те, що він не може стати частиною іншої нешкідливої програми.

– Троянська програма маскується в інших нешкідливих програмах. До того моменту як користувач не запустить цю саму нешкідливу програму, троян не несе ніякій небезпеці. Троянська програма може завдати різного збитку для комп'ютера. В основному трояни використовуються для крадіжки, зміни або видалення даних.

– Spyware. Шпигуни збирають інформацію про дії і поведінку користувача. В основному їх цікавить інформація (адреси, логіни, паролі).

– Зомбі. Дозволяють зловмисникові управляти комп'ютером користувача. Комп'ютери - зомбі можуть бути об'єднані в мережу і використовуватися для масової атаки на сайти або розсилки спаму. Користувач може не здогадуватися, що його комп'ютер зомбований і використовується зловмисником.

– Програми - блокувальники. Це програми, які блокують користувачеві доступ до операційної системи. При завантаженні комп'ютера з'являється вікно,

в якому користувача звинувачують в скачування неліцензійного контенту або порушення авторських прав.

5. Мережеві вразливості систем цифрового відеоспостереження

Загрозою інформації є порушення цілісності та (або) доступності відеосигналу. Передача відеосигналу без механізму автентифікації даних дозволяє зловмисникові підмінити сигнал реального часу з відеокамер, а відсутність механізмів підтвердження автентичності дозволяє коригувати дані відеоархіву. Найбільш суттєві загрози системам IP-відеоспостереження представлено на рис. _

Взагалі, мережеві атаки класифікують за принципом дії на пасивні і активні. Пасивні дії є, у більшості випадків, діставанням доступу до особистої інформації з видаленого комп'ютера, якось: читання кореспонденції, що входить і витікаючої, читання блогів і так далі. Пасивні мережеві атаки важко виявити, оскільки при пасивній дії не залишається ніяких слідів. Активні мережеві атаки здійснюються не лише з метою діставання доступу до конфіденційних даних, але також з метою їх зміни. Активні дії можливо виявити, оскільки при активній мережевій атаці в системі відбуватимуться зміни, що залишить свій слід.

Рисунок 1.3. Мережеві вразливості систем цифрового відеоспостереження

1.1.3 Загрози безпроводових мереж систем відеоспостереження

Розглянемо загрози безпроводових мереж, які зараз часто присутні в екосистемі сучасних систем відеоспостереження

1. Wardriving

Мало хто знає, що таке вардрайвінг, хоча він існує давно. На відміну від звичних способів злому, навчитися вардрайвінгу набагато простіше, так як для нього не потрібні специфічні знання дизасемблювання, необхідні при зломі програм.

Вардрайвінг - (англ. wardriving - бойове водіння) сканування ефіру на частоті 2,4 Ghz з метою знайти якомога більше бездротових точок доступу Wi -Fi (Acces Point або хотспотів). Виробляється як правило «на колесах», звідси й назва WarDriving . Вардрайвінг - не обов'язково злом. Найчастіше це всього лише невинне колекціонування, прагнення виявити якомога більше точок доступу і нанести їх на карту на доказ своїх досягнень. Проте багато хто в корисливих цілях або просто приколу заради зламують бездротові мережі, використовуючи обладнання та спецсофт для експлуатації вразливостей в Wi – Fi, благо його захист в першій реалізаціях як була, так і залишається дірявої як решето.

Для перехоплення інформації (моніторингу) точок доступу можуть використовуватися, наприклад, такі програми, як Kismet і NetStumbler. Коли така програма знаходить сигнал точки доступу, вона заносить в журнал назву мережі, SSID, MAC-адреса точки доступу, найменування її виробника, прослуховується канал, силу сигналу, співвідношення сигнал/шум, факт використання WEP. Атакуючий переміщається навколо на своїй машині з ноутбуком, на якому запущена програма NetStumbler, що виробляє активний пошук точок доступу. Зазвичай, вона може виявити точки доступу в радіусі до 100 метрів, але з потужнішою антеною атакуючий може знаходити точки доступу і набагато далі. NetStumbler розсилає тестові запити кожну секунду, очікуючи відповіді точки доступу. Якщо на точці доступу використовується WEP, для злому і

перехоплення ключів можуть використовуватися такі програми, як Airsnarf, AirSnort або WEP - Crack .

2. DoS- атака (атака типу «відмова в обслуговуванні», від англ. Denial of Service) - атака на обчислювальну систему з метою довести її до відмови, тобто, створення таких умов, при яких легальні користувачі системи не можуть отримати доступ до надаваних системним ресурсів (серверів), або цей доступ ускладнений. Відмова «ворожої» системи може бути і кроком до оволодіння системою (якщо в нештатній ситуації ПЗ видає якусь критичну інформацію - наприклад, версію, частину програмного коду тощо). Проте, частіше це міра економічного тиску.

Рисунок 1.4. Атака "відмова в обслуговуванні" в безпроводових мережах

DDoS- атака (від англ. Distributed Denial of Service , розподілена атака типу «відмова в обслуговуванні ») - атака виконується одночасно з великої кількості комп'ютерів. Яскравим прикладом цього є виведення з ладу сайту, який ще вчора радував Вас своєю стабільністю і швидкодією .

DDoS- атака - розподілена атака типу відмова в обслуговуванні, яка являє собою одну з найбільш поширених і небезпечних мережевих атак. В результаті атаки порушується або повністю блокується обслуговування законних користувачів, мереж, систем та інших ресурсів. Метою DDoS-атак є не крадіжка даних, і навіть не знищення інформації. Мета - "загальмувати" або повністю зупинити роботу сервера, що атакується.

3. Глушіння

Глушіння в мережах відбувається тоді, коли навмисна чи ненавмисна інтерференція перевищує можливості відправника чи одержувача в каналі зв'язку, таким чином, виводячи цей канал з ладу. Атакуючий може використати різні способи глушіння. Глушіння клієнтської станції дає можливість шахраєві підставити себе на місце заглушеного клієнта (рис. 2). Також глушіння можуть використовувати для відмови в обслуговуванні клієнта, щоб йому не вдавалося реалізувати з'єднання. Більш витончені атаки переривають з'єднання з базовою станцією, щоб потім вона була приєднана до станції зловмисника

Глушіння базової станції надає можливість підмінити її атакуючою станцією Таке глушіння позбавляє користувачів доступу до послуг.

Як зазначалося вище, більшість бездротових мережевих технологій використовує неліцензовані частоти. Тому багато пристроїв, такі як радіотелефони, системи стеження і мікрохвильові печі, можуть впливати на роботу безпроводових мереж і приглушувати безпроводове з'єднання.

Щоб запобігти таким випадкам ненавмисного глушіння, перш ніж купувати дороге безпроводове обладнання, треба ретельно проаналізувати місце його встановлення. Такий аналіз допоможе переконатися в тому, що інші пристрої не завадять комунікацій.

4. Вторгнення і модифікація даних

Вторгнення відбувається, коли зловмисник додає інформацію до існуючого потоку даних, щоб перехопити з'єднання або пересилати дані або команди в своїх цілях. Атакуючий може маніпулювати керуючими командами і потоками інформації, відсилаючи пакети або команди на базову станцію, і навпаки. Подаючи керуючі команди в потрібний канал управління, можна домогтися від'єднання користувачів від мережі.

Вторгнення може використовуватися для відмови в обслуговуванні. Атакуючий переповнює точку доступу в мережу командами з'єднання, «обдуривши» її перевищенням максимуму можливих звернень, - таким чином, іншим користувачам буде відмовлено в доступі. Подібні атаки можливі також ,

якщо протоколи верхнього рівня не забезпечують перевірки потоку даних на цілісність у реальному часі.

Досвідчений атакуючий може організувати точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї помилкової точки доступу і повідомляють їй свої важливі реквізити, наприклад, автентифікаційну інформацію. Цей тип атак іноді застосовують в застосовують прямим глушінням, щоб «заглушити» справжню точку доступу в мережу.

5. MITM-атака

Атака посередника , атака «людина посередині», MITM - атака (англ. Man in the middle) - термін в криптографії , що позначає ситуацію, коли криптоаналітик (атакуючий) здатний читати і видозмінювати по своїй волі повідомлення, якими обмінюються кореспонденти, причому жоден з останніх не може здогадатися про його присутність в каналі.

Найбільше поширені MITM-атаки, коли зловмисник використовує Wi-Fi-маршрутизатор в якості інструменту перехоплення повідомлень. У даному випадку створюється підміна використовуваного роутера і підміна самої мережі (див. рис 2.5). Або використовуються помилки в налаштуванні і захисту мережі, які дозволяють цілком легально перехоплювати сесії. У першому сценарії зловмисник налаштовує у своєму ноутбуці точку бездротового доступу, даючи їй те ж ім'я , що й використовується в громадському місці з доступним Wi-Fi. Коли користувачі підключаються до цієї псевдомережі, то при спробі вчинити будь-яку дію з комерційними сайтами, банківськими або іншими фінансовими ресурсами, їх інформація перехоплюється, після чого зловмисник вже може користуватися їй на свій розсуд.

В системі виробника обладнання застосований алгоритм пошуку шляху для забезпечення максимально ефективної передачі даних і пошуку найбільш надійних маршрутів, що ведуть до одержувача. Цей алгоритм дуже схожий на той, що зазвичай використовується в відеоіграх для прокладання маршруту, по якому персонаж повинен пройти, щоб, обійшовши всі перешкоди, потрапити в кінцевий пункт. Алгоритм пошуку шляху, який використовується в системі

відеоспостереження, використовує кілька змінних, найважливіші з яких - сила сигналу між сусідніми вузлами, а також число вузлів, через які проходить пакет на шляху до кінцевого пункту. Здійснюючи MitM-атаки на камери, зловмисники можуть замінити реальні дані на своє відео, чи просто кажучи, змінити контент.

6. Абонент-шахрай

Після ретельного вивчення роботи абонента мережі атакуючий може «прикинутися» їм чи клонувати його клієнтський профіль, щоб спробувати отримати доступ до мережі і її послугам. Крім того, досить вкрасти пристрій для доступу, щоб увійти в мережу. Забезпечення безпеки всіх бездротових пристроїв - справа дуже непроста, оскільки вони навмисно робляться невеликими для зручності пересування користувача. Найбільший загальний механізм забезпечення безпеки - управління доступом до ресурсів на другому рівні. Цей механізм давав збої , коли адміністратори з його допомогою MAC намагалися обмежити доступ до мереж стандарту безпроводових LAN 802.11 з використанням MediaAccessControls (MAC - управління доступом до середовища.

7. Помилкова точка доступу

Досвідчений атакуючий може організувати помилкову точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї помилкової точки доступу і повідомляють їй свої важливі реквізити, наприклад автентифікаційну інформацію. Цей тип атак іноді застосовують у поєднанні з прямим глушінням , щоб « заглушити » справжню точку доступу в мережу. Користувачі, що мають доступ до провідної мережі, можуть також сприяти встановленню помилкових точок доступу, ненавмисно відкриваючи мережу для нападів. Іноді користувач встановлює безпроводову точку доступу , прагнучи до зручностей, які надає безпроводовий зв'язок, але не замислюючись про проблеми безпеки. Сьогодні обладнання для точок доступу можна купити в будь-якому магазині електроніки за помірну ціну. Ці точки можуть виявитися «чорним ходом» для проникнення в проводову мережу, оскільки зазвичай вони встановлюються в такій конфігурації, яка схильна всіляким атакам. Атакуючі

можуть запросто під'єднуватися до призначених для користувача точок доступу і входити в проводову мережу подібно до звичайних її відвідувачам. Більшість мереж покладаються на захист брандмауера (firewall), що забезпечує недоторканність периметра , але абсолютно не підготовлені до відбиття атаки , що виходить зсередини.

8. Таємні бездротові канали (потайний вхід в мережу)

Один з найважливіших факторів , який користувачі безпроводових систем повинні брати до уваги, створюючи або оцінюючи мережу. Оскільки вартість точок бездротового доступу низька і створити точку доступу на основі ПЗ, стандартного ноутбука і NIC-карти для бездротового зв'язку досить просто, потрібно пильно відстежувати некоректно сконфігуроване або непродумано розгорнуте безпроводове обладнання в проводовій мережі. Зловмисник (можливо із співробітників організації мережі) може навмисно залишити так званий чорний хід в мережу. Це обладнання може виконати дуже помітні «дірки» в провідний інфраструктурі , куди можуть попрямувати атакуючі з відстані в кілька кілометрів від мережі. За допомогою аналогічної конструкції можна прокласти своєрідний «безпроводовий місток» і викачувати дані з мережі поза захищеного будівлі, утворивши цілий ланцюг точок доступу.

Рисунок 1.5. Основні загрози безпроводових мереж при використанні систем відеоспостереження

1.1.4 “Людський фактор” в фокусі інформаційної безпеки систем відеоспостереження

Як відомо, слабкою ланкою будь-якої системи завжди є людина і системи відеоспостереження не є виключенням.

Для детального розбору цього питання пригадаємо такий термін як інсайдер. Інсайдер – це будь-яка особа, яка має доступ до конфіденційної інформації про діяльність фірми в силу свого службового становища або родинних зв'язків. Інсайдер, який володіє інформацією «з внутрішніх першоджерел», може краще оцінити стан справ, ніж будь-який інший фахівець, який користується «зовнішньою» інформацією. Наведемо базову класифікацію інсайдерів:

1. Халатний інсайдер. Цей вид інсайдерів є найчисленнішим. Зазвичай, це рядовий внутрішній співробітник, який порушив вимоги конфіденційності інформації внаслідок своєї неуважності. Таким чином, в діях даного виду інсайдерів не можна виявити ні користі, ні умислу, ні будь-яких цілей. Він порушує вимоги про конфіденційність інформації невмотивовано.

2. Маніпульований інсайдер. Такі інсайдери переважно є жертвами соціальної інженерії. Дані прийоми використовуються не тільки для отримання неправомірним шляхом персональної інформації користувачів, їх паролів, номерів кредитних карт тощо.

3. Ображений інсайдер. Такі інсайдери відносяться до зловмисних, які діють переконливо і усвідомлено, знаючи про негативні наслідки своєї діяльності. Отже, скривджений інсайдер – це співробітник компанії, що розкриває конфіденційну інформацію для того, щоб помститися компанії з особистих мотивів. Його метою є нанесення шкоди, а не викрадення інформації як такої.

4. Нелояльні інсайдери – співробітники, які планують найближчим часом змінити нинішнє місце роботи. Саме ці співробітники потрапляють під підозри в першу чергу, якщо мова заходить про внутрішні загрози. Нелояльні, як і скривджені інсайдери можуть легко перетворитися на мотивованих ззовні.

5. Підробляючий інсайдер. Ситуація з нелояльними і скривдженими інсайдерами змінюється докорінно, якщо вони попередньо вийшли на зв'язок з покупцем інформації, необхідної для викрадення. Мотивувати підробляючих інсайдерів можуть різні причини: від бажання заробити суму, до дії по неволі, коли такі співробітники шантажуються тими чи іншими структурами і вже не мають іншого вибору, як викрасти конфіденційну інформацію.

6. Впроваджений інсайдер – це співробітник, який влаштовувався на роботу для викрадення інформації або з метою саботувати роботу підприємства. Головна небезпека, що виходить від впроваджених інсайдерів, полягає в тому, що вони забезпечені необхідними технічними навичками, що дозволяють їм подолати всі технічні бар'єри на шляху до отримання конфіденційної інформації.

