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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Павлової Валерії Олександрівни*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Вдосконалення системи захисту інформації в інформаційно-телекомунікаційній системі медичної установи «Сім'я»*

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

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Павловій Валерії Олександрівні*** **академічної групи** ***125-17-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Вдосконалення системи захисту інформації в інформаційно-телекомунікаційній системі медичної установи «Сім'я»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.21р. № 317-с

Розділ	Зміст	Термін виконання
Розділ 1	Огляд каналів витоку інформації, впливу загроз на ОІД, опис ОІД	29.03.2021
Розділ 2	Аналіз та впровадження засобів захисту інформації для вдосконалення системи захисту	24.05.2021
Розділ 3	Розрахунки на вдосконалення системи захисту інформації	14.06.2021

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

Дата видачі: 08.01.2021р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 92 арк., 4 рис., 19 табл., 11 джерел.

Об'єкт дослідження – комп'ютерний центр медичної установи "Сім'я".

Мета роботи – удосконалення підсистеми захисту інформації, що забезпечує належний рівень безпеки та впровадження методів захисту інформації.

У роботі здійснений огляд стану та перспектив розвитку захисту інформації в інформаційних системах. Розглянуті аспекти постановки задачі та вирішена задача захисту інформації інформаційно-телекомунікаційної системи підприємства до заданого профілю захищеності. Проведене технічно-економічне обґрунтування вибору засобів забезпечення технічного захисту інформації, яка циркулює в інформаційно-телекомунікаційній системі підприємства. В запропонованій підсистемі захисту інформації забезпечений комплекс захисту інформації, а саме протидія загрозам від можливого витоку інформації за рахунок несанкціонованого доступу.

Галузь застосування − на підприємстві для запобігання витоку інформації та порушенню конфіденційності, цілісності й доступності інформації, яка циркулює в інформаційно-телекомунікаційній системі.

ІНФОРМАЦІЯ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ЗАГРОЗА, ПОРУШНИК, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ПОСЛУГИ БЕЗПЕКИ, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ.

РЕФЕРАТ

Текстовая часть дипломной работы: 92 л., 4 рис., 19 табл., 11 источников.

Объект исследования - компьютерный центр медицинского учреждения "Семья".

Цель работы - усовершенствование подсистемы защиты информации, для обеспечения должного уровня безопасности и внедрение средств защиты информации.

В работе осуществлен обзор состояния и перспектив развития защиты информации в информационных системах. Рассмотрены аспекты постановки задачи и решена задача защиты информации информационно-телекоммуникационной системы предприятия до заданного профиля защищенности. Проведенное технико-экономическое обоснование выбора средств обеспечения технической защиты информации, циркулирующей в информационно-телекоммуникационной системе предприятия. В предлагаемой подсистеме защиты информации обеспечен комплекс защиты информации, а именно противодействие угрозам от возможной утечки информации за счет несанкционированного доступа.

Область применения - на предприятии для предотвращения утечки информации и нарушения конфиденциальности, целостности и доступности информации, которая циркулирует в информационно-телекоммуникационной системе.

ИНФОРМАЦИЯ, НЕСАНКЦИОНИРОВАНИЙ ДОСТУП, УГРОЗА, НАРУШИТЕЛЬ, ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННАЯ СИСТЕМА, УСЛУГИ БЕЗОПАСНОСТИ, КОМПЛЕКС МЕР ЗАЩИТЫ.

ABSTRACT

Text of thesis: 92 pg., 4 fig., 19 tables, 11 source.

Object of study - computer center of medical institution "Family"

Purpose - to improve information security subsystem that provides the appropriate level of security and the methods of protection.

In the thesis work carried out by review status and prospects of development of information security in information systems. The aspects of setting the problem and solved the problem of protection of information and telecommunications systems company to a given profile protection. Conducted feasibility study of the choice of technical protection of information that circulates in the information and telecommunications system of the enterprise. In the proposed subsystem protection provided complex information security, including combating the threats of a possible information leakage through unauthorized access.

Field of application - the company to prevent information leakage and breaches of confidentiality, integrity and availability of information that circulates in information and telecommunications system.

INFORMATION, UNAUNTHORIZED ACCESS, THREATS, BREAKER, INFORMATION AND TELECOMMUNICATION SISTEM, SERVICES SECURITY COMPLEX REMEDIES.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДВ-1 – ручне відновлення після збоїв;

ДЗ-1 – модернізація;

ДР-1 – використання ресурсів (квоти);

ДС-1 – стійкість при обмежених відмовах;

ЖМД – жорсткий магнітний диск;

ЗАТ – закрите акціонерне товариство;

ІзОД – інформація з обмеженим доступом;

ІТС– інформаційно-телекомунікаційна система;

КА-1 – мінімальна адміністративна конфіденційність;

КА-2 – базова адміністративна конфіденційність;

КЕО – коефіцієнт природної освітленості;

КЗЗ – комплекс засобів захисту;

КПК – кишеньковий персональний комп ютер;

КСЗІ – комплексна система захисту інформації;

ЛБ – люмінесцентними лампами;

ЛОМ – локальна обчислювальна мережа;

НД – нормативний документ;

НИ-1 – зовнішня ідентифікація і автентифікація;

НИ-2 – одиночна ідентифікація та автентифікація;

НК-1 – однонаправлений достовірний канал;

МУ – медична установа;

НО -2 – розподіл обов'язків адміністраторів;

НР-1 – зовнішній аналіз;

НР-2 – захищений журнал;

НЦ-1 – цілісність комплексу засобів захисту;

НСД – несанкціонований доступ;

ОІД – об єкт інформаційної діяльності;

ОС – операційна система;

ПЕОМ – персональна електронна обчислювальна машина;

ПЗ – програмне забезпечення;

ПЗУ – постійно запам ятовуючий пристрій;

ПК – персональний комп ютер;

СЗІ – служба захисту інформації;

ЦА-1 – мінімальна адміністративна цілісність;

ЦА-2 – базова адміністративна цілісність;

ЦВ-1 – цілісність при обміні;

ЗМІСТ

с.

ВСТУП

Застосування обчислювальних засобів у системі управління державних і комерційних структур вимагає наявності потужних систем обробки і передачі даних. Вирішення цього завдання призвело до створення єдиної інфраструктури. Її використання дозволило людям, що мають комп'ютер і модем, отримати доступ до інформації найбільших бібліотек і баз, даних світу, оперативно виконувати складні розрахунки, швидко обмінюватися інформацією з іншими респондентами мережі незалежно від відстані та країни проживання. Але такі системи спричинили низку проблем, одна з яких - безпека обробки і передачі інформації. В наш час над проблемою захищеності інформації працює велика кількість фахівців практично в усіх економічно розвинених країнах світу. Можна сказати, що інформаційна безпека сформувалася в окрему дисципліну. Однак, незважаючи на зусилля численних організацій, що займаються захистом інформації, забезпечення інформаційної безпеки продовжує залишатися надзвичайно гострою проблемою.

З одного боку, використання інформаційних технологій дає ряд очевидних переваг: підвищення ефективності процесів управління, обробки і передачі даних і т.п. У наш час вже неможливо уявити велику організацію без застосування новітніх інформаційних технологій, починаючи від автоматизації окремих робочих місць і закінчуючи побудовою корпоративних розподілених інформаційних систем.

З іншого боку, розвиток мереж, їх ускладнення, взаємна інтеграція, відкритість призводять до появи якісно нових загроз, збільшення числа зловмисників, які мають потенційну можливість впливати на систему. Для забезпечення захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів: використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії і т.д. Комплексний характер захисту виникає з комплексних

дій зловмисників, які прагнуть будь-якими засобами здобути важливу для них інформацію.

Сьогодні можна стверджувати, що народжується нова сучасна технологія -технологія захисту інформації в телекомунікаційних мережах.

РОЗДІЛ 1. ОГЛЯД ШЛЯХІВ ВИТОКУ ІНФОРМАЦІЇ, ВПЛИВУ ЗАГРОЗ НА ОІД, ОПИС ОІД

1.1 Сутність проблеми і завдання захисту інформації в інформаційних і телекомунікаційних мережах

Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах. Захист інформації в комп'ютерних системах має низку специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку. Відомо дуже велика кількість загроз інформації, які можуть бути реалізовані як з боку зовнішніх порушників, так і з боку внутрішніх порушників.

Захист інформації перетворюється на найважливішу проблему державної безпеки, коли мова йде про державну, дипломатичної, військової, промислової, медичної, фінансової та іншої довірчій, секретної інформації. Величезні масиви такої інформації зберігаються в електронних архівах, обробляються в інформаційних системах і передаються по телекомунікаційних мережах. Основні властивості цієї інформації – конфіденційність, доступність і цілісність, повинні підтримуватися законодавчо, юридично, а також організаційними, технічними та програмними методами.

Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби.

Останнім часом в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється

небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем.

Наскільки актуальна проблема захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

1. несанкціонований доступ — 2 %
2. укорінення вірусів — 3 %;
3. технічні відмови апаратури мережі — 20 %;
4. цілеспрямовані дії персоналу — 20 %;
5. помилки персоналу (недостатній рівень кваліфікації) — 55%.

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.

Відповідно до вимог законів України "Про інформацію" [1], "Про державну таємницю" [2] та "Про захист інформації в інформаційно-телекомунікаційних системах" [3] основним об'єктом захисту в інформаційних системах є інформація з обмеженим доступом, що становить державну або іншу, передбачену законодавством України, таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження.

Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Порушник — користувач, який здійснює несанкціонований доступ до інформації.

Загроза несанкціонованого доступу — це подія, що кваліфікується як факт спроби порушника вчинити несанкціоновані дії стосовно будь-якої частини інформації в інформаційній системі.

Потенційні загрози несанкціонованого доступу до інформації в інформаційних системах поділяють на цілеспрямовані (умисні) та випадкові. Умисні загрози можуть маскуватися під випадкові шляхом довгочасної масованої атаки несанкціонованими запитами або комп'ютерними вірусами.

1.2 Шляхи витоку інформації і несанкціонованого доступу

Розглянемо можливі канали витоку-інформації та варіанти несанкціонованого доступу до неї.

За відсутності законного користувача, контролю та розмежування доступу до робочої станції, кваліфікований порушник легко використовує його функціональні можливості для несанкціонованого доступу до інформації, що підлягає захисту, шляхом уведення відповідних запитів або команд.

За наявності вільного доступу до приміщення можна візуально спостерігати інформацію на засобах відбиття і документування, викрасти паперовий носій, зняти зайву копію, а також викрасти інші носії з інформацією: лістинги, магнітні носії та ін.

Особливу загрозу становить безконтрольне завантаження програмного забезпечення, в якому можуть бути змінені установки, властивості, дані, алгоритми, введено "троянську" програму або вкорінено комп'ютерний вірус, що виконують деструктивні несанкціоновані дії. Наприклад, записування інформації на сторонній носій, незаконне передавання у канали зв'язку, несанкціоноване друкування документів, порушення їх цілісності, несанкціоноване копіювання важливої інформації, вагомість якої визначається та обмежується на дуже короткий або, навпаки, тривалий час.

Загрозливою є ситуація, коли порушник — санкціонований користувач інформаційної системи, який у зв'язку зі своїми функціональними обов'язками

має доступ до однієї частини інформації, а користується іншою за межами своїх повноважень. З боку санкціонованого користувача є багато способів порушення роботи інформаційної системи й одержання, модифікування, поширювання або знищення інформації, що підлягає захисту. Для цього можна використовувати, насамперед, привілейовані команди введення-виведення, неконтрольованість санкціонованості або законності запиту і звернень до баз та банків даних, серверів тощо. Вільний доступ дає порушникові можливість звертатись до чужих файлів і баз даних та змінювати їх випадково або умисно.

Під час технічного обслуговування апаратури можуть бути виявлені залишки інформації на її носіях (поверхні твердих дисків, магнітні стрічки та інші носії). Стирання інформації звичайними методами (засобами операційних систем, спеціальних програмних утиліт) неефективне з погляду технічного захисту інформації. Порушник може поновити і прочитати її залишки, саме тому потрібні тільки спеціальні засоби стирання інформації, що підлягає захисту.

Під час транспортування носіїв територією, яка не охороняється, виникає загроза перехоплення інформації, що підлягає захисту, і подальшого ознайомлення з нею сторонніх осіб.

Зловмисник може стати санкціонованим користувачем інформаційної системи у режимі розподілу часу, якщо він попередньо якось визначив порядок роботи санкціонованого користувача або якщо він працює з ним на одних лініях зв'язку. Він може здійснити підключення до лінії зв'язку між терміналом та процесором. Крім того, без переривання роботи санкціонованого користувача порушник може продовжити її від його імені, анулювавши сигнали відключення санкціонованого користувача.

Обробка, передавання та зберігання інформації апаратними засобами інформаційної системи забезпечуються спрацюванням логічних елементів на базі напівпровідникових приладів. Спрацювання логічних елементів зумовлено високочастотним зміщенням рівнів напруг і струмів, що призводить до виникнення в ефірі, ланках живлення та заземлення, а також у паралельно

розміщених ланках й індуктивностях сторонньої апаратури електромагнітних полів, які несуть в амплітуді, фазі й частоті своїх коливань ознаки оброблюваної інформації. Використання порушником різних приймачів може призвести до несанкціонованого витоку та перехоплення дуже важливої інформації, що зберігається в інформаційній системі. Зі зменшенням відстані між приймачем порушника й апаратними засобами інформаційної системи ймовірність приймання таких інформаційних сигналів збільшується.

Окремим видом дуже небезпечної перспективної загрози професійних порушників є так звані радіочастотні засоби електромагнітного ураження, які спричиняють ураження напівпровідникової елементної бази за рахунок надпотужної енергетичної дії електромагнітних випромінювань радіочастотного діапазону, що може призвести до повної або тимчасової відмови в роботі інформаційної системи у найбільш відповідальних ситуаціях.

Несанкціоноване підключення порушником приймальної апаратури та спеціальних датчиків до ланцюгів електроживлення та заземлення, інженерних комунікацій і каналів зв'язку при передачі даних може спричинити модифікацію та порушення цілісності інформації в комп'ютерних мережах. Таким чином, порушники технічного захисту інформації можуть створювати такі потенційні загрози для безпеки інформації в інформаційних системах:

– загрози конфіденційності (несанкціонованого одержання) інформації всіма потенційними і можливими каналами її витоку, особливо каналами побічних електромагнітних випромінювань і наведень, таємними каналами зв'язку в імпортному обладнанні та розвідувальними закладними пристроями ;

– загрози цілісності (несанкціонованої зміни) інформації;

– загрози доступності інформації (несанкціонованого або випадкового обмеження) та ресурсів самої інформаційної системи;

– загрози спостереженості роботи інформаційної системи (порушення процедур ідентифікації та аутентифікації, процедур контролю доступу і дій користувачів, повна або часткова втрата керованості інформаційної системи,

загрози від несанкціонованих атак і вторгнень порушників технічного захисту інформації до програмних, телекомунікаційних та апаратних засобів інформаційної системи, загрози для передачі даних і маніпуляцій з протоколами обміну (контролю) та із загальносистемним програмним забезпеченням, реєстрація, вірогідний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, аутентифікація під час обміну, аутентифікація відправника (невідмова від авторства), аутентифікація одержувача (невідмова від одержання) та ін.);

– загрози проникнення комп'ютерних вірусів;

– загрози радіочастотних засобів електромагнітного ураження високопрофесійних порушників.

Загрози порушників технічного захисту інформації можуть здійснюватись технічними каналами:

– акустичними, оптичними, хімічними тощо;

– каналами спеціального впливу шляхом формування полів і сигналів для руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання засобів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

1.3 Способи впливу загроз на об'єкти захисту інформації

Способи впливу загроз на об'єкти захисту інформації поділяються на інформаційні, апаратно-програмні, фізичні, радіоелектронні та організаційно-правові.

