Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)
Навчально-науковий інститут інформаційних технологій та робототехніки
(повна назва інституту)
Кафедра комп'ютерних та інформаційних технологій і систем
(повна назва кафедри)

Пояснювальна записка
до дипломного проекту (роботи)
магістра
(рівень вищої освіти)
на тему

Розробка автоматизованої системи кіберзахисту на підприємстві

Виконав: студент II курсу, групи 602-ТН
спеціальності
122 Комп'ютерні науки
(шифр і назва спеціальності)
Масліченко С.В.
(прізвище та ініціали)
Керівник _д.т.н, професор Ляхов О.Л._
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)

Полтава – 2025 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

НАВЧАЛЬНО НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА РОБОТОТЕХНІКИ

КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

спеціальність 122 «Комп'ютерні

науки» на тему

«Розробка автоматизованої системи кіберзахисту на підприємстві»

Студент групи 602-ТН Масліченко Станіслав Валерійович

Керівник роботи
д.т.н, професор
Ляхов О.Л.

Консультант
к.т.н., доцент Головко
Г.В.

Завідувач кафедри
кандидат фізико-
математичних наук,
Двірна О.А.

Полтава – 2025

РЕФЕРАТ

Захист інформаційних систем та мереж у сучасному світі визначається кількома важливими аспектами. По-перше, стрімкий розвиток комп'ютерних та телекомунікаційних технологій. По-друге, постійне розширення сфери використання комп'ютерів і збільшення обсягів даних, що захищаються різними системами управління. По-третє, зростаюча інтеграція людей і організацій в процес інформаційної взаємодії і, як наслідок, підвищення вимог до обміну та зберігання інформації. Важливу роль у цьому контексті відіграють ринкові тенденції, які розглядають інформацію як економічний ресурс і товар, а також перехід до конкурентних відносин у багатьох сферах діяльності.

У цьому контексті особливого значення набуває захист комп'ютерних систем та інформаційного середовища від несанкціонованого доступу, крадіжок, зловмисного знищення та інших шкідливих дій. Комплексний підхід до вирішення цих питань стає пріоритетним для забезпечення інформаційної безпеки в сучасних умовах. Оцінка спектру існуючих загроз показує, що найбільшу небезпеку становлять технічні шляхи витоку даних.

Завдання захисту залежить від поставленої мети, чи то забезпечення національної безпеки, чи то захист інтересів окремих організацій, компаній або приватних осіб. Важливим інструментом у цій роботі є диференціація інформації за рівнем її конфіденційності та вразливості. В рамках магістерської кваліфікаційної роботи було проаналізовано впровадження заходів кібербезпеки на прикладі будівельної компанії. В ході роботи були розроблені рекомендації щодо вдосконалення систем інформаційної безпеки під час передачі даних та повідомлень. Крім того, було створено програмний додаток, що гарантує безпечну передачу інформації з використанням алгоритму шифрування RSA та одноалфавітної заміни. Програмний продукт був розроблений з використанням мови програмування C# та технології Windows Presentation Foundation для створення інтерфейсу користувача. Результатом стала програмна система, яка повністю відповідала технічним вимогам і була готова до практичного використання.

ABSTRACT

The protection of information systems and networks in the modern world is determined by several important aspects. First, the rapid development of computer and telecommunications technologies. Second, the constant expansion of the scope of computer use and the increase in the volume of data protected by various management systems. Third, the growing integration of people and organizations into the process of information interaction and, as a result, increasing requirements for the exchange and storage of information. An important role in this context is played by market trends that consider information as an economic resource and commodity, as well as the transition to competitive relations in many areas of activity.

In this context, the protection of computer systems and the information environment from unauthorized access, theft, malicious destruction and other harmful actions is of particular importance. An integrated approach to addressing these issues is becoming a priority for ensuring information security in modern conditions. An assessment of the spectrum of existing threats shows that the greatest danger is posed by technical ways of data leakage.

The task of protection depends on the goal set, whether it is ensuring national security or protecting the interests of individual organizations, companies or individuals. An important tool in this work is the differentiation of information according to its level of confidentiality and vulnerability. As part of the master's qualification work, the implementation of cybersecurity measures was analyzed using the example of a construction company. During the work, recommendations were developed for improving information security systems during data and message transmission. In addition, a software application was created that guarantees secure information transmission using the RSA encryption algorithm and single-letter substitution. The software product was developed using the C# programming language and Windows Presentation Foundation technology to create a user interface. The result was a software system that fully met the technical requirements and was ready for practical use.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС – автоматизовані системи

ОС – операційна система

ПЗ – програмне забезпечення

DES – симетричний алгоритм шифрування

IDEA – симетричний блоковий алгоритм шифрування даних

ВСТУП

Поняття інформації є одним із фундаментальних концептів сучасної науки, яке має ключове значення для різних дисциплін. Як первинна категорія, інформація не піддається однозначному науковому визначенню, оскільки є багатовимірним і філософськи складним явищем. У загальному розумінні під інформацією слід розуміти будь-які відомості або дані, що зберігаються на матеріальному носії чи представлені в електронному форматі. Незважаючи на її концептуальну невизначеність, інформація має вирішальне значення для людської діяльності, зокрема як основа для ухвалення обґрунтованих рішень у різноманітних життєвих і професійних ситуаціях.

Інформаційна безпека - це стан, у якому підтримуються характеристики інформації, визначені політикою безпеки. Як стандартні моделі безпеки часто наводять три категорії

- конфіденційність - стан інформації, доступ до якої можуть отримати тільки особи, які мають права доступу;

- цілісність - недопущення несанкціонованої модифікації інформації;

- доступність - недопущення тимчасового або постійного приховування інформації від користувачів, які отримали права доступу.

Кібербезпека - це сукупність засобів, процесів, практик і технологічних рішень для захисту критично важливих компютерних систем і данихінформаційних ресурсів від несанкціонованого доступу. Ефективна програма знижує ризик переривання бізнесу через атаки.

Кібератака - це спроба здійснити кіберзагрозу, тобто будь-яка ситуація або подія, що може призвести до порушення політики інформаційної безпеки та/або пошкодження автоматизованих систем. Українське законодавство визначає це поняття наступним чином: «Кібератака - це спрямовані (умисні) дії в кіберпросторі, що здійснюються з використанням електронних комунікацій (у тому числі інформаційно-комунікаційних технологій, програмних, програмно-

апаратних та інших технічних і технологічних засобів та обладнання), спрямовані на досягнення однієї або сукупності наведених нижче цілей.

Модель безпеки також включає [1], крім цього, - non-repudiation - неспростування автора; - accountability - забезпечення ідентифікації суб'єкта доступу та реєстрації його дій; - authenticity - відповідність передбачуваній операції або результату; - authenticity або genuineness - відповідність суб'єкта або ресурсу заявленому.

Є категорії, які не обов'язково мають бути ключовими, наприклад, природа, що запевняє в автентичності суб'єкта чи ресурсу відповідно до заявленого. Інформаційний захист являє собою сукупність організаційних, технічних заходів та правових механізмів, спрямованих на запобігання порушенню прав та інтересів власників інформації.

Політика безпеки – набір законів, правил, обмежень, яке регламентує порядок обробки інформації спрямований на захист інформації від певних загроз [2].

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

1.1 Аналіз проблеми захисту інформації

Актуальність питань, пов'язаних із захистом інформаційних технологій у сучасному світі, зумовлена кількома ключовими факторами. По-перше, стрімким розвитком комп'ютерної та телекомунікаційної техніки. По-друге, невпинним розширенням сфер застосування комп'ютерів і зростанням кількості захищених даних у різних системах управління. По-третє, дедалі ширшою інтеграцією людей та організацій у процеси інформаційної взаємодії, що супроводжується еволюцією їхніх інформаційних потреб. Крім того, важливу роль відіграє ринковий підхід до інформації як до товару, а також перехід до ринкових відносин і природної конкуренції.

У зв'язку з цим набуває особливої ваги необхідність захисту комп'ютерних систем та інформації від несанкціонованого доступу, крадіжок, знищення та інших злочинних і небажаних дій [3].

Розвиток кібербезпеки ґрунтується на найновіших наукових, технічних та технологічних досягненнях. У зв’язку з цим заходи, а саме засоби технічного захисту інформації (ТЗІ), мають створюватися з урахуванням сучасних умов та викликів. Загалом, розробка і виробництво ТЗІ, а також удосконалення методів і підходів до їх використання є вкрай складними, наукомісткими і багатогранними процесами. Це створює необхідність зосередження наукового та інженерного потенціалу на вирішенні таких ключових завдань [5]:

1. Дослідження перспектив і шляхів розвитку технічної розвідки у контексті інформаційної невизначеності та викликів, пов’язаних із нею.

2. Виявлення, аналіз і оцінка змісту інформації за умов можливих комбінацій технічних каналів, що можуть стати причиною витоку даних.

3. Забезпечення захисту інформації, її безпечної обробки, а також оцінка рівня захищеності.

4. Розробка та виробництво національних технічних засобів для ефективного захисту інформації.

Таким чином, комплексний підхід до цих проблем є необхідною умовою забезпечення інформаційної безпеки в сучасному світі. Розглядаючи весь спектр загроз, можна дійти висновку, що найсерйознішу небезпеку зазвичай становлять технічні канали витоку інформації. Найбільш уразливими категоріями тут є голосова інформація, дані, що передаються через інформаційно-комунікаційні системи, а також інформація, що циркулює в автоматизованих системах управління. Завдання захисту різняться залежно від мети: від гарантування національної безпеки до охорони інтересів конкретних організацій, компаній чи окремих осіб, зокрема через диференціацію інформації за рівнем її чутливості та вразливості. [1]

1.2 Постановка задачі

У магістерській кваліфікаційній роботі потрібно спроектувати систему програмного захисту інформаціїї на базі підприємства «Компанія ГОТ» та захистити інформацію від кібератак.

1.2.1 Мета дослідження захисту інформації полягає в тому, що на сьогодні загальновизнаним є той факт, що ефективне функціонування підприємства значною мірою залежить від забезпечення належного захисту інформації від несанкціонованого доступу, особливо з боку співробітників, які не мають відповідних повноважень для роботи з нею. Саме тому питання інформаційної безпеки в організаціях набуває дедалі більшої актуальності та поширення. Основною метою такого захисту є розробка комплексної системи інформаційної безпеки, яка включає як технологічні засоби захисту інформації, так і механізми безпечної передачі даних і повідомлень.

1.2.2 Цілі захисту інформації в підприємства « Компанія ГОТ»:

1. Конфіденційнісь інформації (олбмеження доступу до інформації лише тому користувачу, хто має право).

2. Аутетифікація об'єкта, тобто «підтвердження того, що об'єкт, бере участь у взаємнодії, є тим, хто має відповідне право» [7].

3. Управління доступом до ресурсів тобто «У захисті від неавторизованого використання ресурсу» [7].

1.3 Захист інформраційних ресурсів. Законодавча база України

Зростання рівня загроз для інформаційних ресурсів, зумовлене лібералізацією суспільних і міждержавних відносин, активним використанням технічних засобів для обробки даних та засобів зв’язку іноземного виробництва, а також поширенням технологій несанкціонованого доступу до інформації та можливості впливу на неї, вимагає реалізації стратегічних заходів. Зокрема, необхідним є проведення науково-технічних досліджень, розробка відповідних регуляторних документів, а також впровадження комплексної системи технічного захисту інформації для забезпечення її безпеки в сучасному інформаційному середовищі.

Станом на сьогодні правова основа для забезпечення технічного захисту інформації (ТЗІ) включає Концепцію національної безпеки України, закони України, зокрема «Про інформацію», «Про державну таємницю», «Про захист інформації в автоматизованих системах», а також інші нормативно-правові акти та міжнародні угоди, що визначають інформаційні відносини [8].

Не зважаючи на певні позитивні зміни у сфері захисту інфрмації, слід відзначити, що нинішнє законодавство України, хоча й включає прогресивні на час прийняття норми, зокрема положення Закону України «Про інформацію», лише частково відповідає сучасним вимогам розвитку інформаційних відносин. Відсутність необхідного оновлення створює перешкоди для ефективного розв’язання нагальних питань, зокрема щодо захисту персональних даних,

регулювання доступу до інформації для службового користування та інших складних аспектів.

Більшість чинних інформаційних нормативно-правових актів було прийнято ще до того, як Конституція України набула юридичної сили. Це створює необхідність їх перегляду та адаптації до нових конституційних вимог. Недоліки в системі правового регулювання негативно позначаються на формуванні цивілізованих інформаційних відносин і гальмують процес забезпечення державної інформаційної безпеки.

Як уже зазначалося, питання правового забезпечення інформаційної безпеки залишається недостатньо врегульованим, якщо не враховувати аспекти, що стосуються державної таємниці. Щодо решти категорій інформації нормативно-правова база здебільшого обмежується загальними та декларативними нормами. Водночас навіть такі ключові положення, як регулювання й захист таємної інформації, що не вважається державною таємницею, залишаються невизначеними. Це стосується також особливостей правового захисту відкритої інформації, персональних даних, комерційної таємниці й інших видів конфіденційної інформації, які потребують чіткого і сучасного регулювання.

Уведений і дію у жовтні 1992 року Закон України “Про інформацію” [3] заклав правові основи інформаційної безпеки і, в першу чергу, хоч і не в достатній мірі та не завжди виразно, основи законодавства про захист інформації з обмеженим доступом, яка за своїм правовим режимом поділяється на кон-фіденційну та таємну (ст. 30). На сьогодні існуюча нормативно-правова база не дає чіткого поняття «іншої передбаченої законом таємниці» професійного, ді-лового, виробничого, банківського, комерційного та іншого характеру”. Цей перелік можна продовжити (тільки в Законах України згадується близько 20 подібних термінів) [4].

В Україні було прийнято низку нормативно-правових актів і розпорядчих документів, що регламентують процедури поводженння з інформацією, у тому числі і з її захистом [3, 4, 5]:

«Стаття 10 Закону України «Про захист інформації в інформаційно–телекомунікаційних системах». Забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно – телекомунікаційних системах» - [3].