Як мі можемо бачити з рис. 2.7 найбільшу загрозу становлять саме діючі співробітники компанії(30%), не дуже від них відстають і колишні робітники, ті що покинули компанію з будь-яких причин(24%).

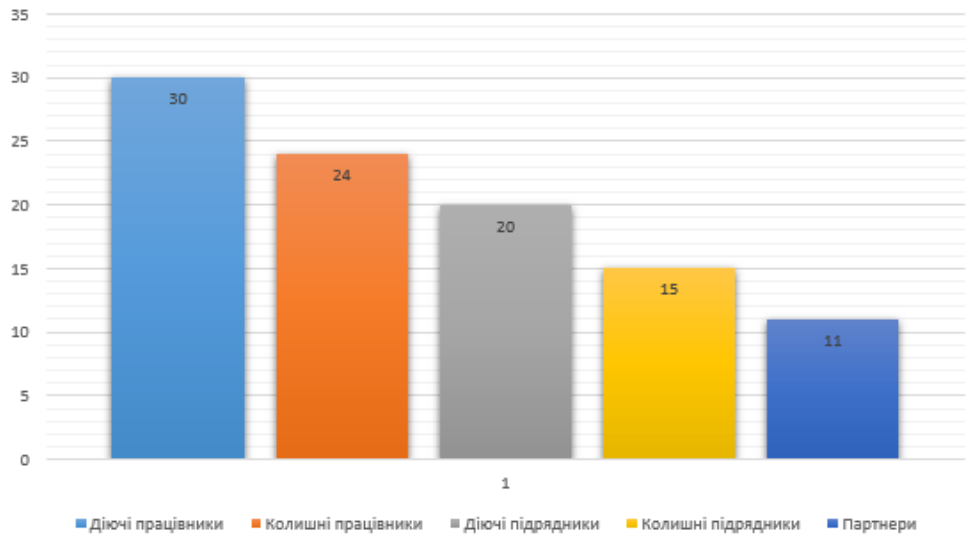


Рисунок 1.6. Основні групи порушників внутрішнього корпоративного середовища

Сформулюємо основні загрози, які можуть виникнути з боку персоналу який працює та обслуговує системи відеоспостереження, до них відносяться:

1. Неспроможність виконувати службові обов’язки.

Нажаль у наш час не рідкість коли люди потрапляють на свої робочі місця не маючи достатньої кваліфікації та навичок. Це нерідко спричиняє цілу низку неприємних ситуацій. Кили один чи декілька співробітників не можуть виконувати свої обов’язки це може знизити ефективність роботи їх колег або навіть звести нанівець роботу усієї служби безпеки. Проте на це можуть бути і інші причини. Наприклад занадто велика кількість роботи на одного працівника, або погані умови праці.

2. Помилки/Ненавмисне заподіяння шкоди

Кожна людина може припуститися помилки, але помилка співробітника служби безпеки, або людини що налагоджує систему безпеки, може коштувати для компанії дуже дорого.

3. Низька ефективність працівників

Дуже часто компанії стикаються з тим, що їх співробітники не викладаються на повну. У випадку з працівником, що забезпечує безпеку на підприємстві це неприпустимо від якості його роботи може залежати не лише фінансовий добробут компанії, а і життя людей.

4. Умисне заподіяння шкоди

Це дії що спричиняються усвідомлено, знаючи про негативні наслідки. Під винуватців цієї загрози потрапляють ображений, нелояльний, підробляючий та впроваджений інсайдери.

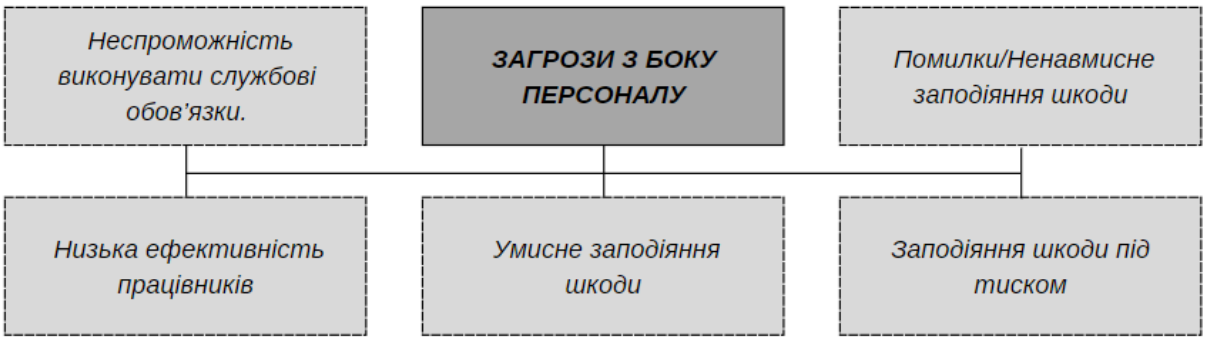


Рисунок 1.7. Основні загрози з боку персоналу

1.1.5 Формування екосистеми загроз та вразливостей СОТ

Як ми бачимо сучасна система відеоспостереження не обділена вразливостями. Хоч у деяких напрямках їх більше, а у інших менше (див. рис. 2.9), всі напрямки безпеки є важливими, бо як відомо із принципу «рівноміцності захисту»: “Захищеність системи визначається її найуразливішим місцем”.

Рисунок 1.8. Комплексне представлення загроз типової системи відеоспостереження

Із пунктів описаних вище виділимо основні загрози які є найбільш розповсюдженими у сучасних умовах та зведемо їх у таблицю 1.1.

Таблиця 1.1 – Деякі загрози сучасних систем відеоспостереження

Загрози	Механізм захисту
Мережеві загрози	
DDOS – атаки	DDoS- атака - розподілена атака типу відмова в обслуговуванні, яка являє собою одну з найбільш поширених і небезпечних мережевих атак. В результаті атаки порушується або повністю блокується обслуговування законних користувачів, мереж, систем та інших ресурсів.
Вторгнення і модифікація даних	Вторгнення відбувається, коли зловмисник додає інформацію до існуючого потоку даних, щоб перехопити з'єднання або пересилати дані або команди в своїх цілях. Атакуючий може маніпулювати керуючими командами і потоками інформації, відсилаючи пакети або команди на базову станцію, і навпаки. Подаючи керуючі команди в потрібний канал управління, можна домогтися від'єднання користувачів від мережі.
Вардрайвінг	Вардрайвінг – сканування ефіру на частоті 2,4 Ghz з метою знайти якомога більше бездротових точок доступу Wi -Fi та спроби під’єднатися до них.
Абонент-шахрай	Після ретельного вивчення роботи абонента мережі атакуючий може «прикинутися» їм чи клонувати його клієнтський профіль, щоб спробувати отримати доступ до мережі і її послугам.
Man-in-Middle	MITM - атака – термін в криптографії , що позначає ситуацію, коли криптоаналітик (атакуючий) здатний читати і видозмінювати по своїй волі повідомлення, якими обмінюються кореспонденти, причому жоден з останніх не може здогадатися про його присутність в каналі.
Атаки на мережеве обладнання	Атаки на мережеве обладнання з метою змінити його налаштування, вивести його з ладу або отримання доступу до певної інформації.
Помилкова точка доступу	Досвідчений атакуючий може організувати помилкову точку доступу з імітацією мережевих ресурсів.
Загрози інфраструктури	
Глушіння	Глушіння в мережах відбувається тоді, коли навмисна чи ненавмисна інтерференція перевищує можливості відправника чи одержувача в каналі зв'язку, таким чином,

	виводячи цей канал з ладу.
Фізичне пошкодження кабельної інфраструктури	Пошкодження кабельної інфраструктури може як частково, так і повністю паралізувати працездатність системи.
Перехоплення сигналу поза КЗ	Одним із основних недоліків бездротових систем залишається те шо їх корисний сигнал розповсюджується за межами контрольованої зони.
Відсутність або нестабільність електроживлення	Електроживлення може бути відсутнє з багатьох причин, починаючи з планового відключення і закінчуючи стихійними лихами, техногенними катастрофами та диверсіями.
Загрози ПЗ	
Комп’ютерні віруси	Комп'ютерний вірус - програма, потайно працююча в системі, з метою завдання шкоди комп'ютеру. Вірус здатний самостійно створювати і поширювати свої копії.
Прості паролі	Більшість користувачів використовують короткі паролі що дуже легко піддаються злому чи взагалі залишають стандартні паролі.
Уразливості в прошивках відеосерверів та камер	Існує велика кількість відеосерверів та камер у ПЗ яких було знайдено критичні вразливості які дозволяли без жодних клопотів отримати повний контроль над системою.
Застаріле ПЗ	ПЗ що не оновлюється з часом може стати причиною зависання та навіть збоїв у системі.
Загрози обладнання	
Пошкодження камер, а також закриття, зафарбовування, заклеювання, засвічування об'єктива	Камери дуже часто страждають від фізичного впливу, як навмисного так і випадкового.
Погодні умови	Зовнішні камери спостереження піддаються впливу вітру, дощу, снігу та критичних температур.
Пошкодження відеоархіву	Відеоархів може бути пошкоджений як навмисно так і випадково , як з території компанії так і дистанційно.
Відмова обладнання (брак, несправності, знос)	Обладнання може мати заводський брак яких може проявити себе не тільки на ранніх стадіях експлуатації обладнання, а і після певного терміну роботи.

Загрози з боку персоналу	
Неспроможність виконувати службові обов’язки.	Люди потрапляють на свої робочі місця не маючи достатньої кваліфікації та навичок, занадто велика кількість роботи на одного працівника, погані умови праці тощо
Помилки/Ненавмисне заподіяння шкоди	Кожна людина може припуститися помилки, але помилка співробітника служби безпеки, або людини що налагоджує систему безпеки, може коштувати для компанії дуже дорого. Цю загрозу можуть спричиняти халатні та маніпульовані інсайдери.
Низька ефективність працівників	Дуже часто компанії стикаються з тим, що їх співробітники не викладаються на повну. У випадку з працівником, що забезпечує безпеку на підприємстві це неприпустимо від якості його роботи може залежати не лише фінансовий добробут компанії, а і життя людей.
Умисне заподіяння шкоди	Це дії що спричиняються усвідомлено, знаючи про негативні наслідки. Під винуватців цієї загрози потрапляють ображений, нелояльний, підробляючий та впроваджений інсайдери.

1.2 Дослідження методів та засобів захисту систем відеоспостереження

1.2.1 Фізичний захист камер відеоспостереження

Вуличні відеокамери, будучи частиною системи безпеки об'єкту, самі досить уразливі і тому нерідко викрадаються. Розглянемо можливі заходи щодо захисту відеокамер.

Простий спеціалізований блок охоронної сигналізації для відеокамери з гнучким вибором функцій повинен відповідати наступним вимогам:

1. Має бути передбачена можливість підключення охоронного датчика, а також сирени і строб-спалахи (що відлякують потенційного викрадача), які розташовуються поблизу відеокамери

2. Блок повинен містити вбудований зумер і сигнальний світлодіод, що привертають увагу охорони при спробі викрадання.

3. Блок повинен допускати підключення зовнішньої кнопки, яка дозволяє охоронцеві примусово включати сирену і строб-спалах, щоб відлякувати викрадачів (вона ж може використовуватися для контролю роботи системи).

4. У блоці мають бути входи, розраховані на підключення вихідних релейних контактів тривоги відеомультиплексора або роздільника екрану (квадратора) - спрацьовування при пропажі відеосигналу.

5. Один з входів блоку, використовуваний для підключення датчика, що працює на розмикання, повинен використовуватися для підключення дроту, що заходить в кожух і транзитом що виходить з нього, утворюючи при цьому петлю (при обриві загального кабелю обірветься і цей дріт, приводячи до спрацьовування охоронної сигналізації).

6. У якості оповіщувачів, що сигналізують про викрадання, можуть служити детектори ударів і вібрацій, що розташовуються в кожухах, - спрацьовування до обриву кабелю.

7. У блоці мають бути передбачені запобіжники, що забезпечують працездатність сигналізації навіть при перерізанні кабелю, що йде до відеокамери або сирени (і можливому при цьому короткому замиканні по ланцюгу живлячої напруги).

Для проводового з'єднання дуже важливо грамотно розташувати дроти. Над даним питанням слід подумати під час проектування, проклавши найбільш оптимальні та безпечні маршрути. Самий недорогий і простий спосіб - здійснювати прокладку в спеціальних коробах. Дроти будуть надійно захищені від навмисного ушкодження і капризів природи. Другий спосіб, вмуровувати дротові лінії у стіни та стелю. Це забезпечить захист та сховає дроти від оточуючих. Проте, можуть виникнути складнощі при перепланування приміщення або модернізації системи. Також існує імовірність ненавмисного пошкодження кабелю у стіні некомпетентними робітниками.

1.2.2 Захист систем IP-відеоспостереження

З урахуванням комп'ютерів поста відеоспостереження, ми можемо виділити три ділянки (рис. 3.3.1) системи IP-відеоспостереження, які важливі з точки зору забезпечення безпеки:

– відеокамера та кабель підключення відеокамери до мережного обладнання - найбільш незахищений фізично ділянку

– мережеве обладнання у вигляді маршрутизаторів і комутаторів, які здійснюють передачу інформації в необхідну точку розташування поста спостереження

– зона кабельного підключення комп'ютерів поста спостереження до мережного обладнання, яке здійснює передачу відеосигналу.

Рисунок 1.9. Основні ділянки цифрової системи відеоспостереження

Розглянемо механізми захисту для кожної ділянки.

На фізичних аспектах захисту першого ділянки зупинятися немає сенсу, так як вони нічим не відрізняються від традиційних систем аналогового відеоспостереження. Єдине, що може отримати зловмисник без ризику бути виявленим (за умови вільного доступу до кабелю), - лише картинку з камери. При цьому, однак, йому потрібно спеціалізований програмно-апаратний комплекс на базі ноутбука, виготовити який під силу тільки експерту, який розбирається в комп'ютерних мережах, програмуванні та цифрової електроніки одночасно. Спроба ж вплинути на відеосигнал, що йде з камери (не кажучи вже про підключенні будь-якого джерела відеосигналу замість відеокамери), буде миттєво виявлена і запротокольована системою. Таку реакцію забезпечують

механізми контролю цілісності інформації, що передається, закладені в мережеві протоколи FastEthernet, IP і HTTPS, які здійснюють передачу даних від відеокамер по мережі. Таким чином, безпека ділянки підключення відеокамера - кабель у систем IP-відеоспостереження вище, ніж у аналогових систем.

Розглянемо з точки зору безпеки ділянку мережевого обладнання, який абсолютно незнайомий більшості фахівців з аналоговим системам відеоспостереження. Не володіючи спеціальними знаннями про принципи захисту інформації в корпоративних мережах і необхідним для цього обладнанням, деякі фахівці роблять поспішні заяви і проводять так звані тест-драйви мережевого обладнання, яке призначене не для створення корпоративних мереж, а для домашнього застосування. Давайте ж, нарешті, проллємо світло на це часто використовуваний для спекуляцій питання.