До інформаційних способів відносяться:

– порушення адресності та своєчасності інформаційного обміну;

– несанкціонований доступ до інформаційних ресурсів;

– незаконне копіювання даних в інформаційних системах;

– розкрадання інформації з банків і баз даних;

– порушення технології обробки інформації.

Апаратно-програмні засоби включають:

– впровадження комп'ютерних вірусів;

– встановлення програмних та апаратних закладних пристроїв;

– знищення або модифікацію даних в інформаційних системах.

Фізичні способи включають:

– знищення або руйнування засобів обробки інформації та зв'язку;

– знищення, руйнування або розкрадання машинних чи інших оригіналів носіїв інформації;

– вплив на персонал;

– поставку "заражених" компонентів інформаційних систем.

Радіоелектронними засобами є:

– перехоплення інформації в технічних каналах її витоку;

– впровадження електронних пристроїв перехоплення інформації в технічні засоби передачі інформації та приміщення;

– перехоплення, дешифрування та впровадження помилкової інформації в мережах передачі даних і лініях зв'язку;

Організаційно-правові способи включають:

– закупівлі недосконалих або застарілих інформаційних технологій та комп'ютерних засобів;

– неправомірне обмеження доступу до документів.

Завдання забезпечення безпеки

– Захист інформації в каналах зв'язку і базах даних;

– Підтвердження автентичності об'єктів даних і користувачів (аутентифікація сторін, встановлюють зв'язок);

– Виявлення порушень цілісності об'єктів даних;

– Забезпечення захисту технічних засобів і приміщень, в яких ведеться

обробка конфіденційної інформації, від витоку;

– Забезпечення захисту програмних продуктів і засобів обчислювальної техніки від впровадження в них програмних вірусів і закладок;

– Організаційно-технічні заходи, спрямовані на забезпечення доступноті, цілісності, конфіденційності даних.

1.4 Методи і засоби захисту інформації

Для забезпечення безпеки інформації в офісних мережах проводяться різні заходи, що об'єднуються поняттям «система захисту інформації».

Система захисту інформації - це сукупність заходів, програмно-технічних засобів, правових та морально-етичних норм, спрямованих на протидію загрозам з метою зведення до мінімуму можливих збитків користувачам і власникам системи.

Традиційні заходи для протидії витоку інформації поділяються на технічні та організаційні .

До технічних заходів можна віднести захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок, прийняття конструктивних заходів захисту від розкрадань, саботажу, диверсій, вибухів, установку резервних систем електроживлення, оснащення приміщень замками, установку сигналізації і багато чого іншого.

До організаційних заходів можна віднести охорону серверів, ретельний підбір персоналу, виключення випадків ведення особливо важливих робіт лише однією людиною, наявність плану відновлення працездатності сервера після виходу його з ладу, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво).

Несанкціонований доступ до інформації може відбуватися під час профілактики або ремонту комп'ютерів за рахунок прочитання залишкової інформації на носіях, незважаючи на її видалення користувачем звичайними

методами. Інший спосіб - прочитання інформації з носія під час його транспортування без охорони всередині об'єкта.

Традиційними методами захисту інформації від несанкціонованого доступу є ідентифікація та аутентифікація, захист паролями.

У комп'ютерних системах зосереджується інформація, право на користування якою належить певним особам або групам осіб, що діють у порядку особистої ініціативи або відповідно до посадових обов'язків. Щоб забезпечити безпеку інформаційних ресурсів, усунути можливість несанкціонованого доступу, посилити контроль санкціонованого доступу до конфіденційної інформації, впроваджуються різні системи розпізнавання, встановлення дійсності об'єкта (суб'єкта) і розмежування доступу.

Ключовими поняттями в цій системі є ідентифікація та автентифікація. Ідентифікація - це присвоєння будь-якого об'єкта чи суб'єкту унікального імені або образу. Аутентифікація - це встановлення автентичності, тобто перевірка, чи є суб'єкт дійсно тим, за кого він себе видає.

Кінцева мета процедур ідентифікації і аутентифікації об'єкта (суб'єкта) - допуск його до інформації обмеженого користування у разі позитивного результату або відмова в допуску у випадку негативного результату перевірки.

Об'єктами ідентифікації і аутентифікації можуть бути:

- люди (користувачі, оператори та ін);
- технічні засоби (монітори, робочі станції, абонентські пункти);
- документи;
- магнітні носії інформації;
- інформація на екрані монітора та ін.

Встановлення дійсності об'єкта може здійснюватися апаратним пристроєм, програмою, людиною і т.д.

Захист паролями. Пароль - це сукупність символів, що визначає об'єкт (суб'єкта).

У разі застосування пароля необхідно періодично замінювати його на новий, щоб знизити ймовірність його перехоплення шляхом прямого

розкрадання носія, зняття її копії та навіть фізичного примусу людини. Пароль використовується для ідентифікації і встановлення автентичності терміналу, з якого входить в систему користувач, а також для зворотного встановлення автентичності комп'ютера по відношенню до користувача.

Для ідентифікації користувачів можуть застосовуватися складні у плані технічної реалізації системи, що забезпечують встановлення автентичності користувача на основі аналізу його індивідуальних параметрів: відбитків пальців, малюнка ліній руки, райдужної оболонки очей, тембру голосу і ін

Широке поширення знайшли фізичні методи ідентифікації з використанням носіїв кодів паролів. Такі носії є пропуском в контрольно-пропускних системах; пластикові картки з ім'ям власника, його кодом, підписом; пластикові картки з магнітною смугою; пластикові картки з вбудованою мікросхемою (smart-card); карти оптичної пам'яті та ін.

Засоби захисту інформації за методами реалізації можна розділити на три групи:

- Програмні;
- Програмно-апаратні;
- Апаратні.

Програмними засобами захисту інформації називаються спеціально розроблені програми, які реалізують функції безпеки обчислювальної системи, здійснюють функцію обмеження доступу користувачів по паролях, ключам, багаторівневому доступу і т.д. Ці програми можуть бути реалізовані практично в будь-якій операційній системі. Як правило, ці програмні засоби забезпечують досить високу ступінь захисту системи і мають помірні ціни. При підключенні такої системи в глобальну мережу ймовірність захисту збільшується. Отже, цей спосіб захисту прийнятний для локальних замкнених мереж, які не мають зовнішній вихід.

Програмно-апаратними засобами називаються пристрої, реалізовані на універсальних або спеціалізованих мікропроцесорах. Ці пристрої також адаптуються в будь-якій операційній системі, мають великий ступінь захисту.

При цьому даний тип пристроїв є самим гнучким інструментом, що дозволяє вносити зміни в конфігурацію на вимогу замовника. Програмно-апаратні засоби забезпечують високий ступінь захисту локальної мережі.

Апаратними засобами називаються пристрої, в яких функціональні вузли реалізуються на надвеликих інтегральних системах з незмінним алгоритмом функціонування. Цей тип пристроїв адаптується в будь-якій операційній системі, є найдорожчим в розробці, пред'являє високі технологічні вимоги при виробництві. У той же час ці пристрої мають найвищий ступень захисту, в них неможливо потрапити і внести конструктивні чи програмні зміни. Застосування апаратних засобів ускладнюється через їх високу вартість і статичності алгоритму. Програмно-апаратні засоби, поступаючись апаратним за швидкістю, дозволяють у той же час легко модифікувати алгоритм функціонування і не володіють недоліками програмних методів.

До окремої групи заходів щодо забезпечення збереження інформації та виявлення несанкціонованих запитів відносяться програми виявлення порушень в режимі реального часу.

Захисту інформації останнім часом приділяється все більше уваги на самих різніх рівнях - і державному, і комерційному.

Система захисту інформації від несанкціонованого доступу повинна забезпечувати виконання наступних функцій:

– ідентифікація ресурсів, тобто присвоєння ресурсам ідентифікаторів — унікальних ознак, по яких надалі система робить аутентифікацию;

– автентификация ресурсів, що захищаються, тобто встановлення їхньої дійсності на основі порівняння з еталонними ідентифікаторами;

– розмежування доступу користувачів по операціях над ресурсами (програми, дані), що захищаються за допомогою програмних засобів;

– адміністрування:

– визначення прав доступу до ресурсів, що захищаються;

– контроль цілісності і працездатності систем захисту.

1.5 Мета роботи

Основною метою кваліфікаційної роботи є удосконалення підсистеми захисту інформації, що забезпечує належний рівень безпеки та впровадження методів захисту інформації.

Поставлена мета досягається шляхом вирішення наступних завдань:

1) окреслити сутність проблеми і розглянути задачі захисту інформації в інформаційно-телекомунікаційній системі.

2) встановити загрози інформації і способи їх впливу на об'єкт захисту інформації.

3) впровадити методи та засоби захисту інформації в інформаційно-телекомунікаційній системі підприємства.

1.6 Попереднє обстеження об’єкту інформаційної діяльності.

Об’єктом інформаційної діяльності (далі ОІД) є комп’ютерний центр медичної установи “Сім’я”. Далі (МУ “ Сім’я ”).

Специфікація діяльності ОІД:

Комп’ютерний центр включає в себе декілька відділів закладу, а саме:

- відділ кадрів;
- економічний відділ;
- серверна.

Час роботи понеділок-п’ятниця з 8:00-17:00.

Таблиця 1.1 – Штат співробітників комп’ютерного центру

Відділ	Посада	Кількість співробітників
Відділ кадрів	Керівник відділу кадрів	1 людина
	Співробітники відділу кадрів	2 людини
Економічній відділ	Головний економіст	1 людина
	Економісти	5 чоловік

	Секретар головного економіста	1 людина
Комп'ютерний кабінет	Системній адміністратор	1 людина
	Помічник системного адміністратора	1 людина
-	Прибиральниця	3 чоловіка

1.7 Опис ОІД:

ОІД знаходиться на другому поверсі "МУ " Сім'я " і складається з трьох окремих приміщень. Будівля знаходиться в 200 метрах від траси стратегічного призначення та оточена іншими корпусами лікарні з усіх боків. Площа ОІД 50 $м^2$.

Централізовані системи опалення, вентиляції та каналізації виходять за межі контрольованої зони. Вентиляція організована за допомогою вентиляційних труб. Комунікації знаходяться на поверсі. ОІД має автономні системи електропостачання, водопостачання.

Контрольована зона: периметр комп'ютерного центру.

Вікна: двостулковий метало-пластиковий склопакет по 1шт. на приміщення розміром 2500 х 2700 мм. Внутрішні захисні металеві решітки на вікнах. Вікна в приміщеннях орієнтовані на північний схід. Віконні отвори обладнані регульованими пристроями типу: жалюзі.

Двері в приміщення металеві 180см в ширину, 10 см. в товщину і 210 см у висоту. Дверні петлі захищені антизрізами. Захисна металева внутрішня розсувна решітка на двері при вході до комп'ютерного центру.

Проведена телефонна лінія, яку надає ВАТ «Укртелеком». Комп'ютери кожного з відділів з'єднані в локальну мережу і мають вихід в Інтернет через безлімітне ADSL-підключення від ВАТ «Укртелеком».

План комп' ютерного центру приведений в додатку «Б».

1.8 Аналіз структури ІТС на ОІД:

ІТС ОІД являє собою мережу типу «зірка», з виділеним сервером, побудовану з використанням одного комутатору. Структурна схема мережі представлена на рисунку 1.2.

ІТС являє собою багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності, а також має ADSL доступ до мережі Інтернет, який забезпечує ВАТ «Укртелеком». Відноситься до треотьго класу.

1) обчислювальна система у складі:

– одинадцять ПЕОМ (Microsoft Windows 10 Professional), об'єднаних у ЛОМ витою парою 5-ої категорії для внутрішньої прокладки ;

– сервер управління доступом до мережі Інтернет з централізованим оновленням антивірусних баз і управліннм системними оновленнями;

– активне мережеве обладнання (1 комутатор першого рівня на 16 портів);

– програмні засоби активного мережевого обладнання, що реалізують спеціальні алгоритми управління мережею;

– прикладне ПЗ (Microsoft Office, Total Commander, WinRAR, Adobe Reader, 1С-бухгалтерія, Avast Antivirus 21.2, «Медичні кадри», Norton 360);

– модем ZXV10H108L;

2) периферійні пристрої вводу\виводу даних Canon MP 460 (4 прилади);

3) фізичне середовище − виділені приміщення підприємства, в яких розташована ІТС, що знаходяться у межах контрольованої зони;

4) користувачі ІТС:

− системний адміністратор мережі;

− користувачі з рівними повноваженнями;

5) в інформаційно-телекомунікаційній системі підприємства циркулює конфіденційна інформація, яка накопичується у базі даних та обробляється на робочих станція та зберігається на зовнішніх носіях, на які здійснюється

архівування баз даних.

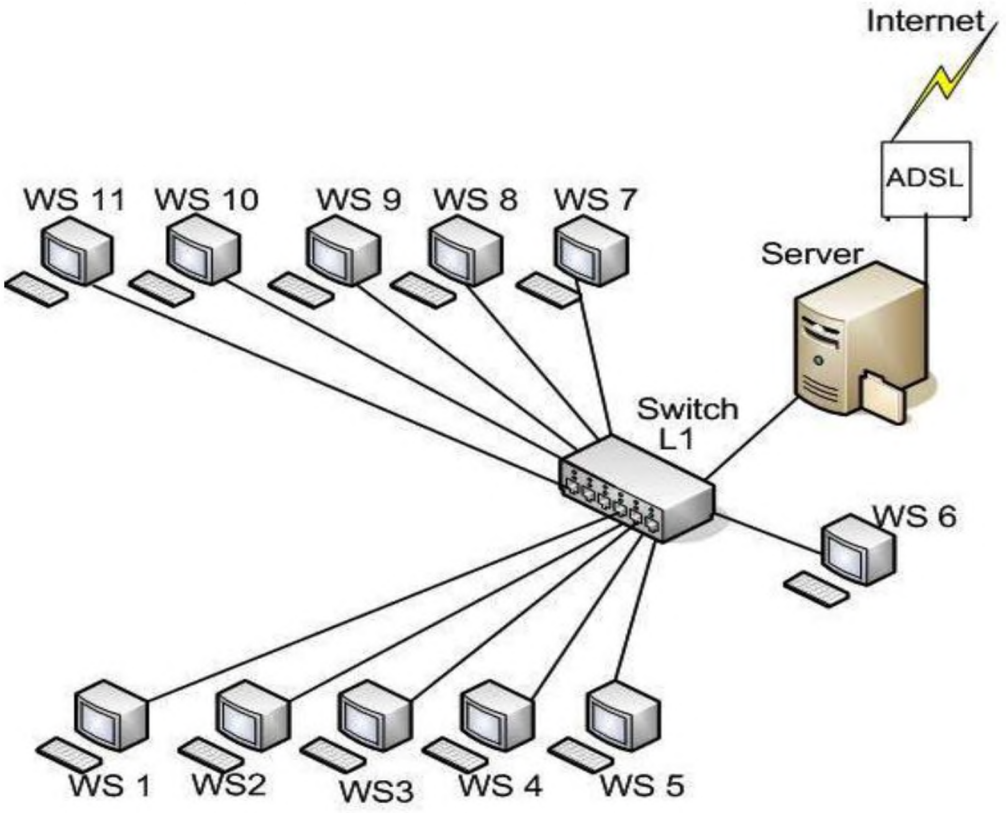


Рисунок 1.2. «Структура ІТС

1.9 Висновок

На основі розглянутих шляхів витоку інформації та способів впливу загроз на об’єкт інформаційної діяльності, а також на основі проведеного обстеження ОІД, було прийнято рішення вдосконалити нинішні засоби захисту інформації, оскільки існує загроза витоку інформації, що може призвести до потенційних збитків.

РОЗДІЛ 2. АНАЛІЗ ТА ВПРОВАДЖЕННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ

2.1 Технічне завдання

2.1.1 Найменування і сфера застосування

Найменування: «Підсистема захисту інформації інформаційно-телекомунікаційної системи ».

Сферою застосування є комп'ютерний центр медичної установи "Сім'я".