«Стаття 11 Закону України «Встановлення вимог і правил по захисту інформації». Вимоги і правила по захисту інформації, що є власністю держави, або інформації, захист якої гарантується державою, установлюються державним органом, уповноваженим Кабінетом Міністрів України. Ці вимоги і правила є обов'язковими для власників АС, де така інформація опрацьовується, і носить рекомендаційний характер для інших суб'єктів права власності на інформацію» - [3].

«Стаття 12 Закону України «Умови опрацювання інформації». Інформація, що є власністю держави або інформація, захист якої гарантується державою, повинна опрацьовуватися в АС, що має відповідний сертифікат (атестат) захищеності, у порядку, обумовленому уповноваженим Кабінетом Міністрів України органом» - [3].

У процесі сертифікації або атестації таких автоматизованих систем проводиться також перевірка і сертифікація створених засобів захисту інформації. Дані, що належать іншим суб'єктам, можуть оброблятися в зазначених автоматизованих систем за рішенням їхнього власника. При цьому власник інформації має право звернутися до органів сертифікації з проханням провести аналіз можливостей конкретної автоматизованої системи для забезпечення належного рівня захисту його інформації та отримати відповідні консультації.

«Стаття 13 Закону України «Політика в області захисту інформації». Політика в області захисту інформації в автоматизованих системах визначається Верховною Радою України» - [4].

«Стаття 14 Закону України «Державне керування захистом інформації в АС». Уповноважений Кабінетом Міністрів України орган здійснює керування захистом інформації шляхом: проведення єдиного технічної політики по захисту інформації; розробки концепції, вимог, нормативно – технічних документів і науково – методичних рекомендацій по захисті інформації в автоматизованих системах; ствердження порядку організації, функціонування і контролю за виконанням мір, спрямованих на захист оброблюваної в автоматизованих системах інформації, що є власністю держави, а також рекомендацій по захисті інформації власності юридичних і фізичних осіб; організації іспитів і сертифікації засобів захисту інформації в автоматизованих системах, у якій здійснюється опрацювання інформації, що є власністю держави; створення відповідних структур для захисту інформації в автоматизованих системах; проведення атестації сертифікаційних (іспитових) органів, центрів і лабораторій, видача ліцензії на право проведення сервісних робіт в області захисту інформації в автоматизованих системах здійснення контролю захищеності оброблюваної в автоматизованих системах інформації, що є власністю держави; визначення порядку доступу осіб і організацій закордонних держав до інформації в автоматизованих системах, що є власністю держави, або до інформації власності фізичних і юридичних осіб, щодо поширення і використання якої державою встановлені обмеження» - [7].

Міністерства, відомства й інші центральні органи державної влади забезпечують рішення питань захисту інформації в автоматизованих системах у межах своїх повноважень [8].

«Стаття 15 Закону України «Служби захисту інформації в АС». У державних заснуваннях і організаціях можуть створюватися підрозділи, служби, що організують роботу, пов'язану з захистом інформації, підтримкою рівня захисту інформації в АС, і відповідають за ефективність захисту інформації відповідно до вимог дійсного Закону» - [7].

«Стаття 20 Закону України «Забезпечення інформаційних прав України». Фізичні і юридичні особи в Україні на підставі Закону України "Про

інформацію" можуть встановлювати взаємозв'язок з АС інших держав із метою опрацювання, обміну, продажі, покупки відкритої інформації. Такі взаємозв'язки повинні виключати можливість несанкціонованого доступу з боку інших держав або їхніх представників резидентів України або осіб без громадянства до інформації, наявної в автоматизованих системах України, незалежно від форм власності і підпорядкування, у відношенні якої установлені вимоги нерозповсюдження її за межі України без спеціального дозволу.

Іноземні держави, а також фізичні та юридичні особи з-за кордону можуть володіти автоматизованими системами в Україні, інформацією, яка обробляється чи поширюється в таких системах, або створювати спільно з українськими компаніями чи громадянами підприємства для розробки автоматизованих систем, а також для обміну інформацією між системами України та інших країн. Окремі види цієї діяльності потребують наявності спеціального дозволу (ліцензії), виданого відповідним уповноваженим органом» - [9].

1.3.1 Закон України «Про інформацію» - це закон що закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності. Грунтуючись на Декларації про державний суверенітет України та Акті проголошення її незалежності, Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації [2].

Закон України «Про захист інформації в автоматизованих системах»

Метою цього Закону є встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації. Дія Закону поширюється на будь – яку інформацію, що обробляється в автоматизованих системах [2].

1.3.2 Закон України «Про державну таємницю»: Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.[3]

1.4 Загроза інформаційної безпеки

Загроза інформаційній безпеці охоплює ризики, пов'язані з викраденням, модифікацією або знищенням інформації. У найзагальніших випадках ці загрози можуть проявлятися наступним чином:

– дії зловмисників, спрямовані на спостереження за джерелами інформації;

– підслуховування конфіденційних розмов чи акустичних сигналів працюючих механізмів;

– перехоплення електричних, магнітних та електромагнітних полів, електричних сигналів або радіоактивного випромінювання;

– несанкціоноване поширення фізичних носіїв інформації за межі контрольованої території;

– умисне або ненавмисне розголошення секретної чи конфіденційної інформації особами, що мають до неї доступ;

– втрата носіїв інформації, включаючи документи, машиночитані носії чи матеріальні зразки;

– неконтрольоване поширення даних через випадкові електричні сигнали чи поля, що виникають у результаті старіння пристроїв, помилок у конструюванні або порушень правил експлуатації електронного чи радіоелектронного обладнання;

– стихійні явища, такі як пожежі чи затоплення під час аварій водопостачання та гасіння пожеж;

– технічні збої в роботі засобів збору, обробки, зберігання та передачі інформації через несправності обладнання або помилки користувачів чи технічного персоналу, впливу потужних електромагнітних і електричних промислових і природних завад.[4]

Усі ці фактори становлять серйозні виклики для забезпечення інформаційної безпеки та потребують ретельного контролю і управління ризиками.

Загрози інформаційній безпеці - це сукупність умов або чинників, що створюють небезпеку життєво важливим інтересам особи, суспільства і держави в інформаційному просторі. Основні загрози інформаційній безпеці можна поділити на три групи - загроза поширення неякісної інформації (недостовірної, неправдивої або дезінформації), що впливає на особу, суспільство та державу; - загроза несанкціонованого та протиправного впливу третіх осіб на інформацію та інформаційні ресурси (інформаційне виробництво, інформаційні ресурси, системи створення та використання інформації); - інформаційні права і свободи особи (право виробляти, передавати, шукати, одержувати, передавати та використовувати інформацію, право інтелектуальної власності та право на свободу вираження поглядів); - загрози правам і свободам особи на інформацію (право виробляти, передавати, шукати, одержувати, передавати та використовувати інформацію)[5].

1.5 Аспекти захисту та безпеки інформації

Щоб програма інформаційної безпеки була успішною, вона повинна охоплювати всю організацію. Програма інформаційної безпеки повинна включати посадові інструкції та обов'язки кожного учасника, визначення робочих процесів, методи аудиту та підтримки тощо. Основною метою розподілу обов'язків з інформаційної безпеки є інтеграція інформаційної

безпеки в бізнес-середовище. Одним із кроків у цій інтеграції є необхідність визначення посад для забезпечення безпеки всіх операцій.

Один з підходів полягає в тому, щоб розділити відповідальність і контроль над активами організації, наприклад, координуючи роботу всіх, включаючи тих, хто відповідає за інформацію, і тих, хто несе фінансову відповідальність. Такий підхід усуває невизначеність щодо того, хто за що і коли відповідає. Іншим аспектом дослідження є питання про те, як організовано управління безпекою в організації. Зазвичай організації мають основну групу управління інформаційною безпекою.

Ця основна група відповідає за впровадження та моніторинг виконання правил і процедур безпеки. У цьому розділі розглядається підхід, прийнятий для необмежених систем, де основна група управління інформаційною безпекою призначає адміністраторів безпеки для багатокористувацької системи з багатьма відділами. У таких випадках кожному бізнес-підрозділу призначається власний співробітник з безпеки або офіцер зв'язку, який допомагає у впровадженні програми безпеки цього бізнес-підрозділу. У такий спосіб співробітники служби безпеки можуть тісніше співпрацювати з користувачами. Це схоже на систему дільничних офіцерів поліції, які працюють у поліції.

Тісна співпраця між співробітниками служби безпеки та останньої також допомагає керувати спілкуванням зі сторонніми організаціями в режимі реального часу. Однак загрози безпеці походять не тільки від власних співробітників, а й від клієнтів, постачальників і будь-яких осіб, які мають можливість підключитися до інформаційних активів організації та порушити правила безпеки. Посередники мають відповідати за навчання вищезгаданих сторонніх осіб, контролювати та стимулювати їхню діяльність. Саме так працюють невеликі організації. Багато з них, особливо аутсорсингові, ділять свій невеликий штат на «відділи» і призначають одну людину відповідальною за зв'язок із безпекою. Однак це не найкраще рішення.

Деякі люди, які тривалий час працюють в організації, розуміються на тонкощах системи і можуть знайти спосіб використати її у своїх цілях. Єдиний спосіб запобігти цьому - не дозволяти співробітнику ставати посередником у забезпеченні безпеки протягом тривалого періоду часу, наприклад, протягом одного-двох років. Після закінчення цього терміну завдання має бути передано комусь іншому. Інший спосіб - встановити процедури перевірки та реєстрації. Ланцюжок поставок організації - це процес управління. Незважаючи на те що більшість закупівель проходить через етап затвердження керівництвом, найчастіше це затвердження є формальністю, і оплата здійснюється без додаткового повідомлення. Однак посередники в бухгалтерії відстежують порушення в процесі закупівлі та відвантаження замовлень. Один з аудиторів розповів про своє враження від своєї роботи, яку всі вважають дуже важкою.

Далеко не всі люди можуть впоратися з цією роботою. Аудитори повинні знати всі тонкощі бізнесу, відомості про клієнтів і постачальників, нові та старі правила оформлення документів і навіть рух грошових коштів організації. Тільки знаючи все це, аудитор може зрозуміти рахунки-фактури та замовлення на поставку і визначити, чи є в них порушення. Останній аспект, який необхідно враховувати під час реалізації програми інформаційної безпеки, - це цикл розроблення програмного забезпечення. Незалежно від того, чи було програмне забезпечення розроблено власними силами, чи підрядником, і незалежно від того, чи було придбано комерційний готовий програмний продукт (COTS - Commerce lOff-the-shelf), безпечна система, в якій легко можна виявити помилки та спроби вторгнення, має бути безпечною. Мета має полягати у створенні Крім того, можна запровадити стандарти кодування та тестування, щоб забезпечити високу якість виробничого процесу. Крім того, використання парадигми живучості може стати основою для розроблення програмного забезпечення, яке не буде створювати проблем під час розгортання або експлуатації.

1.6 Конкретні завдання інформаційної безпеки

Єдиний спосіб переконатися, що існуючі працівники, нові працівники та користувачі усвідомлюють, що безпека є частиною їхньої роботи, - це включити відповідні формулювання до посадових інструкцій. Визначення посадових обов'язків та вимог безпеки в посадових інструкціях може показати працівникам важливість інформаційної безпеки та допомогти їм усвідомити, що вона є невід'ємною частиною їхньої роботи. Коли ці обов'язки та вимоги включені до посадових інструкцій, до них ставляться з розумінням того, що вони впливають на професійну придатність працівника.

Сторонні підрядники, постачальники та інші особи, які надають послуги безпосередньо в мережі компанії, повинні використовувати подібні формулювання у своєму технічному завданні (ТЗ). Такі документи документують зобов'язання компанії, а також зобов'язання внутрішніх працівників, а також покладають на підрядників і постачальників відповідальність за дотримання вимог безпеки організації, оскільки вони використовуються для оцінки якості послуг, що надаються підрядниками та постачальниками.

1.7 Види загроз і атак та їх прояви

Загрози за своєю природою не проявляються самостійно. Вони реалізуються лише за наявності вразливостей — слабких місць, характерних для об'єкта, що підлягає інформатизації. Вразливість — це недолік або слабкість, яку можна використати для порушення функціонування інформаційної автоматизованої системи чи яка вже закладена в її структурі. Цю концепцію визначено у стандарті ДСТУ ISO 7498-2-99 «Інформаційна технологія. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Архітектура захисту інформації».

Під час аналізу інформаційної безпеки особливу увагу варто приділяти джерелам загроз, які можуть бути як суб’єктивними (пов’язаними з особами), так і об’єктивними (зовнішніми чинниками). Джерела поділяються на внутрішні або зовнішні залежно від їхнього розташування стосовно об’єкта інформатизації.

До джерел загроз можна віднести такі категорії, як:

1. «Антропогенні джерела» — дії суб’єктів, що можуть бути умисними або випадковими, але призводять до порушень, в тому числі злочинів.

2. «Техногенні джерела» — фактори, що пов’язані з технократичною діяльністю людини та розвитком цивілізації.

3. «Стихійні джерела» — природні катаклізми чи інші обставини, які важко або неможливо передбачити та запобігти їм із сучасним рівнем розвитку науки і технологій.

Незважаючи на різноманіття загроз, найбільшої шкоди інформаційним системам завдають неправомірні дії працівників організацій та комп’ютерні віруси. За даними американських дослідників, до 85% випадків промислового шпигунства здійснюється за участю співробітників компаній. Водночас понад третина втрат фінансових ресурсів і даних у організаціях спричинена діями тих самих внутрішніх працівників.

Рішення цих проблем потребує глибокого впровадження заходів безпеки адміністрацією та відповідними службами захисту організації. Однією з базових рекомендацій є шифрування навіть внутрішнього корпоративного листування задля мінімізації ризиків перехоплення конфіденційної інформації.

Віруси є поширеним явищем, що суттєво впливає на комп'ютерних користувачів, особливо тих, хто працює в мережах або використовує неліцензійне програмне забезпечення. Їх виникнення стало можливим завдяки створенню самозапускних програм. Подібність поведінки таких програм до процесів у біології та медицині призвела до формування специфічного термінологічного апарату: вірус, зараження, лікування, профілактика, щеплення, «доктор» тощо.