При побудові сучасних корпоративних комп'ютерних мереж до них пред'являються високі вимоги в частині надійності і безпеки переданих даних. Ці вимоги, як правило, навіть вище вимог до надійності та безпеки систем відеоспостереження. Адже найчастіше інформація для службового користування, що циркулює в корпоративній мережі, має значно більшу цінність, ніж зображення з відеокамери, встановленої біля входу на склад. Мережеве обладнання для корпоративних мереж таких виробників, як Cisco Systems або Allied Telesis, має централізовану багаторівневу захист і розмежування прав доступу на рівні користувачів та мережних пристроїв, забезпечує фільтрацію переданих даних на основі правил, встановлених адміністратором. Розглянемо докладніше такі механізми безпеки мережевих комутаторів, як віртуальні локальні мережі VLAN, Port Security, авторизація доступу на базі 802.1 x.

VLAN, як базову і найбільш поширену технологію обмеження доступу, підтримують практично всі комутатори для корпоративних мереж. Можна навіть сказати, що якщо в комутаторі немає підтримки VLAN, цей комутатор явно не для мережі сучасного підприємства.

За допомогою цієї технології всі пристрої системи IP-відеоспостереження виділяються в окрему групу, ізольовану від всіх інших пристроїв і користувачів, підключених до мережі, - віртуальну локальну мережу VLAN. Таким чином зводиться бар'єр, який обмежує обмін даними тільки в межах однієї конкретної VLAN. Користувачі, а разом з ними і потенційні зловмисники, природно, підключені до іншої аналогічної VLAN. Це означає, що у зловмисника немає фізичного доступу до пристроїв, роботу яких у нього є бажання порушити. Єдиний шлях - зламати керуючу консоль комутатора і вручну додати свій комп'ютер в VLAN системи IP-відеоспостереження. Одна невдача - доступ до консолі можливий тільки з робочого місця адміністратора, але ніяк не з довільного робочого місця користувача. Коло замкнулося.

Port Security**.** Отже, перший рубіж захисту, блокуючий доступ довільних користувачів комп'ютерної мережі компанії до системи IP-відеоспостереження, встановлено. Другий рубіж покликаний блокувати доступ сторонніх осіб, які не є співробітниками компанії, а значить, і потенційних зловмисників, безпосередньо до комп'ютерної мережі та мережевого обладнання. Цей рубіж і складається з механізмів Port Security. Це найбільш поширене серед виробників комутаторів локальних мереж назва спеціальних функцій, які охороняють кожен порт мережевого обладнання від підключення неавторизованих пристроїв. Адже навіть самому неписьменному хакеру відомо, що вільна розетка локальної мережі в офісі підключена до порту комутатора, який можна використовувати для доступу в корпоративну мережу.

Робота механізмів Port Security полягає в ідентифікації підключаються до портів комутаторів мережевих пристроїв і припиненні несанкціонованого доступу. У момент підключення будь-якого мережевого пристрою, наприклад ноутбука, механізм Port Security по таким характеристикам, як MAC-адресу підключається пристрою, його IP-адресу, однозначно визначає його як свого або чужого, і в останньому випадку (наприклад, для гостей компанії), дозволяє доступ тільки до мережі Інтернет.

Більш жорсткі настройки Port Security полягають у призначенні адміністратором відповідності кожного комп'ютера компанії конкретного порту комутатора, до якого він повинен бути підключений, і при порушенні цього правила порт комутатора повністю вимикається до його ручного включення адміністратором. Безумовно, зловмисник може встановити будь-яку MAC - і IP-адресу на свій ноутбук, однак для цього йому необхідно з'ясувати не тільки самі адреси, але і належність їх до портів комутатора. А ця конфіденційна інформація відома лише адміністратору безпеки комп'ютерної мережі компанії.

Авторизація доступу на базі 802.1x

Нарешті, третій рубіж, який контролює всі мережеві підключення персональних комп'ютерів і ноутбуків користувачів за допомогою паролів, зокрема, за даними їх облікових записів в середовищі Microsoft Windows. Мова йде про протокол 802.1 X. Тут треба зазначити, що часто правила Port Security ускладнюють і збільшують обсяг робіт з адміністрування і доставляють багато клопоту мобільним користувачам з ноутбуками. У таких випадках проектувальники мережевих рішень зупиняються на варіанті, що складається з зв'язки VLAN і протоколу 802.1 X. Цей протокол дозволяє реалізувати централізований контроль доступу до мережі компанії комп'ютерів і користувачів в точках їх підключення, на порти комутаторів.

Для використання в локальній мережі авторизації по протоколу 802.1 X необхідні комутатори з підтримкою 802.1 X і сервер авторизації RADIUS, який виконує авторизацію або з використанням внутрішньої бази даних користувачів, або перенаправляє запит на корпоративний сервер авторизації, наприклад, Active Directory. При успішної аутентифікації та авторизації підключення на комутатор завантажуються встановлені для конкретного користувача та його групи правила обробки мережевого трафіку, які дозволяють (або блокують) доступ користувача до певних частин мережевої інфраструктури компанії. Таким чином, адміністратор може обмежити доступ до системи IP-відеоспостереження тільки з певних комп'ютерів, у певний час і за певних користувачів. Підтримка 802.1 X

вбудована в багато операційні системи, тому, як правило, робота цієї схеми контролю доступу прозора для кінцевого користувача.

У випадках побудови територіально розподілених систем IP-відеоспостереження або вимушеного використання небезпечних ділянок телекомунікаційних мереж операторів зв'язку (таких, де немає можливості реалізувати заходи захисту) необхідно використовувати обладнання з підтримкою шифрування переданих по мережі даних. А саме обладнання з підтримкою технології віртуальних приватних мереж VPN (Virtual Private Network). Цей тип мережного обладнання забезпечує встановлення зашифрованих тунелів для передачі конфіденційних даних через небезпечні мережеві з'єднання. Крім шифрування обладнання підтримує контроль цілісності інформації, що передається та захист від її спотворення зловмисниками.

У більшості випадків типовий схемою підключення для мереж VPN є схема точка -точка з виділеним мережевим центром, в якому встановлюється так званий концентратор VPN. До нього підключаються і з ним взаємодіють маршрутизатори VPN, встановлені на об'єктах спостереження. Маршрутизатори VPN забезпечують захист переданих даних щодо безпечного тунелю від необхідного числа IP-відеокамер на пост спостереження, в якому розміщений концентратор VPN. В той же час ніяких фізичних обмежень на розміщення і число концентраторів VPN немає. Конфігурація мережі, що складається з пристроїв VPN, може бути такою, як потрібно з міркувань безпеки та географії розміщення об'єктів спостереження

У місцях установки IP-відеокамер або в точці їх підключення до небезпечної мережі встановлюються маршрутизатори VPN, які забезпечують безпечне підключення однієї або декількох IP-відеокамер до концентратора VPN. Так само як і IP-відеокамера, VPN маршрутизатор має один або декілька інтерфейсів FastEthernet, що дозволяє підключати до нього IP-відеокамери безпосередньо, тобто без будь-яких додаткових пристроїв.

Концентратори і маршрутизатори VPN розраховані на використання в корпоративних мережах, що підтримують досить сильні алгоритми шифрування 3DES або AES, стійкість до злому яких сьогодні більш ніж достатня для захисту систем IP-відеоспостереження Затримка шифрування, як правило, не перевищує 100 мс у разі апаратного шифрування/дешифрування. Цей важливий момент необхідно врахувати при виборі обладнання, оскільки не всі виробники встановлюють апаратний криптографічний процесор, і - як наслідок - при великих потоках даних можливі суттєві затримки в передачі відеоінформації. Що стосується масштабованості, то, наприклад, такий концентратор VPN, Cisco ASA 5505, зможе обробити дані з 10 точок підключення IP-відеокамер.

1.2.3 Захисні міри в напрямку ПЗ

Архітектура програмних засобів захисту інформації повинна включати:

– контроль безпеки: реєстрації входження в систему, фіксацію в системному журналі, контроль дій користувача;

– активну реакцію на порушення системи захисту контролю доступу до ресурсів мережі;

– контроль доступу;

– контроль захищеності ОС;

– контроль алгоритмів захисту;

– перевірку і підтвердження правильності функціонування технічного та програмного забезпечення.

Для надійного захисту інформації та виявлення випадків неправомірних дій проводиться реєстрація роботи системи: створюються спеціальні щоденники і протоколи, в яких фіксуються всі дії, пов'язані із захистом інформації в системі. Фіксуються час надходження заявки, її тип, ім'я користувача і терміналу, з якого ініціалізується заявка. При відборі подій, що підлягають реєстрації, необхідно мати на увазі, що зі зростанням кількості реєстрованих подій не може перегляд щоденника і виявлення спроб подолання захисту.

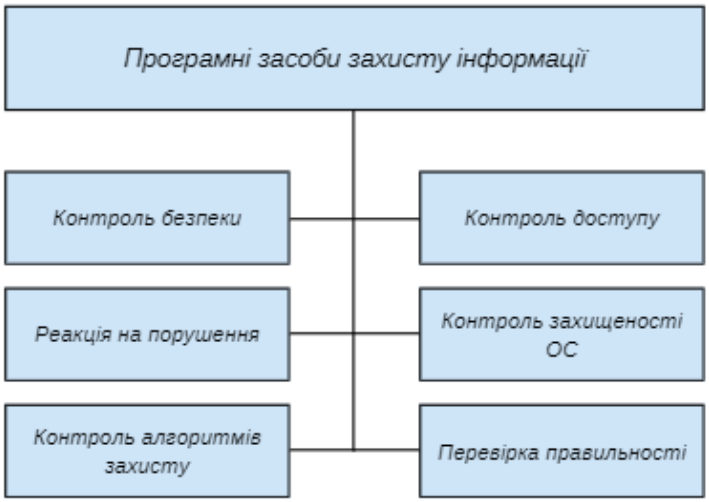


Рисунок 1.10. Архітектура програмних засобів захисту інформації

Використовуються також спеціальні програми для тестування системи захисту. Періодично або у випадково вибрані моменти часу вони перевіряють працездатність апаратних і програмних засобів захисту.

До окремої групи заходів щодо забезпечення збереження інформації та виявлення несанкціонованих запитів відносяться програми виявлення порушень в режимі реального часу. Програми даної групи формують спеціальний сигнал при реєстрації дій, які можуть призвести до неправомірних дій по відношенню до інформації, що захищається. Сигнал може містити інформацію про характер порушення, місці його виникнення та інші характеристики. Крім того, програми можуть заборонити доступ до інформації, що захищається або симулювати такий режим роботи (наприклад, моментальна завантаження пристроїв введення-виведення), який дозволить виявити порушника і затримати його відповідною службою.

Щоб захистити комп’ютери усієї мережі, потрібно одночасно використовувати брандмауер, антивірус і програмне забезпечення проти шкідливого ПЗ (антишпигуни).

Антивірус це спеціалізована програма, призначена для захисту операційної системи від комп'ютерних вірусів, шпигунських програм, хакерських атак і

іншого несанкціонованого доступу з метою крадіжки цінних особистих даних або несанкціонованого управління комп'ютером.

Класифікувати антивірусні продукти можна відразу за кількома ознаками, таким, як: використовувані технології антивірусного захисту, функціонал продуктів, цільові платформи.

По використовуваних технологіях антивірусного захисту:

- Класичні антивірусні продукти – продукти, які застосовують тільки сигнатурний метод детектування;
- Продукти проактивного антивірусного захисту – продукти, які застосовують тільки проактивні технології антивірусного захисту;
- Комбіновані продукти – продукти, які застосовують як класичні, сигнатурні методи захисту, так і проактивні.

За функціоналом продуктів:

- Антивірусні продукти – продукти, що забезпечують тільки антивірусний захист;
- Комбіновані продукти – продукти, що забезпечують не тільки захист від шкідливих програм, але і фільтрацію спаму, шифрування та резервне копіювання даних та інші функції.

1.2.4 Організаційні заходи захисту

Для зниження кількості загроз пов’язаних з низькою компетенцією або вмотивованістю працівників необхідно:

- ретельний підбір персоналу, його навчання, стажування, тренування;
- регулярно проводити чи відправляти робітників на курси підвищення кваліфікації або тренінги;
- заохочувати робітників до вдосконалення їх професійних навичок;
- адекватна заробітна платня та право на відпочинок

Для захисту даних від пошкодження необхідно:

- досліджувати і аналізувати ризики пошкодження даних та розробляти заходи щодо їх зменшення, уникнення чи обходу;

– чітко визначити функцій всіх учасників інформаційних процесів, обумовивши перелік даних, до яких той чи інший працівник має доступ, та порядок цього доступу;

– розробити інструктивні матеріали щодо дій працівників з метою уникнення пошкодження інформації чи зменшення негативного впливу наслідків таких випадків, довести їх до всіх зацікавлених осіб і організувати контроль за їх виконанням;

– мінімізувати ризик для тих, хто працює з особливо важливою інформацією, та членів їх родин з метою запобігання випадкам вимагання даних;

– визначити стратегію та практичні кроки резервування даних. Резервних копій рекомендується мати щонайменше дві. Обидві копії повинні зберігатись в надійних умовах але в територіально розділених місцях;

– розробити заходи з організації розподіленого зберігання та використання важливих даних, що дасть змогу зменшити негативні наслідки втрати даних при втраті частини даних.

Для захисту від несанкціонованого доступу вживаються наступні організаційні заходи:

– система електронних перепусток для персоналу і відвідувачів;

– системи відеоспостереження та відеореєстрації, які дають можливість вести цілодобовий візуальний нагляд за об'єктом як зовні, так і всередині.

– розподіл доступу до інформації, тобто чітке визначення, на які дані має право та чи інша особа. Персонал інформаційних відділів не повинен мати доступу до баз даних, але користувачі баз даних не повинні мати доступу до системи управління базами даних;

– систематичний аналіз журналу роботи мережі, виявлення випадків спроб підбирання паролів.

1.2.5 Розробка методики відповідності механізмів захисту до класу загроз

Проаналізувавши основні механізми захисту сучасних систем відеоспостереження сформуємо таблицю що буде відображати відповідність механізмів захисту до загроз.