2.1.2 Підстава для розробки:

1) Наказ ректора НТУ «ДП» № 317-С від «07» червня 2021 р.
2) Вимоги замовника;

2.1.3 Призначення розробки

Призначенням даного дипломного проекту є підвищення рівня безпеки ІТС. Досягнення необхідного рівня захисту ІзОД за мінімальних затрат і допустимого рівня обмежень видів інформаційної діяльності.

2.1.4 Загальна характеристика підприємства і умови функціонування мережі.

Об'єктом інформаційної діяльності є комп'ютерний центр ЗАТ МУ " Сім'я " . ІТС ОІД являє собою мережу типу «зірка», з виділеним сервером, побудовану з використанням одного комутатору.

ІТС являє собою багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності, а також має ADSL доступ до мережі Інтернет, який забезпечує ВАТ «Укртелеком». Відноситься до треотьго класу.

1) обчислювальна система у складі:

– одинадцять ПЕОМ (Microsoft Windows 10 Professional), об'єднаних у ЛОМ витою парою 5-ої категорії для внутрішньої прокладки ;

– сервер управління доступом до мережі Інтернет з централізованим оновленням антивірусних баз і управліннм системними оновленнями;

– активне мережеве обладнання (1 комутатор першого рівня на 16 портів);

– програмні засоби активного мережевого обладнання, що реалізують спеціальні алгоритми управління мережею;

– прикладне ПЗ (Microsoft Office, Total Commander, WinRAR, Adobe Reader, 1С-бухгалтерія, Avast Antivirus 21.2, «Медичні кадри», Norton 360);

– модем ZXV10H108L;

2) периферійні пристрої вводу\виводу даних Canon MP 460 (4 прилади);

3) фізичне середовище – виділені приміщення підприємства, в яких розташована ІТС, що знаходяться у межах контрольованої зони;

4) користувачі ІТС:

– системний адміністратор мережі;

– користувачі з рівними повноваженнями;

5) в інформаційно-телекомунікаційній системі підприємства циркулює конфіденційна інформація, яка накопичується у базі даних та обробляється на робочих станціях;

2.1.5 Критерії впровадження системи:

Система захисту повинна забезпечувати властивості:

1) для публічної інформації :

– цілісність;

– доступність;

2) для інформації з обмеженим доступом

– цілісність;

– конфіденційність;

– доступність;

– спостережливість.

Необхідно забезпечити функціональний профіль захищеності у визначеній ІТС з підвищеними вимогами до забезпечення конфіденційності, цілісності й доступності оброблювальної інформації не нижчий за стандартний профіль.

Обраний профіль захищеності (опис послуг безпеки приведений у таблиці 2.1):

3.КЦД.1 = { КД-2, КО-1, КВ-1,ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 } з критеріями гарантій до середовища функціонування Г1.

Таблиця 2.1 - Профіль захищеності ІТС

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	1	2
Конфіденційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)
	Адміністративна конфіденційність	КА-2 (Базова адміністративна конфіденційність)
	Повторне використання об'єктів	КО-1 (повторне використання об'єктів)
	Конфіденційність при обміні	КВ-1(мінімальна конфіденційність при обміні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Адміністративна	ЦА-2 (базова адміністративна

	цілісність	цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-1 (мінімальна цілісність при обміні)
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостережності	Реєстрація	НР-2 (захищений журнал)
	Ідентифікація і автентифікація	НИ-2 (одиночна ідентифікація і автентифікація)
	Достовірний канал	НК-1 (однонаправлений достовірний канал)
	Розподіл обов'язків	НО-2 (розподіл обов'язків адміністраторів)
	Цілісність комплексу засобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)
	Самотестування	НТ-2 (самотестування при старті)
	Ідентифікація і автентифікація при обміні	НВ-1(автентифікація вузла)

Базова довірча конфіденційність (КД-2)

Послуга застосовується для розмежування доступу користувачів до захищених об'єктів і дозволяє користувачу керувати потоками інформації в АС від захищених об'єктів, що належать його домену, до інших користувачів.

Політика довірчої конфіденційності поширюється на об’єкти і забезпечує взаємодію зазначених об’єктів:

– користувачів усіх категорій;

– об’єкти, які містять конфіденційну інформацію, за умови визначення в АС груп користувачів з однаковими повноваженнями стосовно такої інформації і тільки в межах цих груп;

– всі інші об’єкти, які підлягають захисту, але не належать до зазначених вище видів.

Політика довірчої конфіденційності, що реалізується КЗЗ, стосується об’єктів, які створюються користувачем у процесі виконання ним функціональних обов’язків.

КЗЗ повинен реалізувати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу, як власнику процесу, можливість визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати цей процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації.

Базова адміністративна конфіденційність (КА-2)

Ця послуга дозволяє адміністраторові безпеки (уповноваженим співробітникам СЗІ) та/або користувачам, яким надано повноваження інших адміністраторів, керувати потоками інформації від захищених об'єктів, що зберігаються й циркулюють в АС, до користувачів.

Політика адміністративної конфіденційності поширюється на: користувачів усіх категорій; сильно- та слабозв'язані об'єкти, що містять конфіденційну інформацію; системне та функціональне програмне забезпечення, що використовується для оброблення конфіденційної інформації; технологічну інформацію КСЗІ; технологічну інформацію щодо управління АС;

доступ користувачів до окремих видів периферійних пристроїв (принтерів, накопичувачів на змінних машинних носіях інформації тощо), задіяних в обробці конфіденційної інформації, - і забезпечує взаємодію зазначених об’єктів. Стосовно об’єктів, для яких додатково в межах визначених доменів реалізується послуга КД-2, ця послуга застосовується для розмежування доступу до інформації користувачів на рівні доменів та для розмежування доступу до інформації користувачів різних доменів. Якщо послуга КД-2 не використовується, то політика адміністративної конфіденційності повинна поширюватися, крім зазначених вище, і на інші об’єкти, яких стосувалася послуга КД-2.

Розмежування доступу користувачів усіх категорій до захищеного об'єкта здійснюється засобами КЗЗ на підставі атрибутів доступу користувача й захищеного об’єкта. Призначення атрибутів доступу користувачам і процесам здійснюється адміністратором безпеки та/або уповноваженим на це співробітником СЗІ, на основі аналізу функціональних обов'язків окремих користувачів або груп користувачів та процесів і об'єктів, що відносяться до їх компетенції.

КЗЗ повинен надавати можливість користувачам, що мають відповідні повноваження : адміністраторам операційних систем, адміністраторам СКБД, адміністраторам мережевого обладнання, адміністраторам сервісів, - права доступу до процесів, що забезпечують ведення системних процесів щодо адміністративного супроводження функціонування АС в цілому, окремих її компонентів та сервісів.

КЗЗ повинен надавати тільки адміністратору безпеки та/або уповноваженим співробітникам СЗІ права доступу до процесів, що забезпечують актуалізацію, супроводження та аналіз технологічної інформації КСЗІ.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки (уповноваженого

співробітника СЗІ) або користувачів, яким надані повноваження інших адміністраторів.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного процесу визначати конкретних користувачів і/або групи користувачів, що мають право ініціювати процес, через керування належністю користувачів і процесів до відповідних доменів.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Повторне використання об’єктів (КО-1)

Послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, він не містить інформації, яка залишилась від використання його попереднім користувачем або процесом.

Політика повторного використання об'єктів, що реалізується КЗЗ, стосується тільки тих об'єктів ЛОМ, які містять конфіденційну інформацію і ресурси яких поділяються між користувачами ЛОМ та прикладними процесами, що виконуються в ЛОМ.

Вимоги цієї послуги поширюються на сегменти оперативної пам'яті робочих станцій та серверів (усіх без виключення типів) та носії інформації на жорстких магнітних дисках (ЖМД), якими укомплектовані робочі станції й сервери, і використовуються системними та функціональними процесами під час оброблення конфіденційної інформації, а також на окремі види периферійних пристроїв, які мають власну пам’ять і задіяні під час експорту (імпорту) конфіденційної інформації з (в) ЛОМ та створенні «твердих» копій тощо.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для

попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Вимога цієї послуги в повному обсязі поширюється і на розділювані одночасно декількома користувачами процеси.

Мінімальна конфіденційність при обміні (КВ-2)

Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

Мінімальна довірча цілісність (ЦД-1)

Послуга застосовується для захисту оброблюваної інформації від несанкціонованої модифікації і дозволяє користувачу будь-якої категорії керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

Політика довірчої цілісності, що реалізується КЗЗ, поширюється на слабо- та сильнозв’язані об’єкти, які створюються користувачем у процесі виконання ним функціональних обов’язків. Користувач, який створив об’єкт, має право визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати цей об'єкт.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Базова адміністративна цілісність (ЦА-2)

Політика базової адміністративної цілісності поширюється на: користувачів усіх категорій; сильнозв'язані об'єкти, що містять конфіденційну інформацію; призначене для оброблення цих об'єктів системне та функціональне програмне забезпечення, а також створену в процесі обробки сильнозв'язаних об'єктів технологічну інформацію КСЗІ та технологічну інформацію щодо управління АС, - і забезпечує взаємодію зазначених об’єктів.

Право визначати множину об'єктів АС, цілісність яких забезпечується КЗЗ, а також визначати атрибути доступу процесу й захищеного об'єкта, на підставі яких КЗЗ буде здійснювати розмежування доступу, надається тільки адміністратору безпеки.

Розмежування доступу здійснюється в межах певного процесу наданням користувачу права (встановленням заборони) за допомогою функціональних можливостей цього процесу модифікувати об’єкт. КЗЗ повинен обробляти запити на зміну атрибутів доступу процесів і захищених об'єктів тільки в тому випадку, якщо вони надходять від адміністратора безпеки або від уповноваженого співробітника СЗІ.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного захищеного об'єкта (сукупності сильнозв'язаних об'єктів або певним чином виділеної підмножини їх, об'єкта, окремого стовпчика або окремого поля запису структурованого об'єкта) визначити домен, якому повинні належати ті процеси і/або групи процесів, що мають право модифікувати об’єкт. Тільки їм надається право включати й вилучати процеси та об'єкти до/з конкретних доменів.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Обмежений відкат (ЦО-1)

Послуга забезпечує можливість відмінити окрему операцію або послідовність операцій й повернути захищений об'єкт, з яким маніпулював користувач, до попереднього наперед визначеного стану.

Політика обмеженого відкату забезпечує взаємодію нижчезазначених об’єктів і поширюється на:

– користувачів усіх категорій;

– сильно- та слабозв’язані об’єкти, які містять конфіденційну інформацію і в процесі обробки яких передбачається можливість їхньої модифікації користувачем, а також технологічну інформацію КСЗІ.

Компоненти КЗЗ повинні мати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певну множину операцій, що вже виконані над захищеним об'єктом за певний проміжок часу.

Факт використання користувачем послуги має реєструватись в системному журналі. Відміна операції не повинна призводити до видалення з журналу запису про операцію, яка пізніше була відмінена, якщо остання підлягала реєстрації відповідно до вимог послуги безпеки .

Мінімальна цілісність при обміні (ЦВ-1)

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через

незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти криптостійкість використовуваних алгоритмів шифрування.

Використання ресурсів (ДР-1)

Послуга дозволяє керувати використанням користувачами послуг та ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, поширюється на нижчезазначені об'єкти і забезпечує взаємодію цих об'єктів, передбачаючи можливість встановлення обмежень на їх використання користувачами всіх категорій.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об'єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження інших адміністраторів. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів.

Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі.

Ручне відновлення після збоїв (ДВ-1)

Політика відновлення після збоїв, що реалізується КЗЗ, поширюється на нижчезазначені об'єкти та забезпечує їх взаємодію:

- системне та функціональне ПЗ;
- засоби захисту інформації та засоби управління КСЗІ;
- засоби адміністрування та управління обчислювальною системою.
- окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.і.), які задіяні для обробки конфіденційної інформації.

Послуга гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.

Політикою відновлення після збоїв повинна бути визначена й задокументована множина типів відмов і переривань обслуговування ЛОМ або окремих її компонентів, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Для кожної з відмов повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція автоматизованої системи.

Повернення АС (окремих компонентів) із режиму, що визначається погіршеними характеристиками обслуговування, в режим нормального функціонування повинно здійснюватися за допомогою ручних (не автоматизованих) процедур.

Захищений журнал - (НР-2)

Послуга реєстрації рівня НР-2 дозволяє контролювати небезпечні для АС дії зі сторони користувачів будь-яких категорій відносно процесів і об'єктів.

Політика реєстрації поширюється та забезпечує взаємодію користувачів усіх категорій.

КЗЗ повинен забезпечувати реєстрацію всіх подій, які мають безпосереднє відношення до його безпеки. До таких відносяться наступні класи подій:

– вхід/вихід або намагання входу/виходу в/із системи користувачів будь-яких категорій;

– реєстрація та видалення або намагання реєстрації та видалення користувачів будь-якої категорії із системи;

– зміна паролю користувачем будь-якої категорії;

– отримання або намагання отримання доступу користувачем будь-якої категорії до будь-яких процесів і об'єктів АС, що мають ступінь обмеження доступу на рівні конфіденційної інформації;

– виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на призначений для цього пристрій друку, або намагання виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на пристрій друку;

– копіювання наборів даних із інформацією конфіденційного характеру на запам'ятовуючих пристроях, які працюють зі змінними носіями, що здатні записувати інформацію, і виділені спеціально для виконання процесів копіювання, або намагання копіювання інформації конфіденційного характеру на запам'ятовуючих пристроях, які згідно з політикою безпеки для цього не призначені;

– виявлення і реєстрація фактів порушення цілісності КЗЗ;

– інші події, обов'язковість реєстрації яких передбачена політикою реалізації окремих послуг безпеки інформації.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який містить інформацію щодо дати, часу, місця (адреси робочої станції в АС), імені користувача, типу й успішності чи неуспішності кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію достатню для однозначної ідентифікації робочої станції, користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Адміністратор безпеки і користувачі, яким надано повноваження інших адміністраторів, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації, а КЗЗ повинен забезпечувати захист журналу реєстрації від НСД, модифікації або руйнування.

Одиночна ідентифікація та автентифікація (НИ-2)

Ідентифікація та автентифікація дозволяють визначити й перевірити особу користувача будь-якої категорії, що намагається одержати доступ до АС або до

захищених об’єктів, та повинні гарантувати, що доступ може бути надано тільки авторизованому користувачу.

Політика ідентифікації та автентифікації поширюється на нижчезазначені об’єкти і забезпечує їх взаємодію .

Кожний користувач, що отримує доступ до АС, повинен ідентифікуватися КЗЗ на підставі присвоєного йому імені. Дозвіл на виконання будь-яких дій, що контролюються КЗЗ, користувач отримує тільки після автентифікації його КЗЗ на підставі введеного ним пароля.

Механізм реалізації послуги повинен відповідати умовам надійного та однозначного виконання ідентифікації та автентифікації.

КЗЗ повинен забезпечувати захист даних автентифікації від НСД, модифікації або руйнування.

Однонаправлений достовірний канал (НК-1)

Послуга повинна гарантувати користувачу будь-якої категорії можливість безпосередньої взаємодії з КЗЗ, а також те, що ніяка взаємодія користувача з ЛОМ не може бути модифікованою іншим користувачем або процесом. Послуга повинна визначати вимоги до механізму встановлення достовірного зв'язку між користувачем і КЗЗ.

Політика достовірного каналу поширюється на користувачів усіх категорій, окремі компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ, і забезпечує взаємодію зазначених об’єктів.

Достовірний канал повинен використовуватися для початкової ідентифікації та автентифікації. Зв'язок із використанням даного каналу повинен ініціюватися виключно користувачем.

Розподіл обов’язків адміністраторів (НО-2)

Послуга дозволяє розмежувати повноваження користувачів, визначивши категорії користувачів із певними й притаманними для кожної з категорій функціями. Послуга призначена для зменшення потенційних збитків від навмисних або помилкових дій користувачів й обмеження авторитарності керування АС.