Зараження передбачає проникнення вірусу в іншу програму, системну область диска чи інші об’єкти. У результаті такі елементи стають зараженими. Віруси належать до класу програм, які нелегально проникають у комп’ютерні системи і спричиняють шкоду як для програмного забезпечення та інформаційних даних, так і для технічних компонентів, зокрема жорстких дисків.

З розвитком мережевих технологій віруси перетворилися на серйозну загрозу для локальних і глобальних комп’ютерних систем. Інфікуванню піддаються навіть кишенькові персональні комп’ютери. Наприклад, у серпні 2004 року була виявлена перша вірусна програма для компютера — Backdoor.WinCE.Brador.a. Вона виконувала функції прихованого дистанційного доступу, що дозволяло додавати, видаляти чи пересилати файли автору вірусу.

Віруси зазвичай містять унікальну послідовність команд і визначені поведінкові патерни, які дають змогу створювати антивірусні програми для їх виявлення. Проте деякі типи вірусів, таких як поліморфні, не мають стандартних сигнатур і здатні змінювати власну структуру, ускладнюючи їх ідентифікацію.

Крім того, проблеми в області інформаційної безпеки пов’язані не лише із діями шкідливого програмного забезпечення, а й із взаємодією людського фактора. Помилкові або навмисні дії людей можуть спричиняти негативний вплив на інформацію, будівлі, приміщення та особисту безпеку як самих користувачів, так і технічно обслуговуючого персоналу.

1.8 Міжнародні стандарти захисту інформації

Критерії оцінки надійності комп'ютерних систем (Trusted Computer Sustem Evaluation Criteria, TCSEC) - це стандарт Міністерства оборони США, який встановлює основні вимоги до засобів контролю комп'ютерної безпеки, вбудованих у комп'ютерні системи. TCSEC використовується для оцінки, класифікації та вибору комп'ютерних систем, що використовуються для

обробки, зберігання та доступу до конфіденційної інформації. TCSEC часто називають Помаранчевою книгою і він є важливою частиною серії «Rainbow Publications». TCSEC, перше видання якої було опубліковане в 1983 році, була замінена міжнародним стандартом «Критерії інформаційної безпеки» в 2005 році. Критерії, що використовуються для оцінки безпечної інформаційної системи, можуть бути використані для визначення семи класів захисту системи

Мінімальний захист: Цей клас зарезервований для систем, які пройшли оцінку, але не відповідають вимогам вищих класів.

Додатковий захист. Гарантована захищена інформаційна база системи класу C1 забезпечує розділення користувачів і даних. Вона включає засоби керування, які можуть застосовувати обмеження доступу для захисту проектної та особистої інформації та запобігання випадковому зчитуванню або знищенню даних іншими користувачами.

Вважається, що середовище, в якому користувачі, що обробляють дані одного рівня секретності, можуть працювати разом.

Захист, заснований на контрольованому управлінні доступом. Всі вимоги класу C1 переносяться на клас C2. Крім того, системи цього класу реалізують структурно більш «дрібнозернистий» контроль доступу в порівнянні з системами класу C1, з додатковими засобами управління обмеженням доступу і розподілом прав, а також системою реєстрації (аудиту) подій, пов'язаних з безпекою системи і розподілом ресурсів. Вводяться специфічні вимоги до «очищення», коли системні ресурси повторно використовуються іншими процесами.

Захист на основі авторизації, що базується на присвоєнні міток об'єктам і активам, які перебувають під контролем CSP. Вимоги до системи класу B1 означають, що виконуються всі вимоги класу C2. Крім того, система повинна забезпечувати неформальне визначення моделі, що лежить в основі політики безпеки, присвоєння міток даним і санкціонований контроль доступу до об'єктів з боку іменованих суб'єктів. Система потребує інструментів, які можуть коректно і надійно присвоювати мітки експортованій інформації.

Структурований захист. Системи класу B2 повинні відповідати всім вимогам класу B1. У системі класу B2 ТКС базується на чітко визначеній і формально задокументованій моделі, в якій засоби контролю доступу застосовуються до всіх суб'єктів і об'єктів автоматизованої системи обробки даних. Крім того, має бути проведений аналіз щодо існування побічних каналів витоку; структура СТЗ має бути розділена на критичні для безпеки та некритичні для безпеки елементи; інтерфейс СТЗ має бути чітко визначений, а його проектування та реалізація мають бути ретельно протестовані та повністю проаналізовані, щоб забезпечити проведення ретельного тестування та повного аналізу. Механізми автентифікації є надійними, засоби контролю безпеки надаються у вигляді інструментів як для системних адміністраторів, так і для операторів, а контроль конфігурації є жорстко обмеженим. Система є відносно стійкою до спроб вторгнення [6].

Зона безпеки. Усі вимоги до систем класу B2 включені у вимоги до систем класу BZ. КТС класу BZ повинні реалізовувати концепцію моніторів доступу, які захищені від несанкціонованої модифікації, спотворення та підробки і гарантовано обробляють всі доступи.

Передбачається впровадження менеджера безпеки системи та розширення механізмів контролю (аудиту) для забезпечення обов'язкового сповіщення про всі події, пов'язані з можливими порушеннями встановлених в системі правил безпеки.

Також обов'язковими є процедури забезпечення повного відновлення системи. Система цього класу має високу стійкість до спроб вторгнення.

Система класу A1 функціонально еквівалентна системі класу B3, оскільки до неї не висуваються нові вимоги до політики безпеки.

Цей клас систем характеризується формальними особливостями проектування та високим ступенем впевненості в тому, що верифікація безпеки, тобто гарантована безпечна обчислювальна база, була реалізована правильно.

1.9 Проактивні і сигнатурні методи

Попри наявні недоліки, проактивні підходи ефективно допомагають виявляти нові загрози ще до створення відповідних сигнатур.

Розглянемо, наприклад, реакцію на антивірусів на хробака Email-Worm.Win32.Nyxem (далі просто Nyxem) (Рис. 1)

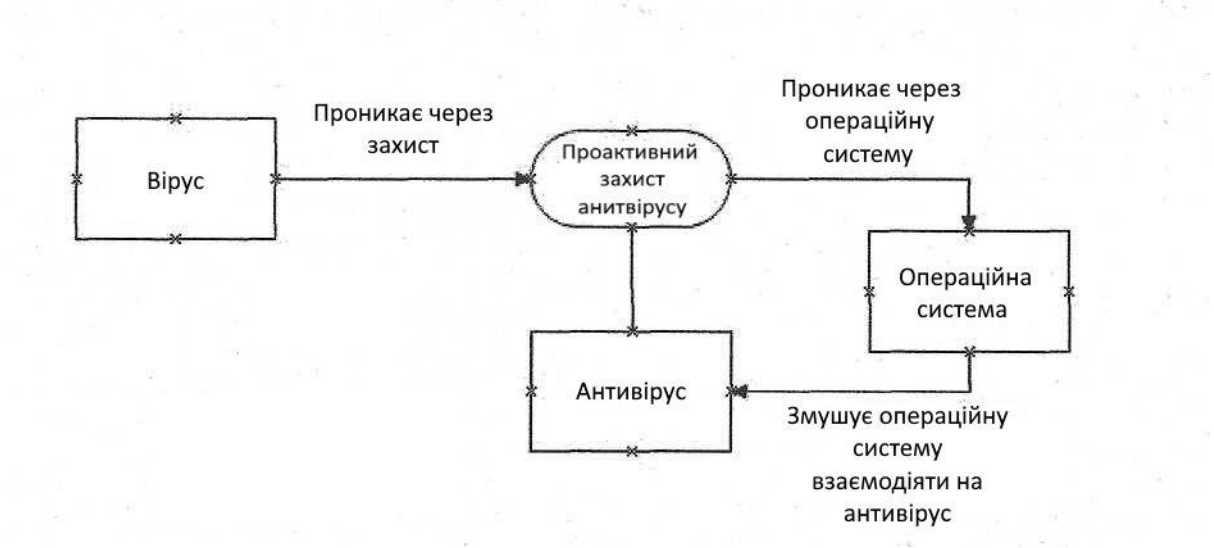

Рисунок 1.1 - Схема проникнення вірусів

Вірус Nyxem (також відомий як Blackmal, BlackWorm, MyWife, KamaSutra, Grew і CME 24) вражає комп'ютери, відкриваючи вкладення електронної пошти або загальнодоступні файли, які містять посилання на порнографічні або еротичні веб-сайти. За короткий проміжок часу вірус стирає інформацію з жорсткого диска і вражає файли 11 різних форматів (включаючи Access, Adobe, Microsoft Word, Excel і PowerPoint). При цьому вся корисна інформація замінюється на набір безглуздих символів. Ще однією особливістю Nyxem є те, що він стає активним на третій день кожного місяця..

Група дослідників з Магдебурзького університету (AV-Test.org) провела незалежну оцінку швидкості реакції розробників антивірусів на появу Nyxem [10].

Результати показали, що кілька антивірусних продуктів змогли виявити хробака за допомогою проактивної технології, тобто до того, як були

опубліковані сигнатури. Серед них TruPrevent Personal від Panda Software, Proventia-VPS від Internet Security Systems і MsEssential.

Проактивні підходи до захисту від шкідливих програм - це відповідь антивірусної індустрії на постійно зростаючу кількість нових шкідливих програм і швидкість їх поширення. Хоча проактивні методи, доступні сьогодні, дійсно можуть боротися з багатьма новими загрозами, припущення, що проактивні методи можуть повністю обійти регулярні оновлення антивірусів, в корені невірне. Насправді проактивні методи, як і методи на основі сигнатур, потребують оновлення. Використання лише найновіших проактивних методів не гарантує високого рівня виявлення шкідливих програм. Більш того, більш високий рівень виявлення в цьому випадку супроводжується збільшенням помилкових спрацьовувань. При цьому швидкість реагування на нові загрози залишається найважливішим критерієм визначення ефективності антивірусної програми.

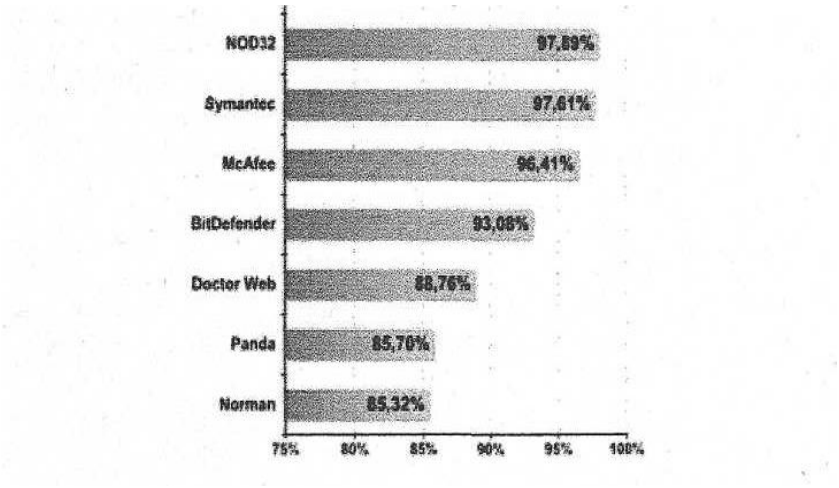

Рисунок 1.2. - Ефективність антивірусних програм

Для забезпечення максимально ефективного антивірусного захисту необхідно використовувати поєднання проактивних і сигнатурних методів. Лише комбінуючи ці підходи, можна досягти найвищого рівня виявлення загроз. На зображенні вище представлені результати досліджень Андреаса Климента (www.av-comparatives.org), які демонструють загальний рівень виявлення шкідливого програмного забезпечення (сигнатурний + евристичний).

На перший погляд, різниця між лідерами тестування здається мінімальною. Однак важливо пам’ятати, що аналіз проводився на вибірці, яка містила понад пятсот тисяч вірусів. Відставання навіть на 1% означає пропуск близько пяти тисяч загроз.

З огляду на це, користувачам не варто сліпо довіряти маркетинговим обіцянкам виробників антивірусних програм. Для отримання об’єктивної оцінки доцільно орієнтуватися на незалежні тестування, що дають змогу порівняти комплексні характеристики доступних рішень та визначити їхню реальну ефективність.

1.10 Задачі інформаційної безпеки

Під інформаційною безпекою зазвичай розуміють забезпечення захисту інформації, її безпосередніх власників та інфраструктури, що її підтримує, від випадкового або зловмисного втручання, яке може призвести до втрати інформації та інфраструктури, що підтримує її зберігання та існування. Інформаційна безпека виконує завдання, пов'язані з передбаченням і запобіганням таких можливих дій, а також мінімізацією можливої шкоди [7].

1.11 Інформаційна безпека і можливі загрози її забезпеченню. Дії, що загрожують або завдають шкоди інформаційній безпеці, поділяються на певні категорії:

1. дії, що виконуються авторизованими користувачами в системі;
2. дії, що виконуються неавторизованими користувачами в системі;
3. дії, що виконуються неавторизованими користувачами в системі;
4. дії, що виконуються неавторизованими користувачами в системі.

До цієї категорії відносяться наступні дії:

1. Зловмисні дії користувачів, які викрадають або повністю або частково знищують дані на серверах або робочих станціях компанії; пошкодження існуючих даних в результаті необережних або недбалих дій користувача;

2. «Електронне» втручання - дії хакерів, які використовують систему для викрадення або знищення даних на серверах або робочих станціях компанії. До категорії хакерів відносяться люди, які беруть активну участь у комп'ютерних злочинах, як професійно, так і з простої людської цікавості. До таких дій відносяться такі методи, як - несанкціоноване проникнення в захищені комп'ютерні мережі - DOS-атаки.

Несанкціоноване вторгнення ззовні з метою нанесення шкоди захищеній мережі компанії (знищення, модифікація існуючих даних), крадіжки та подальшого неправомірного використання конфіденційної інформації, використання мережевої інфраструктури компанії для атак на інші вузли мережі, крадіжки коштів компанії або окремих користувачів тощо. DOS-атаки («відмова в обслуговуванні») здійснюються ззовні і націлені на вузли мережі (поштові, файлові сервери), що відповідають за безпечну, ефективну і стабільну роботу підприємства. Відправляючи великий обсяг будь-яких даних на обраний вузол, зловмисник викликає перевантаження вузла і, таким чином, зупиняє його роботу на деякий час.