Таблиця 1.2 – Відповідність механізмів захисту до загроз сучасної СОТ

Загрози	Механізм захисту
Мережеві загрози	
DDOS – атаки	Спеціальні рішення проти DDOS – атак
	Використовувати ПЗ від виробника обладнання або від надійних розробників, які постійно оновлюють своє ПЗ
	Використовування SSH
	Використання брандмауерів
	Port Security
Вторгнення і модифікація даних	Автентифікація IEEE 802.1X
	Автентифікація за MAC – адресами
	Криптозахист (WPA2)
	VLAN/VPN
	Port Security
Вардрайвінг	Автентифікація IEEE 802.1X
	Автентифікація за MAC – адресами
	Криптозахист (WPA2)
	Port Security
Абонент-шахрай	Приховування SSID
	Автентифікація IEEE 802.1X
	Автентифікація за MAC – адресами
	VLAN/VPN

	Port Security
Man-in-Middle	Криптозахист (WPA2)
	VLAN/VPN
Атаки на мережеве обладнання	Автентифікація IEEE 802.1X
	Криптозахист (WPA2)
	VLAN/VPN
FMS-атака та атака KOREK'A	Криптозахист (WPA2)
Помилкова точка доступу	Приховування SSID
	Автентифікація за MAC – адресами
	Автентифікація IEEE 802.1X
Таємні бездротові канали (потайний вхід в мережу)	Моніторинг ефіру на наявність невідомих бездротових мереж
Загрози інфраструктури	
Глушіння	Наявність модулів відеоаналітики
	Фізична охорона периметра
Фізичне пошкодження кабельної інфраструктури	Закриті жолоби для кабельної інфраструктури
	Відсутність кабелів поза КЗ
	Фізична охорона периметра
Перехоплення сигналу поза контрольованою зоною	Приховування SSID
	Зниження потужності передавача
	Розміщення передавача далі від межі КЗ
	Якість обладнання
Відсутність або нестабільність електроживлення	Наявність генератора
	Наявність акумулятора
	Наявність випрямляча напруги
	Категорія об'єкта по електропостачанню
Загрози ПЗ	
Комп'ютерні віруси	Антивірусне ПЗ
	Налаштування Firewall
	Використання UNIX систем на серверах
Прості паролі	Використання безпечних паролів
	Обмеження доступу працівників до паролів

	Безпечне зберігання паролів
Уразливості в прошивках відеосерверів	Використовувати прошивки лише від виробника обладнання або від надійних розробників
Застаріле ПЗ	Використовувати ПЗ від виробника обладнання або від надійних розробників, які постійно оновлюють своє ПЗ
Загрози обладнання	
Пошкодження камер, а також закриття, зафарбовування, заклеювання, засвічування об'єктива	Наявність модулів відеоаналітики
	Висота монтажу камери більше 2,5 м
	Використання захисних кожухів, гвинтів, кронштейнів та клітки для камери
	Інтеграція із іншими засобами охорони периметру
Погодні умови	Захисні кожухи
	Наявність заземлення та вирівнювачів напруги
Пошкодження відеоархіву	Розмежування доступу (фізичного та мережевого)
	Наявність резервного копіювання даних
	Шифрування даних
	Наявність інших засобів охорони периметра
Відмова обладнання (брак, несправності, знос)	Тестування обладнання при інсталяції та планове під час експлуатації
Загрози з боку персоналу	
Неспроможність виконувати службові обов’язки.	Проведення курсів підвищення кваліфікації або тренінгів
	Заохочення співробітників до вдосконалення їх професійних навичок
	Наявність посадових інструкцій
	Оцінка кількості роботи на для співробітників (перерозподіл обов’язків між співробітниками)
Помилки/Ненавмисне заподіяння шкоди	Проведення курсів підвищення кваліфікації або тренінгів
	Наявність посадових інструкцій
	Розмежування доступу (фізичного та мережевого)
	Наявність модулів відеоаналітики

	Ведення логів на серверах та мережевому обладнанні
	Наявність резервного копіювання даних
Низька ефективність працівників	Стимулювання лояльності співробітників гарними умовами праці та платнею.
	Заохочення співробітників до вдосконалення їх професійних навичок
	Проведення курсів підвищення кваліфікації або тренінгів
Умисне заподіяння шкоди	Розмежування доступу (фізичного та мережевого)
	Наявність резервного копіювання даних
	Ведення логів на серверах та мережевому обладнанні

1.3 Розробка онлайн-рішення з оцінки рівня захищеності системи відеоспостереження

1.3.1 Формування технічного завдання

У попередніх частинах роботи було розглянуто сучасні системи відеоспостереження, виявлено їх вразливості та визначено методи захисту. Використовуючи ці данні, можливо побудувати автоматизовану систему аналізу загроз систем відеоспостереження, яка дозволятиме швидко та без зайвих зусиль визначити слабкі місця у системі відеоспостереження та запропонує методи для підвищення рівня захищеності.

Основні вимоги до системи:

1. Простота – система не повинна викликати труднощі у використанні. Інтерфейс повинен бути зручним та інтуїтивно зрозумілим для більшості інтернет користувачів.

2. Швидкість – як показують дослідження, користувач сприймає очікування не більше 3-4 секунд. Отже система не повинна бути важкою для ПК.

3. Доступність – дана система планується як інструмент який повинен допомогти користувачу без зайвих зусиль провести первинний аналіз рівня захищеності системи відеоспостереження будь-який час та у будь-якому місці .

4. Анонімність – інформація яку збирає система у користувача повинна бути мінімальна та безособова.

Основні області застосування:

1. Малий бізнес – у наш час майже жодний представник малого бізнесу не в змозі собі дозволити витрачати кошти на аудит інформаційної безпеки, а у більшості випадків і на саму інформаційну безпеку. Проте потреба підприємств малого бізнесу у фізичній та інформаційній безпеці зростає з кожним днем.

2. Середній бізнес – у представників середнього бізнесу потреби у інформаційній безпеці значно вищі і функціоналу системи, що проектується, може бути недостатньо. Проте це для тих бізнесменів, що не бажають витрачати кошти на дорогий аудит безпеки, хочуть перевірити рівень захищеності на локальному об’єкті чи просто не дуже переймаються безпекою свого бізнесу можуть задовольнити свої потреби користуючись даним ресурсом.

3. Для домашнього застосування – багато пересічних громадян почали використовувати відеоспостереження для захисту своїх домівок, загородних будинків, місць для паркування тощо. Система допоможе їм захистити не тільки свою інформацію, а і своє приватне життя.

4. Фірми, що займаються монтажем СОТ – фірми підрядники певно мають достатню кваліфікацію для проектування СОТ, проте вони можуть використовувати даний ресурс при роботі з замовником чи просто користуватися як шпаргалкою.

5. У навчальних цілях – зручність та інформативність системи дозволить використовувати її в навчальних цілях.

1.3.2 Дослідження можливостей системи та інструментів

Слідуючи з попереднього пункту, визначимо необхідні технічні заходи та розробимо архітектуру системи.

Для більшої гнучкості та зручності, було прийнято рішення створити цю систему у вигляді WEB-сайту.

Для побудови системи було обрано наступний набір WEB-технологій:

- HTML5;
- CCS3;

– JavaScript, Chartjs.

Даний набір технологій дозволить зробити взаємодію користувача з системо простим, зручним да досить швидким завдяки відсутністю запитів на сервер при заповнені анкети та при побудові діаграм. Вся обробка інформації проводиться на стороні користувача. Це також підвищує безпеку користувача.

Робота із системою складається із 3-х кроків:

1. Сбір даних про СОТ, співробітників, що її обслуговують та фірму підрядника, що займається монтажем та обслуговуванням СОТ;

2. Аналіз отриманих даних, побудова Радару Загроз, який показує на скільки СОТ є захищеною.

3. Формування методів для підвищення рівня захищеності СОТ та візуальне відображення їх ефективності на Радарі Загроз.

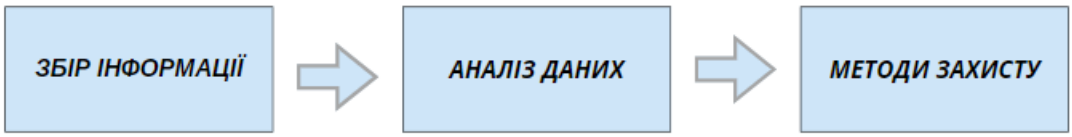


Рисунок 1.11. Алгоритм роботи з системою

Для збору інформації буде використовуватися анкета яка складається з 10-ти пунктів, у кожному з яких будуть питання з варіантами відповідей (див. Додаток А).

Після отримання необхідної інформації від користувача система повинна побудувати радар загроз та вирахувати рівень захищеності системи.

Перш за все необхідно надати всім загрозам коефіцієнти, які будуть відображати на скільки певна загроза є значною у контексті відеоспостереження, а разом із цим надати коефіцієнти механізмам захисту які будуть відображати на скільки ефективні ті чи інші методи. Розглядаємо загрози для відеоспостереження, а не для ЛОМ підприємства.

Для зручності та простоти сприйняття для оцінки будемо використовувати десятибальну шкалу. Наприклад: усі загрози у рамках Загроз інфраструктури

мають сумарний коефіцієнт 10, загроза вважається усунутою чи мінімізованою якщо сума коефіцієнтів методів захисту дорівнює 10. Як ви можете бачити у табл. 4.1 біля деяких механізмів захисту стоїть помітка «обов'язково». Це означає, що без використання цього механізму забезпечення безпеки неможливе та інші методи втрачаюсь свою ефективність.

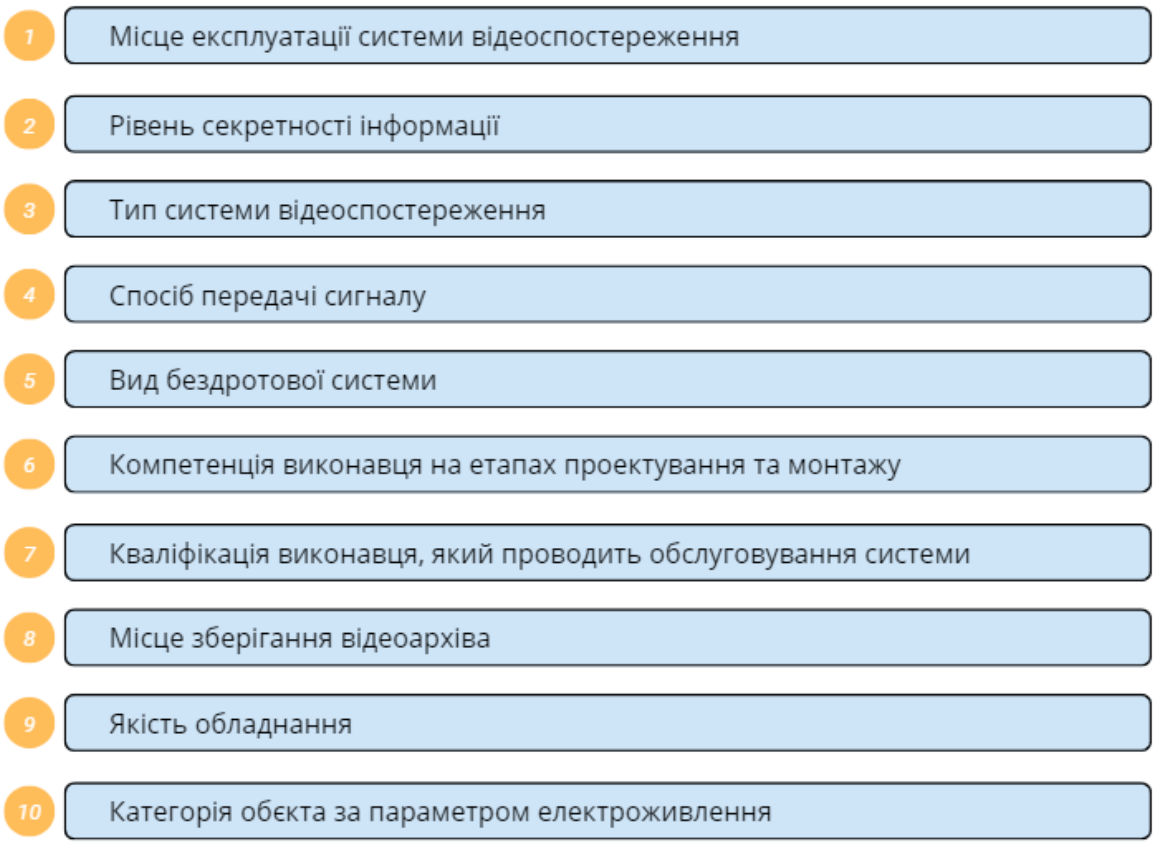


Рисунок 1.12. Алгоритм інтерактивної анкети для подальшого вибору механізмів захисту

Таблиця 4.1 – Коефіцієнти загроз та ефективності механізмів захисту

Загрози	Вага загрози	Механізм захисту	Ефективність механізму захисту
Мережеві загрози			
DDOS – атаки	2	Спеціальні рішення проти DDOS – атак	4
		Використовувати ПЗ	1

		від виробника обладнання або від надійних розробників, які постійно оновлюють своє ПЗ	
		Використовування SSH	2 (обов'язково якщо архів зберігається у хмарному сервісі)
		Налаштування Firewall	2
		Port Security	1
Вторгнення і модифікація даних	1,5	Автентифікація IEEE 802.1X	2
		Використовування SSH	2
		Криптозахист (WPA2)	1 (Обов'язково, для бездротових систем)
		VLAN/VPN	3
		Port Security	2
Вардрайвінг	1 (для бездротових)	Автентифікація IEEE 802.1X	3
		Автентифікація за MAC – адресами	3
		Криптозахист (WPA2)	4
Абонент-шахрай	1	Приховування SSID	0,5
		Автентифікація IEEE 802.1X	3
		Автентифікація за MAC – адресами	1,5
		Використовування SSH	2,5
		Port Security	2,5
Man-in-Middle	1	Криптозахист (WPA2)	5
		VLAN/VPN	5
Атаки на мережеве обладнання	1	Автентифікація IEEE 802.1X	2
		Криптозахист (WPA2)	2 (Обов'язково для

			бездротових систем)
		Port Security	3
		VLAN/VPN	3
FMS-атака та атака KOREK'A	0,5 (для бездротових)	Криптозахист (WPA2)	10
Помилкова точка доступу	1 (для Wi-Fi)	Приховування SSID	1
		Автентифікація за MAC – адресами	4,5
		Моніторинг ефіру на наявність невідомих бездротових мереж	4,5
Таємні бездротові канали (потайний вхід в мережу)	1 (для бездротових)	Моніторинг ефіру на наявність невідомих бездротових мереж	5
		Рівень спеціаліста, що займається безпекою	5
Загрози інфраструктури			
Глушіння	2	Наявність модулів відеоаналітики	6
		Фізична охорона периметра	4
Фізичне пошкодження кабельної інфраструктури	2,5	Закриті жолоби для кабельної інфраструктри	3
		Відсутність кабелів поза КЗ	3
		Фізична охорона периметра	2
		Рівень спеціаліста, що займався монтажем системи	2
Перехоплення сигналу поза КЗ	2 (для бездротових)	Приховування SSID	1
		Зниження потужності передавача	3
		Розміщення передавача далі від межі КЗ	3
		Якість обладнання	3
Відсутність або	3,5	Наявність генератора	3

нестабільність електроживлення		Наявність акумулятора	3
		Наявність заземлення та вирівнювачів напруги	2
		Категорія об'єкта по електропостачанню	2
Загрози ПЗ			
Комп’ютерні віруси	2	Антивірусне ПЗ	2
		Налаштування Firewall	2
		Використання UNIX систем на серверах	3
		Рівень спеціаліста, що займається безпекою	3
Прості паролі	3	Використання безпечних паролів	5 (обов’язково)
		Обмеження доступу працівників до паролів	3
		Безпечне зберігання паролів	2
Уразливості в прошивках відеосерверів	2,5	Використовувати ПЗ від виробника обладнання або від надійних розробників, які постійно оновлюють своє ПЗ	3
		Рівень спеціаліста, що займається безпекою	3
		Якість обладнання	4
Застаріле ПЗ	2,5	Рівень спеціаліста, що займається безпекою	6
		Використовувати ПЗ від виробника обладнання або від надійних розробників, які постійно оновлюють своє ПЗ	4
Загрози обладнання			
Пошкодження камер, а також закриття, зафарбовування, заклеювання, засвічування об'єктива	3	Наявність модулів відеоаналітики	3
		Висота монтажу камери більше 2,5 м	1
		Використання захисних кожухів, гвинтів, кронштейнів та клітки для камери	1