Політика розподілу обов’язків, що реалізується КЗЗ, поширюється на користувачів усіх категорій і повинна визначати щонайменше такі ролі:

– адміністратора безпеки;

– не менше, ніж одного іншого адміністратора (адміністратора баз даних, адміністратора мережевого обладнання, адміністратора сервісів та ін.);

– користувачів, яким надано право доступу до конфіденційної інформації.

Ролі адміністраторів можуть дублюватися уповноваженими на це користувачами. Кількість таких користувачів повинна бути мінімальною.

Адміністратор безпеки повинен мати доступ до технологічної інформації КСЗІ та системного й функціонального ПЗ, яке реалізує механізми захисту. Інший адміністратор повинен мати доступ до технологічної інформації щодо управління автоматизованої системи та системного й функціонального ПЗ, яке реалізує ці функції. Усім іншим користувачам доступ до цих об’єктів повинен бути заборонений.

Повинен заборонятися доступ адміністраторів до сильно- та слабозв'язаних об'єктів, що містять конфіденційну інформацію, за виключенням випадків, коли їхніми функціональними обов’язками передбачено суміщення адміністративних повноважень та повноважень щодо обробки конфіденційної інформації.

КЗЗ з гарантованою цілісністю (НЦ-2)

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Самотестування при старті (НТ-2)

Самотестування дозволяє КЗЗ перевірити й на підставі цього гарантувати правильність функціонування і цілісність множини функцій ЛОМ, що забезпечуються захистом.

Політика самотестування поширюється на нижче зазначені об'єкти і забезпечує їх взаємодію:

– адміністратора безпеки;

– компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ;

– засоби захисту інформації, а також технологічну інформацію КСЗІ.

До складу КЗЗ повинен входити набір тестових процедур, достатній для оцінки правильності виконання в ЛОМ всіх критичних для безпеки конфіденційної інформації та технологічної інформації КСЗІ функцій, а сам КЗЗ повинен бути здатним контролювати їх виконання.

Тести повинні виконуватися при ініціалізації КЗЗ за запитом адміністратора безпеки.

У разі некоректного виконання якогось із тестів КЗЗ повинен перевести АС до стану, в якому забороняється обробка конфіденційної інформації взагалі, або до стану, в якому забороняється обробка конфіденційної інформації з використанням послуг безпеки, для яких тест не було виконано. Повернути АС до нормального функціонування може тільки адміністратор безпеки після відновлення працездатності КЗЗ і повторного виконання повного набору тестів.

Автентифікація вузла (НВ-1)

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, таких як цифровий підпис і коди автентифікації повідомлень. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

2.2 Визначення інформаційних ресурсів, які потребують захисту

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Під інформацією Закон України "Про інформацію" [1] розуміє сукупність документованих або привселюдно оголошуваних відомостей про події або явища, що відбуваються у суспільстві, державі й навколишньому середовищі.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [3] трактує інформацію як сукупність всіх даних і програм, використовуваних в автоматизованій системі, незалежно від способу їхнього подання.

Існує наступний поділ інформації з категорій важливості:

1) життєво важлива незамінна інформація, наявність якої необхідна для функціонування підприємства;

2) важлива інформація – інформація, що може бути замінена або відновлена, але процес відновлення дуже важкий і пов'язаний з більшими витратами;

3) корисна інформація – інформація, яку важко відновити, однак підприємство може ефективно функціонувати й без неї;

4) несуттєва інформація – інформація, що більше не потрібна підприємству.

На практиці віднесення інформації до однієї із цих категорій може являти собою дуже важке завдання, тому що та сама інформація може бути використана багатьма підрозділами підприємства кожне з яких може нести цю інформацію до різних категорій важливості. Категорія важливості, як і цінність інформації, звичайно змінюється згодом і залежить від ступеня відносини до неї різних груп споживачів і потенційних порушників.

Згідно закону України «Про інформацію»[1] за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Інформація з обмеженим доступом - інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами.

Таємна інформація - інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

Конфіденційна інформація - інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними.

Відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" [3] захисту підлягає: відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (відкрита інформація). Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформаційний ресурс — сукупність документів у інформаційних системах.

Документом Закон України "Про інформацію" [1] передбачено матеріальну форму одержання, зберігання, поширення й використання інформації шляхом фіксації її на магнітній, кіно-, відео-, фотоплівці або на іншому носії. Поняття "документа" важливо, оскільки документи є частиною інформаційних ресурсів і мають юридичну значимість.

Інформація з обмеженим доступом (яка підлягає захисту) може оброблятися, передаватися та зберігатися за допомогою обчислювальних ресурсів ІТС, а саме: серверів, робочих станцій, запам'ятовуючих пристроїв, периферійних пристроїв (принтерів, накопичувачів на змінних магнітних носіях інформації), мережевого обладнання, системного та функціонального ПЗ,

засобів, що забезпечують взаємодію об’єктів ІТС.

Для ІТС МУ "Сім’я" необхідний захист наступного інформаційного ресурсу:

1) файлова система (логічні диски, каталоги, підкаталоги);

2) набори даних, які генеруються будь-яким функціональним або системним процесом;

3) файли, набори даних, які оброблюються, зберігаються і передаються в ІТС;

4) системне та функціональне ПЗ;

5) база даних з конфіденційними даними підприємства.

Інформаційні ресурси в ІТС циркулюють в обчислювальних засобах, а саме оперативно-запам'ятовуючий пристрій, дисковод, магнітні диски, дисплей, принтер (сканер), клавіатура, мережеве обладнання, які являються об’єктами захисту.

Таблиця 2.2 – Інформація що циркулює на ОІД

Інформація	Режим доступу	Правовий режим
	1	2
Особові справи працівників, трудові книжки, трудові договори, накази МОЗ, догани	З обмеженим доступом	Конфіденційна
Внутрішні документи (накази, службові записки, інструкції)	З обмеженим доступом	Конфіденційна
Статутні документи	Відкрита	Відкрита
Відомості про фінанси, плани закупівель, перспективні плані	З обмеженим доступом	Конфіденційна

підприємства		
Зміст та характер договорів, контрактів, однією із сторін яких виступає підприємство	З обмеженим доступом	Конфіденційна

Таблиця 2.3 – Визначення рівня конфіденційності, цілісності та доступності інформації

Інформація з обмеженим доступом	Рівень конфіденційності інформації	Рівень цілісності інформації	Рівень доступності інформації
	1	2	3
Особові справи працівників, трудові книжки, трудові договори, накази МОЗ, догани.	К4	Ц3	Д0
Внутрішні документи	К2	Ц3	Д1
Відомості про фінанси, перспективні плани підприємства	К1	Ц1	Д3
Договори , контракти, однією із сторін яких виступає підприємство	К1	Ц2	Д2
Плани закупівель	К2	Ц1	Д3

Конфіденційність

К0 - розголошення інформації призводить до краху роботи суб'єкта або дуже великих матеріальних втрат

К1-розголошення призводить до значних матеріальних втрат, якщо не буде вжито заходів.

К2 - розголошення призведуть до деяких матеріальних втрат.

К3 - Приносить матеріальний збиток в певних випадках.

К4 - може принести малозначний збиток в рідкісних випадках.

Цілістність

Ц0 - призводить до неправильної роботи суб'єкта в цілому або значної його частини і наслідки зміни незворотні.

Ц1 - несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів. Наслідки незворотні.

Ц2 - несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів.

Наслідки оборотні.

Ц3 - несанкціоновані зміни не приведуть до збою в роботі суб'єкта, наслідки оборотні.

Ц4 - несанкціоновані зміни не відражатимуться на роботі системи.

Доступність

Д0 - у разі порушення доступності інформації даного типу підприємство не понесе матеріального збитку, робота підприємства не буде порушена, бажано впровадження, зміни в існуючих технологічних процесах.

Д1 - у разі порушення доступності інформації даного типу підприємство понесе мінімальний збиток матеріального прибутку, робота підприємства не буде порушена, загальний дохід залишиться без зміни.

Д2 - у разі порушення доступності інформації даного типу підприємство понесе середній збиток матеріального прибутку за поточний квартал, робота підприємства не буде порушена, можливі відставання від конкурентних підприємств.

Д3 - в разі порушення доступності інформації даного типу підприємство понесе збиток матеріального прибутку, робота підприємства буде ускладнена, загальний дохід може знизиться до половини існуючого.

Д4 - у разі порушення доступності інформації даного типу підприємство понесе максимально велику шкоду матеріального прибутку протягом декількох

кварталів, необхідно прийняття радикальних рішень стосовно доступності інформації на підприємстві.

2.3 Визначення переліку загроз

Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС (НД ТЗІ 1.1-003-99 [4])

Загрози в залежності від виду впливів на інформацію й НСД до неї можна розділити на випадкові й навмисні.

До випадкових загроз варто віднести:

- відмови й збої апаратури;
- перешкоди на лінії зв'язку від впливів зовнішнього середовища;
- помилки людини як ланки системи;
- системні й системотехнічні помилки розробників;
- структурні, алгоритмічні й програмні помилки;
- аварійні ситуації й інші впливи.
- відмова від функціонування ІТС в цілому, наприклад вихід з ладу електроживлення;
- стихійні лиха: пожежа, повінь, землетрус, урагани, удари блискавки й т.д.

Навмисні загрози пов'язані з діями людини, причинами яких можуть бути певне невдоволення своєю життєвою ситуацією, сугубо матеріальний інтерес або проста розвага із самоствердженням своїх здатностей, як у хакерів, й т.д.

Таблиця 2.4 – Перелік загроз та визначення можливих порушень властивостей інформації

Загроза	Які властивості інформації порушуються		
	К	Ц	Д

	1	2	3
Загрози антропогенного характеру			

Продовження таблиці 2.4

Крадіжка: 1) технічних засобів; 2) носіїв інформації; 3) інформації; 4) засобів доступу (ключі, паролі).	+	+	+
Підміна (модифікація): 1) операційних систем; 2) систем управління базами даних; 3) прикладних програм; 4) інформації (даних), заперечення факту відправки повідомлень; 5) паролів і правил доступу.	+	+	+
Загроза	1	2	3
Знищення (руйнування): 1) технічних засобів (вінчестерів, системних блоків); 2) носіїв інформації (паперових, магнітних, оптичних); 3) програмного забезпечення (ОС,СУБД, прикладного ПЗ); 4) інформації (файлів, даних); паролів і інформації.	-	+	+

Продовження таблиці 2.4

Техногенні загрози			
Порушення нормальної роботи (переривання): 1) швидкості обробки інформації; 2) пропускної здатності каналів зв'язку; 3) обсягів вільної оперативної пам'яті; 4) обсягів вільного дискового простору; 5) електроживлення технічних засобів; хакерські атаки через глобальну мережу Інтернет.	-	-	+
Перехоплення інформації (несанкціоноване): 1) за рахунок ПЕМВ від технічних засобів; 2) при підключенні до каналів передачі інформації; 3) за рахунок порушення встановлених правил доступу; 4) занесення вірусу в робочі станції; 5) хакерські атаки.	+	+	-

Продовження таблиці 2.4

Загроза	1	2	3
Помилки: 1) при інсталяції ПЗ, ОС, СУБД; 2) при експлуатації ПЗ; 3) при експлуатації технічних засобів; 4) недбале ставлення співробітників до документації; помилки при введенні даних.	-	+	+
Порушення нормальної роботи: 1) порушення працездатності системи обробки інформації; 2) порушення працездатності зв'язку; 3) старіння носіїв інформації і засобів її обробки; 4) порушення встановлених правил доступу; електромагнітний вплив на технічні засоби.	-	+	+
Знищення (руйнування): 1) програмного забезпечення, ОС, СУБД; засобів обробки інформації.	-	+	+
Модифікація (зміна): 1) програмного забезпечення, ОС, СУБД; інформації при передачі по каналах зв'язку і телекомунікацій.	+	+	+
Стихійні загрози			
1) Аварії, пожежі,урагани; Непередбачувані ситуації, нез'ясовні явища, інші форс-мажорні обставини.	-	+	+

2.4 Визначення переліку порушників

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

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

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

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

– користувачі, яким надано повноваження розробляти й супроводжувати систему захисту інформації, а також повноваження забезпечувати управління ІТС - адміністратор мережі;

– користувачі, яким надано право доступу до конфіденційної інформації одного або декількох класифікаційних рівнів – головній лікар, начальник відділу кадрів, працівники відділу кадрів, головний економіст, економісти, секретар;

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

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

– технічний персонал, що здійснює повсякденне підтримання життєдіяльності фізичного середовища ІТС - інженер, електрики, технічний персонал з обслуговування будівель, ліній зв'язку.

Модель порушника — абстрактний формалізований або неформалізований

опис порушника. Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

Таблиця 2.5 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника
К0	Не знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем.
К4	Знає структуру, функції й механізми дії засобів захисту, їх недоліки.
К5	Знає недоліки та “вади” механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості.
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення.

Таблиця 2.6 – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника
Ч1	До впровадження АС або її окремих компонентів.
Ч2	Під час бездіяльності компонентів системи (в неробочий час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.).
Ч3	Під час функціонування АС (або компонентів системи).
Ч4	Як у процесі функціонування АС, так і під час пзупинки компонентів системи.

Таблиця 2.7- Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника
Д1	Без доступу на контрольовану територію організації.
Д2	З контрольованої території без доступу у будинки та споруди.
Д3	Усередині приміщень, але без доступу до технічних засобів АС.
Д4	З робочих місць користувачів АС.
Д5	З доступом у зони даних (баз даних, архівів й т.ін.).
Д6	З доступом у зону керування засобами забезпечення безпеки АС.

Таблиця 2.8 – специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення
М1	Безвідповідальність
М2	Самозатвердження
М3	Корисливий інтерес

Таблиця 2.9– Визначення переліку порушників за можливими мотивами, місцем, часом дії та категорією обізнаності

Посада	Можливий мотив	Категорія обізнаності порушника	Можливе місце дії	Можливий час дії
	1	3	3	4
Внутрішні				
Головний лікар	М2,М3	К1	Д6	Ч4
Голова відділу кадрів	М2, М3	К2	Д5	Ч4
Працівники відділу кадрів	М1,М2, М3	К1	Д4	Ч3
Головний економіст	М2,М3	К2	Д5	Ч4
Економісти	М1,М2, М3	К1	Д4	Ч3
Секретар головного економісту	М1,М2, М3	К1	Д4	Ч4
Помічник системного адміністратора	М1,М2, М3,	К4	Д6	Ч4
Системний адміністратор	М2, М3	К5	Д6	Ч4
Прибиральниця	М2, М3	К0	Д3	Ч2
Зовнішні				
Представники організацій, що взаємодіють з питань технічного забезпечення	М3	К5	Д2	Ч1

Продовження таблиці 2.9

Представники організацій, що взаємодіють з питань ПЗ	М3	К4	Д3	Ч1
Хакери	М2, М3	К3	Д1	Ч3

2.5 Визначення можливих каналів каналів несанкціонованого доступу до ІТС на ОІД

Несанкціонований доступ до інформації - доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми.
Доступ порушенням посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, що має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків. Витік інформації - неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання (ДСТУ 3396.2-97 [5]).
Основними каналами витоку інформації в ІТС на ОІД є:

1) змінні носії, та носії на які здійснюється архівування;
2) робочі станції працівників відділів;
3) робоча станція адміністратора системи;
4) засоби вводу\виводу інформації;
5) канали передачі інформації в ІТС;
6) комутатор.

2.6 Аналіз забезпечених критерій профілю захищеності системи до розроблення підсистеми безпеки

Проаналізувавши ІТС підприємства було визначено, що деякі критерії профілю захищеності вже забезпечені, що вказано в таблиці 2.10. Критерії

забезпечуються встановленими в ІТС програмними засобами, що є сертифікованими в Україні.