Такі атаки спричиняють різноманітні збої в поточних бізнес-процесах постраждалих компаній, що призводить до втрати клієнтів та шкоди репутації.

3. Комп'ютерні віруси, як і деякі інші види шкідливого програмного забезпечення, належать до окремої категорії методів електронної дії з подальшим нанесенням шкоди. Ці інструменти становлять реальну загрозу для сучасного бізнесу, що використовує комп'ютерні мережі, електронну пошту та Інтернет в цілому. Наприклад, якщо шкідливій програмі (вірусу) «вдається» потрапити в мережеві вузли компанії, це не тільки перешкоджає стабільній роботі цих вузлів, але й призводить до значних втрат часу, втрати наявних даних і, зокрема, до можливості крадіжки конфіденційної інформації та прямої крадіжки коштів з рахунків.

Вірусні програми, які потрапляють в мережу компанії і залишаються невиявленими, дозволяють зловмисникам отримати повний або частковий контроль над діяльністю компанії, що ведеться в електронному вигляді.

4. Спам Якщо кілька років тому спам був лише незначним джерелом роздратування, то зараз спам-технології відносяться до категорії «природних» загроз До категорії «природних» загроз відносяться різні зовнішні фактори. Наприклад, втрата інформаційної безпеки може бути спричинена крадіжкою носіїв інформації, форс-мажорними обставинами або неналежним зберіганням інформації [8].

1.12 Криптографічні методи та їх застосування

Криптографічні методи та заходи захисту інформації складають основу інформаційної безпеки.

Необхідно пам'ятати, що найбільш надійний захист може бути досягнутий тільки за допомогою комплексного підходу. Це означає, що вирішення проблеми має бути комбінацією організаційних, технічних і криптографічних засобів. В основі криптографічних схем лежить концепція зашифрованого перетворення інформації, яке відбувається за певними математичними законами, що унеможливлюють доступ до цієї інформації неавторизованих користувачів і гарантують, що ті ж самі люди не зможуть змінити інформацію неконтрольованим чином.

Тривалий час криптографія вважалася прерогативою держав, а криптографічні алгоритми - військовою технологією. З поширенням інформаційних технологій криптографія втрачає свій статус військової технології, оскільки потрібні більш надійні механізми захисту, які неможливі без використання надійних криптографічних алгоритмів. Як наслідок такої ситуації, до недавнього часу було складно визначити ступінь надійності криптографічних алгоритмів або навіть знайти їх опис через брак інформації.

Це призводило до використання різних примітивних методів криптографічного захисту або до створення абсолютно ненадійних алгоритмів.

Сьогодні існує велика кількість криптографічних алгоритмів, що відрізняються як загальними характеристиками, так і основними принципами

роботи. Не всі вони однаково надійні, а деякі з них не пропонують ніякого реального захисту, навіть якщо вони розроблені в якості стандартів. Насправді, створення надійного криптографічного логічного алгоритму є дуже складним завданням. Багато алгоритмів, які раніше розроблялися і вважалися надійними, зараз є або ненадійними, або дуже підозрілими. Тому при розробці криптографічних алгоритмів слід враховувати тенденції розвитку комп'ютерних технологій та інші фактори, які можуть знизити їх стійкість в майбутньому.

Традиційні методи шифрування, що використовуються для захисту інформації та даних, які передаються через комп'ютерні мережі, засновані на тому, що відправник і одержувач повідомлення знають і використовують один і той же секретний ключ. Ідея цього методу, який називається криптографія з секретним ключем (симетрична криптографія), полягає в тому, що відправник шифрує текст повідомлення за допомогою секретного ключа, а одержувач розшифровує його за допомогою того ж ключа. Якщо ключ скомпрометований, можливий несанкціонований доступ до даних, тому ключ необхідно регулярно змінювати для забезпечення надійності системи. Особливо важливим питанням є те, як обидві сторони конфіденційно домовляються про ключі, які будуть використовуватися. Якщо відправник і одержувач просторово розділені значною відстанню, виникає питання про надійність засобів зв'язку, що використовуються для передачі конфіденційних даних.

Будь-хто, хто випадково або навмисно отримає секретний ключ, може безконтрольно прочитати, змінити або підробити будь-яке повідомлення, що містить цей ключ.

Управління ключами - це комплекс заходів з генерації, передачі та зберігання ключів, що є особливо складним завданням у відкритих системах з великою кількістю користувачів.

Сьогодні криптографія є невід'ємною частиною всіх інформаційних систем, від електронної пошти до мобільного зв'язку, від доступу до Інтернету до електронних грошей. Криптографія гарантує підзвітність, прозорість і конфіденційність. Вона запобігає шахрайству в електронній комерції та

забезпечує юридичну чинність фінансових операцій. Криптографія допомагає підтвердити вашу особу, водночас забезпечуючи анонімність. Вона не дає шахраям зламати ваші сервери, а конкурентам - отримати доступ до ваших конфіденційних документів. А в майбутньому, коли торгівля і комунікація стануть тісніше пов'язані з комп'ютерними мережами, криптографія стане незамінною. Але наявні на ринку інструменти шифрування не забезпечують того рівня захисту, який обіцяють у рекламі. Більшість продуктів не розробляються і не використовуються спільно з криптографами. Цим займаються інженери, і для них криптографія є лише компонентом програми. Але криптографія - це не компонент.

Ви не можете захистити систему, «встановивши» криптографію після розробки. Щоб правильно реалізувати власну криптографічну систему, необхідно не тільки вчитися на чужих помилках, але в деяких випадках також застосовувати спеціальні захисні методи програмування і спеціальні інструменти розробки. На комп'ютерну безпеку витрачаються мільярди доларів, значна частина яких витрачається на нікчемні продукти. На жаль, коробка зі слабким криптографічним продуктом виглядає так само, як і коробка з сильним криптографічним продуктом: хоча користувацькі інтерфейси обох криптопоштовиків схожі, один з них забезпечує безпеку, а інший дозволяє підслуховувати.

Порівняння може виявити схожість між цими двома програмами, але одна з них має дірки в системі безпеки, тоді як інша не має жодних дірок. Досвідчений криптограф може побачити різницю між цими системами. Зловмисник може зробити те ж саме. Комп'ютерна безпека сьогодні - це картковий будиночок, який може зруйнуватися в будь-який момент. Багато вразливих продуктів не були зламані раніше, тому що вони не отримали широкого розповсюдження. Як тільки вони стануть широко розповсюдженими, вони незабаром привернуть увагу злочинців.

Засоби масової інформації незабаром оприлюднять ці атаки і підірвуть довіру громадськості до криптосистем. Зрештою, крипторинок буде виграний або програний відповідно до ступеня безпеки цих продуктів.

1.12.1 Задачі криптографічних протоколів: криптографічні протоколи - це протоколи, у яких учасники використовують криптографічне перетворення інформації для досягнення певних цілей.

Перелічимо основні завдання забезпечення інформаційної безпеки, що вирішуються за допомогою криптографічних протоколів.

Обмін ключовою інформацією та подальше встановлення безпечного обміну даними. Нині, з широким розповсюдженням відкритих мереж передавання даних, таких як Інтернет і побудовані на його основі інтранет- і екстранет-мережі, криптографічні протоколи дедалі ширше використовують для розв'язання найрізноманітніших завдань, і такі мережі надають дедалі ширший спектр послуг своїм користувачам.

Крім класичних сфер застосування протоколів, описаних вище, існує також широкий спектр специфічних завдань, які вирішуються за допомогою відповідних криптографічних протоколів. В основному це комп'ютерна безпека.

Розроблення криптографічних протоколів.

Динамічних розвиток криптографічних протоколів багато в чому пов'язаний з такими подіями, як поява електронних платіжних систем, смарт-карт і електронних грошей. За зарубіжними оцінками, темпи розвитку електронної комерції постійно зростають. Наприклад, згідно з прогнозами, кількість компаній, що займаються цим видом торгівлі, зросте у світі з 111 000 у 1996 році до 435 000 у 2000 році.

У той же час загальний обсяг продажів через Інтернет зросте з $9,5 млрд. до $196 млрд. Роздрібні продажі через Інтернет, за оцінками, зростуть з 500 мільйонів доларів у 1996 році до 7 мільярдів доларів у 2000 році. При цьому більше половини всіх покупок буде оплачуватися за допомогою нового способу оплати - електронних грошей. Таким чином, збільшиться не тільки кількість

компаній, що ведуть бізнес через Інтернет, та їх загальний оборот, але й очікується зростання середнього доходу на одну компанію. Оскільки протоколи сьогодні є основним криптографічним засобом захисту інформації в Інтернеті, можна сказати, що розвиток таких засобів захисту комерційної таємниці буде продовжуватися як в кількісному, так і в якісному відношенні. У зв'язку з універсальністю використання криптографічних протоколів для вирішення завдання забезпечення інформаційної безпеки як в локальних, так і в розподілених інформаційних системах, необхідне детальне вивчення їх основних видів, проблем практичного застосування таких протоколів і створення спеціальних інформаційних систем на основі таких протоколів. Враховуючи, що основою будь-якого криптографічного протоколу є так званий криптографічний алгоритм, в даній статті розглядаються питання побудови та практичного застосування основних типів таких механізмів. Крім відомих і широко використовуваних криптографічних алгоритмів з-за кордону, увагу також приділено вітчизняним розробкам і стандартизації криптографічних алгоритмів у сфері інформаційної безпеки.

Класична криптографія Перш ніж перейти до криптографічних протоколів та їх практичного застосування, слід звернути увагу на проблему, яка вже давно вважається класичною в практичних застосуваннях, а саме на основи побудови систем секретного зв'язку.

Системи секретного зв'язку - це системи передачі інформації, в яких зміст інформації, що передається, зашифровується шляхом криптографічного перетворення. Факт передачі інформації не приховується. Всі системи секретного зв'язку засновані на використанні криптографічних алгоритмів як основного засобу збереження таємниці."[10] Шифрування - це процес криптографічного перетворення послідовності відкритих повідомлень у послідовність зашифрованих повідомлень. Розшифрування - це процес криптографічного перетворення закритого повідомлення у відкрите.

Розшифрування - це процес знаходження відкритого повідомлення, що відповідає заданому закритому повідомленню при невідомому

криптографічному перетворенні. Набір відкритих текстових повідомлень може бути представлений у вигляді бітового потоку, мережевого кадру, файлу тощо. Таким чином, систему засекреченого зв'язку можна визначити як сукупність відображень з множини відкритих повідомлень на множину закритих повідомлень.

Вибір конкретного типу відображення визначається ключем дешифрування (або шифрування). Відображення повинні мати взаємно невизначений характер. Тобто процес дешифрування повинен давати єдиний результат, який відповідає вихідному відкритому повідомленню (див. Рисунок 1. 3). У загальному випадку ключі шифрування і дешифрування можуть бути різними, але для простоти міркувань тут вони вважаються однаковими. Простір ключів - це множина, з якої вибираються ключі. Алгоритм шифрування - це набір операцій, набір відкритих повідомлень, набір можливих секретних повідомлень і простір ключів. Алгоритм дешифрування - це набір операцій дешифрування, набір можливих секретних повідомлень, набір можливих відкритих повідомлень і простір ключів.

Рисунок 1.3 - Загальна структура системи засекреченого зв'язку

Безпека алгоритмів шифрування.

Механізм вибору відкритих повідомлень може бути виражений як імовірнісний процес, тому для кожного відкритого повідомлення існує апріорна ймовірність вибору. Аналогічно, існує апріорна ймовірність вибору кожного ключа. Зловмисник, який перехоплює зашифроване повідомлення, може

обчислити апостеріорні ймовірності як ймовірності появи відкритого тексту, так і ймовірності ключа. Набір апостеріорних ймовірностей - це система знань супротивника про ключ, що використовується, і відправлене відкрите повідомлення.

Крім того, перш ніж почати перехоплення зашифрованого повідомлення, противник має певний набір апріорних ймовірностей щодо відкритого повідомлення і ключа. З практичної точки зору це означає, що противнику відома використовувана система секретного зв'язку. Припустимо, що противнику відомі всі криптографічні перетворення і простори ключів, які використовуються в системі секретного зв'язку, і що секретність системи залежить від вибору конкретного ключа, як зазначалося вище. Після перехоплення певної кількості зашифрованих повідомлень і підрахунку кінцевих ймовірностей противник розуміє, що ці ймовірності відповідають єдиному рішенню: використовувати ключ, який задовольняє ці ймовірності, або відправити відкрите повідомлення (об'єднуюча точка прийняття рішення). Зрозуміло, що такий висновок призведе до розкриття системи противника (строгий математичний доказ існування та обчислення об'єднуючої точки прийняття рішення в цій роботі не наводиться). Розкриття секретної системи зв'язку або алгоритму шифрування передбачає розуміння будь-якої з наступних дій, запланованих противником для досягнення цієї мети противник знаходить секретний ключ системи за допомогою обчислень. Противник знаходить алгоритм, функціонально еквівалентний алгоритму шифрування, не знаючи секретного ключа, що використовується. Противник знаходить відкрите повідомлення, що відповідає одному з перехоплених зашифрованих повідомлень. Противник отримує часткову інформацію про використаний ключ і відкрите повідомлення.

1.12.2 Криптоаналіз – наука, що займається питанням дослідження алгоритмів шифрування.

Кожній з перерахованих вище цілей відповідає різний обсяг інформації

про використовувані ключі і текстові повідомлення, що передаються.

Тому проти систем секретного зв'язку, що використовуються, здійснюється цілий ряд атак. Надалі передбачається, що об'єктом атаки є використовуваний алгоритм шифрування (дешифрування).

Тому під стійкістю алгоритму шифрування розуміється його здатність протистояти всім можливим атакам на нього. У ймовірнісних термінах це визначення можна переформулювати наступним чином.

Алгоритм вважається стійким, якщо перехоплення зашифрованого повідомлення не призводить до досягнення згоди у визначенні ключа, що використовується, або відкритого тексту, що передається.