		Інтеграція із іншими засобами охорони периметру	2
		Рівень спеціаліста, що займається безпекою	1
		Рівень спеціаліста, що займався монтажем системи	2
Погодні умови	1	Якість обладнання	5
		Використання захисних кожухів, гвинтів, кронштейнів та клітки для камери	3
		Наявність заземлення та вирівнювачів напруги	2
Пошкодження відеоархіву	3,5	Розмежування доступу (фізичного та мережевого)	2
		Наявність резервного копіювання даних	2,5 (обов'язково якщо архів зберігається у хмарному сервісі)
		Шифрування даних	1
		Наявність інших засобів охорони периметра	1
		Якість обладнання	2
		Рівень спеціаліста, що займається безпекою	1,5
Відмова обладнання (брак, несправності, знос)	2,5	Тестування обладнання при інсталяції та планове під час експлуатації	4
		Рівень спеціаліста, що займається безпекою	2
		Якість обладнання	4
Загрози з боку персоналу			
Неспроможність виконувати службові обов'язки.	2,5	Рівень спеціаліста, що займається безпекою	4
		Проведення курсів підвищення кваліфікації або тренінгів	2
		Наявність посадових інструкцій	2
		Заохочення співробітників до вдосконалення їх професійних навичок	1

		Оцінка кількості роботи співробітників (перерозподіл обов'язків між співробітниками)	1
Помилки/Ненавмисне заподіяння шкоди	2,5	Проведення курсів підвищення кваліфікації або тренінгів	0,5
		Розмежування доступу (фізичного та мережевого)	2
		Наявність посадових інструкцій	1
		Наявність модулів відеоаналітіки	0,5
		Ведення логів на серверах та архівах	1
		Наявність резервного копіювання даних	2
		Рівень спеціаліста, що займається безпекою	3
Низька ефективність працівників	1	Рівень спеціаліста, що займається обслуговуванням системи	2
		Стимулювання лояльності співробітників гарними умовами праці та платнею	3
		Оцінка кількості роботи співробітників (перерозподіл обов'язків між співробітниками)	1,5
		Заохочення співробітників до вдосконалення їх професійних навичок	1,5
		Проведення курсів підвищення кваліфікації або тренінгів	2
Умисне заподіяння шкоди	4	Розмежування доступу (фізичного та мережевого)	4
		Наявність резервного копіювання даних	4
		Ведення логів на серверах та архівах	2

На перший погляд деякі оцінки не є оптимальними, проте на це є певні причини. Звернемося до статистики кіберзагроз за 2024 рік:

1. Перше місце вже котрий рік поспіль зберігають за собою DDOS-атаки. Їх особливість полягає в тому що їх здатен проводити майже кожен користувач просто переглянувши декілька відео на YouTube;

2. Фішингові атаки займають друге місце. Цілями цих атак є люди. Зловмисник розсилає шкідливі електронні повідомлення від імені служб технічної підтримки, роботодавців, соціальних мереж, банків і т. д., щоб отримати особисті дані користувача. Небезпека полягає у тому, що не обов'язково атака одразу буде спрямована проти організації. Заволодівши особовими даними працівника, зловмисник може завербувати його і використати посадове становище жертви. Саме тому у даній роботі стільки уваги приділено роботі з людьми.

3. Недолік управління патч-файлами. Багато організацій не зобов'язують співробітників оновлювати системи безпеки браузерів, програм і баз даних, тим самим відкриваючи доступ хакерам.

4. Помилки співробітників. Співробітники також піддають ризику безпеку компанії, коли втрачають корпоративні пристрої, обмінюються паролями або коли не здатні виконувати свої службові повноваження. За статистикою 46% прогалин у системі безпеки відбувається з вини співробітників.

1.3.3 Програмна реалізація онлайн-рішення

З програмної точки зору система складається с 5 файлів (код представлено в додатках):

1. index.html – головний файл сайту. У ньому зберігається верстка сайту та приєднуються усі інші частини системи.

2. style.css – файл у якому зберігаються стилі. Цей файл визначає статичний зовнішній вигляд сторінки.

3. form.js – тут обробляється інформація що поступає від користувача при заповнені анкети.

4. methods.js – у даному файлі обробляються методи які користувач обирає для поліпшення стану системи.

5. chart.js – файл відповідний за відображення діаграм.

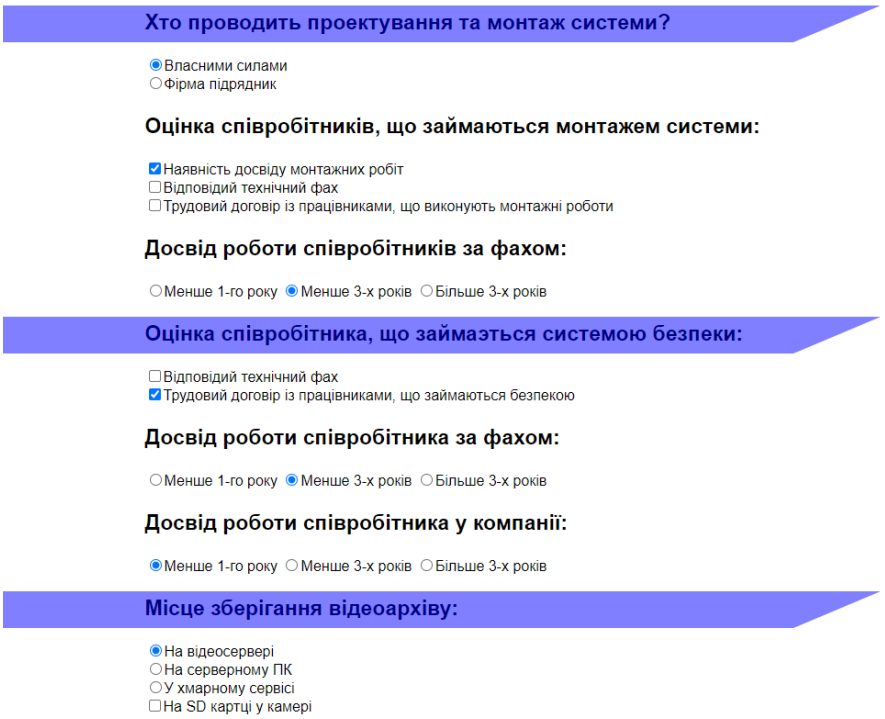


Рисунок 1.13. Частина питань з інтерактивного опитувального листа

1.3.4 Побудова радару загроз та оцінка захищеності системи відеоспостереження

Радар загроз – діаграма, яка графічно відображає захищеність системи відеоспостереження від загроз по кожному напрямку (Мережеві загрози, загрози інфраструктури, загрози обладнання, загрози ПЗ та людські загрози). Після відповідей на питання з інтерактивної анкети будується радар загроз, де у візуальній формі відразу видно поточну ситуацію з рівня безпеки системи відеоспостереження. Так, на рис. 1.14 представлено радар загроз в ситуації, коли рівень захисту системи низький.

На радарі присутні 3 статичні та 2 динамічні зони які допомагають зрозуміти поточний рівень захисту:

– Зона високого ризику – статична зона, позначається червоним кольором. Якщо якийсь із показників знаходиться у цій зоні, то це означає що необхідно прийняти заходи для захисту системи у цьому напрямку.

– Допустима зона – статична зона, позначається жовтим кольором. Ця зона є задовільною для більшості користувачів, проте вона не гарантує безпеки.

– Безпечна зона – статична зона, позначається зеленим кольором. Показує що захисту даному напрямку на високому рівні.

– Поточний рівень захисту – динамічна зона, позначається синім кольором. Показує поточний стан захищеності системи з урахуванням усіх прийнятих методів захисту.

Початковий рівень захисту – необов'язкова зона, динамічна зона, позначається фіолетовим кольором. З'являється тільки після натискання кнопки «Зберегти стан системи». Дозволяє порівняти систему до та після прийняття методів захисту. Радар дає розуміння де та якими методами та засобами користувач системи безпеки має можливість підвищити рівень захисту безпосередньо системи відеоспостереження, як складової загальної системи безпеки об'єкта. Як видно з рис.1.14 чотири з п'яти напрямів захисту системи відеоспостереження знаходяться в червоній зоні, що потребує термінових дій. Далі потрібно вивести параметр в жовту, або, оптимально – в зелену зону.

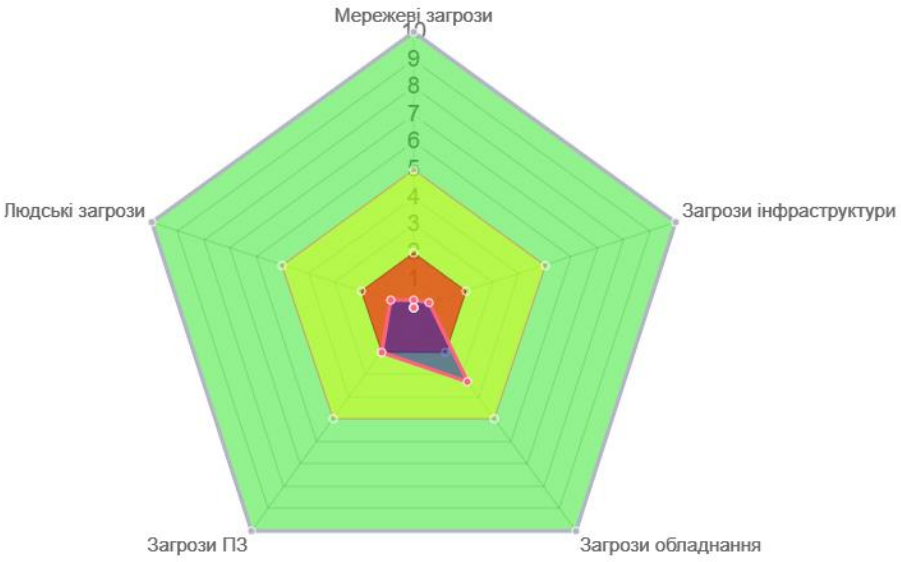


Рисунок 1.14. Візуалізація стану рівня захисту системи відеоспостереження при низькому рівні

Розглянемо дії на прикладі загроз інфраструктури. Захист в цьому напрямку представлено в чотирьох категоріях в кількості 11-ти механізмів. Отже, обираючи їх, ми підвищуємо рівень захисту та отримуємо план подальших дій. На рис.4.5 показано обрані механізми захисту.

Загрози інфраструктури	
Загрози	Механізми захисту
Глушіння	☐ Наявність відеоаналітки ☑ Фізична охорона периметра
Фізичне пошкодження кабельної інфраструктури	☐ Закриті жолоби для кабельної інфраструктри ☑ Фізична охорона периметра ☑ Відсутність кабелів поза КЗ
Перехоплення сигналу поза КЗ	☑ Приховування SSID ☐ Зниження потужності передавача ☐ Розміщення передавача далі від межі КЗ
Відсутність або нестабільність електроживлення	☑ Наявність генератора ☑ Наявність акумулятора ☐ Наявність випрямляча напруги

Рисунок 1.15. Фрагмент інтерактивної таблиці з обраними механізмами захисту

На рис. 1.16 представлено радар загроз після застосування механізмів захисту в напрямку інфраструктури. Як видно, показних знаходиться на межі між жовтою та зеленою зоною, що говорить про високий рівень захисту в цьому напрямку.

Використання навіть базових механізмів захисту прибирає більшість загроз та ризиків, які направлені на систему відеоспостереження. Тож, розуміння реального стану безпеки системи відеоспостереження та можливість щодо моделювання механізмів захисту дає можливість усунути проблеми та вивести захист на високий рівень.

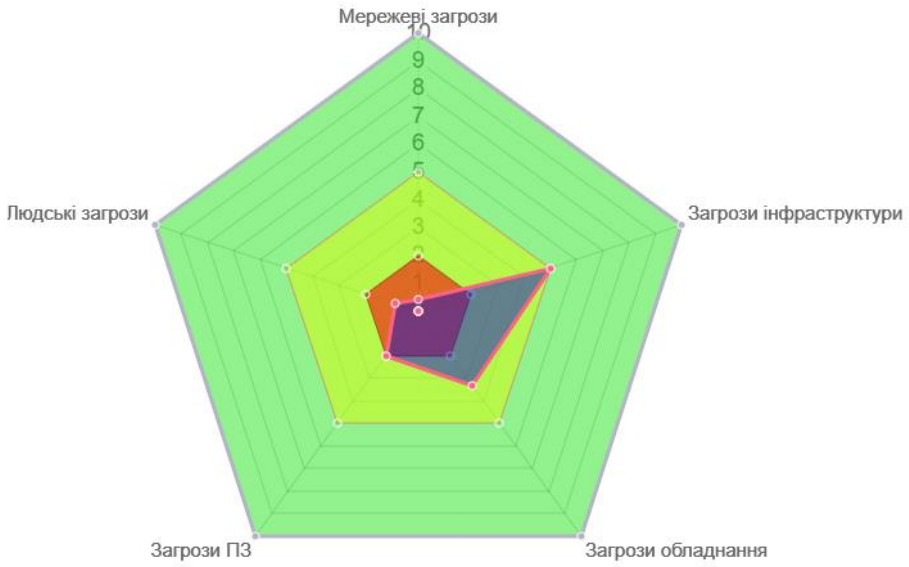


Рисунок 1.16. Радар загроз після застосування механізмів захисту в напрямку інфраструктури

.

Рисунок 1.17. Радар загроз після застосування механізмів захисту базових напрямах аудиту стану ІБ системи відеоспостереження

2 ЕКОНОМІЧНИЙ РОЗДІЛ

2.1 Резюме

В даному дипломному проекті виконано розробку онлайн-рішення з оцінки захищеності систем відеоспостереження. Оцінка якості програмного продукту з точки зору користувача визначається необхідним на стадії функціонування розміром оперативної пам'яті ЕОТ, витратами машинного часу, пропускною спроможністю каналів передачі даних. Оцінка якості програмного продукту включає визначення трудомісткості і вартості його створення.

Проведемо розрахунки визначення трудомісткості розробки даного програмного продукту.

2.2 Розрахунок ціни програмного продукту нормативним методом

Тривалість розробки програмного продукту залежить від його обсягу, трудомісткості розробки, кваліфікації виконавців, а також планових термінів, визначених умовами ринку.

Методом структурної аналогії по відповідних каталогах аналогів програмного забезпечення визначається обсяг програмних засобів, у тисячах умовних машинних команд програми аналога.

У таблиці 2.1 представлені аналоги програмного забезпечення, функції яких, у більшому або меншому ступені, виконує розроблений програмний продукт.

Таблиця 2.1 - Аналоги програмного забезпечення

Найменування ПП	Обсяг функції ПП – V_o, усл. машинних командах.
1. ПП СУБД	2500 – 9800
2. Комплексні системи ведення БД	950 – 7430
3. ПП введення інформації	1060 – 5750
4. ПП оптимізації розрахунків	1300 – 4200

5. ПП автоматизації засобів по каталогу	680 – 7000
6. ПП автоматизованих розрахунків	1300 – 8600
7. ПП загальної математики і ПП імітаційного моделювання	7800 – 8800
8. ПП організації обчислювального процесу	13000 – 10200

Для нашого варіанта виділено сірим кольором.