Таблиця 2.10 – Забезпечені критерії профілю захищеності в ІТС

Критерії	Вимоги до рівнів послуг безпеки	З допомогою чого реалізовані
Конфіденційності	КД-2 (базова довірча конфіденційність)	ОС Microsoft Windows 10 Professional
	КА-2 (Базова адміністративна конфіденційність)	-
	КО-1 (повторне використання об'єктів)	ОС Microsoft Windows 10 Professional
	КВ-1(мінімальна конфіденційність при обміні)	-
Цілісності	ЦД-1 (мінімальна довірча цілісність)	-
	ЦА-2 (базова адміністративна цілісність)	-
	ЦО-1 (обмежений відкат)	ОС Microsoft Windows 10 Professional
	ЦВ-1 (мінімальна цілісність при обміні)	-
Доступності	ДР-1 (квоти)	-

Продовження таблиці 2.10

	ДВ-1 (ручне відновлення)	ОС Microsoft Windows 10 Professional, Avast Antivirus 21.2
Спостережності	НР-2 (захищений журнал)	ОС Microsoft Windows 10 Professional, Avast Antivirus 21.2
	НИ-2 (одиночна ідентифікація і автентифікація)	-
	НК-1 (однонаправлений достовірний канал)	-
	НО-2 (розподіл обов'язків адміністраторів)	-
	НЦ-2 (КЗЗ з гарантованою цілісністю)	ОС Microsoft Windows 10 Professional
	НТ-2 (самотестування при старті)	ОС Microsoft Windows 10 Professional та Avast Antivirus 21.2
	НВ-1(автентифікація вузла)	-

2.7 Вибір заходів захисту інформації та реалізація захисту в ІТС підприємства

Забезпечення безпеки інформації в ІТС досягається шляхом застосування комплексу заходів щодо захисту інформації: організаційних, організаційно-технічних, застосування програмних, апаратних та програмно-апаратних засобів захисту, застосування технічних засобів захисту.

2.7.1 Впровадження організаційних заходів захисту на ОІД:

Згідно НД ТЗІ 1.1-003-99 [4] матриця доступу — n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об'єктів КС одного типу (об'єктів-користувачів, об'єктів-процесів чи пасивних об'єктів), і містить визначені права доступу суб'єктів до кожного із типів об'єктів.

Згідно з Законом України „Про захист інформації в інформаційно-телекомунікаційних системах"[3]:

Доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Таблиця 2.11 – Матриця керування доступом

	O1	O2	O3	O4	O5	O6	O7
C1	Ч, З, Д, Зн, К, М	Ч, З, Д, Зн, К, М	Ч, З, Д, Зн, К, М	Ч, З, Д, К, М	Ч, З, Д, Зн, К, М	Ч, З, Д, Зн, К, М	Ч, З, Д, К, М
C2	Ч, З, Д, Зн, К, М	Ч, З, Зн,Д, К, М	-	Ч, Д, К	-	Ч, З, Д, Зн, К, М	Ч,Д, К,М
C3	Ч	Ч, Д, К, М	-	Ч, Д, К	-	Ч, Д, К,М	Ч, Д,К
C4	-	Ч, Д, К	Ч, З, Д, Зн, К, М	Ч, Д, К	Ч, З, Д, Зн, К, М	Ч,Д	-
C5	-	Ч, Д, К	Ч, З, Д, К, М	Ч, Д, К	Ч, Д	Ч,Д	-

Продовження таблиці 2.11

С6	-	Ч, Д, К	Ч, Д,М,К	Ч, Д, К	Ч,Д	-	-
С7	-	Ч, Д, К	-	Ч, Д, К	-	-	-
С8	-	Ч, Д, К	-	Ч, Д, К	-	-	-

Позначення:

Суб'єкти доступу:

С1 головний лікар(1)

С2 голова відділу кадрів(1)

С3 працівники відділу кадрів(2)

С4 головний економіст(1)

С5 економісти(7)

С6 секретар головного економісту(1)

С7 помічник системного адміністратора(1)

С8 системний адміністратор(1)

Об'єкти доступу:

О1 база даних відділу кадрів

О2 облік внутрішніх документів

О3 плани підприємства (плани закупівель, продажу, поточні і перспективні плани виробництва)

О4 статутні документи підприємства

О5 відомості про фінанси підприємства

О6 інформація про робітників

О7 трудові договори робітників

Операції з файлами:

Ч читання

К копіювання

З зберігання

М модифікація

Д друкування

Зн знищення

2.7.2 Рекомендовані інструкції для користувачів та системних адміністраторів на ОІД:

1) Розробити та впровадити посадові інструкції користувачів та персоналу ІТС, а також інструкції, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до ІТС;

2) Обмежити доступ в приміщення, в яких відбувається обробка та зберігати інформації з обмеженим доступом згідно матриці доступу;

3) Розробити та впровадити розпорядчі документи щодо правил перепусткового режиму на територію, де розташована ІТС;

4) Розробити та впровадити розпорядчі документи щодо використання робочих станцій користувачами та зазначити в них що користувач несе матеріальну відповідальність за цілісність робочої станції;

5) Визначити правила обліку, зберігання, розмноження, знищення носіїв конфіденційної інформації, яка обробляється на ОІД згідно матриці доступу;

6) Створити на програмному рівні системи розпізнання й розмежування доступу до інформації засобами ідентифікації й автентифікації користувачів даної ІТС;

7) Розмежувати права користувачів ІТС у групи користувачів, згідно з матрицею доступу, програмними методами ОС;

8) Блокувати облікові записи користувачів після певного числа невдалих спроб входу в систему, що зменшить вірогідність підбору паролю неавторизованим користувачем за допомогою функції Менеджера облікових записів, до якої входить підтримка механізму ідентифікації і перевірки дійсності користувачів при вході в систему, блокувати ПЕОМ на час відсутності користувача;

9) Створити набір прав, що дозволяє надавати користувачеві доступ на виконання окремих операцій та використання окремих програм за допомогою програмного продукту DeviceLock;

10) Організувати захист атрибутами файлів. При цьому передбачена можливість встановлювати, чи може індивідуальний файл бути змінений або розділений визначеним користувачем. Захист атрибутами файлів використовується для запобігання випадкових змін або видалення окремих файлів. При захисті даних використовуються файлові атрибути: «модифікація, читання, копіювання, друкування, знищення» програмними засобами;

11) Контролювати доступ користувачів до CD-і DVD-дисководів, жорстких дисків, зовнішніх USB-носіїв, USB- портів за допомогою програмного продукту DeviceLock, чим забезпечиться мінімізація занесення вірусу з боку зовнішніх носіїв та зменшиться вірогідність копіювання інформації;

12) Знищувати інформацію, що зберігається в ПЗУ, при списанні або відправці ПЕВМ в ремонт;

13) Захищати локальні розділи диску від випадкового або навмисного форматування;

14) Ідентифікувати зовнішні носії на які здійснюється архівування даних, ідентифікувати периферійні засоби вводу\виводу інформації (клавіатури, миші, принтери), надаючи користувачеві доступ до пристрою з відповідним ідентифікатором (драйвером або серійним номером) програмним методом;

15) Протоколювати всі дії користувачів з пристроями і файлами згідно матриці доступу (копіювання, читання, знищення і т.п);

16) Встановити нове антивірусне програмне забезпечення та налаштування між сітьового екрану;

17) Зберігати конфіденційну інформацію на окремому спеціально виділеному локальному диску та обмежити до нього сітьовий доступ програмними засобами.

18) Обмежувати доступ до соціальних мереж та засобів миттєвого обміну повідомленнями, а також до сайтів, які не зв'язані з робочим процесом програмними засобами;

19) Заборонити користувачам скачування та встановлення будь-яких програм програмними засобами;

20) Налаштувати поштовий антивірусний монітор, який сканувatиме кожне повідомлення і доставить на ящик листи які не містять ні вбудованого шкідливого коду, не інфікованих вкладень ;

21) Заблокувати невживані порти комутатора програмними засобами.

22) Роздяти обов'язки системних адміністраторів програмними засособами.

23) При виникненні необхідності обміну даними через незахищене середовище налаштувати міжсітьовий екрану на використання тільки протоколів SSL та Ipsec, а також використання електронного цифрового підпису для забезпечення цілісності документів, що передаватимуться через незахищений канал зв'язку.

2.7.3 Вибір програмних засобів захисту на ОІД

2.7.3.1 Огляд програмного продукту DeviceLock DLP Suite версії 9.x

Використання неавторизованих USB-пристроїв та записуючих CD / DVD-приводів становить загрозу для ІТС. Може бути спричинений витік конфіденційної інформації через USB-порт. Віруси або троянські програми можуть бути занесені всередину мережі, минаючи серверні файрволи та антивіруси.

Для рішення цієї проблеми рекомендовано встановлення програмного продукту DeviceLock DLP Suite версії 9.x.

DeviceLock - програмний засіб, призначений для захисту та адміністрування локальних і мережевих комп'ютерів шляхом запобігання неконтрольованих дій користувача при обміні інформацією через комп'ютерні порти і пристрої зі змінними носіями.

Забезпечує контроль і протоколювання доступу користувачів до пристроїв і портів введення-виведення. DeviceLock дозволяє контролювати : USB-порти, дисководи, CD / DVD-приводи, а також інфрачервоні, паралельні і послідовні порти, WiFi і Bluetooth-адаптери, стрічкові накопичувачі, КПК, будь-які внутрішні і зовнішні змінні накопичувачі і жорсткі диски, принтери (локальні, мережеві і віртуальні)

DeviceLock здійснює детальний аудит (включаючи тіньове копіювання) дій користувачів з пристроями і даними. Закриває потенційну вразливість у захисті простим і економічним способом. Агент DeviceLock Service, будучи основним компонентом програмного комплексу «DeviceLock DLP Suite версії 9.x» встановлюється на кожен комп'ютер та автоматично запускається при завантаженні ОС.

Даний програмний продукт сертифікований в Україні з 02.11.2011. Експертний висновок № 324.

Реалізовані послуги відповідають вимогам документа НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»[6].

DeviceLock дозволяє контролювати доступ користувачів і груп користувачів до будь-яких локальних пристроїв введення-виведення в залежності від часу та дня тижня. Для змінних носіїв, дисководів, жорстких дисків, CD / DVD-приводів і стрічкових накопичувачів можна встановлювати доступ «тільки читання».

DeviceLock дозволяє задати для певних користувачів / груп свій список пристроїв, доступ до яких завжди буде дозволений, навіть якщо заборонено використання USB-порту. Пристрої можна ідентифікувати по моделі і унікальному серійному номеру. Дозволяє надавати тимчасовий доступ до USB-пристроїв. Адміністратор повідомляє такому користувачеві спеціальний короткий код, який тимчасово розблоковує доступ тільки до необхідного пристрою на певний час.

DeviceLock забезпечує детальний аудит всіх дій користувачів з пристроями і файлами (копіювання, читання, видалення і т. п.). Додатково можна включити аудит системних подій в DeviceLock і дій адміністраторів.

DeviceLock дозволяє зберігати точні копії файлів і даних, що копіюються користувачами з їх комп'ютерів на зовнішні пристрої та носії, надрукованих документів, даних, що передаються через COM-і LPT-порти, і в каналах мережевих комунікацій.

Централізоване зберігання журналів аудиту та тіньового копіювання. Дані аудиту та тіньові копії скопійованих користувачами файлів можна зберігати як локально на комп'ютерах користувачів, так і в базі даних DeviceLock Enterprise Server, що дозволяє забезпечити централізовану обробку даних аудиту.

Програмний засіб забезпечує контекстний контроль каналів мережевих комунікацій на робочих станціях, включаючи розпізнавання мережних протоколів незалежно від використовуваних портів, детектування комунікаційних програм та їх блокування, реконструкцію повідомлень і сесій з відновленням файлів.

2.7.3.2 Обгрунтування вибору програмного продукту

Рекомендований програмній засіб відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі «Державна експертиза за критеріями технічного захисту інформації програмного засобу захисту інформації DeviceLock DLP Suite. Технічні вимоги» [7] та не має сертифікованих в Україні аналогів.

Для захисту інформації, яка оброблюється в ІТС , в DeviceLock DLP Suite підтримуються послуги безпеки, які визначаються функціональним профілем КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДВ-1, НР-1, НР-2, НИ-1, НО-2, НЦ-1 згідно з НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»[6].

КА-1 - мінімальна адміністративна конфіденційність;

КА-2 - базова адміністративна конфіденційність;

ЦА-1 - мінімальна адміністративна цілісність;

ЦА-2 - базова адміністративна цілісність;

ДР-1 – використання ресурсів (квоти);

ДВ-1 – ручне відновлення після збоїв;

НР-1 - зовнішній аналіз;

НР-2 - захищений журнал;

НИ-1 - зовнішня ідентифікація і автентифікація;

НО -2 - розподіл обов'язків адміністраторів;

НЦ-1- цілісність комплексу засобів захисту.

2.7.3.3 Вибір антивірусних програмних засобів

Проведемо порівняння результатів галузевих тестів і даних. Зрівняємо різні антивірусні продукти: Microsoft Defender версії 4.18, Антивірус ESET NOD32 для Windows версії 14.1, Avast Antivirus версії 21.2.

Тест антивірусів на лікування та виявлення активного зараження.

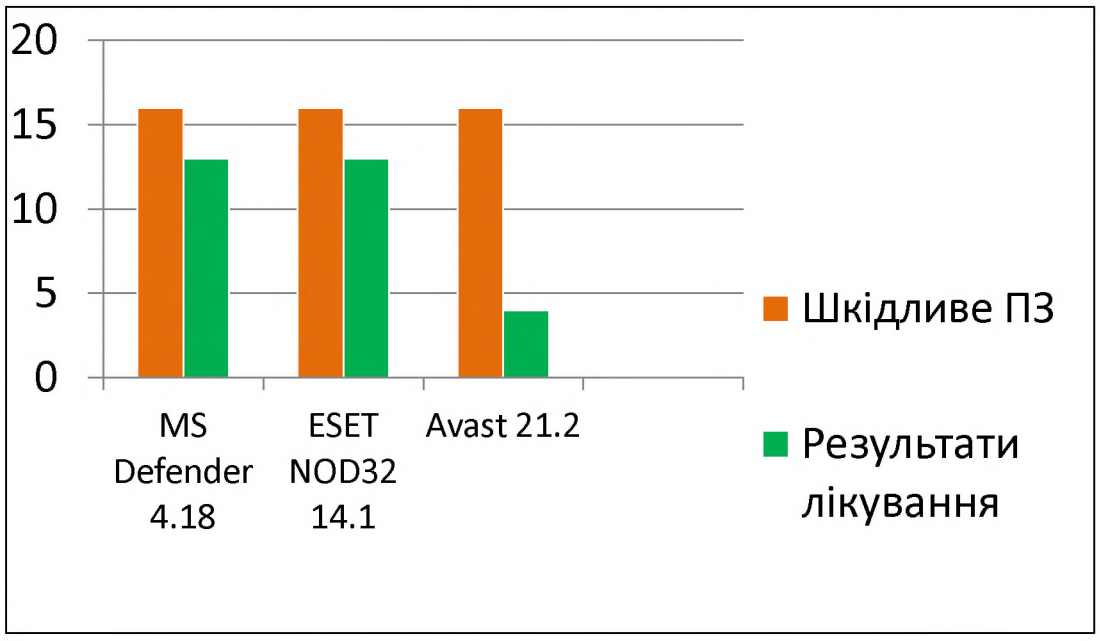


Рисунок 2.1 «Результати тестування антивірусів»

У даному тесті вивчаються здібності популярних антивірусів в лікуванні найбільш складних активних заражень комп'ютера, коли шкідлива програма вже була раніше запущена і встановлена, більше того, може перешкоджати своєму виявленню і видаленню.

Більш детальний огляд результатів незалежних тестів програмного забезпечення з інформаційної безпеки, підготовлених та проведених командою експертів інформаційно-аналітичного центру Anti-Malware [8] приведені у додатках В,Г,Д,Е,Ж .