1.12.3 Класифікація типів кіберзагроз на криптографічні алгоритми: Існує досить загальний підхід до формальної оцінки цієї концепції. Безпека криптографічного алгоритму має розглядатися стосовно пари «атакувальник-мета», де мета противника розуміється як планована загроза. У світовій літературі розроблено такі сертифікації для різних типів атак на криптографічні алгоритми.

Атаки з відомим шифртекстом (атаки тільки на шифртекст). Противник знає криптосистему, тобто алгоритм шифрування, але не секретний ключ. Крім того, противник знає тільки набір перехоплених шифртекстів.

Проста атака з вибором відкритого тексту. Противник має можливість вибрати необхідну кількість текстів і отримати відповідні шифротексти. У цьому випадку противник має можливість вибирати відкриті тексти, враховуючи той факт, що шифротексти всіх попередніх відкритих текстів відомі.

Атака за обраним шифртекстом (атака за обраним шифртекстом). Співробітник має можливість вибрати необхідну кількість шифртекстів і отримати відповідні відкриті тексти. При виборі наступного шифртексту противник знає всі відкриті тексти, що відповідають попередньому шифртексту.

Супротивник має можливість обирати як шифртекст (і його розшифровку), так і відкритий текст (і його шифровку). Противник не знає самого ключа, але знає деякі відмінності між ключами. У цьому списку атаки представлені в порядку зростання їхньої сили. З погляду криптоаналізу, остання атака є найсильнішою, але існують і ще сильніші атаки. Це атака, в якій закритий ключ отримують шляхом викрадення або підкупу.

Аналізуючи атаки та їхні цілі, можна зробити висновок, що алгоритми найстійкіші, коли вони здатні протистояти найсильнішим атакам противника і коли вони переслідують найслабшу можливу мету (загрозу) атаки. [11].

1.12.4 Причини здійснення успішних атак на алгоритми шифрування: Розглянемо найпоширеніші причини успішних атак на алгоритми шифрування, які актуальні на сьогодні:

1. Наявність статистичної структури, властивої природним мовам. Історично мови мають певні символи чи їхні комбінації, які зустрічаються частіше за інші. Це дозволяє при перехопленні зашифрованого повідомлення для деяких типів алгоритмів аналізувати частотність появи окремих символів або їх послідовностей (наприклад, біграм чи триграм). У певних випадках такий підхід може допомогти дешифрувати окремі частини повідомлення з високим рівнем точності [10].

2. Присутність передбачуваних слів. Йдеться про слова чи фрази, які очікувано можуть бути використані у перехопленому тексті. Наприклад, у діловому листуванні часто зустрічаються шаблонні вирази. Для англійської мови характерними є слова на кшталт "and", "the", "are" тощо, які зазвичай зустрічаються у великій кількості [12].

1.12.5 Типи алгоритмів шифрування:

Шифрування - це процес кодування даних для захисту їх від несанкціонованого доступу. Процес кодування називається шифруванням,

а процес розшифрування - дешифруванням. Саме зашифроване повідомлення називається шифротекстом, а метод, що використовується, - криптографією [13].

Основна вимога криптографії полягає в тому, що розшифрування (а в деяких випадках і шифрування) можливе лише за наявності авторизації, тобто додаткової інформації (або пристрою), яка називається криптографічним ключем. Процес розшифрування шифру без ключа називається дешифруванням.

Галузь знань про криптографію, методи її побудови та розкриття називається криптологією. Властивість шифру протистояти розкриттю називається криптографічною стійкістю або надійністю і зазвичай визначається складністю алгоритму дешифрування. У практичній криптографії стійкість шифру оцінюють з економічних міркувань.

Якщо вартість розшифрування шифру більша (в грошовому еквіваленті, включаючи необхідні комп'ютерні ресурси та спеціальне обладнання), ніж сама зашифрована інформація, то шифр вважається достатньо стійким.

Симетричне шифрування - це схема шифрування, яка використовує один і той самий ключ шифрування для шифрування і розшифрування [14].

Більшість симетричних шифрів використовують складні комбінації багатьох підстановок і перестановок. Багато з цих шифрів виконуються за кілька проходів (до 100 проходів), причому для кожного проходу використовується свій ключ. Набір «ключів проходу» для всіх проходів називається розкладом ключів. Цей ключ зазвичай формується шляхом виконання певних операцій над ключем, включаючи перестановки і заміни.

Найважливішими параметрами для всіх симетричних алгоритмів шифрування є:

- потужність;

- довжина ключа;

- кількість раундів;

- довжина оброблюваних блоків;

- складність апаратної/програмної реалізації;

- складність перетворення.

Перевагами симетричних систем є:

- відносно висока швидкість (втричі вища, ніж у асиметричних систем),

- легка реалізація (завдяки простішій обробці),

- невелика довжина ключа, необхідна для достатньої потужності.

Однак на практиці цей метод наразі рідко використовується через такі суттєві недоліки Складність управління ключами у великих мережах. Це означає, що кількість ключів, які необхідно генерувати, зберігати, передавати і знищувати в мережі, збільшується в чотири рази.

Мережа з 10 абонентів потребує 45 ключів, 100 абонентів - 4500 ключів, а 1000 абонентів - 499500 ключів. Складність обміну ключами Для використання симетричної системи необхідно вирішити проблему надійної передачі ключів кожному абоненту.

Асиметрична криптосистема з відкритим ключем (або асиметрична криптосистема, асиметричне шифрування) - це криптосистема, в якій відкритий ключ передається по відкритому (тобто незахищеному) каналу зв'язку і використовується для шифрування повідомлень. Закритий ключ використовується для розшифрування повідомлення.

Існування двох ключів, відкритого і закритого, робить систему асиметричною. Відкритий ключ надається всім, хто хоче надіслати повідомлення одержувачу, тоді як закритий ключ зберігається в одержувача і не повинен нікому передаватися. Навіть якби був відомий відкритий ключ і всі розшифровані відправлені повідомлення, знайти

закритий ключ було б неможливо.

Підхід у системах з відкритим ключем базується на існуванні односторонньої функції (функції Dx). За відомим x легко знайти значення функції Dx, але неможливо або дуже складно знайти значення аргументу x, тобто обчислити обернену функцію. Візьмемо RSA, один з найвідоміших і найпоширеніших алгоритмів.

Цей алгоритм в основному використовується для передачі даних по захищених каналах зв'язку в Інтернеті - HTTPS, SSH. Іншим відомим алгоритмом є алгоритм Діффі-Хеллмана (DX), який був першим асиметричним алгоритмом шифрування.Алгоритм RSA заснований на властивостях простих і взаємно простих чисел, тобто на задачі множення і ділення комплексних чисел на прості множники.

Ця задача є обчислювально односторонньою. Іншими словами, дуже легко знайти комплексне число за заданим простим множником; в реальних системах, що використовують складні числа розміром 100 біт і більше, час, необхідний для вирішення задачі ділення числа на прості множники, вимірюється роками. На відміну від симетричної криптографії, секретним ключем володіє лише одна сторона. У той час як симетрична криптографія вимагає зміни ключа після кожного сеансу передачі даних, асиметрична криптографія дозволяє ключу залишатися незмінним протягом тривалого періоду часу. У більшості мереж кількість ключів в асиметричній криптографії набагато менша, ніж в симетричній. Недоліки - повідомлення надійно шифруються, але самі сторони піддаються впливу фактом передачі (може бути використано як основа для атаки) - асиметричні алгоритми використовують набагато довші ключі, ніж симетричні - оскільки в чистому вигляді асиметрична система вимагає значних обчислювальних ресурсів, на практиці їх часто використовують в комбінації з іншими алгоритмами.

Кілька слів слід сказати про криптографічну стійкість асиметричних криптосистем. Можливі атаки на такі системи включають в себе наступне. Припустимо, що сторони А і В обмінюються повідомленнями, як описано вище. Якщо сторона С хоче порушити цей процес, вона може підслухати канал зв'язку між А і В і замінити свої повідомлення на оригінальні. Наприклад, коли А надсилає свій відкритий ключ Ra Б, С може перехопити цей ключ і надіслати Б свій власний ключ РС. Потім В шифрує повідомлення, використовуючи неправильний ключ РС. Як тільки С перехоплює ці повідомлення, він може розшифрувати їх за допомогою свого закритого ключа і відправити А ще одне фальшиве повідомлення, закодоване ключем RA замість оригінального повідомлення. Така атака називається «людина посередині».

Цифрові підписи.

Асиметричні системи з відкритим ключем також використовуються для систем цифрового підпису. Процес ґрунтується на переключенні операцій шифрування та розшифрування: щоб підтвердити, що це повідомлення дійсно надіслано стороною А, ця сторона надсилає парі (M, c) стороні В, супроводжуючи її підписом C = M mod n.

Сторона В, яка отримує це підписане повідомлення, шифрує повідомлення M за допомогою відкритого ключа RA: C = M mod n. Якщо C = C', то повідомлення M дійсно надійшло від сторони А. Якщо C = C', то повідомлення дійсно надійшло від сторони В. Якщо ні, то повідомлення було пошкоджено або змінено третьою стороною» [16].

Однією з основних проблем, що виникають при використанні асиметричних алгоритмів, є низька швидкість обробки шифрування та дешифрування. Цей факт є типовим, особливо при реалізації алгоритмів на пристроях з низькою обчислювальною потужністю (реалізація ЕЦП на смарт-картах). Одним з рішень є зменшення розмірності параметрів

системи, але це може призвести до зниження стійкості алгоритму. Іншим рішенням цієї проблеми є виконання основних типів математичних обчислень, що використовуються в асиметричних алгоритмах шифрування, в ефективній процедурі. Залежно від ситуації, під ефективністю можна розуміти не тільки швидкість обчислень, але і мінімальний обсяг пам'яті, мінімальний обсяг програмного коду або їх комбінацію.

Суть більшості методів прискорення обчислень полягає у зведенні операцій модульного множення та піднесення до степеня до послідовності операцій модульного додавання/віднімання.

РОЗДІЛ 2
ПРАКТИЧНА ЧАСТИНА
АНАЛІЗ ІСНУЮЧОГО АПАРАТНОГО І ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПІДПРИЄМСТВА «КОМПАНІЯ ГОТ»

2.1 Загальні відомості про підприємства «Компанія ГОТ»

ПІДПРИЄМСТВО «КОМПАНІЯ ГОТ»

Адреса: м. Полтава, вул. Соборності, буд.77

ЕГРПОУ 40864860

Телефон 0501430383

Дата реєстрації 09.05.2021р.

Кількість персональних комп'ютерів - **25 штук**

Тип локальної мережі - **Шина**

Антивірус, що використовується – **NOD 32**

Провайдер – фірма «Тріолан»

Сфера діяльності - «Компанія ГОТ» спеціалізується на будівництві житлових і нежитлових будівель, також здійснює консультування з питань комерційної діяльності й керування, дослідження кон'юнктури ринку та виявлення громадської думки, оброблення даних, розміщення інформації на веб-вузлах і пов'язана з ними діяльність, надання інших інформаційних послуг, оптова торгівля деревиною, будівельними матеріалами та санітарно-технічним обладнанням, організацію будівництва будівель

Компанія прагне збільшувати свою асортиментну лінійку. Для частини своїх клієнтів компанія здійснює логістичні послуги.

Метою компаніє є стати джерелом інноваційних ідей та сучасних рішень для клієнтів, перевершувати їхні очікування, пропонувати унікальні та принципово нові види сервісів, а також виступати об'єктивним експертом у оцінці якості товарів, що поставляються. Одним із ключових принципів

діяльності компанії є постійний розвиток і вдосконалення у всіх напрямах її роботи.

Протягом своєї успішної роботи компанія створила ефективну систему продажів, яку постійно вдосконалює. Завдяки оптимізації всіх бізнес-процесів забезпечується формування конкурентоспроможної цінової політики. Основу успіху та стабільності компанії становить команда висококваліфікованих професіоналів.

Інформаційний відділ на підприємства «Компанія ГОТ»

В підприємства «Компанія ГОТ» існує відділ програмного та апаратного забезпечення, котрий відповідає за ряд певних функцій:

– встановлення спеціалізованого програмного забезпечення та його використання;

– сервісне обслуговування компютерних систем і мереж.

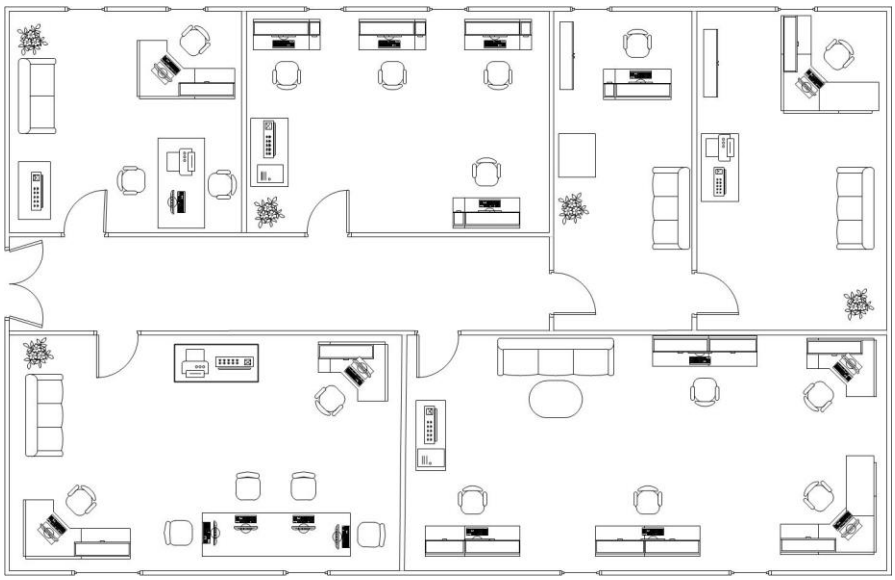

Рисунок 2.1 - План розміщення обладнання на підприємстві

2.2 Апаратне забезпечення

2.2.1 Програмне забезпечення:

1.– Операційна система

Операційна система для компютерних ситсем версії: Windows XP

2.– Мережа

В мережі підприємства встановлено 25 комп'ютерів. Майже всі вони мають можливість спільного доступу.