Вибравши аналог ПП, що містить Vo в умовних машинних командах, трудомісткості визначати на основі табл.2.2

Таблиця 2.2

Обсяг ПП, тис.умов.машинних команд	Норма часу, люд/год
1.00	229
2.00	244
3.00	262
4.00	283
5.00	306
6.00	330
7.00	357
8.00	385
9.00	414
10.00	445
12.00	510
14.00	580
16.00	654
18.00	731
20.00	812

На підставі отриманого значення, по довіднику, визначається укрупнена норма часу на розробку аналога програмного забезпечення (коректується

поправочним коефіцієнтом враховуючої умови розробки ПП, тобто в умовах комп'ютера, Кк=0,7÷0,8): Тар = 229 х 0,7 = 160,3 (люд/годин).

Трудомісткість програмного продукту визначається по кожному етапу розробки окремо на підставі трудомісткості аналога з урахуванням складності розробки, ступеня новизни і ступеня використання в розробці стандартних модулів на підставі формул:

$$T_{ТЗ} = T^a p \times L_1 \times K_H \quad (2.1)$$

$$T_{ТП} = T^a p \times L_2 \times K_H \quad (2.2)$$

$$T_{РП} = T^a p \times L_3 \times K_H \times K_T \quad (2.3)$$

Для розрахунку необхідні наступні коефіцієнти:

Li – питома вага і-го етапу розробки (див. табл. 2.2);

Кн – поправочний коефіцієнт, що враховує ступінь новизни (див. табл. 2.3);

Кт – поправочний коефіцієнт, що враховує ступінь використання в розробці типових програм (див. табл. 2.4).

Таблиця 2.3. Значення питомих коефіцієнтів трудомісткості стадії в загальній трудомісткості розробки ПП

Код стадії	Ступінь новизни		
	А	Б	В
ТЗ (L_1)	0,15	0,12	0,12
ТП (L_2)	0,16	0,15	0,11
РП (L_3)	0,55	0,58	0,61

Для нашого варіанта виділено сірим кольором.

Таблиця 2.4. Значення поправочного коефіцієнта, що враховує ступінь новизни

Код ступеня новизни	Ступінь новизни	Значення $К_н$
А	Принципово нове ПЗ	1,75 – 1,2
Б	ПЗ – розвиток визначеного параметричного ряду	1,0 – 0,8
В	ПЗ, що має аналог	0,7

Для нашого варіанта виділено сірим кольором.

Тому що розробка системи є ПЗ, що має аналоги програмних продуктів, то код ступеня новизни для мого ПЗ – В, а значення коефіцієнта $К_н$=0,7. По таблиці 2.3, знаючи код ступеня новизни, тепер можна визначити значення питомих коефіцієнтів трудомісткості:

L_1=0,12;

L_2=0,11;

L_3=0,61;

Таблиця 2.5. Значення коефіцієнта ступеня використання в розробці типових програм

Ступінь охоплення реалізованих функцій розроблювального ПЗ типовими програмами, %	Значення $К_т$
60 і вище	0,6
40-60	0,7
20-40	0,8
До 20	0,9

Для нашого варіанта виділено сірим кольором.

У розробленому програмному продукті використовується від 40 до 60 відсотків існуючих функцій, це значить, що $К_т$=0,7.

Тепер розраховуємо трудомісткість по кожному етапу окремо:

Трудомісткість технічного завдання

$$Т_{тз}=Та*L_1*К_н=160,3 *0,12*0,8= 15,38 \text{ (люд/годин)} \quad (2.4)$$

Трудомісткість розробки технічного проекту

$$Т_{тп}=Та*L_2*К_н=160,3 *0,11*0,8 = 14,11 \text{ (люд/годин)} \quad (2.5)$$

Трудомісткість розробки робочого проекту

$$Т_{рп}=Та*L_3*К_н*К_т=160,3 *0,61*0,8*0,8= 62,58 \text{ (люд/годин)} \quad (2.6)$$

Для подальших розрахунків визначили кількість папера, витраченого на кожен етап:

- технічне завдання $N_{тз}$=3 (стр),

- розробка ТП $N_{тп}$=15(стр),

- розробка робочого проекту $N_{рп}$=20 (стр),

- пояснювальна записка відповідно $N_{пз}$=30 (стр)

Таблиця 2.6. Розрахунок трудомісткості ПП

Найменування етапів	Розрахунок, годин.		
1	2	3	4
1.ТЗ	$T_{Ртз}$=15,38	$T_{кк}$=0,7*$N_{тз}$= 0,7*3=2,1	$T_{нк}$=0,15*$N_{тз}$=0,15*3= 0,45
2.Розробка ТП	$T_{Ртп}$=14,11	$T_{кк}$=0,7*$N_{тп}$=0,7*15=10,5	$T_{нк}$=0,15*$N_{тп}$=0,15*15 =2,25
3.Розробка РП	$T_{Ррп}$= 62,58	$T_{кк}$=0,7*$N_{рп}$=0,7*20=14,0	$T_{нк}$=0,15*$N_{рп}$=0,15*20 =3,0
4.Розробка ПЗ	$T_{пз}$=1,5**$N_{пз}$= 1,5*30 =45	$T_{кк}$=0,7*$N_{тз}$=0,7*30=21,0	$T_{нк}$=0,15*$N_{пз}$=0,15*30 =4,5
Усього, в т.ч.:	194,87		
- на розробку	$\Sigma T_р$=137,07		
- контроль керівника		$\Sigma T_{кк}$=47,6	
- нормоконтроль			$\Sigma T_{нк}$=10,2

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Роботодавець або уповноважені ним органи зобов'язані дбати про умови праці працівників, полегшувати їх, оздоровляти навколишнє середовище, дбати про виконання правил безпеки і інструкцій по техніці безпеки.

Координує всю цю діяльність служба охорони праці, яка в залежності від чисельності працюючих може функціонувати як самостійний структурний підрозділ (число працюючих 50 і більше), або у вигляді групи спеціалістів чи одного спеціаліста, у тому числі за сумісництвом (число працюючих 20 і менше). Задачі службі охорони праці та її функції викладені в Типовому положенні про службу охорони праці», яке затверджено наказом Комітетом Держнаглядохоронпраці (ДНАОП 0.00-4.21-93) .

Працівники також повинні відповідально ставитись до охорони праці, знати та виконувати вимоги, визначені нормативною документацією. В сучасних умовах кожному працівнику необхідно постійно підтримувати високий фізичний, психологічний та фаховий рівень, запобігати виникненню випадків травматизму та профзахворювань.

Безпечні умови праці на підприємстві досягаються за рахунок забезпечення безпеки виробничих процесів, які обґрунтовані і прийняті в технологічній частині дипломного проекту.

3.1 Аналіз небезпечних та шкідливих чинників, що впливають на працівника

Для установлення можливого впливу на здоров'я користувачів ВДТ виробничих чинників має значення ряд якісних характеристик робочого середовища. Це середовище у приміщеннях (офісах) в основному характеризується такими фізичними параметрами, як температура, вологість та електричний опір підлоги. Фізико-хімічні показники включають інформацію про

вміст у повітрі іонів та різноманітних забруднювачів, а також деякі інші якісні характеристики середовища

3.2 Розробка заходів з охорони праці

3.2.1 Виробничі приміщення

Будівлі та приміщення, де розміщені робочі місця програмістів повинні відповідати вимогам СНіП 2.09.02-85 «Производственные здания» та ДСанПіН 3.3.2.007 «Державні санітарні правила і норми роботи з ВДТ ЕОМ» Вони мають бути не нижче другого ступеня вогнестійкості. Для всіх приміщень повинно бути визначено клас зони згідно з НПАОП 40.1-1.01-97. Відповідне позначення повинно бути нанесено на вхідних дверях кожного приміщення.

Не дозволяється розташування приміщень з робочими місцями операторів ПК у підвалах і цокольних поверхах. Площа приміщення із розрахунку на одне робоче місце має бути не менше 6,0 кв.м, а об'єм – не менше 20,0 куб.м.

Для внутрішнього оздоблення приміщень з ПК слід використовувати дифузно-відбивні матеріали з коефіцієнтом відбитті для стелі 0,7 – 0,8, для стін 0,5 – 0,6. Покриття підлоги повинне бути матовим, поверхня рівною, не слизькою, з антистатичними властивостями.

Віконні прорізи приміщень для роботи з ПК мають бути обладнані регульованими пристроями (жалюзі, завіски, зовнішні козирки).

Забороняється для оздоблення інтер'єру приміщень з ПК застосовувати полімерні матеріали, що виділяють у повітря шкідливі хімічні речовини. Приміщення можуть обладнуватись шафами для зберігання документів, полицями, стелажами.

У приміщеннях слід щоденно робити вологе прибирання. Вони мають бути оснащені аптечками першої медичної допомоги.

При приміщеннях з ВДТ мають бути обладнані побутові приміщення для відпочинку під час роботи, кімната психологічного розвантаження, де слід передбачити встановлення пристроїв для приготування й роздачі тонізуючих напоїв, а також місця для занять фізичною культурою (СНиП 2.09.04 – 87).

3.2.2 Мікроклімат робочої зони працівників, вентиляція

Висока температура повітря негативно позначається на функціональному стані людини. Хоч генерація теплоти дисплеєм досягає критичного рівня тільки у саму теплу пору року, необхідно створювати комфортні теплові умови постійно.

Оптимальні та допустимі мікрокліматичні параметри у приміщеннях повинні враховувати специфіку технологічного процесу при використанні комп'ютерів. Згідно з діючими у нашій країні нормативними документами (ДСанПіН 3.3.2-007-98 у холодні періоди року температура повітря, швидкість його руху та відносна вологість повітря повинні відповідно складати: 22-24^{0}С; 0,1 м/с; 40-60%. Температура повітря може коливатись у межах від 21 до 25^{0}С при збереженні інших параметрів мікроклімату.

В теплі періоди року температура повітря, його рухливість та відносна вологість повинні відповідно становити: 23-25^{0}С; 0,1-0,2 м/с; 40-60 %.

Оптимальним рівнем аероіонізації у зоні дихання користувача вважається вміст легких аерофонів обох знаків від 150 до 5000 у 1 см^3 повітря.

Нормалізуючий вплив на склад повітря робочої зони справляють примусова вентиляція, захисні екрани (оснащені заземленням) та застосування іонізаторів.

3.2.3 Освітлення робочого місця, шум, вібрація

Освітлення у приміщеннях з ВДТ має бути змішаним – природним та штучним. Природне освітлення повинно здійснюватись у вигляді бічного освітлення та відповідати нормам ДБН В.2.5-28-2006 «Природне і штучне освітлення».

При природному освітленні слід передбачити наявність сонцезахисних засобів, що знижують перепади яскравостей між природним світлом та свіченням екрана ВДТ. З цією метою можна використовувати плівки з металізованим покриттям або жалюзі з вертикальними лам елями, що регулюються.

Штучне освітлення у приміщеннях з ВДТ треба здійснювати у вигляді комбінованої системи освітлення з використовуванням люмінесцентних джерел світла у світильниках загального освітлення. На робочих місцях має бути забезпечена рівномірна освітленість за допомогою переважно відбитого або розсіяного світлорозподілу. Світлових відблисків з клавіатури, екрана та від інших частин ВДТ у напрямку очей користувача не повинно бути.

Норма освітленості на робочих місцях складає 300-500лк.

Деякі ВДТ є потенційними джерелами цілого ряду звуків, що містять як коливання, які можна почути, так і коливання ультразвукового діапазону. Цей шум справляє негативний вплив на стан користувача, особливо при тривалому впливі.. У користувача, діяльність якого пов'язана з переробкою інформації це виражається у знижені розумової працездатності, зростає кількість помилок, розвиток зорового втомлення, зміні відчуття кольорів, появі головного болю, послаблення уваги. Нормованим параметром шуму на робочих місцях є рівень 50 дБ. Основними заходами боротьби з шумом є усунення або ослаблення причин шуму в самому його джерелі у процесі проектування, використання засобів звукопоглинання, раціональне планування виробничих приміщень.

3.2.4 Електробезпека

Причинами ураження працівника електрострумом можуть бути:

- Випадковий дотик до струмоведучих частин, у результаті ведення робіт поблизу або на цих частинах;
- Випадковий дотик до струмоведучих частин, у результаті ведення робіт поблизу або на цих частинах;
- Несправність захисних засобів, якими потерпілий доторкався до струмоведучих частин;

Помилкове прийняття устаткування, що перебуває під Електробезпека.

Значення сили струму, що проходить через організм людини, залежить від напруги, під якою перебуває людина й від опору ділянки тіла, до якого прикладена ця напруга. Джерелом живлячої напруги є мережа змінного струму з напругою 229В, на яку поширюється ГОСТ 25861-83.

Основними причинами електротравматизму є:

- напругою, як відключеного;
- Несподіване виникнення напруги через ушкодження ізоляції там, де в нормальних умовах його бути не повинно;
- Контакт струмопровідного устаткування із проводом, що перебуває під напругою.

Для попередження поразок електричним струмом необхідно чітко й у повному обсязі виконувати правила провадження робіт і правил технічної експлуатації. Необхідно виключити можливість доступу оператора до частин устаткування, що працює під небезпечною напругою, до неізольованим частинам, призначеним для роботи при малій напрузі й не підключеним до захисного заземлення, а також підводити електроживлення до ПЕОМ від розетки за допомогою спеціальної вилки із заземлюючим контактом.

3.2.5 Організація робочого місця користувача ПК

Обладнання і організація робочого місця з ВДТ мають забезпечувати відповідність конструкцій всіх елементів робочого місця та їх взаємного розташування, ергономічним вимогам, з урахуванням характеру і особливостей трудової діяльності (ДСанПіН 3.3.2.-007-98).

Конструкція робочого місця й взаємне розташування всіх його елементів відповідають антропометричним, фізіологічним і психологічним вимогам, а також характеру роботи. Конструкція робочих меблів дає можливість забезпечувати можливість індивідуального регулювання їх відповідно до потреб працівника для підтримки зручної пози. Робочий стіл повинен бути пофарбований матовою фарбою. Дисплей розташований так, що його верхній край перебуває на рівні очей, на відстані близько 70 см, що укладається в припустимі рамки від 60 до 90 см. Частота мерехтіння екрана дорівнює 100 Гц, що відповідає умові більше 70 Гц.

Для зниження нервово-емоційного напруження, стомлювання, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільно впроваджувати виконання комплексу вправ.

ВИСНОВКИ

Сьогодні майже на кожному підприємстві та компанії встановлена система відеоспостереження. Але часто мало уваги забезпечується безпеці самих систем відеоспостереження. Статистика говорить про чимало загроз і ризиків, спрямованих на системи відеоспостереження. При цьому користувач може замість безпеки отримати ілюзію захисту. Захист систем відеоспостереження – це комплексний багатоступеневий процес, для успішного проведення якого потрібен досвід монтажних робіт, знання новітніх технологій та мережевого обладнання.