Програмне забезпечення Microsoft Defender
потребує 375 МБ вільного місця на жорсткому диску та 256 МБ вільної оперативної пам'яті. Сумісний з ОС Microsoft Windows 10 Home Edition, Microsoft Windows 10 Professional, Microsoft Windows 10 Professional x64 Edition.

Програмне забезпечення ESET NOD32. Для роботи антивірусного агента і антивірусного пакету потрібно не менше 32 МБ оперативна пам'ять, вільне місце на жорсткому диску не менше 128 МБ. Сумісний з ОС Windows Windows 10/8/7/Vista/XP.

Програма оновлюється дуже часто і містить найбільш свіжі бази даних всіляких шкідливих програм.

Порівнюючи між собою вище перераховані антивірусні продукти було встановлено, що антивірусне програмне забезпечення Avast Antivirus, яке встановлена в ІТС на ОІД, лікує активне зараження лише на 25% в порівнянні з Microsoft Defender та ESET NOD32.

Microsoft Defender потребує більших ресурсів ніж ESET NOD32 та коштує значно дорожче.

Обраний антивірусний засіб для захисту інформації в ІТС - ESET NOD32, який сертифікований в Україні з 12.01.2010. Експертний висновок № 209.

Забезпечує захист файлових серверів під керуванням ОС Windows від дій вірусів та шкідливих програм.

Відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі "Технічні вимоги за критеріями технічного захисту інформації програмного продукту антивірусного захисту [7] «Антивірус ESET для Windows» версії 14.1, «Dr.Web Security Space» версії 12.6, «Антивірус ESET для файлових

серверів Windows» версії 14.1, сукупність яких визначається функціональним профілем: КА-2, ЦА-2, ЦВ-1, ДС-1, ДЗ-1, ДВ-1, НР-1, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 згідно з НД ТЗІ 2.5-004-99[6].

КА-2 - адміністративна конфіденційність;

ЦА-2 - базова адміністративна цілісність;

ЦВ-1 - цілісність при обміні;

ДС-1 - стійкість при обмежених відмовах;

ДЗ-1 - модернізація;

ДВ-1 - ручне відновлення;

НР-1 – зовнішній аналіз;

НИ-2 - одиночна ідентифікація та автентифікація;

НК-1 - однонаправлений достовірний канал;

НО-1 - розподіл обов'язків;

НЦ-1 - КЗЗ з гарантованою цілісністю;

НТ-2 - самотестування при старті.

2.7.4 Впровадження організаційно-технічних заходів захисту на ОІД:

Створення віртуальних мереж за допомогою реалізації і VLAN (Virtual Local-Area Network).

Віртуальна мережа - група вузлів мережі, трафік якої, на канальному рівні повністю ізольований від інших вузлів мережі.

Передача кадрів між різними віртуальними мережами на підставі адреси канального рівня неможлива.

При використанні технології віртуальних мереж в комутаторах одночасно вирішуються два завдання: підвищення продуктивності в кожній з віртуальних мереж, так як комутатор передає кадри в такій мережі тільки вузлу призначення, ізоляція мереж друг від друга для управління правами доступу користувачів і створення захисних бар'єрів на шляху широкомовних штормів.

Технологія VLAN підприємству велику кількість переваг. Збільшення продуктивності локальної мережі підприємства. Відхід від обмежень, що накладаються традиційною концепцією організації локальних мереж. Зниження витрат, що виникають в результаті переміщення персоналу. VLAN забезпечує і істотне зниження витрат праці, а значить, і коштів при переміщенні співробітників. Спрощення мережевого адміністрування.

Технологія VLAN надає можливість створення робочих груп, грунтуючись на функціональності, а не на фізичному розташуванні робочих станцій.

Робочі групи, засновані на загальних функціях користувачів і загальних ресурсах, в доступі до яких вони потребують. За допомогою реалізації VLAN користувачі кожного відділу можуть бути логічно описані і згруповані в різні робочі групи з різними доступними ресурсами мережі.

Обмін даними ведеться тільки всередині конкретної VLAN, комп'ютери з різних віртуальних мереж не можуть отримувати трафік, що генерується в інших VLAN.Кожна VLAN це закрита, логічно оголошена група.

Існує декілька методів створення віртуальних локальних мереж: на базі портів, MAC-адрес та протоколів третього рівня. Кожен тип VLAN має свої переваги і недоліки.

VLAN на базі портів. Організовуються шляхом логічного об'єднання обраних фізичних портів комутатора. Наприклад, мережевий адміністратор може вказати, що порти комутатора з номерами 1, 2, 5 утворюють VLAN1, а порти з номерами 3, 4, 6 утворюють VLAN2 і т.д.. До одного порту комутатора може бути підключено кілька комп'ютерів (наприклад, через хаб). Всі вони будуть належати до однієї VLAN - до тієї, до якої приписаний обслуговуючий їх порт комутатора.

VLAN на базі MAC-адрес. Цей спосіб дозволяє будувати VLAN, ґрунтуючись на унікальному шістнадцятковому адресі канального рівня, який має кожен мережевий адаптер сервера або робочої станції мережі. Це більш гнучкий спосіб організації VLAN в порівнянні з попереднім, так як до одного

порту комутатора можуть бути підключені пристрої, що належать до різних VLAN. Крім того, переміщення комп'ютерів з одного порту комутатора на інший відслідковуються комутатором автоматично і дозволяють зберегти приналежність переміщеного комп'ютера до певної VLAN без втручання адміністратора. Діє це доволі просто: комутатор підтримує таблицю відповідності MAC-адрес комп'ютерів віртуальним мережам. Як тільки комп'ютер перемикається на інший порт комутатора, порівнюючи поле MAC-адреси відправника в заголовку першого переданого після переміщення комп'ютером кадру з даними своєї таблиці, комутатор робить правильний висновок про належність переміщення комп'ютера до VLAN.

VLAN на базі протоколів третього рівня. Даний спосіб рідко використовується в комутаторах рівня відділу і робочої групи. Він характерний для магістральних маршрутизируючих комутаторів, що мають вбудовані засоби маршрутизації основних протоколів ITC . Відповідно до цього способу, група портів комутатора, що належать до певної VLAN, асоціюється з певною підмережею IP або мережею IPX. Гнучкість тут забезпечується тим, що переміщення користувача на інший порт, що належить тій же VLAN, відстежується комутатором і не вимагає його переконфігурації. Перевагою даного способу є також простота конфігурації VLAN, яка може здійснюватися автоматично, оскільки комутатор аналізує мережеві адреси комп'ютерів, що співвідносить з кожної VLAN. До того ж, як уже згадувалося, що підтримують спосіб організації VLAN на базі протоколів третього рівня пристрої мають вбудовані засоби маршрутизації, що забезпечує можливість взаємодії між різними VLAN без використання додаткових засобів. Недолік у цього способу, мабуть, всього один - висока ціна комутаторів, в яких він реалізований.

2.7.4.1 Обґрунтування обраного методу створення віртуальних локальних мереж на базі MAC-адрес

VLAN на базі портів простий в налагодженні, але менш захищений в порівнянні з іншими способами створення віртуальних мереж.

VLAN на базі MAC-адрес визначається MAC адресою джерела. Комутатор підтримує таблицю MAC адрес і їх співвідношення з VLAN. Ключова перевага цього методу полягає в тому, що не потрібна переконфігурація комутатора при перепідключенні користувачів до різних портів. Спосіб потребує тих самих технічних характеристик комутатора що й попередній. Привласнення MAC адрес VLAN не буде завдавати значних часових затрат через невелику кількість робочих станцій. VLAN на базі MAC-адрес - це більш гнучкий спосіб організації VLAN в порівнянні з VLAN на базі портів, так як до одного порту комутатора можуть бути підключені пристрої, що належать до різних VLAN. Крім того, переміщення комп'ютерів з одного порту комутатора на інший зберігає приналежність переміщеного комп'ютера до певної VLAN без втручання адміністратора.

VLAN на базі протоколів третього рівня та VLAN теж мають свої переваги, але використовування їх на рівні відділу або робочої групи є нераціональним, та вимагає більших навичок від системного адміністратора, окрім того потребує більших технічних характеристик комутатора, ніж два попередні способи.

2.7.4.2 Впровадження обраного методу створення віртуальних локальних мереж на базі MAC-адрес

Пропонується об’єднати 5 робочих станцій співробітників економічного відділу, робочу станцію голови економічного відділу , робочу станцію секретаря в окрему віртуальну комп’ютерну мережу – VLAN2 та 2 робочі станції співробітників відділу кадрів і начальника відділу кадрів в віртуальну

комп'ютерну мережу – VLAN3 та робочу станцю системного адміністратора у VLAN4 як показано на рисунку (2.2).

В результаті чого VLAN2 має доступ до серверу та до VLAN4 , але не має доступу VLAN3.

VLAN3 також не зможе обмінюватися даними з VLAN2 але матиме доступ до серверу та VLAN4. В результаті чого відбудеться розмежування відділів, їх даних та зменшиться загальний широкомовний потік даних, звільниться смуга пропускання для потоку даних користувачів і знизиться загальна чутливість мережі до широкомовного потоку даних. Для сервера налаштовується тегований порт. Системному адміністратору через сервер доступні VLAN2 і VLAN3, тому у разі виникнення ускладнень роботи системи він зможе легко їх усунути.

Впровадження технології забезпечує більшу захищеність мережі порівняно з влаштованою на підприємстві та робить неможливим підключення до активного порту без дозволу в мережу і отримання таким способом доступу до всіх даних, що передаються по сегменту. Для реалізації технології потрібно придбати комутатор, який дозволяє обмінюватись данними на канальному рівні.

При реалізацій данної технології залишається така вразливість, як атака – «підміна MAC-адреси». Захист від атаки забезпечується організаційними заходами з використанням програмного забезпечення.

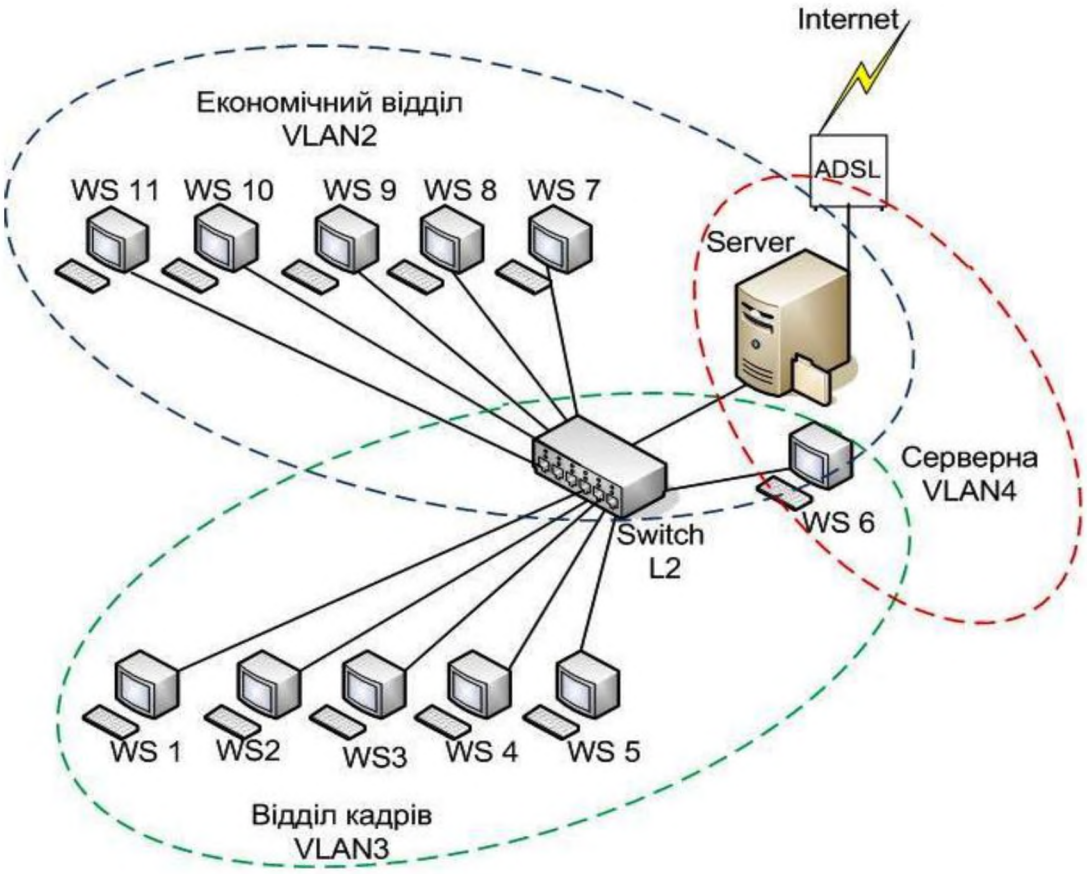


Рисунок 2.3 «Логічна структура створеної VLAN»

2.7.4.3 Обгрунтування обраного засобу реалізації технології VLAN

Для забезпечення критерій гарантій до середовища функціонування потрібно використовувати лише сертифіковані засоби. Замовником виставлені вимоги обмеженого бюджету.

Для реалізації VLAN обране мережеве обладнання: комутатор ZXR10 2920-SI призначений для роботи на рівні доступу в корпоративних або міських мережах, забезпечують захист інформації від НСД.

Відповідає вимогам НД з ТЗІ . Технічні вимоги за критеріями технічного захисту інформації", сукупність яких визначається функціональним профілем: КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДВ-1, НР-1, НИ-1, НИ-2, НК-1, НО-2, НЦ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99[6].

КА-1 - мінімальна адміністративна конфіденційність;

КА-2 - базова адміністративна конфіденційність;

ЦА-1 - мінімальна адміністративна цілісність;

ЦА-2 - базова адміністративна цілісність;

ДР-1 - квоти;

ДВ-1 - ручне відновлення;

НР-1 - реєстрація;

НИ-1 - зовнішня ідентифікація і автентифікація;

НИ-2 - одиночна ідентифікація і автентифікація;

НК-1 - однонаправлений достовірний канал;

НО-2 - виділення адміністратора;

НЦ-1 - КЗЗ з контролем цілісності.

Технічні характеристики засобу приведені в додатку З.

В таблиці 2.12 приведені реалізовані послуги профілю захищеності.

Таблиця 2.12 – Реалізовані послуги профілю захищеності в ІТС після розробки підсистеми захисту

Критерії	Вимоги до рівнів послуг безпеки	З допомогою чого реалізовані
	1	2
Конфіденційності	КД-2 (базова довірча конфіденційність)	Організаційними заходами з використанням ОС Microsoft Windows 10 Professional, DeviceLock DLP Suite 9.x
	КА-2 (Базова адміністративна	Організаційними заходами з використанням технології VLAN,

конфіденційність)	DeviceLock DLP Suite 9.x, антивірус ESET NOD32 14.1
КО-1 (повторне використання об'єктів)	ОС Microsoft Windows 10 Professional
КВ-1(мінімальна конфіденційність при обміні)	Організаційними заходами з використанням ОС Microsoft Windows 10 Professional, Norton 360, DeviceLock DLP Suite 9.x

Продовження таблиці 2.12

	1	2
Цілісності	ЦД-1(мінімальна довірча цілісність)	Організаційними заходами з використанням ОС Microsoft Windows 10 Professional
	ЦА-2(базова адміністративна цілісність)	Організаційними заходами з використанням технології VLAN та DeviceLock DLP Suite 9.x
	ЦО-1(обмежений відкат)	ОС Microsoft Windows 10 Professional
	ЦВ-1(мінімальна цілісність при обміні)	Організаційними заходами з використанням ОС Microsoft Windows 10 Professional
	ДР-1 (квоти)	Організаційними заходами з використанням технології VLAN, ОС Microsoft Windows 10 Professional, DeviceLock DLP Suite 9.x
	ДВ-1 (ручне відновлення)	Всіма запропонованими програмними засобами та організаційно-технічними заходами

Продовження таблиці 2.12

Спостережності	НР-2 (захищений журнал)	ОС Microsoft Windows 10 Professional та DeviceLock DLP Suite 9.x
	НИ-2 (одиночна ідентифікація і автентифікація)	Організаційними заходами з використанням технології VLAN та ОС Microsoft Windows 10 Professional
	НК-1 (однонаправлений достовірний канал)	Організаційними заходами з використанням технології VLAN та ОС Microsoft Windows 10 Professional
	НО-2 (розподіл обов'язків адміністраторів)	Організаційними заходами з використанням технології VLAN, ОС Microsoft Windows 10 Professional та DeviceLock DLP Suite 9.x
	НЦ-2 (КЗЗ з гарантованою цілісністю)	ОС Microsoft Windows 10 Professional
	НТ-2 (самотестування при старті)	ОС Microsoft Windows 10 Professional та антивірус ESET NOD32 14.1
	НВ-1(автентифікація вузла)	Організаційними заходами з використанням ОС Microsoft Windows 10 Professional, Norton 360, DeviceLock DLP Suite 9.x

Також на етапі розробки підсистеми захисту реалізуються критерії гарантій до середовища функціонування Г1 - конфігурація засобів, яка пропонується, є сертифікованою. Забезпечений захист КС від несанкціонованої модифікації. В таблиці 2.13 приведений описується за рахунок чого реалізується захист від загроз.