На даному підприємстві використовується: Топологія мережі: Шина

Топологія мережі «шина» самою своєю структурою дає можливість формувати мережного устаткування комп’ютерів, а також забезпечувати рівноправність усіх абонентів. У цьому типі з'єднання наявна лише одна лінія зв'язку, тому передача даних між комп’ютерами можлива виключно послідовно. В іншому разі інформація зазнає спотворень через дублювання, зіткнення чи виникнення колізій. З цієї причини шини даних працюють у напівдуплексному режимі, що дозволяє двонаправлений обмін, але виключно почергово, а не одночасно.

Вищезазначена топологія є більш стійкою, оскільки вона не залежить від центрального вузла, який мав би передавати всю інформацію. У разі відмови центру в інших топологіях вся система, керована цим центром, може вийти з ладу. Натомість у «шинній» топології додавання нових пристроїв доволі просте і зазвичай може виконуватись без зупинки роботи мережі. До того ж, для цієї топології зазвичай потрібно значно менше кабельної інфраструктури порівняно з іншими. Тим не менш, варто зазначити, що кожен комп’ютер у мережі (за винятком двох крайніх) потребує підключення через два окремих кабелі, що може бути не завжди зручним рішенням.

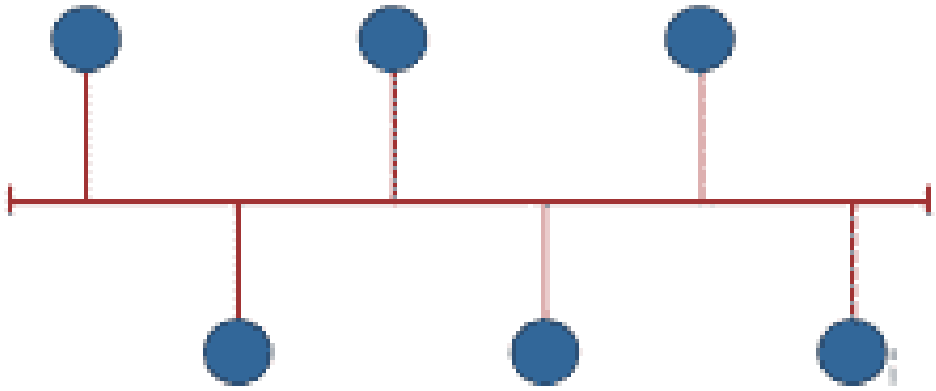

Рисунок 2.2 - Топологія «шина»

Основним недоліком шинної топології є те, що при виникненні несправності на одній ділянці мережевого кабелю, вся мережа може перестати працювати. Для того, щоб знайти несправність, необхідно розділити шину на дві частини і з'ясувати, яка з них несправна. Цей процес займає багато часу, але не виключає використання шинних топологій. Це ідеальний метод для з'єднання комп'ютерів в класах і для створення невеликих мереж, де кабелі можна прокласти в легкодоступних місцях..

2.3 Технічний та організаційний захист

Під технічним захистом розуміється комплекс спеціальних організаційно-технічних заходів і засобів, що застосовуються для захисту конфіденційної інформації. Організаційний захист - це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, яка виключає або суттєво обмежує неправомірне заволодіння конфіденційною інформацією та виникнення внутрішніх і зовнішніх загроз.

Організаційний захист інформації є організаційною основою, так званим «ядром», загальної системи захисту конфіденційної інформації підприємства.

Ефективність загальної системи захисту інформації залежить від цілісності та якості організаційної роботи, проведеної керівництвом і менеджерами підприємства.

Роль і місце корпоративного захисту інформації в загальній системі заходів, спрямованих на захист конфіденційної інформації підприємства, залежить від виняткової важливості своєчасного і правильного прийняття управлінських рішень на основі наявних у розпорядженні керівництва повноважень, засобів і методів захисту інформації, а також визначеного ним існуючого нормативно-методичного апарату. Основними напрямами захисту інформації є організаційний захист, а також правовий і технічний захист інформації.

До інженерно–технічного захисту на підприємстві відноситься:

– служба охорони на підприємстві;

– встановлення відеоспостереження;

– встановлення датчиків сигналізації;

– датчики пожежної безпеки;

– установка огорожі та решіток на вікнах.

Також на підприємстві існує спеціаліст з захисту інформації.

Антивірусний захист

Для захисту комп'ютерних систем і мереж від шкідливих програм та вторгнень, на підприємстві використовується антивірус NOD 32.

На сьогоднішній день ця версія не вважається актуальною, тому що вона вже застаріла і має недоліки в захисті.

Вартість використання антивірусного захисту на підприємстві становить 620 грн. за один персональний компютер за 3 роки. Загальна вартість антивірусного програмного забезпечення, що використовується на підприємстві становить: 15.5 тис. гривень.

2.4 Пропозиції по захисту

Для покращення захисту інформації на підприємстві пропонується наступне:

2.4.1 Операційна система для ПК Windows XP – наразі вважається застарілою операційною системою, оскільки компанія Microsoft припинила її підтримку. Це означає, що вона більше не отримує оновлень і вдосконалень, через що значно поступається сучасним версіям операційних систем.

На теперішній час однією з кращих операційних систем для підприємства є – **Window 10** тому що;

– має більш надійну архітектуру за Windows XP та Windows 7;

– має показники швидкодії на рівні останнього продукту Microsoft – Windows 11;

– має зручний та зрозумілий інтерфейс та графічні додатки.

2.4.2 Мережа Наразі на підприємствах використовується топологія мережі: топологія мережі: шина, але в неї є серйозні недоліки:

- у разі виходу з ладу будь-якої ділянки мережевого кабелю може вийти з ладу вся мережа;

- пошук несправностей ускладнений.

Тому рекомендується встановлювати топологію «зірка», яка вважається однією з найкращих топологій, що використовуються на підприємствах.

Переваги:

- висока пропускна спроможність мережі завдяки використанню провідників високого рівня;

- легко діагностується;

- завжди легко знайти «саботажника», тому досить по черзі відключати вузли від мережі;

- навіть якщо пошкоджено один мережевий кабель, у разі виходу з ладу одного вузла може бути пошкоджена вся мережа. Не потрібно турбуватися про пошкодження мережі;

- дорого, але легко розширюється - навіть якщо проводка до головного концентратора розташована далеко, можна встановити додаткові концентратори поруч із найближчим і підключити нових клієнтів. Звичайно, важливо враховувати передбачуване використання мережі;

- підвищена безпека мережі від несанкціонованого доступу та контрольований доступ системного адміністратора до інформації.

2.4.3 Антивірусний захист ПК – Microsoft Security Essentials – це вдосконалений інструмент для захисту вашого ПК від широкого спектра шкідливих програм, включаючи віруси, трояни та шпигунські програми. Антивірус відзначається високою оптимізацією, споживає мінімум системних ресурсів (приблизно 50 МБ оперативної пам'яті) та працює швидко й плавно. Після його встановлення ви навряд чи зіткнетеся з помітним зниженням загальної продуктивності системи. За результатами тестів AV-Test.org, антивірус виявив 98% із пів мільйона перевірених шкідливих програм, що підтверджує його ефективність. Завдяки цьому MSE може на рівних конкурувати з багатьма платними антивірусними програмами й часто перевершує навіть деякі безкоштовні аналоги.

Основні переваги Microsoft Security Essentials включають:

– простий і зрозумілий інтерфейс, який підійде навіть для недосвідчених користувачів;

– ненав'язливість у роботі: програма не перевантажує користувача непотрібними сповіщеннями. У разі виявлення загрози антивірус просто висвітлює інформаційне вікно зі запитом на видалення зараженого файлу;

– перевірку об’єктів у реальному часі під час виконання таких дій, як відкриття чи зміна файлів;

– можливість запуску ручної перевірки за потреби.

Доступні режими сканування також додають гнучкості у використанні:

– «Quick scan» – проводить швидке сканування найбільш вразливих областей, таких як реєстр, оперативна пам'ять і системні файли;

– «Full scan» – здійснює повне сканування всіх розділів жорсткого диска;

– «Custom scan» – дозволяє перевірити лише вибрані області диска.

І найкраще те, що Microsoft Security Essentials пропонується абсолютно безкоштовно, що робить його ще більш привабливим варіантом на ринку антивірусних рішень.

Висновок:

MSE можна сміливо назвати чудовим антивірусним рішенням. На мою думку, саме цього так довго бракувало користувачам Windows. Це оптимальний вибір, який позбавляє від зайвого клопоту. Простота у використанні, ефективність роботи та мінімальні вимоги до ресурсів створюють ідеальну формулу для базового захисту комп’ютера на платформі Windows. І найприємніше те, що цей інструмент абсолютно безкоштовний!

2.4.4 Облікові записи являють собою набори даних, необхідних для ідентифікації користувача під час доступу до системи. Ці записи також зберігають інформацію, пов’язану з авторизацією та обліком. У більшості випадків основними компонентами є ім'я користувача та пароль або альтернативний засіб аутентифікації, наприклад, біометричні дані.

З міркувань безпеки паролі або їх аналоги зазвичай зберігаються у зашифрованій або хешованій формі. Для посилення захищеності системи можуть застосовуватися додаткові методи аутентифікації, наприклад, спеціальні

секретні запитання з такими відповідями, які відомі лише користувачу. Самі запитання та відповіді на них теж стають частиною облікового запису.

Типи даних, що вносяться до облікового запису, визначаються адміністраторами системи. Обліковий запис може містити фотографії чи аватари користувача, а також зберігати різноманітну статистику щодо його активності. Наприклад, може враховуватися час останнього входу до системи, тривалість перебування в ній, IP-адреса пристрою, інтенсивність використання системи, загальна кількість або питома частка певних виконаних дій тощо.

Процес ідентифікації передбачає надання суб’єктом вхідної інформації про себе системі – такого як ім'я, обліковий номер або інші дані. Ідентифікація дозволяє визначити особу, яка намагається отримати доступ.

Аутентифікація додає наступний етап – підтвердження того, що суб’єкт є саме тією особою, за яку себе видає. Це відбувається шляхом надання додаткової інформації, яка підтверджує зв’язок з раніше введеною ідентифікуючою інформацією. Наприклад, під час введення імені користувача та пароля ім'я служить інструментом ідентифікації, тоді як пароль виконує роль аутентифікаційного елемента. Ввівши пароль, користувач доводить, що він є власником облікового запису, наданого в процесі ідентифікації.

Авторизація об'єкта доступу здійснюється після успішного завершення процесів ідентифікації та автентифікації. Під час авторизації операційна система виконує необхідні дії для введення об'єкта в роботу. Наприклад, у системах на кшталт UNIX цей процес передбачає створення операційної оболонки у вигляді нового процесу, який користувач зможе використовувати для подальшої роботи. Фактично, авторизація вирішує технічні аспекти запуску доступу уже підтвердженого та ідентифікованого суб'єкта.

Комплексна безпека інформаційної системи неможлива без належного регулювання доступу на рівні операційної системи. У зв’язку з цим вважаю за доцільне впровадження практики створення індивідуальних облікових записів для користувачів, а також забезпечення їх обов’язкової ідентифікації, автентифікації та наступної авторизації.

Оскільки у чинній інфраструктурі компанії відсутня система облікових записів та механізми для ідентифікації й автентифікації користувачів, пропоную запровадити такі заходи для підвищення рівня безпеки та захисту даних.

Таблиця 2.1 — Матриця доступу

Посада	Ресурс		
	База користувачів	Налаштування серверу	Повідомлення
Адміністратор	зчитування	Повний доступ	доступу немає
Директор	зчитування, запис (власні дані)	доступу немає	Зчитування, запис (власні дані)
Начальник відділу	зчитування, запис (власні дані)	доступу немає	Зчитування, запис (власні дані)
Бухгалтерія	запис (власні дані)	доступу немає	Зчитування, запис (власні дані)
Відділ планування	запис (власні дані)	доступу немає	Зчитування, запис (власні дані)

РОЗДІЛ 3
ПРАКТИЧНА ЧАСТИНА
РОЗРОБКА КРИПТОГРАФІЧНОГО ЗАХИСТУ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ В МЕРЕЖІ

Інформація в мережах має комерційну цінність.

Одним з найнадійніших способів захисту інформаційних ресурсів в інформаційно-комунікаційних системах є використання криптографічних засобів.

Для забезпечення конфіденційної передачі інформації сучасна криптографія дозволяє використовувати широкий спектр симетричних криптографічних алгоритмів. До типових симетричних алгоритмів, призначених для шифрування даних, належать DES, 3DES, IDEA, AES, Twofish, Blowfish і CAST-5 (CAST-128), які можуть використовуватися в таких режимах, як ECB, CBC, OFB і CFB, або окремо.

Типовою сферою застосування є передача даних. Проблемою, яка виникає під час передачі інформації, є надійність алгоритму.

Ця надійність визначається рядом критеріїв, таких як:

– довжина ключа,

– кількість раундів шифрування,

– довжина блоку відкритих даних,

– математична складність реалізації раунду шифрування.

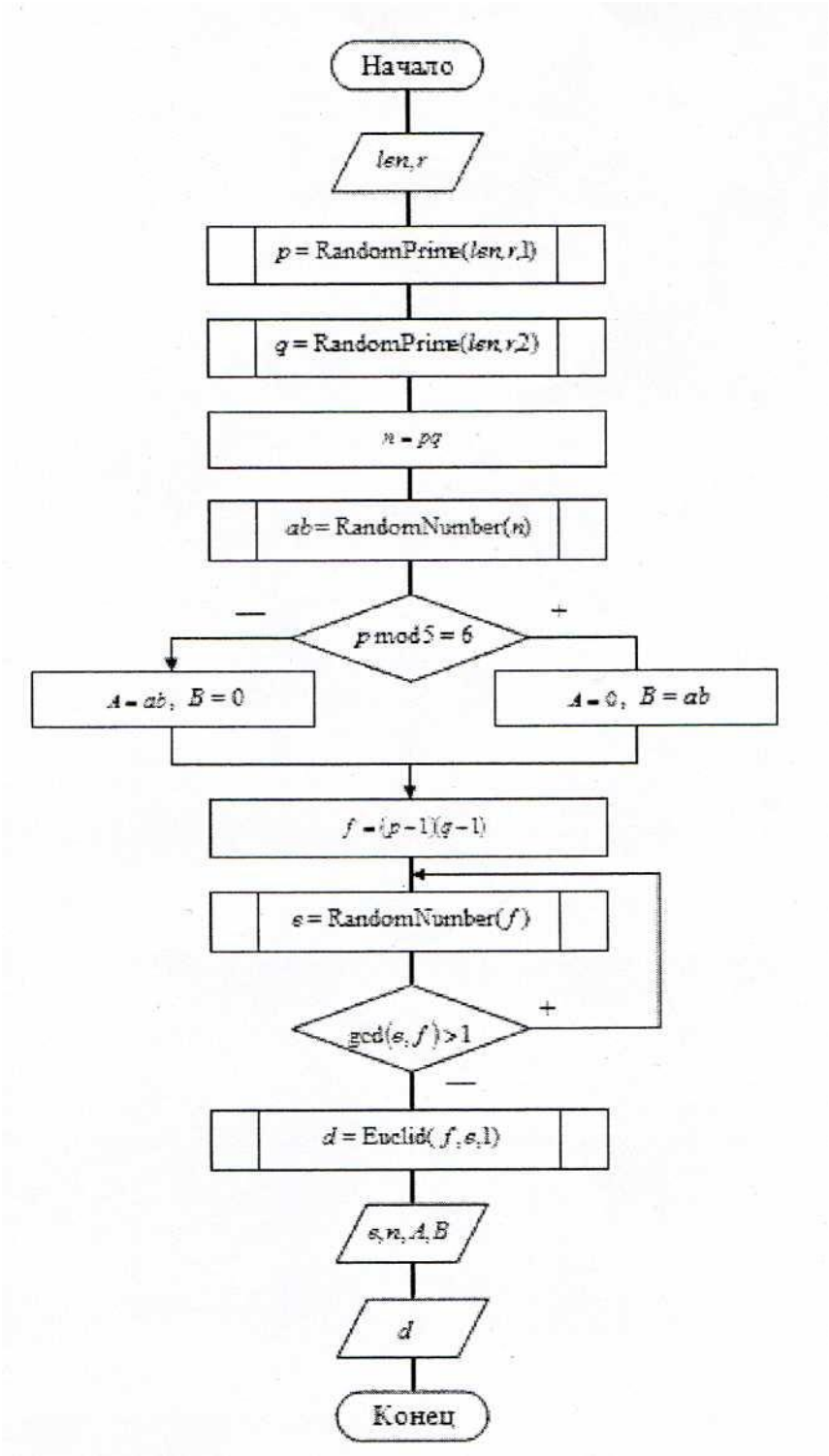

Рисунок 3.1 - Блок-схема RSA

Де *p* та *n* - закритий та відкритий ключ відповідно

3.1. Програмна реалізація

У магістерській роботі використовується мова програмування C#.

Для реалізації методу RSA задіяно два ключі: один призначений для шифрування даних, інший — для їх розшифрування. Спочатку необхідно передати приватний ключ одержувачу для виконання розшифрування (цей ключ залишається недоступним для сторонніх осіб). Після цього можна відкрито обмінюватися зашифрованим повідомленням разом із публічним ключем, який доступний усім. Приклад коду подано нижче.

Лістинг коду

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Mail;
using System.Net.Mime;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace Shif
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }

        /*Вивід*/
        private void button1_Click(object sender, EventArgs e)
        {
            //string url;
            //url = Convert.ToString(textBox2);
            /*
            FileStream stream = new FileStream("123" + ".txt", FileMode.Open);
            StreamReader reader = new StreamReader(stream);
            string str = reader.ReadToEnd();
            stream.Close();
            MessageBox.Show(str);
            */
            MessageBox.Show(textBox3.Text);
        }

        private void label1_Click(object sender, EventArgs e)
        {
```

```
}

private void richTextBox1_TextChanged(object sender, EventArgs e)
{

}

private void textBox2_TextChanged(object sender, EventArgs e)
{

}

private void button2_Click(object sender, EventArgs e)
{
    string a = Convert.ToString(textBox4.Text);
    if (a == "Ktg53^3ft*24f")
    {
        string startText = "";
        string outText = "";
        int i = 0;
        string gg = "";
        gg = textBox1.Text;
        int LONG = gg.Length;

        for (i = 0; i < LONG; i++)
        {
            if ((i % 2) != 0)
            {
                char ch = gg[i];
                int cod = (int)ch;
                int shifr = cod + 2;
                ch = (char)shifr;
                outText += ch.ToString();
            }
            if ((i % 2) == 0)
            {
                char ch = gg[i];
                int cod = (int)ch;
                int shifr = cod + 1;
                ch = (char)shifr;
                outText += ch.ToString();
            }
        }
        textBox2.Text = outText;
    }
    else
    {
        MessageBox.Show("Код зашифровки невірний");
    }

}

private void textBox3_TextChanged(object sender, EventArgs e)
{

}

private void button4_Click(object sender, EventArgs e)
{
    string a = Convert.ToString(textBox5.Text);
    if (a == "FvregHwEki$23G46")
```

```
    {
        string startText = "";
        string outText = "";
        int i = 0;
        string gg = "";
        gg = textBox2.Text;
        int LONG = gg.Length;

        for (i = 0; i < LONG; i++)
        {
            if ((i % 2) != 0)
            {
                char ch = gg[i];
                int cod = (int)ch;
                int shifr = cod - 2;
                ch = (char)shifr;
                outText += ch.ToString();
            }
            if ((i % 2) == 0)
            {
                char ch = gg[i];
                int cod = (int)ch;
                int shifr = cod - 1;
                ch = (char)shifr;
                outText += ch.ToString();
            }
        }
        textBox3.Text = outText;
    }
    else
    {
        MessageBox.Show("Код розшифровки невірний");
    }

}

private void button3_Click_1(object sender, EventArgs e)
{
    using (var sr = new StreamReader(@"123.txt"))
    {
        var str = sr.ReadToEnd();
        textBox1.Text = str.ToString();
    }
}

private void button5_Click(object sender, EventArgs e)
{
    try
    {
        SaveFileDialog saveFileDialog1 = new SaveFileDialog();
        saveFileDialog1.Filter = "Datafeed File|*.txt";
        saveFileDialog1.Title = "Select a txt";

        if (saveFileDialog1.ShowDialog() == DialogResult.Cancel)
            return;
        // отримуємо обраний файл
        string filename = saveFileDialog1.FileName;
        // збереження тексту в файл
        System.IO.File.WriteAllText(filename, textBox1.Text);
        MessageBox.Show("Файл збережено");
    }
```

```
    catch
    {
        MessageBox.Show("Файл не вибрано");
    }

}

private void button6_Click(object sender, EventArgs e)
{
    try
    {
        SaveFileDialog saveFileDialog1 = new SaveFileDialog();
        saveFileDialog1.Filter = "Datafeed File|*.txt";
        saveFileDialog1.Title = "Select a txt";

        if (saveFileDialog1.ShowDialog() == DialogResult.Cancel)
            return;
        // отримуємо обраний файл
        string filename = saveFileDialog1.FileName;
        // збереження тексту в файл
        System.IO.File.WriteAllText(filename, textBox2.Text);
        MessageBox.Show("Файл збережено");
    }
    catch
    {
        MessageBox.Show("Файл не вибрано");
    }

}

private void button7_Click(object sender, EventArgs e)
{
    try
    {
        SaveFileDialog saveFileDialog1 = new SaveFileDialog();
        saveFileDialog1.Filter = "Datafeed File|*.txt";
        saveFileDialog1.Title = "Select a txt";

        if (saveFileDialog1.ShowDialog() == DialogResult.Cancel)
            return;
        // отримуємо обраний файл
        string filename = saveFileDialog1.FileName;
        // збереження тексту в файл
        System.IO.File.WriteAllText(filename, textBox3.Text);
        MessageBox.Show("Файл збережено");
    }
    catch
    {
        MessageBox.Show("Файл не вибрано");
    }

}

private void button8_Click(object sender, EventArgs e)
{
    try
    {
        string name = "";
        OpenFileDialog openFileDialog1 = new OpenFileDialog();
        openFileDialog1.Filter = "Datafeed File|*.txt";
        openFileDialog1.Title = "Select a txt";
```

```
                if (openFileDialog1.ShowDialog() ==
System.Windows.Forms.DialogResult.OK)
                {
                    name = openFileDialog1.FileName;
                }
                textBox1.Text = File.ReadAllText(@name, Encoding.GetEncoding(65001));
            }
            catch
            {
                MessageBox.Show("Файл не вибрано");
            }

        }

        private void button9_Click(object sender, EventArgs e)
        {
            try
            {
                string name = "";
                OpenFileDialog openFileDialog1 = new OpenFileDialog();
                openFileDialog1.Filter = "Datafeed File|*.txt";
                openFileDialog1.Title = "Select a txt";

                if (openFileDialog1.ShowDialog() ==
System.Windows.Forms.DialogResult.OK)
                {
                    name = openFileDialog1.FileName;
                }
                textBox2.Text = File.ReadAllText(@name, Encoding.GetEncoding(65001));
            }
            catch
            {
                MessageBox.Show("Файл не вибрано");
            }

        }

        private void button10_Click(object sender, EventArgs e)
        {
            try
            {
                string name = "";
                OpenFileDialog openFileDialog1 = new OpenFileDialog();
                openFileDialog1.Filter = "Datafeed File|*.txt";
                openFileDialog1.Title = "Select a txt";

                if (openFileDialog1.ShowDialog() ==
System.Windows.Forms.DialogResult.OK)
                {
                    name = openFileDialog1.FileName;
                }
                textBox3.Text = File.ReadAllText(@name, Encoding.GetEncoding(65001));
            }
            catch
            {
                MessageBox.Show("Файл не вибрано");
            }

        }
```

```
        private void Form1_Load(object sender, EventArgs e)
        {

        }

        private void textBox4_TextChanged(object sender, EventArgs e)
        {

        }

        private void button11_Click(object sender, EventArgs e)
        {
            string a = Convert.ToString(textBox4.Text);
            string b = Convert.ToString(textBox5.Text);
            if (a == "1002" || b == "2001")
            {
                Form2 f2 = new Form2();
                f2.Show();
            }
            else
            {
                MessageBox.Show("Невірно введено коди");
            }
        }