Для виявлення загроз та визначення стану захищеності систем відеоспостереження в роботі представлено онлайн-рішення на базі WEB-технологій. Використовуючи рішення можна оперативно отримати наглядну інформацію стосовно поточного рівня безпеки системи відеоспостереження та отримати рекомендації щодо підвищення рівня захищеності.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Лыткин А. IP -видеонаблюдение. Наглядное пособие / А. Лыткин., 2011. – 200 с.
2. Техническое руководство по сетевому видео. // AXIS, 2009. - 120 с.
3. Гонта А. Проектування відеосистем з врахуванням вимог безпеки об’єкта //Алгоритм безпеки. № 1, 2008.
4. Кононович В.Г., Стайкуца С.В. Угрозы и риски современных систем видеонаблюдения. Бизнес и безопасность. 2018. С. 62–63.
5. Стайкуца С.В., Дигол С.А., Полищук К.В. Анализ угроз, рисков и уязвимостей современных систем видеонаблюдения : Матеріали другої науково-практичної конференції «Перспективні напрями захисту інформації». 2016, С. 73–76.
6. Стайкуца С.В. Аналіз загроз безпеки телекомунікаційних компаній з розробкою методології захисту / С.В. Стайкуца, О.С. Семенов // Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS’2016)”, НАУ, МТУ ” Миколаївська політехніка ”. – Миколаїв – Коблево, 2016, – С. 48-50.
7. Гаджиєв, М. М., Стайкуца, С. В., Жук, О. І., & Козарезнюк, А. О. (2023). Кібербезпека сучасних систем відеоспостереження. *Молодий вчений*.
8. Сетевые атаки [електронний ресурс] – Режим доступу: http://seocyber.net/setevye-ataki-chto-eto-i-kakimi-oni-byvayut
9. Безпека бездротових мереж: стаття [електронний ресурс] – Режим доступу: http://alls.in.ua/5062-bezpeka-bezdrotovih-merezh-instrukciya-do-zastosuvannya.html
10. Хорошо ли защищены от взлома IP-камеры видеонаблюдения? Security News: стаття [електронний ресурс] – Режим доступу: http://sec4all.net/modules/myarticles/article.php?storyid=1564

Додаток Б. ЕЛЕМЕНТИ ЛІСТИНГА КОДУ

ДОДАТОК А – ЛІСТИНГ КОДУ ПРОГРАМИ

```
var countNetwork = 0;
var countInfrastr = 0;
var countSofrware = 0;
var counthardware = 0;
var countHuman = 0;

var chartData = [0, 0, 0, 0, 0];
var savedChartData = [0, 0, 0, 0, 0];
var save = document.querySelector(".save");
// ------------------------------
var specialDDOS = document.querySelector(".specialDDOS");
var SSH = document.querySelectorAll(".SSH");
	for(var i=0; i<SSH.length;i++) {
		SSH[i].addEventListener("click",function() {
			if (this.checked) {
				for(var i=0; i<SSH.length;i++){
					SSH[i].checked = true;
					}
				}else {for(var i=0; i<SSH.length;i++){
					SSH[i].checked = false;
				}	}	});
	}
var firewall = document.querySelectorAll(".firewall");
	for(var i=0; i<firewall.length;i++) {
		firewall[i].addEventListener("click",function() {
			if (this.checked) {
				for(var i=0; i<firewall.length;i++){
					firewall[i].checked = true;
					}
				}else {for(var i=0; i<firewall.length;i++){
					firewall[i].checked = false;
				}	}	});
	}
var portSecurity = document.querySelectorAll(".portSecurity");
	for(var i=0; i<portSecurity.length;i++) {
		portSecurity[i].addEventListener("click",function() {
			if (this.checked) {
				for(var i=0; i<portSecurity[i].length;i++){
					portSecurity.checked = true;
```

```
                }
            }else {for(var i=0; i<portSecurity.length;i++){
                portSecurity[i].checked = false;
            }       }       });
    }
var IEEE = document.querySelectorAll(".IEEE");
    for(var i=0; i<IEEE.length;i++) {
        IEEE[i].addEventListener("click",function() {
            if (this.checked) {
                for(var i=0; i<IEEE.length;i++){
                IEEE[i].checked = true;
                }
            }else {for(var i=0; i<IEEE.length;i++){
                IEEE[i].checked = false;
            }       }       });
    }
var WPA2 = document.querySelectorAll(".WPA2");
    for(var i=0; i<WPA2.length;i++) {
        WPA2[i].addEventListener("click",function() {
            if (this.checked) {
                for(var i=0; i<WPA2.length;i++){
                WPA2[i].checked = true;
                }
            }else {for(var i=0; i<WPA2.length;i++){
                WPA2[i].checked = false;
            }       }       });
    }
var VPN = document.querySelectorAll(".VPN");
    for(var i=0; i<VPN.length;i++) {
        VPN[i].addEventListener("click",function() {
            if (this.checked) {
                for(var i=0; i<VPN.length;i++){
                VPN[i].checked = true;
                }
            }else {for(var i=0; i<VPN.length;i++){
                VPN[i].checked = false;
            }       }       });
    }
var MAC = document.querySelectorAll(".MAC");
    for(var i=0; i<MAC.length;i++) {
        MAC[i].addEventListener("click",function() {
            if (this.checked) {
                for(var i=0; i<MAC.length;i++){
                MAC[i].checked = true;
```

```
                }
            }else {for(var i=0; i<MAC.length;i++){
                MAC[i].checked = false;
            }       }       });
    }
var SSID = document.querySelectorAll(".SSID");
    for(var i=0; i<SSID.length;i++) {
        SSID[i].addEventListener("click",function() {
            if (this.checked) {
                for(var i=0; i<SSID.length;i++){
                SSID[i].checked = true;
                }
            }else {for(var i=0; i<SSID.length;i++){
                SSID[i].checked = false;
            }       }       });
    }
var efir = document.querySelector(".efir");
var software = document.querySelectorAll(".software");
    for(var i=0; i<software.length;i++) {
        software[i].addEventListener("click",function() {
            if (this.checked) {
                for(var i=0; i<software.length;i++){
                software[i].checked = true;
                }
            }else {for(var i=0; i<software.length;i++){
                software[i].checked = false;
            }       }       });
    }
//-------------------------------
var videoAnalitic = document.querySelectorAll(".videoAnalitic");
    for(var i=0; i<videoAnalitic.length;i++) {
        videoAnalitic[i].addEventListener("click",function() {
            if (this.checked) {
                for(var i=0; i<videoAnalitic.length;i++){
                videoAnalitic[i].checked = true;
                }
            }else {for(var i=0; i<videoAnalitic.length;i++){
                videoAnalitic[i].checked = false;
            }       }       });
    }
var fizikProt = document.querySelectorAll(".fizikProt");
    for(var i=0; i<fizikProt.length;i++) {
        fizikProt[i].addEventListener("click",function() {
            if (this.checked) {
```

```
                        for(var i=0; i<fizikProt.length;i++){
                                fizikProt[i].checked = true;
                                }
                        }else {for(var i=0; i<fizikProt.length;i++){
                                fizikProt[i].checked = false;
                        }       }       });
        }
var zoloby = document.querySelector(".zoloby");
var kabelPoza = document.querySelector(".kabelPoza");
var lowerPower = document.querySelector(".lowerPower");
var locationWifi = document.querySelector(".locationWifi");
var generator = document.querySelector(".generator");
var acamulator = document.querySelector(".acamulator");
var vipramitel = document.querySelectorAll(".vipramitel");
        for(var i=0; i<vipramitel.length;i++) {
                vipramitel[i].addEventListener("click",function() {
                        if (this.checked) {
                                for(var i=0; i<vipramitel.length;i++){
                                vipramitel[i].checked = true;
                                }
                        }else {for(var i=0; i<vipramitel.length;i++){
                                vipramitel[i].checked = false;
                        }       }       });
        }
//-------------------------------
var antiVirus = document.querySelector(".antiVirus");
var UNIX = document.querySelector(".UNIX");
var passwords = document.querySelector(".passwords");
var passwordsHuman = document.querySelector(".passwordsHuman");
var passwordsStore = document.querySelector(".passwordsStore");

//-------------------------------
var heit25 = document.querySelector(".heit25");
var kozuh = document.querySelector(".kozuh");
var integr = document.querySelectorAll(".integr");
        for(var i=0; i<integr.length;i++) {
                integr[i].addEventListener("click",function() {
                        if (this.checked) {
                                for(var i=0; i<integr.length;i++){
                                integr[i].checked = true;
                                }
                        }else {for(var i=0; i<integr.length;i++){
                                integr[i].checked = false;
                        }       }       });
```

```
	}
var rozmDostupu = document.querySelectorAll(".rozmDostupu");
	for(var i=0; i<rozmDostupu.length;i++) {
		rozmDostupu[i].addEventListener("click",function() {
			if (this.checked) {
				for(var i=0; i<rozmDostupu.length;i++){
					rozmDostupu[i].checked = true;
					}
				}else {for(var i=0; i<rozmDostupu.length;i++){
					rozmDostupu[i].checked = false;
				}	}	});
	}
var rezerv = document.querySelectorAll(".rezerv");
	for(var i=0; i<rezerv.length;i++) {
		rezerv[i].addEventListener("click",function() {
			if (this.checked) {
				for(var i=0; i<rezerv.length;i++){
					rezerv[i].checked = true;
					}
				}else {for(var i=0; i<rezerv.length;i++){
					rezerv[i].checked = false;
				}	}	});
	}
var shifr = document.querySelectorAll(".shifr");
var inshiZasobi = document.querySelector(".inshiZasobi");
	for(var i=0; i<inshiZasobi.length;i++) {
		inshiZasobi[i].addEventListener("click",function() {
			if (this.checked) {
				for(var i=0; i<inshiZasobi.length;i++){
					inshiZasobi[i].checked = true;
					}
				}else {for(var i=0; i<inshiZasobi.length;i++){
					inshiZasobi[i].checked = false;
				}	}	});
	}
var testing = document.querySelector(".testing");
//-------------------------------
var courses = document.querySelectorAll(".courses");
	for(var i=0; i<courses.length;i++) {
		courses[i].addEventListener("click",function() {
			if (this.checked) {
				for(var i=0; i<courses.length;i++){
					courses[i].checked = true;
					}
```

```
                }else {for(var i=0; i<courses.length;i++){
                        courses[i].checked = false;
                }       }       });
        }
var instructions = document.querySelectorAll(".instructions");
        for(var i=0; i<instructions.length;i++) {
                instructions[i].addEventListener("click",function() {
                        if (this.checked) {
                                for(var i=0; i<instructions.length;i++){
                                        instructions[i].checked = true;
                                        }
                                }else {for(var i=0; i<instructions.length;i++){
                                        instructions[i].checked = false;
                                }       }       });
        }
var vdoskonal = document.querySelectorAll(".vdoskonal");
        for(var i=0; i<vdoskonal.length;i++) {
                vdoskonal[i].addEventListener("click",function() {
                        if (this.checked) {
                                for(var i=0; i<vdoskonal.length;i++){
                                        vdoskonal[i].checked = true;
                                        }
                                }else {for(var i=0; i<vdoskonal.length;i++){
                                        vdoskonal[i].checked = false;
                                }       }       });
        }
var robota = document.querySelectorAll(".robota");
        for(var i=0; i<robota.length;i++) {
                robota[i].addEventListener("click",function() {
                        if (this.checked) {
                                for(var i=0; i<robota.length;i++){
                                        robota[i].checked = true;
                                        }
                                }else {for(var i=0; i<robota.length;i++){
                                        robota[i].checked = false;
                                }       }       });
        }
var log = document.querySelectorAll(".log");
        for(var i=0; i<log.length;i++) {
                log[i].addEventListener("click",function() {
                        if (this.checked) {
                                for(var i=0; i<log.length;i++){
                                        log[i].checked = true;
                                        }
```

```
                        }else {for(var i=0; i<log.length;i++){
                                log[i].checked = false;
                        }       }       });
        }
var stimul = document.querySelector(".stimul");
//-------------------------------
var allMethods = document.querySelector(".methods *");

//-------------------------------
var calcMethods = function() {
        countNetwork = 0;
        countInfrastr = 0;
        countSofrware = 0;
        counthardware = 0;
        countHuman = 0;
//1-------------------------------
        if (specialDDOS.checked) {
                countNetwork += 0.8;
        }
        if (SSH[0].checked) {
                countNetwork += 0.3+0.4+0.25;
        }
        if (firewall[0].checked) {
                countNetwork += 0.4;
                countSofrware += 0.4;
        }
        if (portSecurity[0].checked) {
                countNetwork += 0.2+0.3+0.25+0.3;
        }
        if (IEEE[0].checked) {
                countNetwork += 0.3+0.3+0.3+0.4;
        }
        if (WPA2[0].checked) {
                countNetwork += 0.15+0.4+0.5+0.2+0.5;
        }
        if (VPN[0].checked) {
                countNetwork += 0.45+0.5+0.3;
        }
        if (SSID[0].checked) {
                countNetwork += 0.05+0.1;
                countInfrastr += 0.2;
        }
        if (efir.checked) {
                countNetwork += 0.45+0.5;
```

```
        }
        if (software[0].checked) {
                countNetwork += 0.4;
                countSofrware += 0.75+1;
        }
//2-------------------------------
        if (videoAnalitic[0].checked) {
                countInfrastr += 1.2;
                counthardware += 0.9;
                countHuman += 0.125;
        }
        if (fizikProt[0].checked) {
                countInfrastr += 0.8+0.5;
        }
        if (zoloby.checked) {
                countInfrastr += 0.75;
        }
        if (kabelPoza.checked) {
                countInfrastr += 0.75;
        }
        if (lowerPower.checked) {
                countInfrastr += 0.6;
        }
        if (locationWifi.checked) {
                countInfrastr += 0.6;
        }
        if (generator.checked) {
                countInfrastr += 1.05;
        }
        if (acamulator.checked) {
                countInfrastr += 1.05;
        }
        if (vipramitel[0].checked) {
                countInfrastr += 0.7;
        }
//3-------------------------------
        if (antiVirus.checked) {
                countSofrware += 0.4;
        }
        if (UNIX.checked) {
                countSofrware += 0.6;
        }
        if (passwords.checked) {
                countSofrware += 1.5;
```

```
        }
        if (passwordsHuman.checked) {
                countSofrware += 0.9;
        }
        if (passwordsStore.checked) {
                countSofrware += 0.6;
        }
//4-------------------------------
        if (heit25.checked) {
                counthardware += 0.3;
        }
        if (kozuh.checked) {
                counthardware += 0.3+0.3;
        }
        if (integr[0].checked) {
                counthardware += 0.6;
        }
        if (rozmDostupu[0].checked) {
                counthardware += 0.875;
                countHuman += 0.5 + 1.6;
        }
        if (rezerv[0].checked) {
                countSofrware += 0.875;
                countHuman += 0.5 + 1.6;
        }
        if (shifr.checked) {
                counthardware += 0.35;
        }
        if (inshiZasobi.checked) {
                counthardware += 0.35;
        }
        if (testing.checked) {
                counthardware += 1.6;
        }
//5-------------------------------
        if (courses[0].checked) {
                countHuman += 0.5 + 0.12 + 0.2;
        }
        if (instructions[0].checked) {
                countHuman += 0.5+0.25;
        }
        if (vdoskonal[0].checked) {
                countHuman += 0.25 + 0.15;
        }
```

```
            if (robota[0].checked) {
                countHuman += 0.25 + 0.2;
            }
            if (log[0].checked) {
                countHuman += 0.5 + 0.8;
            }
            if (stimul.checked) {
                countHuman += 0.3;
            }
        // Уровень специалиста занимающегося безопасностью
            var specialistSec = formData[7];
            var specialistMont = formData[6];
            var obor = formData[10];

            countNetwork += (specialistSec*0.05);
            countInfrastr += 0;
            countSofrware += specialistSec*0.06 + specialistSec*0.075 +
specialistSec*0.15;
            counthardware += specialistSec*0.03 + specialistSec*0.0525
+specialistSec*0.05;
            countHuman += specialistSec*0.1 + specialistSec*0.075;
        //--------------------------------------
            chartRadar.data.datasets[1].data[0] = countNetwork;
            chartRadar.data.datasets[1].data[1] = countInfrastr;
            chartRadar.data.datasets[1].data[2] = countSofrware;
            chartRadar.data.datasets[1].data[3] = counthardware;
            chartRadar.data.datasets[1].data[4] = countHuman;
            chartdata = [countNetwork,
countInfrastr,countSofrware,counthardware,countHuman];
            console.log(chartdata);

        }
        var reboot = document.querySelector(".reboot");
        var nextLast = document.querySelector(".last");
        var ctx = document.getElementById("chartRadar");


        reboot.addEventListener("click", calcMethods);
        reboot.addEventListener("mouseup", function() {
            chartRadar.update();
        });
        nextLast.addEventListener("click", calcMethods);
        nextLast.addEventListener("click", function() {
            chartRadar.update();
```

```
});

save.addEventListener("click", function(){
        calcMethods();

        chartRadar.data.datasets[0].data[0] = chartdata[0];
        chartRadar.data.datasets[0].data[1] = chartdata[1];
        chartRadar.data.datasets[0].data[2] = chartdata[2];
        chartRadar.data.datasets[0].data[3] = chartdata[3];
        chartRadar.data.datasets[0].data[4] = chartdata[4];
});
```