Таблиця 2.13 – Загрози та засоби, якими реалізований захист в ІТС

Загроза	З допомогою чого реалізований захист
Крадіжка технічних носіїв інформації	Організаційні заходи
Крадіжка інформації (несанкціоноване копіювання)	Технологія VLAN, ОС Microsoft Windows 10 Professional та DeviceLock DLP Suite 9.x
Крадіжка засобів доступу (ключі, паролі)	Організаційні заходи , ОС Microsoft Windows 10 Professional та DeviceLock DLP Suite 9.x
Підміна (модифікація):ПЗ, інформації , паролів	Організаційні заходи , ОС Microsoft Windows 10 Professional та DeviceLock DLP Suite 9.x, технологія VLAN
Знищення (руйнування): технічних засобів, носіїв ПЗ та інформації	Організаційні заходи
Порушення швидкості обробки інформації, пропускної здатності каналів зв'язку	Організаційні заходи, технологія VLAN, ОС Microsoft Windows 10 Professional та DeviceLock DLP Suite 9.x
Занесення вірусу на робочі станції, хакерські атаки	Norton 360, DeviceLock DLP Suite 9.x, антивірус ESET NOD32 14.1

Продовження таблиці 2.13

Перехоплення інформації : при підключенні до каналів передачі інформації	Організаційні заходи, технологія VLAN
Модифікація (зміна): з робочих станцій користувачів.	Організаційні заходи, технологія VLAN, ОС Microsoft Windows 10 Professional та DeviceLock DLP Suite 9.x
Недбале ставлення співробітників до технічних засобів обробки інформації.	Організаційні заходи

Висновок

В результаті прийняття запропонованого комплексу заходів щодо захисту інформації значно збільшиться рівень захищеності ІТС, зменшиться вірогідність реалізацій загроз, збільшиться зручність використання ІТС та обробки інформації. Усі запропоновані засоби підвищення рівня безпеки пройшли Державну експертизу та мають сертифікати. Розроблена системи забезпечує підвищення рівня захисту конфіденційності, цілісності й доступності оброблювальної інформації та відповідає послугам обраного стандартного функціонального профілю захищеності.

РОЗДІЛ 3. РОЗРАХУНКИ НА ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Вдосконалення системи захисту інформації в інформаційно-телекомунікаційній системі потребує обгрунтування економічної її доцільності, виходячи з аналізу витрат на розробку та впровадження. Тому метою економічного розділу є здійснення відповідних розрахунків, які дозволять встановити економічного ефекту від вдосконалення системи захисту інформації в інформаційно-телекомунікаційній системі.

3.1 Розрахунок (фіксованих) капітальних витрат

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

До капітальних витрат належать витрати на вдосконалення системи захисту інформації, які визначаються виходячи з трудомісткості вдосконалення системи захисту інформації.

Визначення трудомісткості вдосконалення системи захисту інформації

Трудомісткість вдосконалення системи захисту інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин,}$$

де $t_{тз}$ – тривалість складання технічного завдання на вдосконалення системи захисту інформації;

$t_{в}$ – тривалість розробки концепції вдосконалення безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення засобів вдосконалення системи захисту інформації.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій склала наступні величини:

$t_{тз}$=30 годин, $t_{в}$=50 годин, $t_{тз}$=25 годин, $t_{вз}$=23 годин, $t_{озб}$=12 годин, $t_{овр}$=9 годин, $t_{д}$=9 годин.

Отже, t=30+50+25+23+12+9+9= 158 годин,

Розрахунок витрат на вдосконалення системи захисту інформації Витрати на розробку вдосконалення системи захисту інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для вдосконалення системи захисту інформації Змч.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 41080 + 943,26 = 42023,26 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 158*260 = 41080 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для вдосконалення системи захисту інформації на ПК визначається за формулою:

$$З_{мч} = t*С_{мч}=158*5,97=943,26 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = 0,9 \cdot 3 \cdot 1,64 + \frac{3800 \cdot 0,4}{1920} + \frac{7200 \cdot 0,2}{1920} = 5,97 \text{ грн.}$$

Відповідно до розроблених рекомендації щодо удосконалення існуючої системи інформаційної безпеки мережі медичної установи «Сім'я», а також рекомендацій та інструкції по безпосередній роботі з системою планується використання антивірусу NOD32, який вже встановлений на комп'ютерах підприємства та потребує лише подовження ліцензії.

Серед апаратних засобів, які відповідно до розроблених рекомендації, необхідно придбати, належить комутатор ZXR10 2920-SI, який буде встановлений для захисту інформації в комп'ютерній мережі медичної установи «Сім'я». Вартість комутатора ZXR10 2920-SI складає 8910 грн.

Також планується придбання програмного забезпечення DeviceLock DLP Suite 9.x, вартість якого складає 7920 грн.

Також планується придбання програмного забезпечення ESET NOD32 14.1, вартість якого складає 296 грн. Оскільки до мережі підключено одинадцять комп'ютерів, то витрати на придбання програмного забезпечення ESET NOD32 14.1 становитимуть 3256 грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 20% відсотків від первісної вартості програмного забезпечення, тобто 4017,2 грн.

Таким чином, капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$

$= 42023,26 + 16830 + 3256 + 4017,2 = 66\ 126,46$ грн.

де $К_{пр}$ – вартість розробки проекту вдосконалення безпеки інформації у організації та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн.$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н$ = 5000 грн.).

$С_а$ - річні амортизаційні відрахування. Річні амортизаційні відрахування комутатора ZXR10 2920-SI, DeviceLock DLP Suite 9.x, а також програмного забезпечення ESET NOD32 14.1 вартістю 8910, 7920 та 3256 грн відповідно із корисним строком використання 2 роки, за прямолінійним методом нарахування амортизації складуть:

$$Са = (8910 + 7920 + 3256) / 2 = 10043$$

Вартість подовження ліцензії антивірусу ESET NOD32, який вже встановлений на 11 комп'ютерах підприємства, складає 335 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 14000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$$С_з = 14000*12 + 14000*12*0,1= 184800 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2019 р. складає 22%.

$$С_{єв} = 184800*0,22 = 40656 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,2 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,2*1920*1,64 = 3778,56 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос = 66 126,46 *0,01= 661,26 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 5000+10043+335+184800+40656+3778,56+661,26 = 240779,82 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 240779,82 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

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

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 6 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 4 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 10 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 10000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 14000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 12 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 300 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 10.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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

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

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

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

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{14000 \cdot 12}{176} \cdot 6 = 5\,727{,}27 \quad \text{грн},$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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

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

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{14000 \cdot 12}{176} \cdot 10 = 9\,545{,}45 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{10000 \cdot 1}{176} \cdot 4 = 227{,}27 \text{ грн.}$$

$$П_в = 9545{,}45 + 227{,}27 = 9\ 772{,}72 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{300000}{2080} \cdot (6 + 4 + 10) = 2\ 884{,}61 \text{ грн.}$$

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

$$U = 5727{,}27 + 9\ 772{,}72 + 2\ 884{,}61 = 18\ 384{,}6 \text{ грн.}$$

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

$$B = \Sigma_i \Sigma_n U = \Sigma_1 \Sigma_{40} 18384{,}6 = 735\ 384 \text{ грн.}$$

3.2.2 Загальний ефект від вдосконалення системи захисту інформації

Загальний ефект від вдосконалення системи захисту інформації визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.,}$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (35%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 735384*0,35 - 240779,82 = 16604,58 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності вдосконалення системи інформаційної безпеки

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

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{16604,58}{66126,46} = 0,25, \quad \text{частки одиниці,}$$

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

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,25 > (18 – 11)/100 = 0,25 > 0,07.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,25} = 4, \text{ роки.}$$

3.4 Висновок

Вдосконалення системи захисту інформації в інформаційно-телекомунікаційній системі медичної установи «Сім'я» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 66 126,46 грн., експлуатаційні – 240779,82 грн. Величина річного економічного ефекту складає 16604,58 грн. Коефіцієнт повернення інвестицій ROSI складає 0,25 грн./грн.

ВИСНОВКИ

В кваліфікаційній роботі розроблено підсистему захисту для ОІД, яка являє собою комплекс заходів та засобів захисту направлений на окремий сегмент об'єкту інформаційної діяльності - інформаційно-телекомунікаційну систему.

Під час розробки підсистеми захисту був виконаний аналіз об'єкту інформаційної діяльності, визначено перелік інформації, що потребує захисту, розроблено модель загроз та визначено перелік порушників, ідентифіковані можливі канали витоку інформації.

Запропонована підсистема захисту інформації забезпечує умови функціонування середовища ІТС, при яких інформація обробляється тільки за визначеними правилами, які забезпечують безпосередній захист її об'єктів і суб'єктів та задовольняє послуги стандартного функціонального профілю захищеності:

3.КЦД.1 = { КД-2, КО-1, КВ-1,ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 } з критеріями гарантій до середовища функціонування Г1.

Проведене технічно-економічне обґрунтування вибору засобів забезпечення захисту інформації.

Вибір засобів забезпечення захисту інформації, яка циркулює в ІТС підприємства, здійснений з позиції комплексного підходу, тобто забезпечена одночасно протидія загрозам від можливого витоку інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1 Закон України "Про інформацію".

2 Закон України "Про державну таємницю".

3 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

4 НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу".

5 НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу".

6 НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

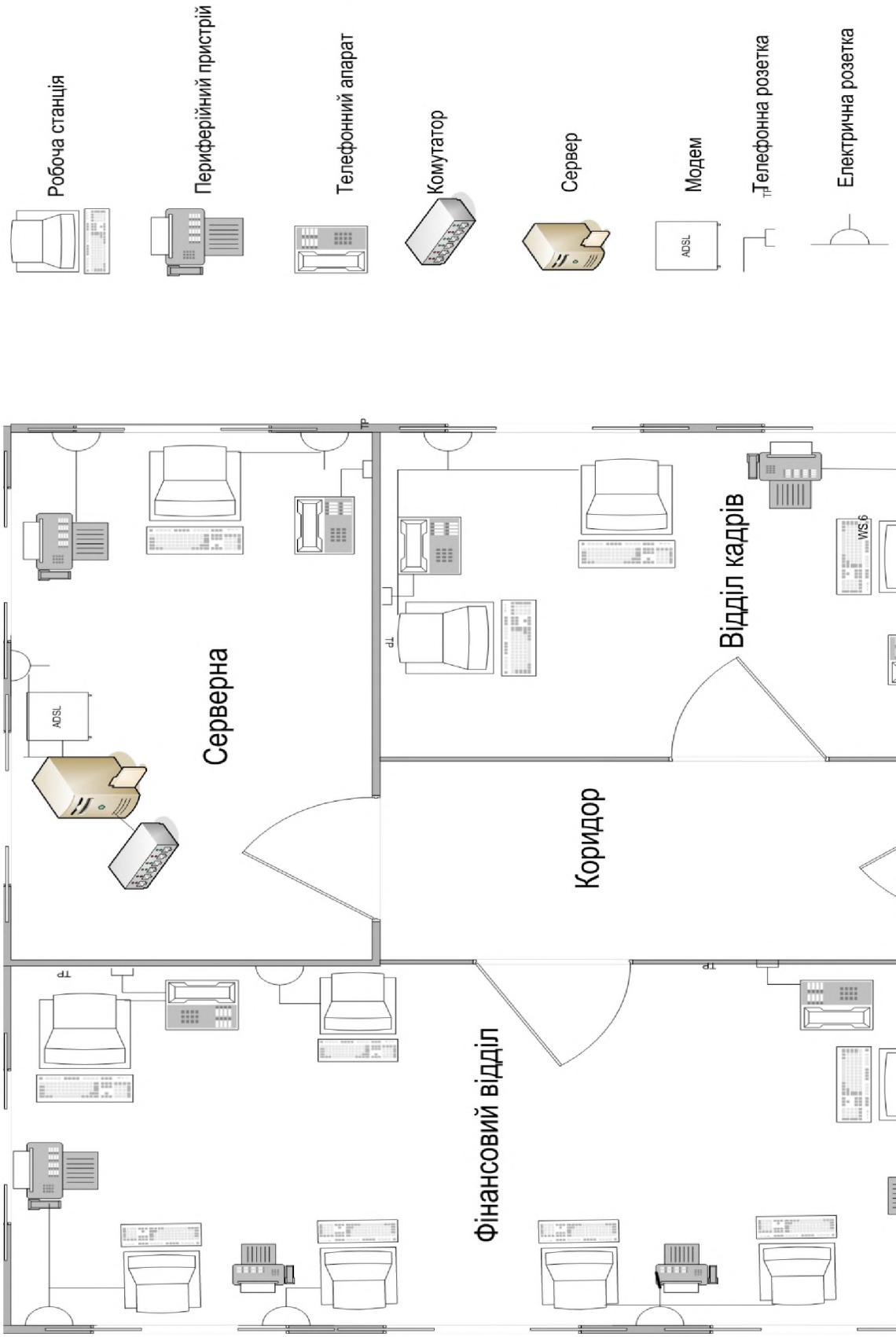
7 Документ "Державна експертиза за критеріями технічного захисту інформації програмних засобів захисту інформації. Технічні вимоги".

8 Міжнародний інформаційно-аналітичний центр Anti-Malware.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Позначення	Наименування	Кількість листів	Примітка
1	А4		Реферат	3	-
2	А4		Список умовних скорочень	2	-
3	А4		Зміст		-
4	А4		Вступ	2	-
5	А4		Стан питання. Постановка задачі		-
6	А4		Спеціальна частина		-
7	А4		Економічна частина		-
8	А4		Охорона праці		-
9	А4		Висновки	1	-
10	А4		Перелік посилань	1	-
11	А4		Додоток А	1	-
12	А4		Додаток Б	1	-
13	А4		Додаток В	4	-
14	А4		Додаток Г	1	-
15	А4		Додаток Д	1	-
16	А4		Додаток Е	1	-
17	А4		Додаток Ж	1	-
18	А4		Додаток І	3	-

ДОДАТОК Б. План комп’ютерного центру



ДОДАТОК В. Опис вірусів, які використовувались при тестуванні антивірусних засобів

Повне ім'я вірусу за класифікацією Лабораторії Касперського	Короткий опис
1	2
AdWare.Win32.Virtumonde.nmz	Троянська програма. Є бібліотекою. При інсталяції реєструє себе в системному реєстрі - Winlogon \ Notify, Explorer \ ShellExecuteHooks, Explorer \ Browser Helper Objects. Дані ключі постійно перевіряються і у разі відсутності - відновлюються. Бібліотека розташована в системному каталозі з довільним ім'ям. Файл постійно відкритий, що не дозволяє його видалити / переіменувати. Шкідливий код моніторить створення ключа відкладеного переміщення / переіменування і, в разі виявлення імені своєї бібліотеки в значенні параметра цього ключа, видаляє його.
Backdoor.Win32.NewRest.z	Троянська програма-спам-ботів. Є KernelMode руткітом. При інсталяції створює драйвер в каталозі Drivers з довільним ім'ям. Блокує доступ до свого файлу перехопленням обробників драйвера файлової системи, постійно перестворює свій файл. Блокує свій ключ реєстру від читання і видалення перехопленнями в ядрі.
Backdoor.Win32.Sinowal.fkp	Троянська програма-шпигун. При запуску модифікує головний завантажувальний запис (MBR) жорсткого диска з метою завантаження свого драйвера ще до старту ОС. Драйвер зберігається в непоміченій області диска. Перехоплює обробники драйвера, розташовується в стеку слідом за пристроєм \ Device \ Harddiskx \ DRx з метою блокування читання.

Продовження ДОДАТКА В

1	2
Email-Worm.Win32.Scano.ao	Поштовий черв. При інсталяції створює свою копію в \ WINDOWS \ csrss.exe і реєструє в системному реєстрі відладником explorer.exe (Image File Execution Options \ explorer.exe \ параметр - Debugger). Створює в системних процесах троянські потоки, які відновлюють файл і ключ автозавантаження в разі їх видалення. Якщо антивірус видаляє тіло віруса, але не видаляє ключ його автозавантаження, то при старті системи не завантажиться Explorer.exe, що не дозволить працювати з ПК.
Packed.Win32.TDSS.z	При інсталяції створює драйвер в \ WINDOWS \ system32 \ drivers з ім'ям aliserv3.sys і бібліотеку alil.dll в системному каталозі. Драйвер є фільтром драйвера файлової системи, чим і досягається маскування на диску. Блокує відкриття томів. Маскується в реєстрі перехопленнями в ядрі і в пам'яті. Блокує читання своїх файлів.
Packed.Win32.TDSS.z	Троянська програма. При інсталяції створює драйвер в \ WINDOWS \ system32 \ drivers \ gasfky *. Sys і дві dll в системному каталозі. Шкідлива програма маскується на диску, в реєстрі і пам'яті. Блокує відкриття диска, читання томів, перестворює свої ключі автозавантаження і файли в разі видалення. Знімає права доступу до своїх ключів. Переустановлює свої перехоплення в разі їх зняття.
Trojan.Win32.Srizbi.cb	Троянська програма. При інсталяції створює драйвер в \ WINDOWS \ system32 \ drivers з довільним ім'ям. Троян маскує свій ключ автозавантаження перехопленням функцій за допомогою модифікації машинного коду ядра, а так же маскує себе на диску перехопленням обробників драйвера файлової системи. Драйвер завантажується безпосередньо після ядра.

Продовження ДОДАТКА В

1	2
Rootkit.Win32.Podnuha.a	Троянська програма. При інсталяції створює драйвер в \ WINDOWS \ system32 \ drivers і бібліотеку в \ Windows \ system32 \ з довільним ім'ям. Dll зареєстрована з розширенням Winlogon (Winlogon \ Notify. Доступ до драйвера заблокований, так само як і можливість видаляти ключі автозавантаження в реєстрі. Бібліотека захищена від перейменування / видалення.
Rootkit.Win32.Pakes.zp	Троянська програма. Інсталює драйвер в \ WINDOWS \ system32 \ drivers з довільним ім'ям. Маскує себе на диску.
Rootkit.Win32.Protector.cd	Троянська програма-спамбот. При інсталяції створює драйвер в \ Windows \ system32 \ drivers \ Ati *. Sys. Драйвер блокує до себе доступ перехопленням обробників драйвера файлової системи і захищає свій ключ від видалення
Virus.Win32.Protector.b	Троянська програма-спамбот. При інсталяції заражає системний драйвер ndis.sys і маскується від виявлення, підсовуючи при читанні зараженого файлу оригінальний його вміст. Інфектор створює свою копію в системному каталозі з іменем reader_s.exe, прописується в ключі Run, інжектується в створюваний процес svchost для розсилки спаму.
Trojan.Win32.Agent.xlg	Троянська програма. Є бібліотекою - \ documents and settings \ all users \ Documents \ settings \ abc32.dll, відкрита з монопольним доступом. Має атрибут "прихований" разом з каталогом в якому знаходиться. Бібліотека зареєстрована для автоматичного запуску в системному реєстрі, права на читання залишає тільки у групи System. У разі видалення ключа автозавантаження, моментально перестворює його.

Продовження ДОДАТКА В

1	2
Trojan-Spy.Win32.Zbot.gen	Троянська програма-шпигун. Перехоплює безліч функцій в UserMode з метою маскування і шпигунства. При інсталяції створює файл sdra64.exe в системному каталозі і реєструє в реєстрі (Winlogon \ параметр Userinit), з метою завантаження його при кожному старті системи. У разі видалення шляху до свого файлу в значенні параметра Userinit, він тут же дописує шлях до себе (відновлює свій ключ автозавантаження). Троян блокує доступ до себе монопольним відкриттям і маскується на диску.
Trojan-PSW.Win32.Ambera.n	Троянська програма-шпигун. При запуску створює файл xas32.dll в системній директорії і реєструє його в реєстрі для автоматичного завантаження. У разі відсутності файлу xas32.dll (видалення його антивірусом), але наявності ключів Winsock - буде відсутній доступ до Інтернету.
Trojan.Win32.Small.yc	Троянська програма. При інсталяції створює base * 32.dll (* - довільні символи) в системному каталозі і змінює значення параметра Windows в Session Manager \ SubSystems таким чином, щоб csrss.exe завантажував dll шкідливої програми, а не системну basesrv.dll. Якщо в ході лікування системи видаляється файл шкідливої програми, а ключ windows не відновлюється в первісний стан, то система буде постійно падати при завантаженні. Завантаження з останньої вдалої конфігурації не допоможе зробити систему робочою, тому що шкідлива програма змінює параметр Windows.
Trojan.Win32.Cosmu.cyq	Троянська програма. При інсталяції заражає системний порт або міні-порт драйвер (наприклад, atapi.sys) таким чином, що його розмір не змінюється і дозволяє завантажити в пам'ять драйвер, розташований в останніх секторах жорсткого диска на віртуальній файловій системі.

ДОДАТОК Г. Результати тестування Avast Antivirus

Назва вірусу	Вердикт	Подробиці
AdWare.Virtumonde (Vundo)	+	Залишилися ключі автозапуску в реєстрі.
Rustock (NewRest)	-	Детектує наявність , але нічого не може зробити.
Sinowal (Mebroot)	-	Детектує наявність, але нічого не може зробити.
Email-Worm.Scano (Areses)	-	Файл видалений, але при старті системи зникає робочий стіл (не вилучений ключ автозапуску)
TDL (TDSS, Alureon, Tidserv)	-	Наявність трояна не виявлено.
TDL2 (TDSS, Alureon, Tidserv)	-	Детектує бібліотеку. Драйвер не виявлений.
Srizbi	-	Наявність трояна не виявлено.
Rootkit.Podnuha (Boaxxe)	-	Детектує бібліотеку, але не може з нею нічого зробити. Драйвер не виявлений.
Rootkit.Pakes (synsenddrv)	+	Залишився ключ автозавантаження.
Rootkit.Protector (Cutwail, Pandex)	-	Наявність трояна не виявлено.
Virus.Protector (Kobcka, Neprodoor)	-	Виявляє і видаляє інфектора. Заражений драйвер не виявлений.
Xorpix (Eterok)	+	Залишився ключ автозавантаження.
Trojan-Spy.Zbot	+	Залишився ключ автозавантаження.
Win32/Glaze	-	Файл видалений. Пропав доступ в Інтернет.
SubSys (Trojan.Okuks)	-	Систему неможливо завантажити.
TDL3 (TDSS, Alureon, Tidserv)	-	Детектує наявність, але нічого не може зробити.

ДОДАТОК Д. Результати тестування Microsoft Defender

Назва вірусу	Вердикт	Подробиці
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	+	+
Sinowal (Mebroot)	-	Перезавантаження системи при запуску сканера.
Email-Worm.Scano (Areses)	+	+
TDL (TDSS, Alureon, Tidserv)	+	+
TDL2 (TDSS, Alureon, Tidserv)	-	Не дозволяє запустити власні компоненти.
Srizbi	+	+
Rootkit.Podnuha (Boaxxe)	+	+
Rootkit.Pakes (synsenddrv)	+	+
Rootkit.Protector (Cutwail, Pandex)	+	+
Virus.Protector (Kobcka, Neprodoor)	+	+
Xorpix (Eterok)	+	+
Trojan-Spy.Zbot	+	+
Win32/Glaze	-	Файл видалений. Пропав доступ в Інтернет.
SubSys (Trojan.Okuks)	+	+
TDL3 (TDSS, Alureon, Tidserv)	+	+

ДОДАТОК Е. Результати тестування : ESET NOD32

Назва вірусу	Вердикт	Подробиці
AdWare.Virtumonde (Vundo)	+	+
Rustock (NewRest)	-	Після установки продукт не працює.
Sinowal (Mebroot)	-	Постійно падає процес антивіруса.
Email-Worm.Scano (Areses)	-	Зависає при виявленні.
TDL (TDSS, Alureon, Tidserv)	+	+
TDL2 (TDSS, Alureon, Tidserv)	+	+
Srizbi	+	+
Rootkit.Podnuha (Boaxxe)	+	+
Rootkit.Pakes (synsenddrv)	+	+
Rootkit.Protector (Cutwail, Pandex)	+	+
Virus.Protector (Kobcka, Neprodoor)	+	+
Xorpix (Eterok)	+	+
Trojan-Spy.Zbot	+	+
Win32/Glaze	+	+
SubSys (Trojan.Okuks)	+	+
TDL3 (TDSS, Alureon, Tidserv)	+	+

ДОДАТОК Ж. Результати лікування активного зараження різними антивірусними продуктами

Шкідливе ПЗ	Microsoft Defender	Avast Antivirus	ESET NOD32
AdWare.Virtumonde (Vundo)	+	+	+
Rustock (NewRest)	+	-	-
Sinowal (Mebroot)	-	-	-
Email-Worm.Scano (Areses)	+	-	-
TDL (TDSS, Alureon, Tidserv)	+	-	+
TDL2 (TDSS, Alureon, Tidserv)	-	-	+
Srizbi	+	-	+
Rootkit.Podnuha (Boaxxe)	+	-	+
Rootkit.Pakes (synsenddrv)	+	+	+
Rootkit.Protector (Cutwail, Pandex)	+	-	+
Virus.Protector (Kobcka, Neprodoor)	+	-	+
Xorpix (Eterok)	+	+	+
Trojan-Spy.Zbot	+	+	+
Win32/Glaze	-	-	+
SubSys (Trojan.Okuks)	+		+
TDL3 (TDSS, Alureon, Tidserv)	+	-	+
Вилыкувано/Всього	13/16	4/16	13/16
+	антивірус успішно усунув активне зараження, працездатність системи відновлена (не порушена).		

ДОДАТОК І. Технічні характеристики комутатора ZXR10 2920-SI

Інтерфейси 16 ;

Фіксований оптичний інтерфейс 24;

Число розширюваних слотів 1;

Типи розширюваних плат 2-портова субплата електричного інтерфейсу GE2-портова субплата оптичного інтерфейсу (SFP) 1 порт електричного і 1 порт оптичного інтерфейсу ;

Інтерфейс SFP / LC: 500 м;

Ємність комутації 32 Гбіт / с;

Швидкість пересилання пакетів 8.3 млн.пак. / С;

Підтримуються стек протоколів IEEE 802.3;

Підтримуються STP, RSTP і MSTP;

Підтримується LACP;

Підтримується 802.1Q VLAN;

Підтримується SVLAN;

Підтримується IGMP Snooping, IGMP Filter;

Підтримується керована багатоадресна передача;

Підтримується QOS;

Підтримується аутентифікація через сервер Radius;

Підтримується фільтрація MAC-адрес;

Підтримується прив'язка MAC-адрес;

Підтримується обмеження широкомовних, багатоадресних і одноадресних пакетів;

Підтримується обмеження по швидкості порту;

Підтримується фільтрація та обмеження по швидкості потоку на базі сервісних потоків, P2P, відеотрафік;

Підтримується накладення на швидкості каналу;

Підтримується ZESR ;

Підтримується захист ЦП і захист від DDOS-атак;

Підтримуються функції безпеки з використанням ACL;

Інтерфейс локального управління Консоль RS232;

Підтримується інтерфейс CLI;

Підтримується дистанційне керування через Telnet;

Підтримується стандартний SNMP;

Підтримується ZXNM01;

Підтримується ZGMP (CLI, GUI);

Підтримується SSHv2.0;

Підтримується локальна та віддалена автентифікація;

Power consumption (max.) Не більше 19 Вт Не більше 20 Вт Не більше 27 Вт Не більше 27 Вт ;

Вимоги до навколишнього середовища;

Робоча температура Від -5 до +45 ° С;

Температура зберігання Від -40 до +70 ° С;

Відносна вологість при зберіганні Від 5 до 95% без конденсату ;

Сейсмостійкість До 8 балів за шкалою Ріхтера;

Надійність Середній час напрацювання на відмову не менше 50000 годин;

Середній час відновлення не більше 30 хв.

ДОДАТОК К. Перелік документів на оптичному носії

1 Титульний аркуш.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Додаток Д.doc

17 Додаток Е.doc

18 Додаток Ж.doc

19 Додаток І.doc

20 Додаток К.doc

21 Додаток Л.doc

22 Додаток М.doc

Презентація.pptx

ДОДАТОК Л. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК М. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:

Вдосконалення системи захисту інформації в інформаційно-телекомунікаційній системі медичної установи «Сім'я»

Павлової Валерії Олександрівни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатка.

Мета роботи: за допомогою програмних, апаратних і організаційних заходів поліпшити захищеність інформації в комп'ютерній мережі медичної установи «Сім'я» від несанкціонованого доступу.

У розділі Огляд каналів витоку інформації, впливу загроз на ОІД, опис ОІД описані найпоширеніші загрози безпеки та основні положення захисту інформації від них.

У розділі Аналіз та впровадження засобів захисту інформації для вдосконалення системи захисту описана коротка характеристика об'єкту інформаційної діяльності медичної установи «Сім'я», розроблені й описані методи підвищення захисту інформації від несанкціонованого доступу.

В економічному розділі наведені розрахунки й обґрунтовані всі заходи щодо вдосконалення системи захисту інформації в комп'ютерній мережі медичної установи «Сім'я».

Студентка показала достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник

Р Е Ц Е Н З І Я

на кваліфікаційну роботу бакалавра на тему:
Вдосконалення системи захисту інформації в інформаційно-телекомунікаційній системі медичної установи «Сім'я»
Павлової Валерії Олександрівни

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на ___ сторінках, та містить ___ рисунків, __ таблиць, __ джерел і __ додатків.

Мета роботи: за допомогою програмних, апаратних і організаційних заходів поліпшити захищеність інформації в комп'ютерній мережі медичної установи «Сім'я» від несанкціонованого доступу.

У розділі Огляд шляхів витоку інформації, впливу загроз на ОІД, опис ОІД описані найпоширеніші загрози безпеки та основні положення захисту інформації від них.

У розділі Аналіз та впровадження засобів захисту інформації для вдосконалення системи захисту описана кратка характеристика об'єкту інформаційної діяльності медичної установи «Сім'я», розроблені й описані методи підвищення захисту інформації від несанкціонованого доступу.

Практичне значення роботи полягає в підвищенні рівня інформаційної безпеки мережі шляхом програмних, апаратних і організаційних заходів.

Зміст та структура роботи дозволяють розкрити поставлену тему повністю.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота виконана у відповідності до вимог, які пред'являються до кваліфікаційної роботи бакалавра і заслуговує оцінки "_____".

Рецензент