        private void textBox5_TextChanged(object sender, EventArgs e)
        {

        }

    }
}
```

Демонстрація роботи

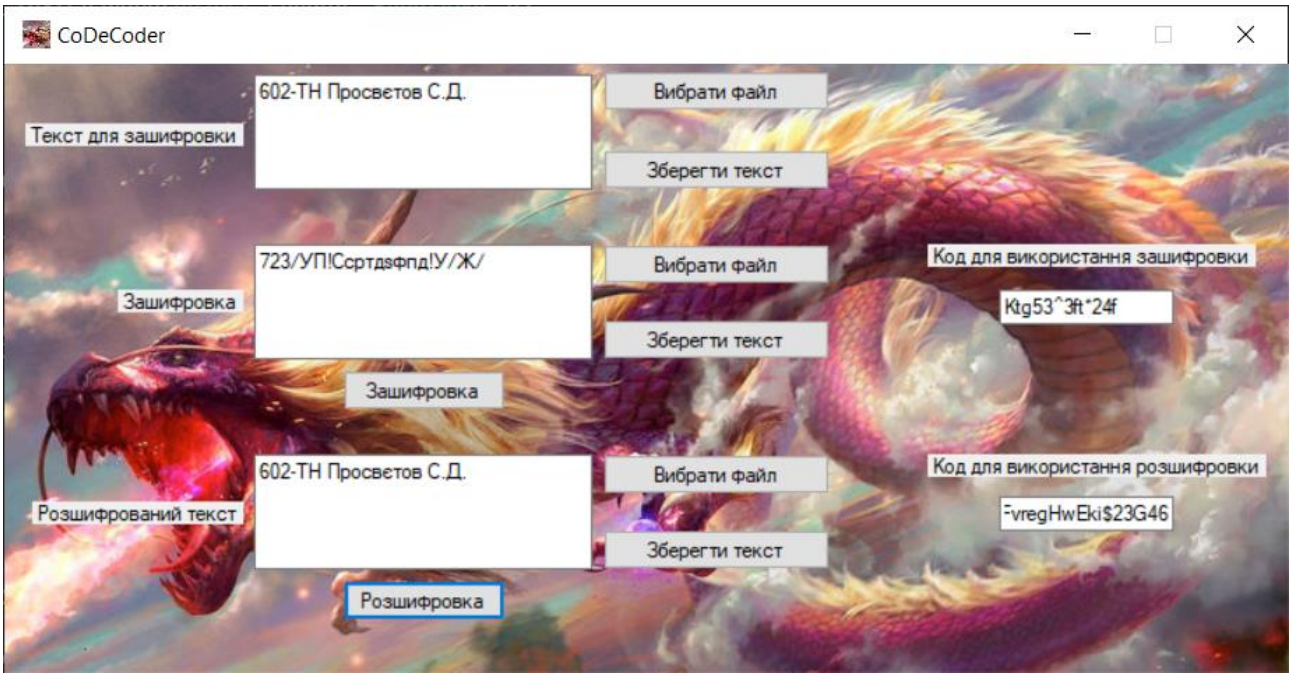

Рисунок 3.2 - Зашифрування та розшифрування тексту

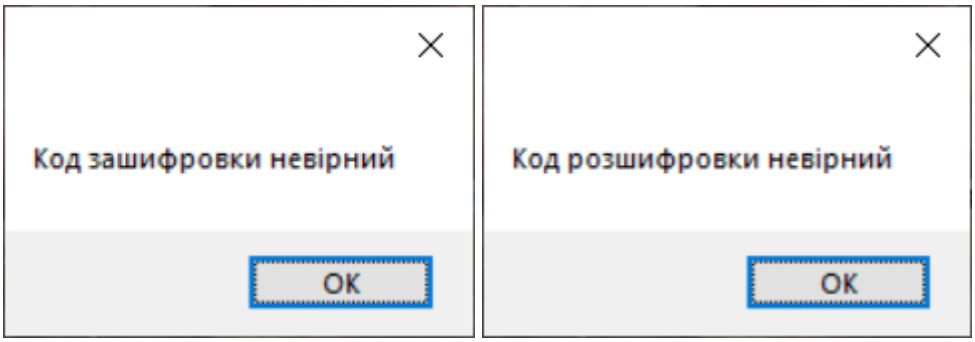

Рисунок 3.3 - Повідомлення при введенні невірного коду зашифровки та розшифровки відповідно

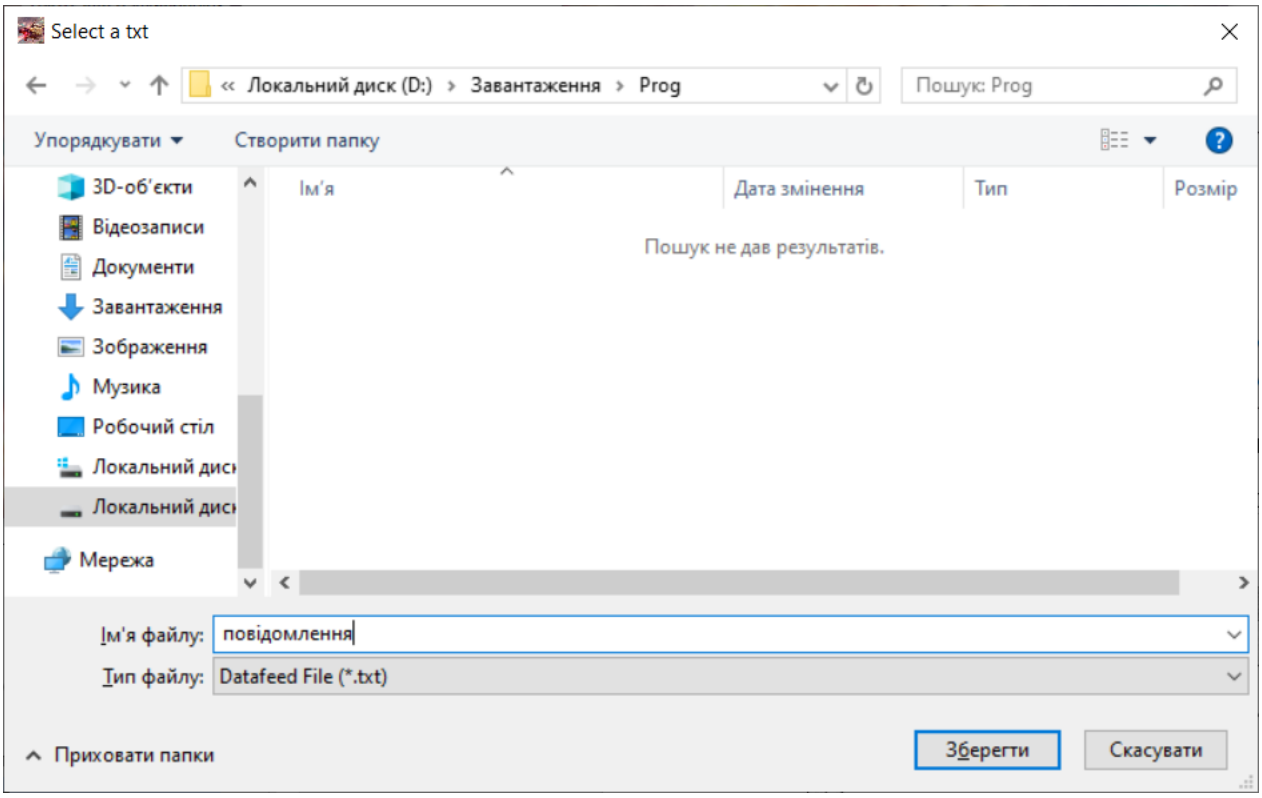

Рисунок 3.4- Завантаження зашифрованого повідомлення

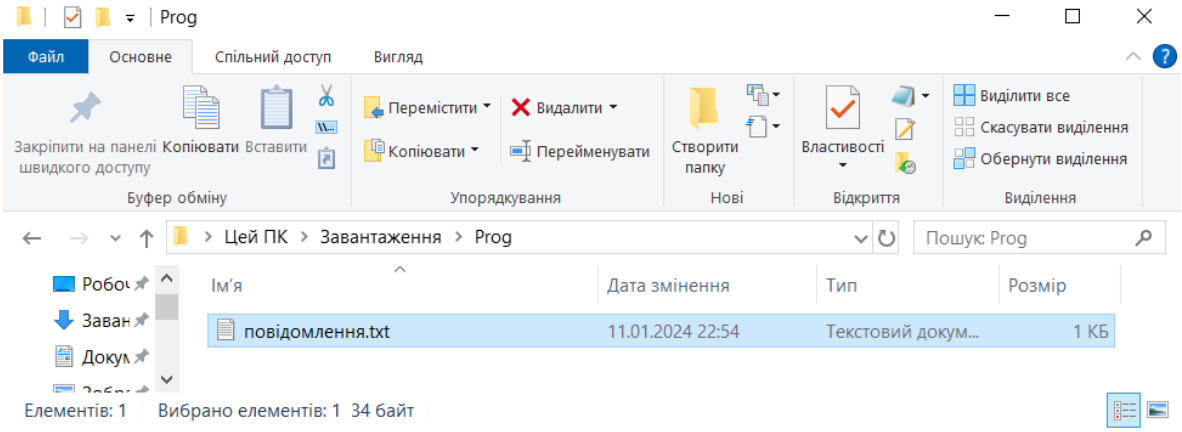

Рисунок 3.5 - Збережений файл з зашифрованим повідомленням

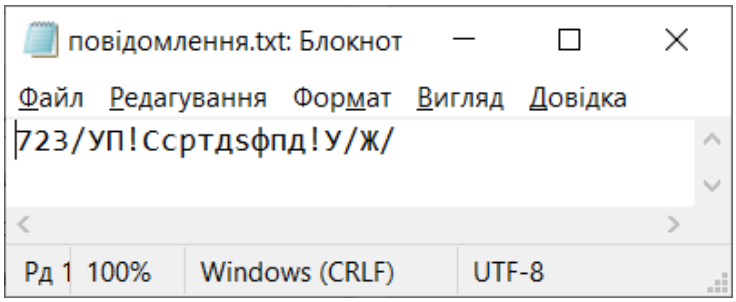

Рисунок 3.6 - Відкриття зашифрованого повідомлення

Аналогічно можна завантажити розшифроване повідомлення.

Також програма дає можливість розшифровувати повідомлення що були надані користувачу у форматі .txt:

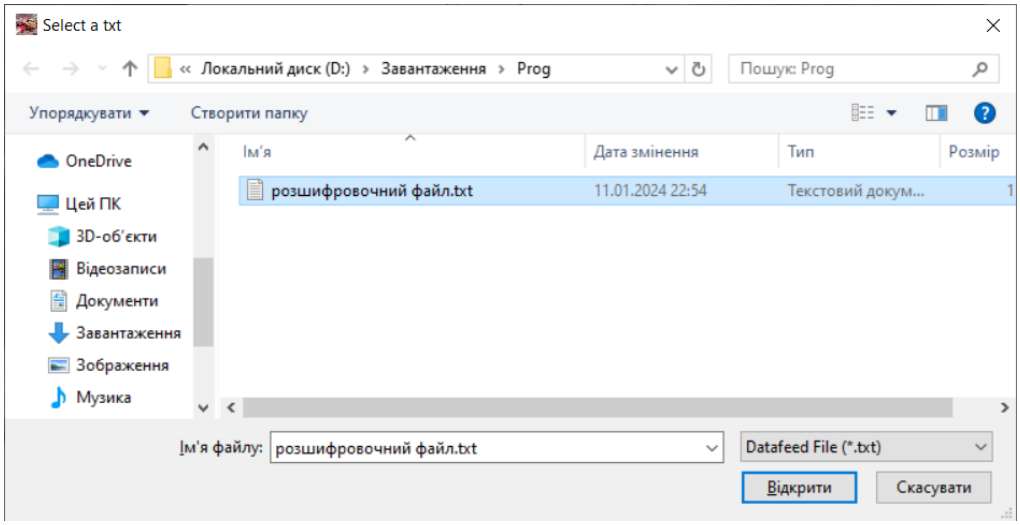

Рисунок 3.7 -. Обираю файл для розшифровки обираючи кнопку «Вибрати файл»

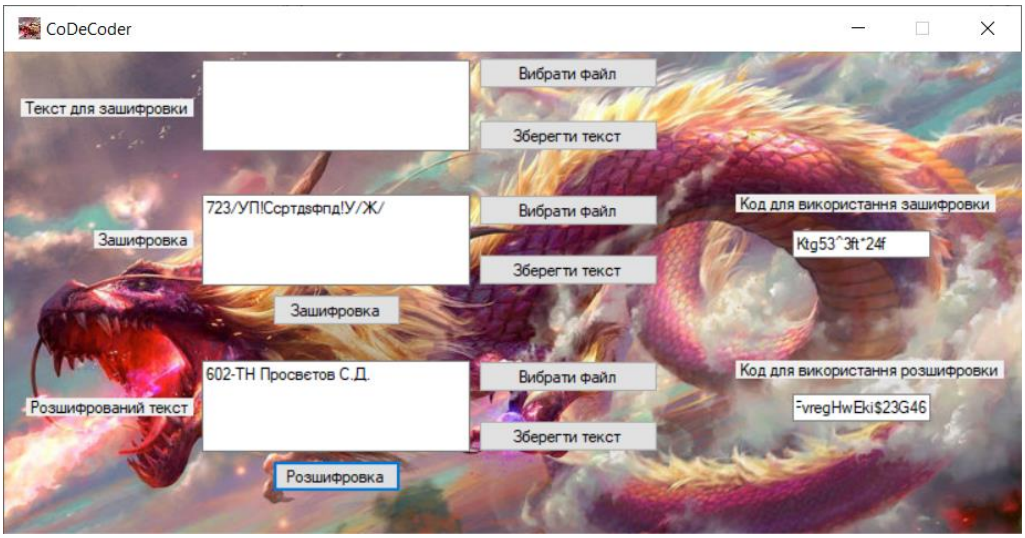

Рисунок 3.8 - Результат розшифрування обреного файлу

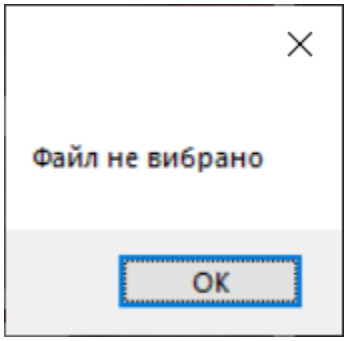

Рисунок 3.9 - Якщо не обрати файл для розшифровки видасться повідомлення про це та можна буде ще раз спробувати обрати файл при необхідності

ВИСНОВКИ

У ході виконання магістерської кваліфікаційної роботи було досліжено стан запровадження заходів кібербезпеки на базі підприємства «Компанія ГОТ».

Розроблено рекомендації щодо вдосконалення систем захисту інформації при передачі даних та повідомлень та створено програмний додаток для захисту передачі даних з використанням алгоритму шифрування RSA та одноалфавітної заміни.

При розробці системи інформаційної безпеки у вигляді програмного продукту використовувалась мова програмування C# та технологія інтерфейсного відображення Windows Presentation Foundation.

Програмний додаток повністю відповідає всім вимогам, поставленим на етапі постановки задачі, та готовий до експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Організація процесу захисту інформаційних ресурсів та баз даних інформаційно-комунікаційних систем та мереж. URL: https://studfile.net/preview/5201996/ (дата звернення: 08.12.2023)

2. Закон України від 02.10.92 N 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 09.12.2023)

3. ЗАКОН УКРАЇНИ №2432-VI. URL: https://www.president.gov.ua/documents/2432-vi-11735 (дата звернення: 10.12.2023)

4. Інформаційна загроза. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0 (дата звернення: 11.12.2023)

5. Інформаційна загроза.URL: https://www.wikidata.uk-ua.nina.az/%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0_(%D0%86%D0%A2).html (дата звернення: 11.12.2023)

6. Критерії оцінки захищеності комп'ютерної системи . URL: https://www.wikidata.uk-ua.nina.az/Trusted_Computer_System_Evaluation_Criteria.html (дата звернення: 11.12.2023)

7. Інформаційна безпека. URL: https://magschool.dnepredu.com/uk/site/informatsiina-bezpeka.html (дата звернення: 11.12.2023)

8. Проблеми забезпечення безпеки в комп'ютерних системах і мережах. URL: https://sites.google.com/view/rudavska/%D1%83%D1%80%D0%BE%D0%BA%D0%B8/11-%D0%BA%D0%BB%D0%B0%D1%81/%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0-

%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0/11-%D1%83%D1%80%D0%BE%D0%BA (дата звернення: 12.12.2023)

9. Дослідження методів кодування в електронних системах передачі інформації. URL: https://openarchive.nure.ua/server/api/core/bitstreams/3e60caeb-ff90-4cec-ad38-098447d8069a/content (дата звернення: 12.12.2023)

10. Потокові шифри. URL: https://ami.lnu.edu.ua/wp-content/uploads/2022/06/Cryptology3.pdf (дата звернення: 12.12.2023)

11. Класифікація криптоалгоритмів. URL: https://wiki.tntu.edu.ua/%D0%9A%D0%BB%D0%B0%D1%81%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D1%96%D0%B2 (дата звернення: 12.12.2023)

12. Захист інформаційних ресурсів. URL: https://vfranchuk.fi.npu.edu.ua/images/files/statty/32_ZIR_cript.pdf (дата звернення: 14.12.2023)

13. Мета й застосування шифрування інформації. Класичні методи шифрування. URL: https://alextexnok.blogspot.com/p/lida-15.html (дата звернення: 14.12.2023)

14. Симетричне шифрування.URL: https://docplayer.net/46229330-Suchasni-informaciyno-telekomunikaciyni-tehnologiyi.html (дата звернення: 14.12.2023)

15. Асиметричні криптосистеми. URL: https://studfile.net/preview/3760006/page:2/ (дата звернення: 15.12.2023)

16. Цифровий підпис. URL:https://studfile.net/preview/3760006/page:3/ (дата звернення: 17.12.2023)