ДОДАТОК А. Слайди мультимедійної презентації

ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ

РОЗРОБКА ОНЛАЙН-РІШЕННЯ З ОЦІНКИ ЗАХИЩЕНОСТІ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

ДИПЛОМНИЙ ПРОЕКТ

Керівник: к.ф.н., доцент Стайкуца С.В.
Виконав: Сапожніков В.Р.

2024

Технології систем відеоспостереження

Технології систем відеоспостереження

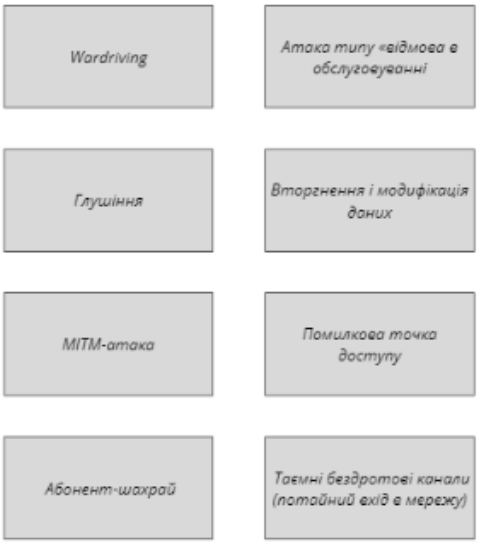
Структурна схема системи відеоспостереження

Загрози сучасним системам відеоспостереження

Методи фізичного впливу на системи відеоспостереження

Основні види вірусів

Дослідження екосистеми загроз безпроводових мереж систем відеоспостереження



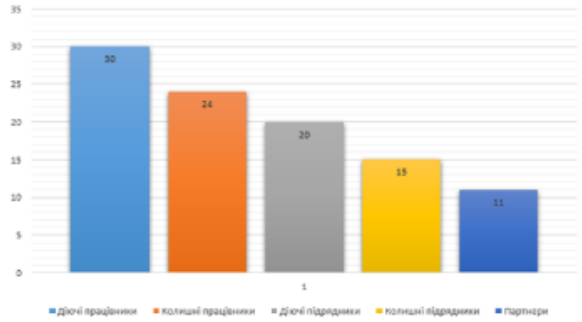
Основні загрози безпроводових мереж при використанні систем відеоспостереження

Атака "відмова в обслуговуванні" в безпроводових мережах

Основні загрози безпроводових мереж при використанні систем відеоспостереження

“Людський фактор” в фокусі інформаційної безпеки систем відеоспостереження

Основні загрози з боку персоналу



Основні групи порушників внутрішнього корпоративного середовища

Комплексний підхід до вивчення загроз сучасних систем відеоспостереження

Механізми та інструменти захисту систем відеоспостереження

Основні ділянки цифрової системи відеоспостереження

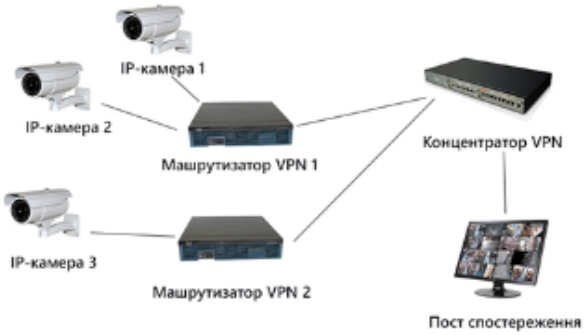
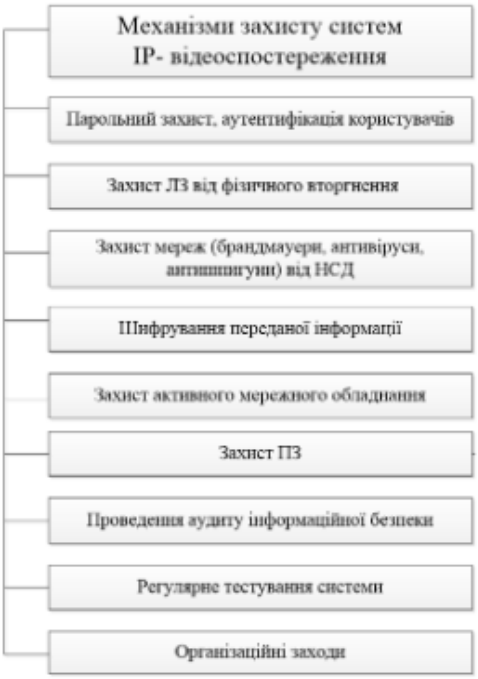
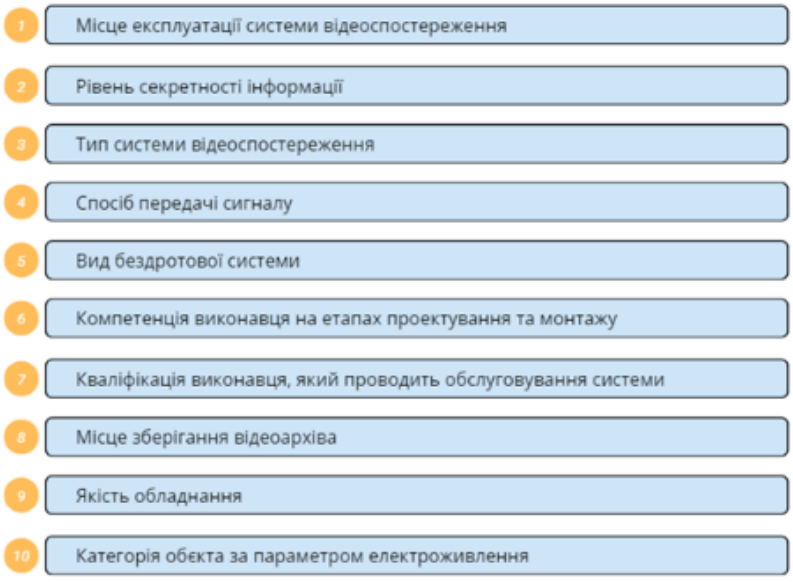


Схема підключення VPN



Етапи побудови радару загроз



Алгоритм інтерактивної анкети для подальшого вибору механізмів захисту

Інструменти програмної реалізації

Набір WEB-технологій

1.***index.html*** *– головний файл сайту. У ньому зберігається верстка сайту та приєднуються усі інші частини системи.*

2.***style.css*** *– файл у якому зберігаються стилі. Цей файл визначає статичний зовнішній вигляд сторінки.*

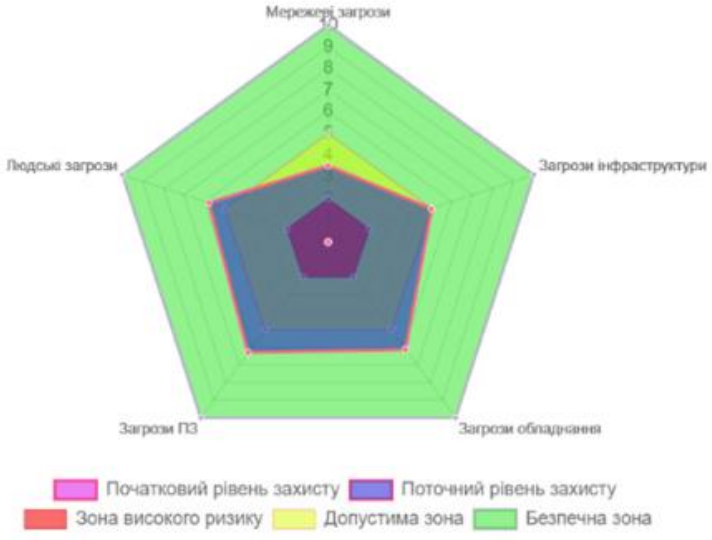
3.***form.js*** *– тут обробляється інформація що поступає від користувача при заповнені анкети.*

4.***methods.js*** *– у даному файлі обробляються методи які користувач обирає для поліпшення стану системи.*

5. ***chart.js*** *– файл відповідний за відображення діаграм.*

Склад програмної реалізації

Радар загроз після застосування механізмів захисту в базових напрямах аудиту стану ІБ систем відеоспостереження



ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Сапожнікова Валерія Романовича

(прізвище, ім`я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

Освітня програма: *«Безпека комп'ютерних систем і мереж»*

Тема дипломного проекту: Розробка онлайн-рішення з оцінки захищеності систем відеоспостереження

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) *Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка містить __ сторінки. У пояснювальній записці розглянуто питання виявлення загроз та ризиків в сучасних системах відеоспостереження для подального вибору оптимальних методів та заобів захисту.. Графічна частина складається з слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.*

б) самостійність роботи над проектом: *Протягом всього строку дипломного проектування та переддипломної практики здобувач освіти Сапожніков В.Р. виконував всі етапи розробки проекту, без порушення термінів. Роботу студент виконував в більшій мірі самостійно, з оглядом на рекомендації керівника та отримуючи зворотній зв'язок.*

в) теоретична підготовка випускника (випускниці): *Здобувач освіти Сапожніков В.Р. під час роботи над дипломним проектом проаналізував достатню кількість літературних джерел та матеріалів за даною тематикою.*

Вважаю, що теоретична підготовка дипломника якісна і він готовий до захисту дипломного проекту.

г) вміння розв'язувати виробничі та конструкторські питання _____

Під час дипломного проектування здобувач освіти Сапожніков В.Р. приймав рішення щодо вибору обладнання, аналізував вимоги на етапах проектування, розробляв проектні рішення, обґрунтовував вибір платформи розробки, мови програмування та алгоритмів реалізації розробленого проекту.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові керівника дипломного проекту

Стайкуца Сергій Володимирович

Місце роботи і посада керівника дипломного проекту

"Державний університет інтелектуальних технологій і зв'язку", доцент кафедри кібербезпеки та технічного захисту інформації, помічник декана факультету інформаційних технологій та кібербезпеки

Підпис

«10» червня 2024 р.

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ
КАДРІВ 2024 р.

ВІДДІЛ КАДРІВ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект (роботу) здобувача (здобувачки) освіти

відділення комп'ютерних систем

Сапожнікова Валерія Романовича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Освітня програма «Безпека комп'ютерних систем і мереж»

Керівник дипломного проекту (роботи) Стайкуца Сергій Володимирович

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) Розробка онлайн-рішення з оцінки захищеності систем відеоспостереження

Обсяг розрахунково-пояснювальної записки 88 сторінок

Обсяг графічної (презентаційної) частини 10 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Представлений на рецензію дипломний проект повністю відповідає меті проектування та технічному завданню. Тематика дипломного проекту є актуальною та присвячена розробці онлайн-рішення з оцінки захищеності в сучасних систем відеоспостереження

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Дипломний проект складається зі вступу, трьох розділів, висновків, переліку використаних джерел. В основній частині проведено аналіз загроз та вразливостей систем відеоспостереження, представлено модель загроз, розглянуто методи та засоби захисту систем, розроблено онлайн-рішення з оцінки рівня захищеності СОТ.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) Графічна частина виконана на достатньо високому рівні у вигляді презентації із використанням офісного пакету Microsoft PowerPoint та Visio. Пояснювальна записка виконана акуратно та у відповідності до норм оформлення документів із використанням офісного пакету Microsoft Word. Загальна якість виконання – добра, академічного плагіату у роботі не виявлено.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Сапожніков Валерій Романович,
здобувач освіти гр. 4КБ-01, та

Стайкуца Сергій Володимирович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проекту фахового молодшого бакалавра на тему:

«Розробка онлайн-рішення з оцінки захищеності систем відеоспостереження»

(автор роботи – Сапожніков В.Р., керівник роботи – Стайкуца С.В.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2024 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Сапожніков В.Р. /

Керівник _____ / Стайкуца С.В. /

«10» червня 2024 р.

г) перелік позитивних якостей дипломного проекту (роботи)

1. Детально розглянуто класифікацію як систем, так і компонентів
2. Проведено досліджено екосистеми загроз та ризиків сучасних систем відеоспостереження, що дало змогу скласти загальну модель загроз
3. Представлено цікаве програмне рішення для експрес-оцінки рівня захищеності

д) основні недоліки дипломного проекту (роботи)

1. Треба було провести аналіз існуючих рішень
2. Було б доцільним розглянути захищеність систем відеоспостереження в розрізі брендів на ринку систем безпеки України

Оцінка розрахункової частини добре

Оцінка графічної частини відмінно

Загальна оцінка добре

Прізвище, ім'я, по батькові рецензента Василіу Євген Вікторович

Місце роботи і посада рецензента Державний університет інтелектуальних технологій і зв'язку, д.т.н., проф. кафедри КБ та ТЗІ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ Факультет інформаційних технологій та кібербезпеки

Підпис

2024 р.

UNICHECK
by Turnitin

Ім'я користувача:
Катерина Григоріївна Краснокутська

ID перевірки:
1016338368

Дата перевірки:
09.06.2024 16:28:46 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
09.06.2024 16:30:48 EEST

ID користувача:
100011688

Назва документа: 4КБ-01 Сапожников Валерий

Кількість сторінок: 51 Кількість слів: 9890 Кількість символів: 74654 Розмір файлу: 1,001.67 KB ID файлу: 101613947

18.4%
Схожість

Найбільша схожість: 2.68% з Інтернет-джерелом (https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%81%D0%B0%D0%

18.4% Джерела з Інтернету 383 ..... Сторінка 53

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел