Оглавление

[ВСТУП](#_Toc515943946) 4

[1. ОСНОВНА ЧАСТИНА](#_Toc515943947) 6

[1.1 Загальна характеристика підприємства](#_Toc515943948) 6

[1.2. Опис інформаційних ресурсів](#_Toc515943949) 8

[1.3 Організація інформаційної безпеки на підприємстві](#_Toc515943950) 9

[2. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ](#_Toc515943951) 10

[2.1 Аналіз політики підприємства в галузі інформаційної безпеки](#_Toc515943952) 10

[2.2. Організація систем безпеки](#_Toc515943953) 11

[2.3 Класифікація активів](#_Toc515943954) 18

[2.4. Безпека та персонал](#_Toc515943955) 20

[2.5 Фізична та зовнішня безпека](#_Toc515943956) 20

[2.6 Менеджмент комп’ютерів та мереж](#_Toc515943957) 21

[2.7. Керування доступом до системи](#_Toc515943958) 21

[2.8. Відповідність системи вимогам стандарту](#_Toc515943959) 27

[3. РУЗУЛЬТАТИ АУДИТА СИСТЕМИ, ДОКУМЕНТ «КОНТРОЛЬНИЙ СПИСОК АУДИТУ»](#_Toc515943960) 29

[4. АНАЛІЗ ПРОГРАМНИХ РЕАЛІХАЦІЙ ТА РАЗРОБКА ЗАСОБІВ НЕСАНКЦІОНОВАНОГО АНАЛІЗУ ПРОГРАМ ТА ДАНИХ](#_Toc515944180) 38

[4.1 Метод експерименту](#_Toc515944181) 38

[4.2 Статичний аналіз](#_Toc515944182) 43

[4.3 Динамічний аналіз](#_Toc515944183) 46

[5. РЕКОМЕНДАЦІЇ АУДИТУ З ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ](#_Toc515944184) 50

[ВИСНОВКИ](#_Toc515944185) 51

Додаток А…………………………………………………………………………..

Досліджуваний продукт………………………………………………………….  
Лістинг програми………………………………………………………………53

ТЕХНІЧНЕ ЗАВДАННЯ………………………………………………………60

### ВСТУП

В даний момент захист інформації є одним з важливих галузей в комп'ютерному співтовариство тому що за останній час в Україні збільшилася кількість кібератак. Проведення і використання аудиту інформаційної безпеки допоможе зменшити ймовірність успішно виконаних кібератак хакерами. Кібербезпека останнім часом все більше розвивається і сприяє цьому як поліпшена програма підготовки так і удосконалення технологій якими користуються системні адміністратори візьмемо наприклад Windows PowerShell, який за допомогою свого функціоналу допомагає сисадмінам виконувати більше обсягу роботи використовуючи при цьому меншу кількість програмних засобів.

На даний момент існує три основні методи, які дозволяють досліджувати програмні реалізації. Це статичний, динамічний і метод експериментів. З цих методів динамічний є найоптимальнішим, тому що з його допомогою з найбільшою ймовірністю можна визначити алгоритм програм і знайти найбільш вразливі місця для злому системи кіберзлочинцями. Так само динамічний метод містить в собі методики вивчення програм, для більш оптимального використання цього методу. На практиці для складних систем рідко застосовується якийсь один метод, зазвичай для більш кращого дослідження системи методи комбінуються, в залежності від досягнення поставленого результату для різних цілей. Кожен метод є по своєму унікальним, що містить в собі свої методики оцінки і дослідження системи для виявлення вразливих місць.

Метод експериментів.

Розрізняють два варіанти завдання:

1) вхід на автомат є випадковим, і його можна тільки спостерігати;

2) дослідник може на свій розсуд ставити вхід автомата і спостерігати вихід (метод прозванювання).

Метод експериментів з «чорним ящиком» зводиться до проведення за певною методикою багаторазових експериментів (наприклад, по зашифрування різних текстів на різних ключах за допомогою аналізованої системи криптографічного захисту) і порівняльного аналізу отриманих результатів (наприклад, шифртекст).

### ОСНОВНА ЧАСТИНА

### 1.1 Загальна характеристика підприємства

Для початку необхідно визначити структуру самого підприємства, в даному випадку - комерційної фірми по ремонту комп'ютерної техніки Smart-service. Вона схематично представлена ​​на рисунку 1.1.

Директор

Заст. директора

Бухгалтер

Технічний відділ

Відділ по роботі з клієнтами

Рисунок 1.1 - Структурна схема комерційної фірми по ремонту комп'ютерної техніки Smart-service.

Виходячи з вищевказаної схеми складена структурна схема обчислювальної мережі фірми. Вона представлена ​​на рисунку 1.2.





















Интернет

Рисунок 1.2 - Структурна схема мережі комерційної фірми по ремонту комп'ютерної техніки Smart-service.

З даної структурної схеми видно, що мережа комерційної фірми по ремонту комп'ютерної техніки Smart-service побудована за схемою базової топології комп'ютерної мережі - «зірка».

Особливістю «зірки» є те, що для функціонування локальної мережі такої топології потрібно додатковий пристрій - концентратор. При виході концентратора з ладу відбувається зупинка в роботі частини мережі.

При розробці політики безпеки можна використовувати наступну модель малюнок 1.3, засновану на адаптації Загальних Критеріїв (ISO 15408) і проведенні аналізу ризику (ISO 17799).



Рисунок 1.3 - Модель побудови корпоративної системи захисту інформації

### 1.2. Опис інформаційних ресурсів

Локальна обчислювальна мережа комерційної фірми по ремонту комп'ютерної техніки Smart-service, охоплює 4 приміщення. Кабінет директора, заст. директора, бухгалтерія, відділу по роботі з клієнтами та технічного відділу. У мережі присутній 3 комутатора, 1 маршрутизатор, 1 сервер. У кожному кабінеті є МФУ. Правила доступу до мережі визначаються адміністратором.

Так само в представленій локальної обчислювальної мережі є вихід в Інтернет. Інформаційний ресурс - це масив даних, складений і відсортованого за нікому ознакою, роду інформації, який має строгу структуру. До інформаційних ресурсів відносять:

− мережеві ресурси;

− друковані видання;

− видання на компакт-дисках.

### 1.3 Організація інформаційної безпеки на підприємстві

Оцінка ризиків для комерційної фірми по ремонту комп'ютерної техніки Smart-service проводилася за допомогою демоверсії ПО «Гриф».

Ця версія програми підтримує можливість аналізу ризиків двома методами.

1. Метод аналізу моделі інформаційних потоків. Оцінює ризик кожного виду цінної інформації на ресурсах.

2. Метод аналізу моделі загроз і вразливостей. Оцінює ризик кожного ресурсу з цінною інформацією.

Приклад аналізу ризиків для комерційної фірми по ремонту комп'ютерної техніки Smart-service представлений в додатку А.

### АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

### 2.1 Аналіз політики підприємства в галузі інформаційної безпеки

Аналіз стану справ у сфері захисту інформації показує, що вже склалася цілком сформована концепція і структура захисту, основу якої складають:

вельми розвинений арсенал технічних засобів захисту інформації, вироблених на промисловій основі;

значне число фірм, що спеціалізуються на вирішенні питань захисту інформації;

досить чітко окреслена система поглядів на цю проблему;

наявність значного практичного досвіду та ін.

І, тим не менш, як свідчить вітчизняна і зарубіжна преса, злочинні дії над інформацією не тільки не зменшуються, але і мають досить стійку тенденцію до зростання. Досвід показує, що для боротьби з цією тенденцією необхідна злагоджена й цілеспрямована організація процесу захисту інформаційних ресурсів. Причому в цьому повинні брати активну участь професійні фахівці, адміністрація, співробітники і користувачі, що і визначає підвищену значимість організаційної сторони питання.

Досвід також показує, що:

забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення та розвитку системи захисту, безперервному контролі її стану, виявленні її вузьких і слабких місць і протиправних дій;

безпеку інформації може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту у всіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі використовувані засоби, методи і заходи об'єднуються в єдиний цілісний механізм - систему захисту інформації (СЗІ). При цьому функціонування системи має контролюватися, оновлюватися і доповнюватися в залежності від зміни зовнішніх і внутрішніх умов;

Ніяка СЗІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і дотримання ними всіх встановлених правил, спрямованих на її захист.

З урахуванням накопиченого досвіду можна визначити систему захисту інформації як організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

З позицій системного підходу до захисту інформації пред'являються певні вимоги. Захист інформації повинна бути:

безперервної. Ця вимога випливає з того, що зловмисники тільки і шукають можливість, як би обійти захист їх цікавить;

планової. Планування здійснюється шляхом розробки кожною службою детальних планів захисту інформації в сфері її компетенції з урахуванням загальної мети підприємства (організації);

цілеспрямованої. Захищається то, що має захищатися в інтересах конкретної мети, а не все підряд;  
 конкретною. Захисту підлягають конкретні дані, об'єктивно що підлягають охороні, втрата яких може заподіяти організації певної шкоди; активною. Захищати інформацію необхідно з достатнім ступенем наполегливості; надійної. Методи і форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до охоронюваним секретів, незалежно від форми їх подання, мови вираження і виду фізичного носія, на якому вони закріплені;  
 універсальної. Вважається, що в залежності від виду каналу витоку або способу несанкціонованого доступу його необхідно перекривати, де б він не виявився, розумними і достатніми засобами, незалежно від характеру, форми і види інформації;

комплексною. Для захисту інформації у всьому різноманітті структурних елементів повинні застосовуватися всі види і форми захисту в повному обсязі. Неприпустимо застосовувати лише окремі форми або технічні засоби.

Комплексний характер захисту виникає з того, що захист - це специфічне явище, що представляє собою складну систему нерозривно взаємопов'язаних і взаємозалежних процесів, кожен з яких в свою чергу має безліч різних взаємообслуговуючих один одного сторін, властивостей, тенденцій.

Зарубіжний і вітчизняний досвід показує, що для забезпечення виконання настільки багатогранних вимог безпеки система захисту інформації повинна відповідати певним умовам:

охоплювати весь технологічний комплекс інформаційної діяльності;

бути різноманітною по використовуваних засобів, багаторівневої з ієрархічною послідовністю доступу;

бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;

бути нестандартною, різноманітною. При виборі засобів захисту не можна розраховувати на непоінформованість зловмисників щодо її можливостей;

бути простою для технічного обслуговування і зручною для експлуатації користувачами;

бути надійною. Будь-які поломки технічних засобів є причиною появи неконтрольованих каналів витоку інформації;

бути комплексною, володіти цілісністю, що означає, що жодна її частина не може бути вилучена без шкоди для всієї системи. До системи безпеки інформації пред'являються також певні вимоги:

чіткість визначення повноваженні і прав користувачів на доступ до певних видів інформації;

надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;

зведення до мінімуму числа загальних для декількох користувачів засобів захисту;

облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;

забезпечення оцінки ступеня конфіденційної інформації;

забезпечення контролю цілісності засобів захисту і негайне реагування на їх вихід з ладу. Система захисту інформації як будь-яка система повинна мати певні види власного забезпечення, спираючись на які вона буде виконувати свою цільову функцію. З огляду на це СЗІ може мати:

правове забезпечення. Сюди входять нормативні документи, положення, інструкції, керівництва, вимоги яких є обов'язковими в рамках сфери їх дій;

організаційне забезпечення. Мається на увазі, що реалізація захисту інформації здійснюється певними структурними одиницями - такими, як служба захисту документів; служба режиму, допуску, охорони; служба захисту інформації технічними засобами; інформаційно-аналітична діяльність та ін .;

апаратне забезпечення. Передбачається широке використання технічних засобів, як для захисту інформації, так і для забезпечення діяльності власне СЗІ;

інформаційне забезпечення. Воно включає в себе відомості, дані, показники, параметри, що лежать в основі рішення задач, що забезпечують функціонування системи.

Сюди можуть входити як показники доступу, обліку, зберігання, так і системи інформаційного забезпечення розрахункових завдань різного характеру, пов'язаних з діяльністю служби забезпечення безпеки;

програмне забезпечення. До нього відносяться різні інформаційні, облікові, статистичні і розрахункові програми, що забезпечують оцінку наявності та небезпеки різних каналів витоку і шляхів несанкціонованого проникнення до джерел конфі-денціальной інформації;

математичне забезпечення. Передбачає використання математичних методів для різних розрахунків, пов'язаних з оцінкою небезпеки технічних засобів зловмисників, зон і норм необхідного захисту;

лінгвістичне забезпечення. Сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері захисту інформації;

нормативно-методичне забезпечення. Сюди входять норми і регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації, різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації.

задовольнити сучасні вимоги щодо забезпечення безпеки підприємства та захисту його конфіденційної інформації може тільки система безпеки. Під системою безпеки будемо розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз.

Як і будь-яка система, система інформаційної безпеки має свої цілі, завдання, методи і засоби діяльності, які узгоджуються за місцем і часу в залежності від умов.

### 2.2. Організація систем безпеки

Елементи і функції системи безпеки

Безпека вашої організації, компанії, офісу, виробничого чи іншого приміщення забезпечується цілим комплексом заходів. До важливої ​​складової виявлення загроз і їх нейтралізації відносяться системи безпеки. Вони необхідні на будь-якому комерційному об'єкті, а в особливості на заводах і промислових підприємствах, в банках і фінансових організаціях, в торгових точках, в освітніх, медичних і державних установах, в телекомунікаційних, енергетичних і нафтогазових компаніях. Системи безпеки забезпечують стабільність роботи організації, виконуючи різні функції захисту і контролю.

Для чого вони потрібні і з якими завданнями справляються?

В першу чергу - це охорона організації від зовнішнім та внутрішнім загрозам таких, як:

спроба розкрадання майна або комерційної таємниці;

підрив діловій репутації компанії;

перехоплення управління;

матеріальна шкода;

виникнення пожежі, аварії та інших небезпечних для життя і здоров'я людей ситуацій.

Саме системи безпеки здатні впоратися з попередженням подібних загроз, забезпечуючи контроль доступу на територію підприємства і об'єкти, що охороняються, моніторинг ситуації в режимі реального часу і прийняття термінових заходів у разі виникнення надзвичайних ситуацій.

Основні системи безпеки

Для забезпечення повної безпеки в організаціях встановлюються системи контролю доступу та сканери безпеки, системи сигналізації та відеоспостереження, системи протипожежного захисту, а також застосовуються інші методи.

Системи контролю доступу

Контроль доступу - це перше, про що повинна подбати будь-яке підприємство. Незалежно від величини вашої об'єкта, ви можете скоротити витрати на звичайну охорону, встановивши сучасну систему контролю доступу. Обмежувати доступ можна як в цілому на об'єкт, так і в окремі його приміщення (наприклад, в сейфи), а також на паркування. Для цього, згідно ГОСТ Р 51241-2008, використовуються:

Огороджуючи пристрої (шлагбауми, турнікети, дорожні блокіратори, шлюзові кабіни і т.д.);

Пропускна система або пристрої введення ідентифікаційних ознак (в тому числі - системи розпізнавання номерів автомобілів, управління пересування транспортних засобів і 3D-розпізнавання осіб);

Пристрій управління, захищене від несанкціонованого доступу.

Система контролю доступу особливо необхідна в фінансових організаціях, банках, навчальних та державних установах, на підприємствах, на режимних і військових об'єктах. Зчитувачами і пристроями, що необхідно обладнати головні і службові входи, КПП, приміщення, в яких зберігаються матеріальні цінності і де працює керівництво. При цьому загальний допуск в будівлю може здійснюватися за однією ознакою, а доступ в інші зони (сейфи, сховища і т.д.) - як мінімум за двома ознаками.

У місцях великого скупчення людей також застосовуються скануючі пристрої - наприклад, сканери безпеки Safety System. Це обладнання, яке дозволяє прискорити процес огляду великої кількості людей на вокзалах, в аеропортах, у великих торгових центрах, на масових заходах.

Сучасні технології ефективно використовувати і на платних або закритих парковках. Для цього застосовується, в тому числі, обладнання з моніторингу вільних місць і платіжні системи.

Провідними світовими виробниками систем контролю доступу та окремих напрямків в області біометричного контролю вважаються Apollo, Assa Abloy, Artec Group, Cognitech, Bosch Security AG, Nedap AVI, Siemens, Schneider Electric, Honeywell Security і інші.

Системи відеоспостереження

Системи відеоспостереження або охоронного телебачення дозволяють стежити за різними об'єктами і територіями. Відеоспостереження ефективно і в контролі багатоповерхових приміщень, адміністративних будівель, і на великих виробничих площах до 300 тисяч кв. м. Крім того, вони допомагають відслідковувати прилеглі території. Головне завдання таких систем - контроль ситуації. У разі отримання тривоги саме відеоспостереження дозволяє визначити характер і місце порушення і прийняти оптимальні заходи.

Особливо актуальні системи відеоспостереження в банках, пунктах обміну валют і інших фінансових організаціях, а також в ювелірних і збройових магазинах.

До складу системи охоронного телебачення, згідно з ГОСТ Р 51558-2000, повинні входити:

Телевізійна камера;

Відеомонітор;

Джерело електроживлення;

Лінія передачі.

На деяких системах можуть бути додаткові функції (наприклад, датчики руху).

Системи відеоспостереження обов'язково розміщуються у головного і службового входів, на КПП, на периметрі території, в приміщеннях, де зберігаються матеріальні цінності і в коридорах, за якими відбувається переміщення матеріальних цінностей.

О камерах, розміщених в різних точках, пред'являються свої вимоги. Так, наприклад, камери на вулицях повинні мати герметичні термокожухи, козирки, які захищають від сонця, і повинні бути поставлені так, щоб промені сонця не потрапляли в об'єктив. Провідні зарубіжні компанії, що займаються виготовленням систем відеоспостереження, - Axis Communications, Dallmeier Electronics AG, Bosch Security AG, Schneider Electric, Samsung, ISS, ITV, Milestone і інші.  
Системи сигналізації Існують різні види систем сигналізації. До них відносяться, зокрема:

Охоронна сигналізація Говорячи про сигналізації, найчастіше мають на увазі саме охоронну сигналізацію, яка використовується для захисту периметра територій і відкритих майданчиків, будівель, приміщень, окремих предметів.

Сигналізація для маломобільних груп населення Необхідність створення сигналізації для маломобільних груп населення у всіх адміністративних та громадських будівлях. Системи сигналізації та зв'язку для МГН створюються на базі обладнання відомих виробників - Zenitel, Intercall.

Автоматична пожежна сигналізація

Основне завдання пожежної сигналізації - виявлення загоряння і сповіщення про небезпеку. Існують різні типи сповіщувачів: димові, полум'я, теплові, диференціальні, аспіраційні. Їх вибір залежить від виникнення передбачуваної загрози. Відповідно, кожен з них буде спрацьовувати при появі характерної ознаки: перевищення граничного значення температури, поява газу, диму або відкритого полум'я. Для підвищення точності і надійності визначення небезпечного фактора рекомендується використовувати комбіновані (або мультикритериальних) пожежні сповіщувачі.

Системи оповіщення при пожежі і системи пожежогасіння

Головне завдання будь-якої системи оповіщення - оперативно інформувати людей про виниклу нештатної ситуації і здійснювати координацію їх дій по виконанню евакуації з небезпечного об'єкта. Це може бути подача звукових та / або світлових сигналів і трансляція мовної інформації про характер небезпеки і шляхах евакуації. Протягом всього часу евакуації повинно працювати аварійне освітлення.

### 2.3 Класифікація активів

За складом і функціональної ролі (характеру використання) майно організації поділяють на дві групи: необоротні та оборотні активи.

Необоротні активи включають в себе: основні засоби; дохідні вкладення в матеріальні цінності; нематеріальні активи; устаткування щодо встановлення; вкладення у необоротні активи.

Оборотні активи включають: запаси і витрати; податки за придбаними товарами, роботами, послугами; дебіторська заборгованість; розрахунки з засновниками; грошові кошти; фінансові вкладення.  
 Прибуткові вкладення в матеріальні цінності - це матеріальні цінності, що здаються в оренду, придбані для передачі в лізинг, а також предмети прокату. Дані матеріальні цінності враховуються на рахунку 03 «Прибуткові вкладення в матеріальні цінності» за первісною вартістю. Нематеріальні активи - це об'єкти довгострокового користування, що не мають фізичної основи, але мають вартісною оцінкою і приносять дохід організації. До них відносяться права (виключні і невиключні на використання об'єктів інтелектуальної власності).

Ліцензія - це дозвіл, що видається компетентними державними органами на здійснення юридичними особами та індивідуальними підприємцями різних видів діяльності.

Устаткування щодо встановлення - це технологічне, енергетичне і виробниче обладнання, яке потребує монтажу і призначене для установки в споруджуваних (реконструйованих) об'єктах.

Устаткування щодо встановлення приймається до бухгалтерського обліку на рахунку 07 «Устаткування до установки» за фактичною вартістю придбання, яка складається з вартості за цінами придбання і витрат з придбання і доставку їх на склад організації.

Вкладення у необоротні активи - це витрати по створенню об'єктів тривалого користування шляхом нового будівництва, реконструкції та розширення діючих об'єктів.

Фактичні витрати організації, що включаються до первісної вартості об'єктів основних засобів, нематеріальних активів та інших відповідних активів враховуються на рахунку 08 «Вкладення у необоротні активи».

Оборотні активи завершують свій оборот протягом одного виробничого циклу і відшкодовуються за рахунок виручки від реалізації вироблених організацією послуг.  
 Витрати - зменшення активів або збільшення зобов'язань, які ведуть до зменшення капіталу. Для обліку витрат майбутніх періодів в бухгалтерському обліку використовується рахунок 97 «Витрати майбутніх періодів». Податки по придбаних товарах, роботах, послугах - це податок на додану вартість, який обліковується на рахунку 18 «Податок на додану вартість по придбаних товарах, роботах, послугах», належний до сплати і оплачений організацією.

### 2.4. Безпека та персонал

Забезпечення безпеки інформації і об'єктів, що відносяться до інформації - важливе завдання для будь-якого бізнесу. Інформаційна безпека на підприємствах

Система менеджменту інформаційної безпеки (ІБ) необхідна будь-якому підприємству для збереження трьох її складових: цілісності, конфіденційності та доступності інформаційних активів підприємства. Для всіх інформаційних активів існують загрози різного ступеня важливості.

Основна вигода впровадження такої системи - виявлення найбільш небезпечних загроз і економія коштів на створення ефективної системи забезпечення інформаційної безпеки (ІБ) - в якій забезпечено своєчасне виявлення (ідентифікація) ризиків, оцінка, контроль, всі процеси формалізовані, документація і відповідні процедури підтримуються.

Для роботи в даному напрямку була розроблена серія стандартів інформаційної безпеки ISO 27000.

### 2.5 Фізична та зовнішня безпека

Фізичний захист інформаційної системи - дуже важлива частина захисту інформації.

У комерційній фірмі по ремонту комп'ютерної техніки Smart-service:

1. Сервер перебувати в кімнаті технічного відділу в спеціальній шафі, доступ до якого має строго обмежене коло осіб. Його корпус опечатаний.

2. У більшості приміщень кімнат знаходяться камери відеоспостереження. Офіс оснащений вогнегасником.

3. Вся техніка запитана від мережевих фільтрів, які оберігають від більшості перешкод.

4. Всі комп'ютери мають джерела безперебійного живлення.

5. Також є резерв комп'ютерів і ноутбуків, на випадок виходу з ладу основних.

6. На випадок відключення електроенергії, а у нас в країні це не рідкість, на нашому підприємстві є автономний генератор, здатний деякий час підтримати роботу найбільш важливих машин. Або просто забезпечити електроенергією при ремонті.

### 2.6 Менеджмент комп’ютерів та мереж

Для комерційної фірми по ремонту комп'ютерної техніки Smart-service можуть бути застосовані такі адміністративні заходи щодо захисту інформації, як:

− наявність антивіруса і т.д.

− наявність камер відеоспостереження;

− охорона офісу;

− наявність засобів аудиту;

− розмежування доступу суб'єктів до об'єктів;

Всі зазначені вище кошти забезпечення безпеки реалізовані у вигляді вбудованих функцій операційних систем, системних додатків, комп'ютерів і мережевих комунікаційних пристроїв.

### 2.7. Керування доступом до системи

Під політикою безпеки розуміють набір норм, правил і практичних прийомів, що регулюють управління, захист і розподіл цінної інформації. Політика безпеки задає механізми управління доступу до об'єкту, визначає як дозволені, так і заборонені доступи.

Політика безпеки реалізується через адміністративно−організаційні заходи, фізичні і програмно−технічні засоби та визначає архітектуру системи захисту. Для конкретної організації політика безпеки повинна носити індивідуальний характер і залежати від конкретної технології обробки інформації і тих програмних і технічних засобів, що використовуються.

Політика безпеки визначається способом управління доступом, який задає порядок доступу до об'єктів системи. Розрізняють два основних види політики безпеки: виборчу і повноважну.

Таблиця 2.1 – Розподілення прав доступу

|  |  |  |  |
| --- | --- | --- | --- |
| Об’єкти  Суб’єкти | Бази даних | Сайт | Електрона пошта |
| Директор | Повний доступ | Повний доступ | Повний доступ |
| Заст. Директора | Повний доступ | Повний доступ | Повний доступ |
| Бухгалтерія | Повний доступ до бухгалтерської бази даних | Читання | Читання |
| Технічний відділ | Повний доступ | Повний доступ | Повний доступ |
| Відділ з роботи с клієнтами | Повний доступ до клієнтської бази даних | Читання | Читання |

Алгоритм формування матриці доступу користувачів до об'єктів комп'ютерної системи.

Алгоритм формування матриці виконується за допомогою функції **public static** String randomCharacter(String characters)яка повертає випадковий символ r – read, w – write. Нижче приведено опис функції

**public static** String randomCharacter(String characters)  
{  
 **int** n = characters.length();  
 **int** r = (**int**) (n \* Math.*random*());  
 **return** characters.substring(r, r + 1);  
}

Заповнення матриці доступу.

Матриця доступу заповнюється за допомогою **private** ObservableList<Person> **personList** = FXCollections.*observableArrayList*(); **personList** включає в себе метод **personList**.add(person); за допомогою якого виконується додавання об'єктів в матрицю. Нижче приведено пример опису заповнення матриці

**personList**.clear();

**personList**.add(**new** Person(**"Administrator"**,**"r,w,ch"**,**"r,w,ch"**,**"r,w,ch"**,**"r,w,ch"**));  
**personList**.add(**new** Person(**"User"**, **password**,**password1**,**password2**,**password3**));  
**personList**.add(**new** Person(**"User1"**, **password2**,**password2**,**password3**,**password2**));  
**personList**.add(**new** Person(**"User2"**, **password3**,**password1**,**password3**,**password1**));  
**personList**.add(**new** Person(**"User3"**, **password2**,**password3**,**password1**,**password1**));  
**personList**.add(**new** Person(**"User4"**, **password2**,**password**,**password2**,**password3**));

Заповнення та читання матриці від User, виконується через запис та читання з файлу в матрицю. Нижче приведено пример запису та читання

**file**.createNewFile();  
FileWriter fileWriter = **new** FileWriter(**file**);  
BufferedWriter bufferedWriter = **new** BufferedWriter(fileWriter);  
**pass** = **password**;  
bufferedWriter.write(**pass**);  
bufferedWriter.newLine();  
bufferedWriter.flush();  
bufferedWriter.close();

FileReader fileReader = **new** FileReader(**file**);  
BufferedReader bufferedReader = **new** BufferedReader(fileReader);  
**while** (bufferedReader.ready())  
{  
 **pass** = bufferedReader.readLine();  
}

Робота модуля з дискреційною моделлю політики безпеки.

Програма працює таким чином, admin – входить у свій кабінет, генерую значення, тобто саму дискреційну модель політики безпеки, потім user – входить у свій кабінет, та перевіряє свої операції над об'єктами комп'ютерної системи.

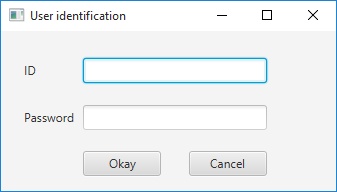


Рис. 2.1 – Вікно ідентифікації користувача

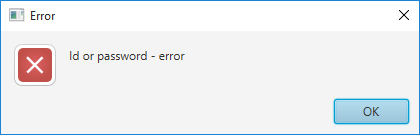


Рис. 2.2 – Вікно неправильно ідентифікованого користувача

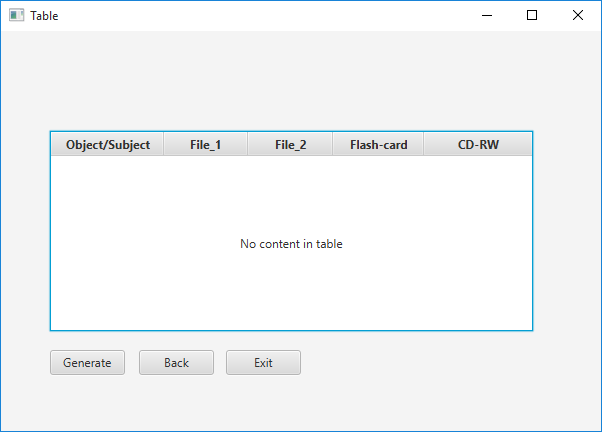


Рис. 2.3 – Вікно адміністратора

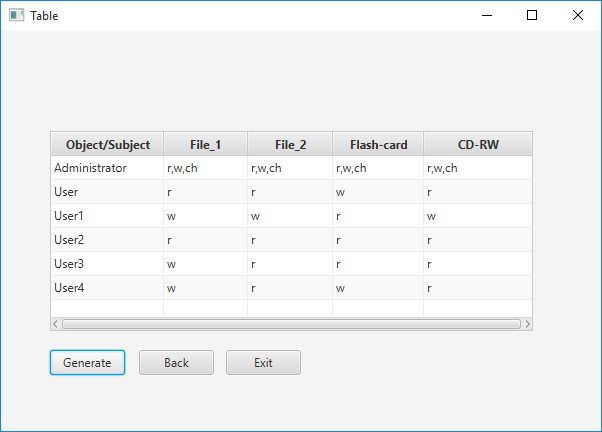


Рис. 2.4 – Пример виконання генерації матриці

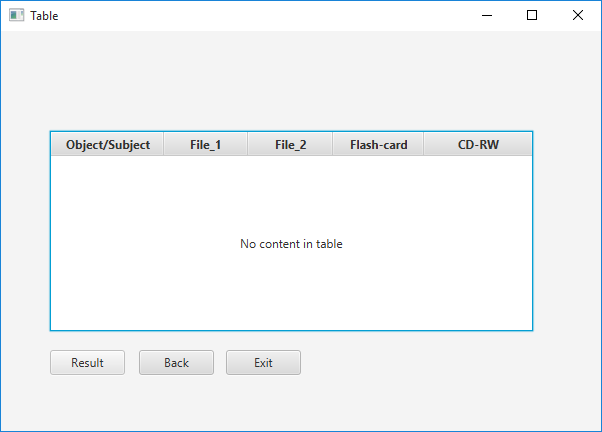


Рис. 2.5 – Вікно користувача

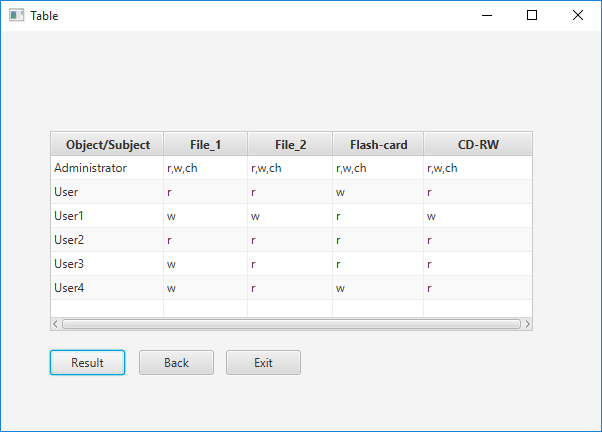


Рис. 2.6 – Пример огляду моделі користувачем

### 2.8. Відповідність системи вимогам стандарту

Стандарти інформаційної безпеки - це обов'язкові або рекомендовані до виконання документи, в яких визначено підходи до оцінки рівня інформаційної безпеки і встановлені вимоги до безпечних інформаційних систем.

Стандарти в області інформаційної безпеки виконують такі найважливіші функції:

− вироблення понятійного апарату і термінології в області інформаційної безпеки;

− формування шкали вимірювань рівня інформаційної безпеки;

− узгоджена оцінка продуктів, що забезпечують інформаційну безпеку; − підвищення технічної та інформаційної сумісності продуктів, що забезпечують інформаційну безпеку;

− накопичення відомостей про кращі практики забезпечення інформаційної безпеки і їх надання різним групам зацікавленої аудиторії - виробникам засобів інформаційної безпеки, експертам, IT-директорам, адміністраторам і користувачам інформаційних систем;

− функція нормотворчості - надання деяким стандартам юридичної сили і встановлення вимоги їх обов'язкового виконання [http://www.arinteg.ru/articles/standarty-informatsionnoy-bezopasnosti-27697.html].

На кінець 2008 року прийняті такі нормативні документи інформаційної безпеки цього сімейства:

− ISO / IEC 27001: 2005 Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги.

− ISO / IEC 27002: 2005 Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою (раніше ISO / IEC 17799: 2005).

− ISO / IEC 27005: 2008 інформаційне технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки.

− ISO / IEC 27006: 2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою.

### РЕЗУЛЬТАТИ АУДИТА СИСТЕМИ, ДОКУМЕНТ «КОНТРОЛЬНИЙ СПИСОК АУДИТУ»

|  |  |  |
| --- | --- | --- |
| Документ политики информационной безопасности | Существует ли политика информационной безопасности, которая одобрена руководством, публикуется и доводится до сведения всех сотрудников | да |
|  | Является ли он заявлением о приверженности руководства и определяет организационный подход к управлению информационной безопасностью. | да |
| Обзор и оценка |  |  |
|  | Имеет ли политику безопасности владелец, который несет ответственность за его обслуживание и проверку в соответствии с определенным процессом рассмотрения. | нет |
|  | Независимо от того, обеспечивает ли процесс проведение обзора в ответ на любые изменения, влияющие на исходную оценку, например: значительные инциденты с безопасностью, новые уязвимости или изменения в организационной или технической инфраструктуре. | да |

|  |  |  |
| --- | --- | --- |
| Форум по безопасности управленческой информации | Есть ли форум управления, чтобы обеспечить четкое руководство и видимую поддержку управления инициативами безопасности внутри организации | нет |
| Координация информационной безопасности | Существует ли межфункциональный форум представителей управления из соответствующих подразделений организации для координации внедрения элементов управления информационной безопасностью. | нет |
| Распределение обязанностей по информационной безопасности | Четко ли определены обязанности по защите отдельных активов и проведению конкретных процессов безопасности. | да |
| Процесс авторизации для объектов обработки информации | Существует ли процесс авторизации управления для любого нового средства обработки информации. Это должно включать все новые средства, такие как аппаратное и программное обеспечение. | да |
| Специалист по информационной безопасности | Независимо от того, получают ли консультации по информационной безопасности специалиста там, где это необходимо. | нет |
|  | Определенный индивидуум может быть идентифицирован для координации внутренних знаний и опыта для обеспечения согласованности и оказания помощи в принятии решений о безопасности | да |
| Сотрудничество между организациями | Были ли поддержаны надлежащие контакты с правоохранительными органами, регулирующими органами, поставщиками информационных услуг и операторами электросвязи для обеспечения быстрого принятия соответствующих мер и получения консультаций в случае инцидента с безопасностью. | да |
| Независимый обзор информационной безопасности | Независимо от того, осуществляется ли проверка политики безопасности на регулярной основе. Это делается для того, чтобы обеспечить уверенность в том, что организационная практика правильно отражает политику и что она возможна и эффективна. | нет |
| ***Безопасность доступа третьих сторон*** |  |  |
| Идентификация рисков от доступа третьих сторон | Требования безопасности в контрактах третьих | нет |

|  |  |  |
| --- | --- | --- |
| **Физическая и экологическая безопасность** | | |
| ***Защищенная область*** |  |  |
| Периметр физической безопасности | Какое физическое устройство защиты границ было реализовано для защиты службы обработки информации. | коммутатор |
|  | Некоторыми примерами такого средства безопасности являются входные ворота для контроля карты, стены, укомплектованный прием и т. к. | да |
| Элементы управления физической записью | Какие существуют средства контроля доступа, позволяющие только уполномоченным персоналом работать в различных областях организации. | Проверка пользователя логин, пароль |
| Обеспечение офисов, помещений и помещений | Будут ли закрыты комнаты, в которых есть служба обработки информации, блокировки или сейфы. | да |
|  | Независимо от того, защищена ли служба обработки информации от стихийного и техногенного бедствия. | нет |
|  | Существует ли какая-либо потенциальная угроза со стороны соседних помещений. | нет |
| Работа в безопасных районах | Информация нужна только для понимания. Существует ли какой-либо контроль безопасности для третьих лиц или для персонала, работающего в безопасной зоне. | нет |
| Изолированные зоны доставки и погрузки | Независимо от того, изолированы ли область доставки и область обработки информации друг от друга, чтобы избежать любого несанкционированного доступа. | да |
|  | Была ли проведена оценка риска для определения безопасности в таких областях. | да |
|  | Были идентифицированы риски безопасности с сторонними подрядчиками, работающими на месте, и были реализованы соответствующие меры контроля. | нет |
| Требования безопасности в контрактах третьих лиц | Существует ли официальный контракт, содержащий или ссылающийся на все требования безопасности для обеспечения соответствия политикам и стандартам безопасности организации. | да |
|  | Подтверждены ли типы доступа, классифицируются и причины доступа. | да |
| ***Безопасность оборудования*** |  |  |
| Защита мест размещения оборудования | Было ли оборудование расположено в соответствующем месте, чтобы свести к минимуму ненужный доступ в рабочие зоны. | нет |
|  | Были ли изолированы элементы, требующие особой защиты, чтобы снизить общий уровень защиты. | нет |
|  | Были ли приняты меры по минимизации риска потенциальных угроз, таких как кража, пожар, взрывчатые вещества, дым, вода, дист, вибрация, химические воздействия, интерфейсы электропитания, электромагнитное излучение, наводнение. | да |
|  | Существует ли политика в отношении еды, питья и курения в непосредственной близости от служб обработки информации. | да |
|  | Наблюдается ли мониторинг состояния окружающей среды, что негативно скажется на средствах обработки информации. | да |
| Источники питания | Независимо от того, защищено ли оборудование от сбоев питания, используя постоянство источников питания, таких как несколько каналов питания, источник бесперебойного питания (ups), резервный генератор и т. д. | да, но не везде |
| ***Безопасность оборудования*** |  |  |
| Безопасность кабелей | Независимо от того, защищен ли кабель питания и телекоммуникационный кабель данными или вспомогательными информационными службами от перехвата или повреждения. | да |
| ***Безопасность оборудования*** |  |  |
|  | Существуют ли какие-либо дополнительные меры безопасности для чувствительной или критической информации. | нет |

|  |  |  |
| --- | --- | --- |
| ***Операционная процедура и обязанности*** |  |  |
| Документированные рабочие процедуры | Независимо от того, указала ли политика безопасности какие-либо рабочие процедуры, такие как резервное копирование, техническое обслуживание оборудования и т. | да |
|  | Будут ли такие процедуры документированы и использованы. | нет |
| Управление операционными изменениями | Независимо от того, подвергаются ли все программы, работающие на производственных системах, строгое управление изменениями, то есть любые изменения, которые должны быть внесены в эти производственные программы, должны пройти авторизацию управления изменениями. | да |
|  | Сохраняются ли журналы аудита для любых изменений, внесенных в производственные программы. | да |
| Процедуры управления инцидентами | Существует ли процедура управления инцидентами для борьбы с инцидентами с безопасностью. | нет |

|  |  |  |
| --- | --- | --- |
| *Требования безопасности систем* |  |  |
| Анализ и спецификации требований безопасности | Независимо от того, включены ли требования безопасности в состав требований бизнес-требований к новым системам или для улучшения существующих систем. | нет |
|  | Требования безопасности и идентифицированные элементы управления должны отражать ценность бизнеса в отношении задействованных информационных активов и последствия отказа от безопасности. | да |
|  | Проводится ли оценка рисков до начала разработки системы. | да |
| *Безопасность в прикладных системах* |  |  |
| Проверка входных данных | Независимо от того, проверены ли данные для системы приложений, чтобы убедиться, что они правильные и соответствующие. | да |
|  | Учитываются ли такие элементы управления, как: различные типы входов для проверки сообщений об ошибках, рассматриваются процедуры реагирования на ошибки проверки, определяющие обязанности всего персонала, вовлеченного в процесс ввода данных и т. Д. | да |
| Контроль внутренней обработки | Определяются ли области рисков в цикле обработки и включены проверки проверки. В некоторых случаях данные, которые были правильно введены, могут быть повреждены ошибками обработки или преднамеренными действиями. | да |
|  | Определены ли соответствующие средства управления для приложений для снижения рисков во время внутренней обработки. | да |
|  | Элементы управления будут зависеть от характера применения и влияния бизнеса на любую коррупцию данных. | да |
| Проверка подлинности сообщений | Была ли проведена оценка риска безопасности для определения необходимости проверки подлинности сообщения; и определить наиболее подходящий метод реализации, если это необходимо. | нет |
| *Требования безопасности систем* |  |  |
|  | Аутентификация сообщений - это метод, используемый для обнаружения несанкционированных изменений или повреждения содержимого передаваемого электронного сообщения. | нет |
| *Требования безопасности систем* |  |  |
| Проверка выходных данных | Независимо от того, проверен ли вывод данных прикладной системы для обеспечения правильности обработки хранимой информации и соответствия ее обстоятельствам. | да |
| *Криптографические средства управления* |  |  |
| Политика использования криптографических средств управления | Существует ли «Политика использования криптографических средств контроля для защиты информации». | нет |
|  | Была ли проведена оценка риска для определения уровня защиты, которую должна предоставлять информация. | да |
| Шифрование | Использовались ли методы шифрования для защиты данных. | да |
|  | Были ли проведены оценки для анализа чувствительности данных и необходимого уровня защиты. | да |

|  |  |  |
| --- | --- | --- |
| *Аспекты управления непрерывностью бизнеса* |  |  |
| Процесс управления непрерывностью бизнеса | Существует ли управляемый процесс для развития и поддержания непрерывности бизнеса во всей организации. | нет |
|  | Это может включать в себя план обеспечения непрерывности бизнеса Организации, регулярное тестирование и обновление плана, разработку и документирование стратегии непрерывности бизнеса и т. Д. | нет |
| Анализ непрерывности бизнеса и воздействия | Были отмечены события, которые могут вызвать перебои в бизнес-процессе: отказ оборудования, наводнение и пожар. | да |
|  | Была ли проведена оценка риска для определения воздействия таких перерывов. | да |
|  | Был ли разработан стратегический план на основе результатов оценки риска для определения общего подхода к непрерывности бизнеса. | да |
| Написание и реализация плана непрерывности | Были ли разработаны планы по восстановлению бизнес-операций в течение требуемого периода времени после прерывания или отказа от бизнес-процесса. | нет |
|  | Будет ли план регулярно проверяться и обновляться. | да |
| Рамки планирования непрерывности бизнеса | Существует ли единая структура плана непрерывности бизнеса. | да |
|  | Поддерживается ли эта основа для обеспечения согласованности всех планов и определения приоритетов для тестирования и обслуживания. | да |
|  | Определяет ли это условия для активации и лица, ответственные за выполнение каждого компонента плана. | нет |
| Тестирование, поддержание и переоценка плана непрерывности бизнеса | Регулярно проверяются ли планы обеспечения непрерывности бизнеса, чтобы они были актуальными и эффективными. | нет |
|  | Были ли продолжены планы обеспечения непрерывности бизнеса регулярными обзорами и обновлениями, чтобы обеспечить их постоянную эффективность. | нет |
|  | Были ли включены процедуры в рамках программы управления изменениями организаций, чтобы обеспечить надлежащее рассмотрение вопросов непрерывности бизнеса. | нет |

|  |  |  |
| --- | --- | --- |
| ***Соблюдение правовых требований*** |  |  |
| Определение действующего законодательства | Были ли четко определены и документированы все соответствующие нормативные, нормативные и контрактные требования для каждой информационной системы. | да |
|  | Были ли определены и документированы конкретные меры контроля и индивидуальные обязанности для удовлетворения этих требований. | да |
| Права интеллектуальной собственности (ПИС) | Существуют ли какие-либо процедуры для обеспечения соблюдения правовых ограничений на использование материалов, в отношении которых могут существовать права интеллектуальной собственности, такие как авторское право, права на дизайн, товарные знаки. | нет |
|  | Хорошо ли выполняются процедуры. | да |
|  | Независимо от того, поставляются ли проприетарные программные продукты в соответствии с лицензионным соглашением, которое ограничивает использование продуктов указанными машинами. Единственным исключением может быть создание собственных резервных копий программного обеспечения. | да |
| Охрана организационных записей | Независимо от того, защищены ли важные записи организации от разрушения убытков и функции фальсификаций. | нет |
| Защита данных и конфиденциальность личной информации | Существует ли структура управления и контроль для защиты данных и конфиденциальности личной информации. | да |
| Предотвращение злоупотребления средствами обработки информации | Независимо от того, рассматривается ли использование средств обработки информации для любых некоммерческих или несанкционированных целей, без одобрения руководства, рассматривается как ненадлежащее использование объекта . | нет |
|  | При входе в систему на экране компьютера отображается предупреждающее сообщение, указывающее, что введенная система является конфиденциальной и что несанкционированный доступ запрещен. | да |
| Регулирование криптографического контроля | Является ли регулирование криптографического контроля в соответствии с сектором и национальным соглашением. | нет |
| Сбор доказательств | Независимо от того, соответствует ли процесс сбора доказательств в соответствии с правовой и отраслевой практикой. | нет |
| ***Обзоры политики безопасности и технического соответствия*** |  |  |
| Соблюдение политики безопасности | Рассматриваются ли все области внутри организации для регулярного обзора для обеспечения соблюдения политики безопасности, стандартов и процедур. | да |
| Проверка технического соответствия | Регулярно проверялись ли информационные системы на соответствие стандартам обеспечения безопасности. | да |
|  | Независимо от того, осуществляется ли техническая проверка соответствия или под контролем компетентных, уполномоченных лиц. | нет |
| ***Вопросы системного аудита*** |  |  |
| Контроль системного аудита | Необходимо ли тщательно планировать и согласовывать требования аудита и действия, связанные с проверкой операционных систем, чтобы свести к минимуму риск сбоев в бизнес-процессе. | да |
| Защита средств системного аудита | Защищен ли доступ к инструментам системного аудита, таким как программное обеспечение или файлы данных, для предотвращения любого возможного злоупотребления или компрометации. | да |

* аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів ІС;

Бухгалтерія ПК1

Конфіденційність рівня – низький (4,95%)

Цілісність рівня – низький (0,66%)

Доступність рівня – низький (3,57%)

Відділ по роботі з клієнтами ПК2

Конфіденційність рівня – низький (0%)

Цілісність рівня – низький (0%)

Доступність рівня – низький (0%)

Технічний відділ Сервер

Конфіденційність рівня – середній (21%)

Цілісність рівня – високий (50%)

Доступність рівня – високий (100%)

* оцінка поточного рівня захищеності ІС;

В цілому розглянута вище методика дозволяє оцінити або переоцінити рівень поточного стану захищеності інформаційних активів компанії, а також виробити рекомендації щодо забезпечення (підвищення) інформаційної безпеки компанії. У тому числі знизити потенційні втрати компанії шляхом підвищення стійкості функціонування корпоративної мережі, розробити концепцію і політику безпеки компанії.

Також розглянута методика дозволяє запропонувати плани захисту конфіденційної інформації компанії, що передається по відкритих каналах зв'язку, захисту інформації компанії від навмисного спотворення

(руйнування), несанкціонованого доступу до неї, її копіювання або використання.

* локалізація вузьких місць в системі захисту ІС;

Локалізація вузьких місць у системі відбувається за допомогою підтримання існуючих стандартів в області інформаційних технологій.

* оцінка відповідності ІС існуючим стандартам в області інформаційної безпеки;

Оцінка відповідності ІС існуючим стандартам в області інформаційної безпеки задовільна т. к. система відповідає існуючим стандартам починаючи з 2008 року.

Виходячи із загального визначення інформаційної системи як системи,

що збирає, зберігає, обробляє і надає користувачам інформацію, процес

функціонування будь-якої інформаційної системи з погляду загроз її

функціонуванню можна подати таким чином (рис. 2.31).

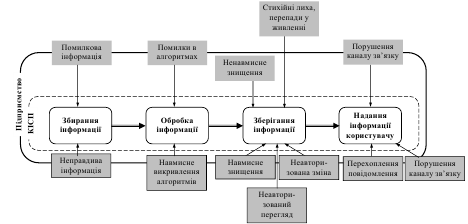


Рис. 3.1. Загрози інформаційній безпеці підприємства

Як уже було зазначено у розд. 1.3, безпечною є інформаційна система,

яка забезпечує такі властивості інформації:

• цілісність — відповідає стану системи, коли інформація є вчасною,

точною і повною;

• конфіденційність — вимога, щоб до приватної або конфіденційної

інформації, яка міститься у системі, мали доступ тільки уповноважені

користувачі;

• доступність — вимога, щоб система працювала коректно і не

відмовляла у доступі легальному користувачу.

Як було показано у розд. 1.3, використання КІСП для потреб управління

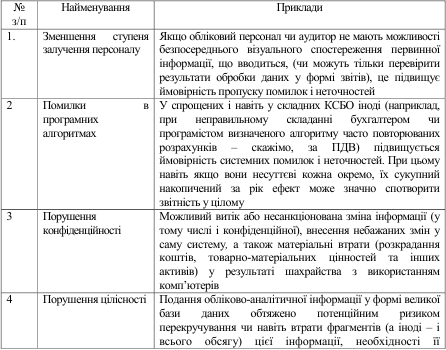
підприємством створює додаткові ризики невиявлення помилок в обліку та

винесення аудитором помилкового судження.

Приклади причин помилок в обліковій інформації при застосуванні

КІСП наведені в табл. 2.11.

Таблиця 2.11. Приклади появи можливих помилок в обліковій

інформації при застосуванні КІСП 



Аналіз ризиків, пов'язаних з безпекою інформаційної системи,

передбачає чотири етапи:

1) ідентифікацію засобів захисту на визначеній ділянці інформаційної

системи;

2) оцінку надійності засобів захисту на цій ділянці;

3) оцінку ймовірності, що акт порушення безпеки буде успішний, з

огляду на набір засобів захисту на цій ділянці інформаційної системи і їхньої

надійності;

4) оцінку втрат, що понесе підприємство, якщо акт порушення безпеки

обійде засоби захисту в цьому місці інформаційної системи.

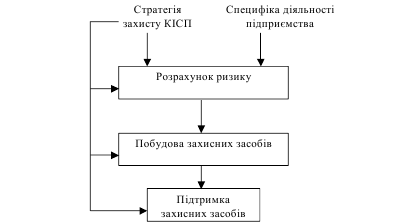


Рис. 3.2 Процес управління захистом КІСП



Рис. 3.3 Схема взаємодії суб’єктів у полі інформаційної безпеки

підприємства

### АНАЛІЗ ПРОГРАМНИХ РЕАЛІХАЦІЙ ТА РАЗРОБКА ЗАСОБІВ НЕСАНКЦІОНОВАНОГО АНАЛІЗУ ПРОГРАМ ТА ДАНИХ

### 4.1 Метод експерименту

Виконавши архівацію вибраних файлів file1.txt і file2.txt з використанням різних методів шифрування (store, best) отримуємо файли file1.rar і ​​file2.rar потім ще раз архівуємо архівіруємі файли на місце колишнього для виконання пошуку маркант в криптосистеми, порівнюємо файли по бітам і отримуємо такий же файл, скріншоти представлені нижче

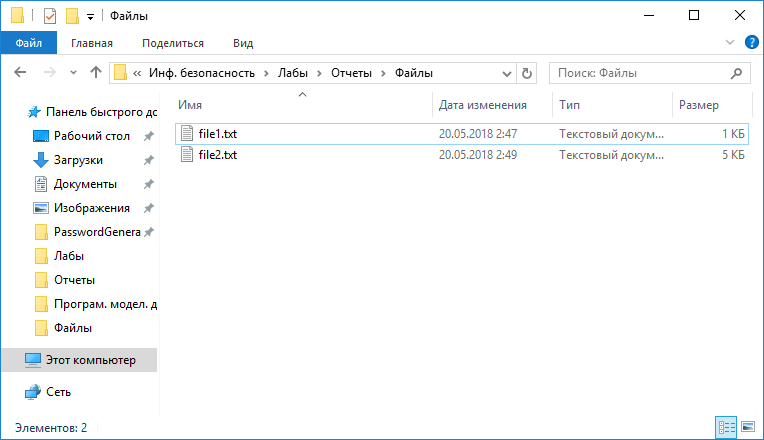


Рис. 4.1 – Каталог файлів

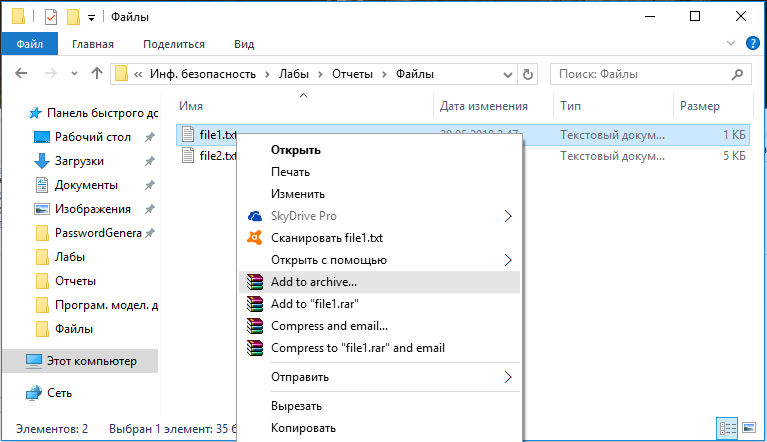


Рис. 4.2 – Добавление в архив

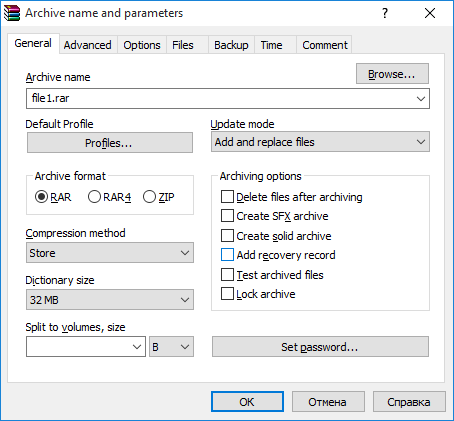


Рис. 4.3 – Створення архива методом store

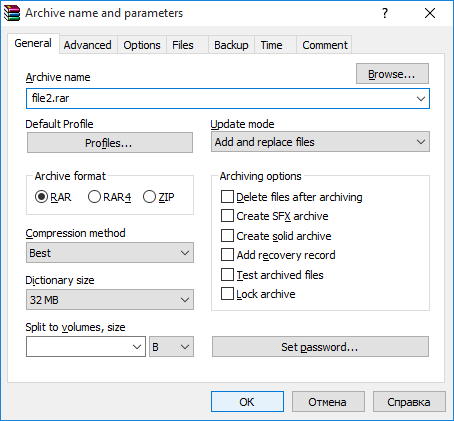


Рис. 4.4 – Создание архива методом best

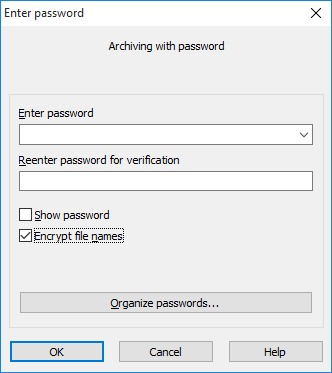


Рис. 4.5 – Шифрування імені заголовка

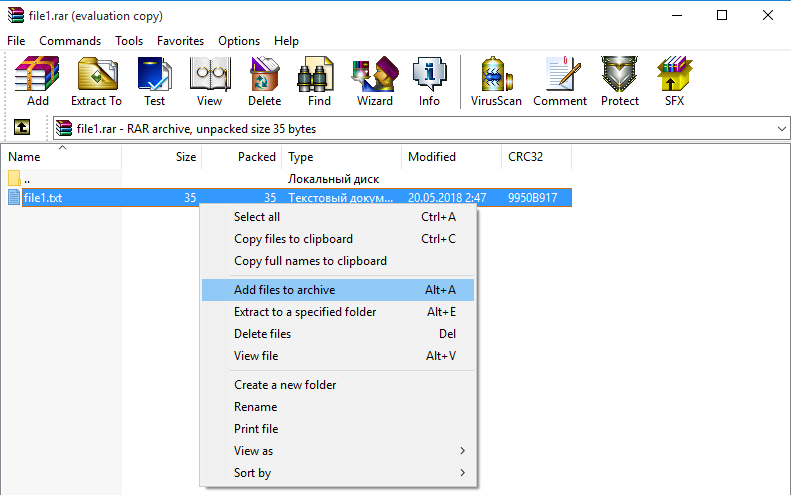


Рис. 4.6 – Додавання в архів архівованного файлу для перевірки манката

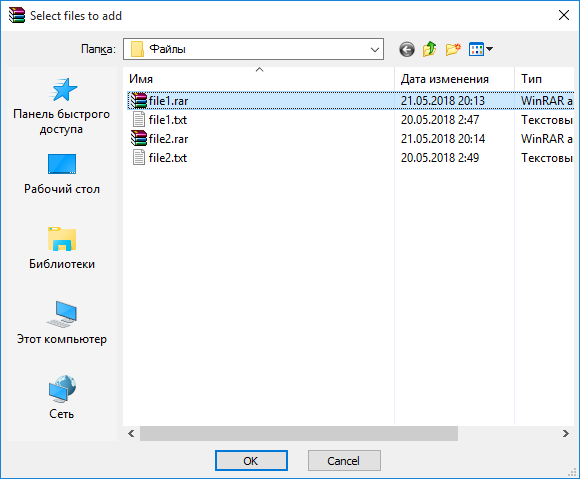


Рис. 4.7 – Додавання до архіву

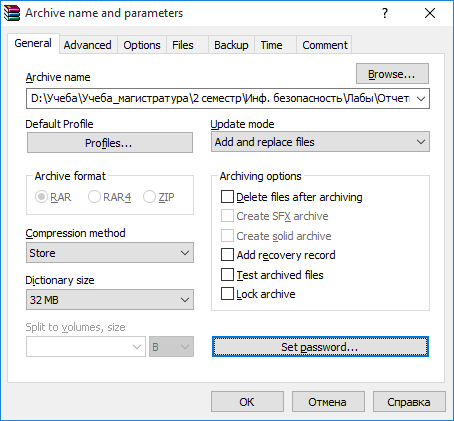


Рис. 4.8 – Архівування

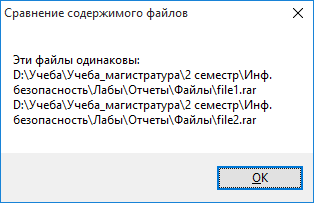


Рис. 4.9 – Порівняння файлів за допомогою Total Commander

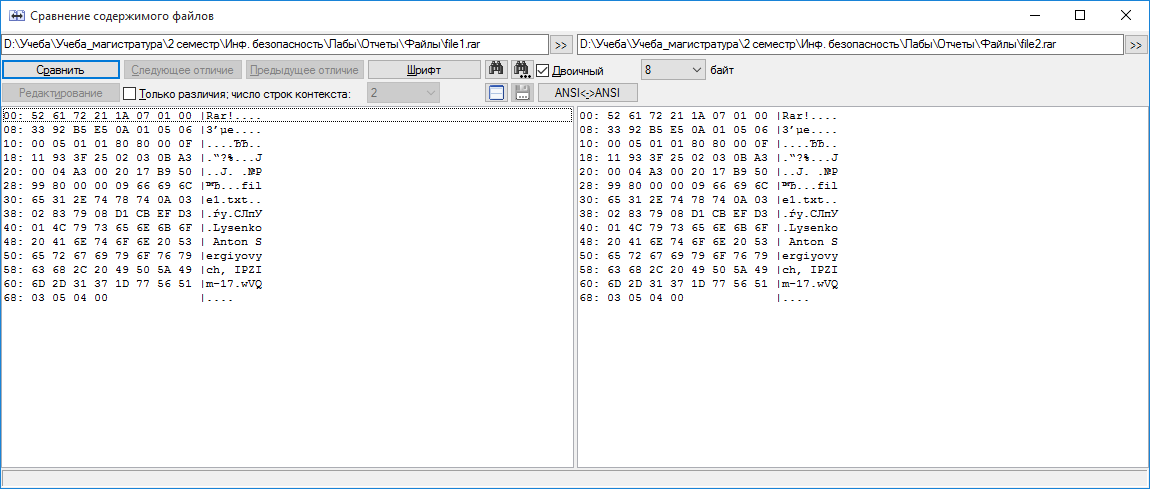


Рис. 4.10 – Порівняння вмісту файлів по бітам в двійковому вигляді

Наявність або відсутність маркант в криптосистеме.

Проводимо дворазове шифрування одного і того ж відкритого тексту на одному і тому ж ключі.

Якщо в результаті двох шифрування отримані різні шифртекст, значить, в криптографическом перетворенні використовується маркант - випадково генерується число або рядок, призначене для утруднення виявлення в потоці зашифрованих даних однакових фрагментів.

Залежність маркант, використовуваного криптосистемою, від поточного часу

Повторюємо попередній експеримент в умовах, коли з точки зору аналізованої програми системний годинник зупинені.  
У Windows це можна зробити, наприклад, модифікувавши машинний код функції GetTickCount в образі бібліотеки kernel32.dll, завантаженому в адресний простір аналізованої програми. Якщо в результаті двох шифрування, проведених в ході справжнього експерименту отримані однакові шифртекст, значить, маркант, що генерується аналізованої програмою, залежить тільки від поточного часу.

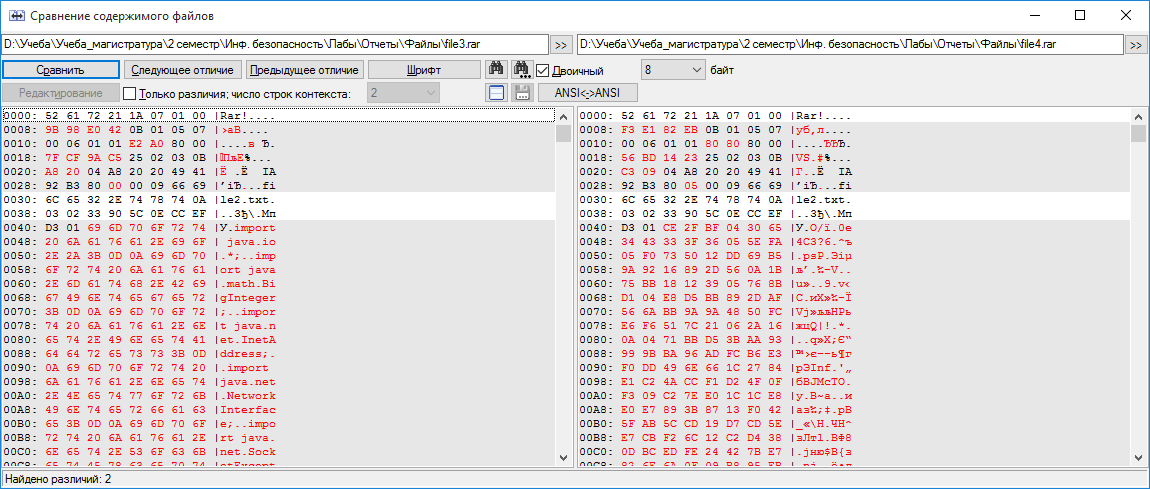


Рис. 4.11 - Порівняння файлів більшої довжини

Як бачимо з попереднього рис. 11 кількість вмісту впливає на архівування файлів, ми виконали ті ж операції, що в попередньому файлі і Total Commander виявив 2 відмінності.

### 4.2 Статичний аналіз

На скріншоті нижче представлені функції зображені на псевдокоді, зараз поясню позначення деяких з них, функція sub\_CE14BF - функція виведення на екран, аналогічна cout << endl; в с ++, далі можемо помітити метод взяття ключа, який укладено в цикл for (); потім слід функція cout << endl і cin >> mess >> endl; за допомогою яких відбувається написати привітання для шифрування і дешифрування, потім в циклах for (); спостерігаємо алгоритми шифрування і дешифрування, де який можна визначити по виводить повідомлення:

v16 = sub\_CE14BF (std :: cout, "Encryption:");

v21 = sub\_CE14BF (std :: cout, "Decryption:");

Потім переходячи в головну функцію можемо побачити виклик функції шифрування і дешифрування

sub\_CE1028 (); - назва збігається з назвою раніше розглянутої функцією

Потім йде перевірка на коректне завершення програми, повернення 0 або 1 це виконується в функції

sub\_CE11FE (v1, v0);

слідом отриманий результат повертається в головній функції за допомогою

return sub\_CE11FE (v3, v2);

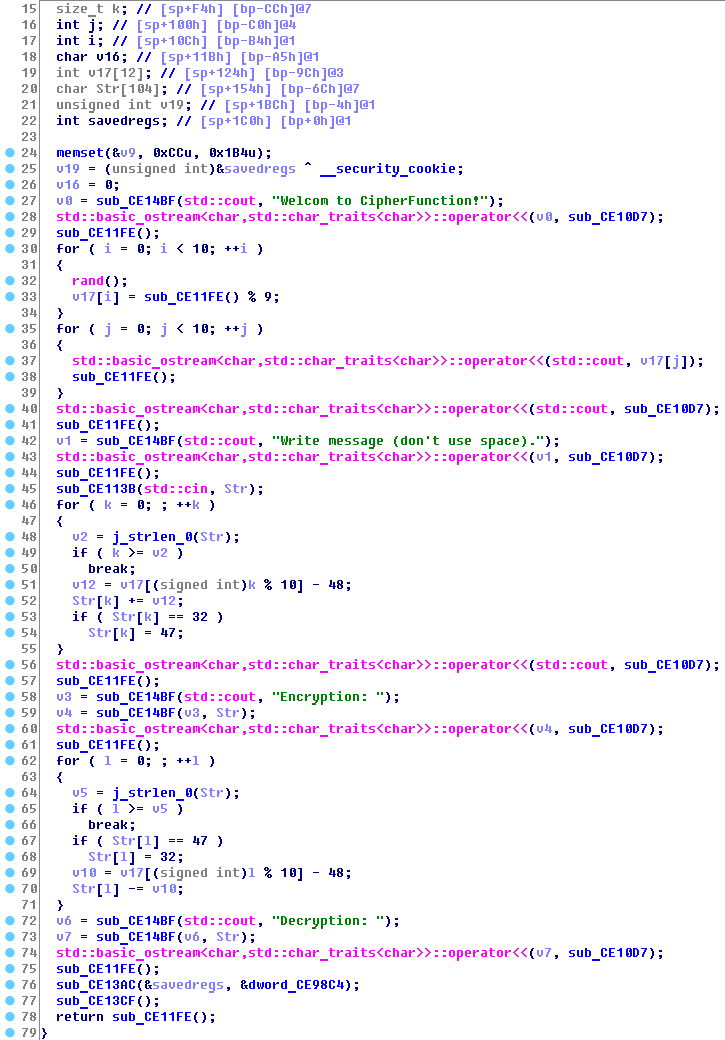


Рис. 4.12 – Псевдокод функції int сipherFunction()

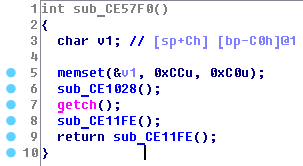


Рис. 4.13 – Псевдокод функциії int main()



Рис. 4.14 – Скриншот роботи програми у IDA Pro Debugger

### 4.3 Динамічний аналіз

Для дизассембліровання буду використовувати програму яка генерує шифрування повідомлення по ключу (ключ генерується випадково), а також дешифрує його, алгоритм роботи шифрування представлений нижче

for (int i = 0; i < strlen(mess); i++) {

int gidit = key[i % 10] - '0';

mess[i] += gidit;

if (mess[i] == 0x20)

mess[i] = 0x2F;

}

Алгоритм роботи дешифрування:

for (int i = 0; i < strlen(mess); i++) {

if (mess[i] == 0x2F)

mess[i] = 0x20;

int gidit = key[i % 10] - '0';

mess[i] -= gidit;

}

Для початку знайдемо функцію, яка виконує шифрування і дешифрування, це робимо за допомогою знаходження функцій по рядках в програмі IDA Pro 6.8. Для відображенні функції по рядках натискаємо клавіші shift + f12



Рис. 4.15 – Функція шифрування та дешифрування

Далі переходимо в цю функцію за допомогою лівої кнопки миші, піднімаємося вище, шукаємо заголовок цієї функції знаходимо, натискаємо клавішу f5 переходимо в режим псевдокоду, скріншоти порівняння представлені на рис. 4.13.

Тут ми можемо помітити int sub\_CE95C0 () - це назва функції, далі можемо побачити цикл for (), де відбувається генерація ключа, а потім по черзі йдуть алгоритми шифрування і дешифрування повідомлення.

Для того щоб знайти головну функцію ми переходимо з допомогою поєднання клавіш ctrl + x в заголовок int cipherFunction (), потім вибираємо вигляд головної панелі Graph overview, за допомогою правої кнопки миші, потім проходимо по функції яка підсвічується зеленим кольором, через ctrl + x і потрапляємо в головну функцію int main (), псевдокод представлений нижче

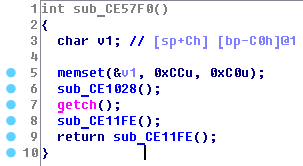


Рис. 4.17 – Псевдокод функції int main()

Далі переходимо в функцію sub\_CE1028 () і бачимо що ця функція повертає значення функції int сipherFunction ()

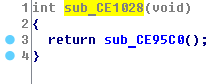


Рис. 4.18 – Псевдокод повернення функції int сipherFunction()

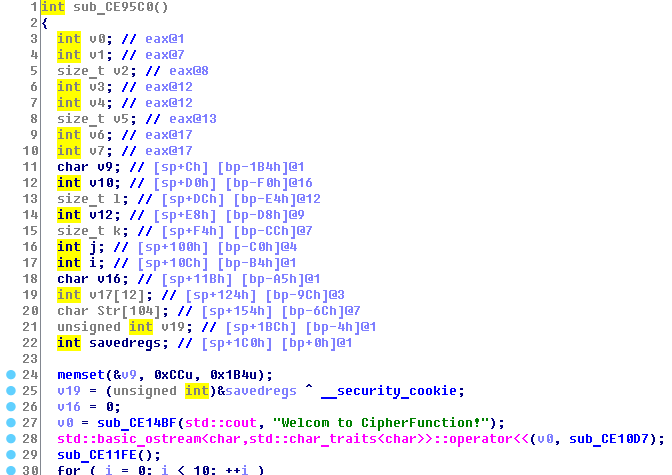


Рис. 4.19 – Псевдокод функції int сipherFunction()

### 5. РЕКОМЕНДАЦІЇ АУДИТУ З ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС

Для підвищення ефективності існуючих механізмів безпеки, треба удосконалити систему за допомогою введення нових способів захисту інформації, генерації ключів, прив’язання даних до конкретних персональних комп’ютерів та девайсів, також можна посилити інтернет захист за допомогою впровадження нових програм для роботи з інтернет ресурсами, чи навпаки оптимізувати ті програми які є на даний момент для роботи без доступу до інтернету, на мою думку перший варіант виглядає гарніше.

### ВИСНОВКИ

Основною метою курсової роботи за курсом «Інформаційна безпека» є отримання знань з організації, проведення та застосування аудиту інформаційної безпеки.

Аудит інформаційної безпеки **-** це оцінка поточного стану безпеки інформаційної системи підприємства чи організації, встановлення рівня її відповідності певним критеріям.

Курсова робота на тему «Аудит політик інформаційної безпеки та розробка комплексу заходів з захисту програм та даних» орієнтована на застосування міжнародного стандарту ISO 27000, сприяє набуттю навичок з проведення аналізу стану захищеності інформаційної системи, відпрацюванню принципів контролю основних параметрів безпеки, комплексного підходу до захисту інформації.

Об'єктом дослідження курсової роботи є гіпотетична система, до якої застосовані початкові заходи інформаційної безпеки, проведено аналіз ризиків, їх оцінювання, розроблено попередні аспекти політик інформаційної безпеки.

Метою роботи є проведення аудиту політики інформаційної безпеки підприємства, встановлення рівня її відповідності міжнародним критеріям та стандарту ISO 27000.

Однією з задач роботи є оцінювання рівня захищеності програмного забезпечення, розробка заходів з захисту програм та даних, встановлених в системі від несанкціонованого дослідження.

Розробка орієнтована на придбання навичок з проведення аудиту інформаційної безпеки на відповідність міжнародному стандарту ISO / IEC 27001: 2005 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги ».

В ході цього аудиту виявляються недоліки в існуючій системі захисту інформації, висуваються пропозиції щодо поліпшення ситуації, надаються рекомендації менеджменту компанії по забезпеченню ефективного управляння системою в критичних ситуаціях з урахуванням бізнес-цілей компанії.

Додаток А.

Досліджуваний продукт

Лістинг програми

Код на С++

Алгоритм шифрування

#include <iostream>

#include <conio.h>

using namespace std;

int cipherFunctuion() {

char mess[100];

int key[10];

char flag = 0;

cout << "Welcom to CipherFunction!" << endl;

for(int i = 0; i < 10; i++)

key[i] = 0 + rand() % 9;

for (int i = 0; i < 10; i++)

cout << key[i];

cout << endl;

cout << "Write message (don't use space)." << endl;

cin >> mess;

for (int i = 0; i < strlen(mess); i++) {

int gidit = key[i % 10] - '0';

mess[i] += gidit;

if (mess[i] == 0x20)

mess[i] = 0x2F;

}

cout << endl;

cout << "Encryption: " << mess << endl;

for (int i = 0; i < strlen(mess); i++) {

if (mess[i] == 0x2F)

mess[i] = 0x20;

int gidit = key[i % 10] - '0';

mess[i] -= gidit;

}

cout << "Decryption: " << mess << endl;

return 0;

}

int main() {

cipherFunctuion();

\_getch();

return 0;

}

Код на Java

Дискреційна модель

Main.java

**package** sample;  
  
**import** javafx.application.Application;  
**import** javafx.fxml.FXMLLoader;  
**import** javafx.scene.Parent;  
**import** javafx.scene.Scene;  
**import** javafx.stage.Stage;  
  
**public class** Main **extends** Application {  
   
 @Override  
 **public void** start(Stage primaryStage) **throws** Exception{  
  
 Stage primaryStage1 = **new** Stage();  
 Parent root1 = FXMLLoader.*load*(getClass().getResource(**"sample.fxml"**));  
 primaryStage1.setTitle(**"User identification"**);  
 Scene scene1 = **new** Scene(root1, 335, 160);  
 primaryStage1.setScene(scene1);  
 primaryStage1.show();  
 }  
  
 **public static void** main(String[] args) {  
 *launch*(args);  
 }  
}

Controller.java

**package** sample;  
  
**import** javafx.event.ActionEvent;  
**import** javafx.fxml.FXML;  
**import** javafx.fxml.FXMLLoader;  
**import** javafx.scene.Node;  
**import** javafx.scene.Parent;  
**import** javafx.scene.Scene;  
**import** javafx.scene.control.\*;  
**import** javafx.scene.control.cell.PropertyValueFactory;  
**import** javafx.stage.Stage;  
  
**import** java.io.IOException;  
  
**public class** Controller {  
  
 **private** CollectionTableModel **tableModel** = **new** CollectionTableModel();  
 **public** TextField **txtID**;  
 **public** Button **btnOkay**;  
 **public** Button **btnCancel**;  
 **public** PasswordField **txtPassword**;  
 **public** Button **btnGenerate**;  
 **public** Button **btnExit**;  
 **public** Button **btnBack**;  
 **public** TableColumn<Person, String> **columnObject**;  
 **public** TableView **tabModel**;  
 **public** TableColumn<Person, String> **columnFile1**;  
 **public** TableColumn<Person, String> **columnFile2**;  
 **public** TableColumn<Person, String> **columnFlashCard**;  
 **public** TableColumn<Person, String> **columnCD\_RW**;  
   
 **public void** accessButtonAction(ActionEvent actionEvent) **throws** IOException {  
 **if**(**txtID**.getText().toLowerCase().equals(**"admin"**) && **txtPassword**.getText().toLowerCase().equals(**"admin"**)) {  
 Stage primaryStage = **new** Stage();  
 Parent root = FXMLLoader.*load*(getClass().getResource(**"DModel.fxml"**));  
 primaryStage.setTitle(**"Table"**);  
 Scene scene = **new** Scene(root, 600, 400);  
 primaryStage.setScene(scene);  
 primaryStage.show();  
 Node source = (Node) actionEvent.getSource();  
 Stage stage = (Stage) source.getScene().getWindow();  
 stage.hide();  
 }  
 **else if**(**txtID**.getText().toLowerCase().equals(**"user"**) && **txtPassword**.getText().toLowerCase().equals(**"user"**)) {  
  
 Stage primaryStage = **new** Stage();  
 Parent root = FXMLLoader.*load*(getClass().getResource(**"DModelUser.fxml"**));  
 primaryStage.setTitle(**"Table"**);  
 Scene scene = **new** Scene(root, 600, 400);  
 primaryStage.setScene(scene);  
 primaryStage.show();  
 Node source = (Node) actionEvent.getSource();  
 Stage stage = (Stage) source.getScene().getWindow();  
 stage.hide();  
 }  
 **else** {  
 *showInfoDialog*(**"Error"**, **"Id or password - error"**);  
 Stage primaryStage1 = **new** Stage();  
 Parent root1 = FXMLLoader.*load*(getClass().getResource(**"sample.fxml"**));  
 primaryStage1.setTitle(**"User identification"**);  
 Scene scene1 = **new** Scene(root1, 335, 160);  
 primaryStage1.setScene(scene1);  
 primaryStage1.show();  
 Node source = (Node) actionEvent.getSource();  
 Stage stage = (Stage) source.getScene().getWindow();  
 stage.hide();  
 }  
  
 }  
 **public static void** showInfoDialog(String title, String text)  
 {  
 Alert alert = **new** Alert(Alert.AlertType.***ERROR***);  
 alert.setTitle(title);  
 alert.setContentText(text);  
 alert.setHeaderText(**""**);  
 alert.showAndWait();  
 }  
  
  
 **public void** cancelButtonAction(ActionEvent actionEvent) {  
 Node source = (Node) actionEvent.getSource();  
 Stage stage = (Stage) source.getScene().getWindow();  
 stage.hide();  
 }  
  
 **public void** generateOnAction(ActionEvent actionEvent) **throws** IOException {  
 **columnObject**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"ID"**));  
 **columnFile1**.setCellValueFactory(**new** PropertyValueFactory< Person, String>(**"File\_1"**));  
 **columnFile2**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"File\_2"**));  
 **columnFlashCard**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"Flash\_card"**));  
 **columnCD\_RW**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"CD\_RW"**));  
  
  
 **tableModel**.testGenerateData(1);  
 **tabModel**.setItems(**tableModel**.getPersonList());  
  
 }  
  
 **public void** exitOnAction(ActionEvent actionEvent) {  
 Node source = (Node) actionEvent.getSource();  
 Stage stage = (Stage) source.getScene().getWindow();  
 stage.hide();  
 }  
  
 **public void** backOnAction(ActionEvent actionEvent) **throws** IOException {  
 Stage primaryStage = **new** Stage();  
 Parent root = FXMLLoader.*load*(getClass().getResource(**"sample.fxml"**));  
 primaryStage.setTitle(**"User identification"**);  
 Scene scene = **new** Scene(root, 335, 160);  
 primaryStage.setScene(scene);  
 primaryStage.show();  
 Node source = (Node) actionEvent.getSource();  
 Stage stage = (Stage) source.getScene().getWindow();  
 stage.hide();  
 }  
  
 **public void** resultOnAction(ActionEvent actionEvent) **throws** IOException {  
 **columnObject**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"ID"**));  
 **columnFile1**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"File\_1"**));  
 **columnFile2**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"File\_2"**));  
 **columnFlashCard**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"Flash\_card"**));  
 **columnCD\_RW**.setCellValueFactory(**new** PropertyValueFactory<Person, String>(**"CD\_RW"**));  
  
  
 **tableModel**.testData(0);  
 **tabModel**.setItems(**tableModel**.getPersonList());  
 }  
}

Person.java

**package** sample;  
  
**public class** Person {  
 **private** String **ID**;  
 **private** String **File\_1**;  
 **private** String **File\_2**;  
 **private** String **Flash\_card**;  
 **private** String **CD\_RW**;  
  
 **public** Person(String ID, String file\_1, String file\_2, String flash\_card, String CD\_RW) {  
 **this**.**ID** = ID;  
 **this**.**File\_1** = file\_1;  
 **this**.**File\_2** = file\_2;  
 **this**.**Flash\_card** = flash\_card;  
 **this**.**CD\_RW** = CD\_RW;  
 }  
  
 **public** String getID() {  
 **return ID**;  
 }  
  
 **public void** setID(String ID) {  
 **this**.**ID** = ID;  
 }  
  
 **public** String getFile\_1() {  
 **return File\_1**;  
 }  
  
 **public void** setFile\_1(String file\_1) {  
 **File\_1** = file\_1;  
 }  
  
 **public** String getFile\_2() {  
 **return File\_2**;  
 }  
  
 **public void** setFile\_2(String file\_2) {  
 **File\_2** = file\_2;  
 }  
  
 **public** String getFlash\_card() {  
 **return Flash\_card**;  
 }  
  
 **public void** setFlash\_card(String flash\_card) {  
 **Flash\_card** = flash\_card;  
 }  
  
 **public** String getCD\_RW() {  
 **return CD\_RW**;  
 }  
  
 **public void** setCD\_RW(String CD\_RW) {  
 **this**.**CD\_RW** = CD\_RW;  
 }  
}

CollectionTableModel.java

**package** sample;  
  
**import** javafx.collections.FXCollections;  
**import** javafx.collections.ObservableList;  
  
**import** java.io.\*;  
**import** java.lang.reflect.Array;  
**import** java.util.ArrayList;  
  
**public class** CollectionTableModel **implements** TableModel  
{  
 **private** ObservableList<Person> **personList** = FXCollections.*observableArrayList*();  
  
 @Override  
 **public void** generateTable(Person person) {  
 **personList**.remove(person);  
 **personList**.add(person);  
 }  
  
 **public** ObservableList<Person> getPersonList() {  
 **return personList**;  
 }  
  
 String **password** = **""**;  
 String **password1** = **""**;  
 String **password2** = **""**;  
 String **password3** = **""**;  
 String **pass** = **""**;  
 String **pass1** = **""**;  
 String **pass2** = **""**;  
 String **pass3** = **""**;  
 **int i**;  
 File **file** = **new** File(**"pass.txt"**);  
 File **file1** = **new** File(**"pass1.txt"**);  
 File **file2** = **new** File(**"pass2.txt"**);  
 File **file3** = **new** File(**"pass3.txt"**);  
 **public void** testGenerateData(**int** length) **throws** IOException {  
  
  
 **for**(**i**=0; **i** < length; **i**++)  
 **password** = *randomCharacter*(**"rw"**);  
 **for**(**i**=0; **i** < length; **i**++)  
 **password1** = *randomCharacter*(**"rw"**);  
 **for**(**i**=0; **i** < length; **i**++)  
 **password2** = *randomCharacter*(**"rw"**);  
 **for**(**i**=0; **i** < length; **i**++)  
 **password3** = *randomCharacter*(**"rw"**);  
 **personList**.clear();  
 **personList**.add(**new** Person(**"Administrator"**, **"r,w,ch"**,**"r,w,ch"**,**"r,w,ch"**,**"r,w,ch"**));  
 **personList**.add(**new** Person(**"User"**, **password**,**password1**,**password2**,**password3**));  
 **personList**.add(**new** Person(**"User1"**, **password2**,**password2**,**password3**,**password2**));  
 **personList**.add(**new** Person(**"User2"**, **password3**,**password1**,**password3**,**password1**));  
 **personList**.add(**new** Person(**"User3"**, **password2**,**password3**,**password1**,**password1**));  
 **personList**.add(**new** Person(**"User4"**, **password2**,**password**,**password2**,**password3**));  
 **file**.createNewFile();  
 FileWriter fileWriter = **new** FileWriter(**file**);  
 BufferedWriter bufferedWriter = **new** BufferedWriter(fileWriter);  
 **pass** = **password**;  
 bufferedWriter.write(**pass**);  
 bufferedWriter.newLine();  
 bufferedWriter.flush();  
 bufferedWriter.close();  
 **file1**.createNewFile();  
 fileWriter = **new** FileWriter(**file1**);  
 bufferedWriter = **new** BufferedWriter(fileWriter);  
 **pass1** = **password1**;  
 bufferedWriter.write(**pass1**);  
 bufferedWriter.newLine();  
 bufferedWriter.flush();  
 bufferedWriter.close();  
 **file2**.createNewFile();  
 fileWriter = **new** FileWriter(**file2**);  
 bufferedWriter = **new** BufferedWriter(fileWriter);  
 **pass2** = **password2**;  
 bufferedWriter.write(**pass2**);  
 bufferedWriter.newLine();  
 bufferedWriter.flush();  
 bufferedWriter.close();  
 **file3**.createNewFile();  
 fileWriter = **new** FileWriter(**file3**);  
 bufferedWriter = **new** BufferedWriter(fileWriter);  
 **pass3** = **password3**;  
 bufferedWriter.write(**pass3**);  
 bufferedWriter.newLine();  
 bufferedWriter.flush();  
 bufferedWriter.close();  
 }  
  
  
  
 **public void** testData(**int** length) **throws** IOException {  
 FileReader fileReader = **new** FileReader(**file**);  
 BufferedReader bufferedReader = **new** BufferedReader(fileReader);  
 **while** (bufferedReader.ready())  
 {  
 **pass** = bufferedReader.readLine();  
 }  
 fileReader = **new** FileReader(**file1**);  
 bufferedReader = **new** BufferedReader(fileReader);  
 **while** (bufferedReader.ready())  
 {  
 **pass1** = bufferedReader.readLine();  
 }  
 fileReader = **new** FileReader(**file2**);  
 bufferedReader = **new** BufferedReader(fileReader);  
 **while** (bufferedReader.ready())  
 {  
 **pass2** = bufferedReader.readLine();  
 }  
 fileReader = **new** FileReader(**file3**);  
 bufferedReader = **new** BufferedReader(fileReader);  
 **while** (bufferedReader.ready())  
 {  
 **pass3** = bufferedReader.readLine();  
 }  
 **personList**.clear();  
 **personList**.add(**new** Person(**"Administrator"**, **"r,w,ch"**,**"r,w,ch"**,**"r,w,ch"**,**"r,w,ch"**));  
 **personList**.add(**new** Person(**"User"**, **pass**,**pass1**,**pass2**,**pass3**));  
 **personList**.add(**new** Person(**"User1"**, **pass2**,**pass2**,**pass3**,**pass2**));  
 **personList**.add(**new** Person(**"User2"**, **pass3**,**pass1**,**pass3**,**pass1**));  
 **personList**.add(**new** Person(**"User3"**, **pass2**,**pass3**,**pass1**,**pass1**));  
 **personList**.add(**new** Person(**"User4"**, **pass2**,**pass**,**pass2**,**pass3**));  
 }  
 **public static** String randomCharacter(String characters)  
 {  
 **int** n = characters.length();  
 **int** r = (**int**) (n \* Math.*random*());  
 **return** characters.substring(r, r + 1);  
 }  
}

TableModel.java

**package** sample;  
  
**public interface** TableModel {  
 **void** generateTable(Person person);  
  
}

DModel.fxml

*<?***xml version="1.0" encoding="UTF-8"***?>  
  
<?***import javafx.scene.control.Button***?>  
<?***import javafx.scene.control.TableColumn***?>  
<?***import javafx.scene.control.TableView***?>  
<?***import javafx.scene.layout.Pane***?>*<**Pane maxHeight="-Infinity" maxWidth="-Infinity" minHeight="-Infinity" minWidth="-Infinity" prefHeight="400.0" prefWidth="600.0" xmlns="http://javafx.com/javafx/9.0.1" xmlns:fx="http://javafx.com/fxml/1" fx:controller="sample.Controller"**>  
 <**TableView fx:id="tabModel" layoutX="49.0" layoutY="100.0" prefHeight="200.0" prefWidth="483.0"**>  
 <**columns**>  
 <**TableColumn fx:id="columnObject" prefWidth="113.0" text="Object/Subject"** />  
 <**TableColumn fx:id="columnFile1" prefWidth="84.0" text="File\_1"** />  
 <**TableColumn fx:id="columnFile2" prefWidth="85.0" text="File\_2"** />  
 <**TableColumn fx:id="columnFlashCard" prefWidth="91.0" text="Flash-card"** />  
 <**TableColumn fx:id="columnCD\_RW" prefWidth="109.0" text="CD-RW"** />  
 </**columns**>  
 </**TableView**>  
 <**Button fx:id="btnResult" layoutX="49.0" layoutY="319.0" mnemonicParsing="false" onAction="#resultOnAction" prefWidth="75.0" text="Result"** />  
 <**Button fx:id="btnExit" layoutX="225.0" layoutY="319.0" mnemonicParsing="false" onAction="#exitOnAction" prefWidth="75.0" text="Exit"** />  
 <**Button fx:id="btnBack" layoutX="138.0" layoutY="319.0" mnemonicParsing="false" onAction="#backOnAction" prefWidth="75.0" text="Back"** />  
</**Pane**>

DModelUser.fxml

*<?***xml version="1.0" encoding="UTF-8"***?>  
  
<?***import javafx.scene.control.Button***?>  
<?***import javafx.scene.control.TableColumn***?>  
<?***import javafx.scene.control.TableView***?>  
<?***import javafx.scene.layout.Pane***?>*<**Pane maxHeight="-Infinity" maxWidth="-Infinity" minHeight="-Infinity" minWidth="-Infinity" prefHeight="400.0" prefWidth="600.0" xmlns="http://javafx.com/javafx/9.0.1" xmlns:fx="http://javafx.com/fxml/1" fx:controller="sample.Controller"**>  
 <**TableView fx:id="tabModel" layoutX="49.0" layoutY="100.0" prefHeight="200.0" prefWidth="483.0"**>  
 <**columns**>  
 <**TableColumn fx:id="columnObject" prefWidth="113.0" text="Object/Subject"** />  
 <**TableColumn fx:id="columnFile1" prefWidth="84.0" text="File\_1"** />  
 <**TableColumn fx:id="columnFile2" prefWidth="85.0" text="File\_2"** />  
 <**TableColumn fx:id="columnFlashCard" prefWidth="91.0" text="Flash-card"** />  
 <**TableColumn fx:id="columnCD\_RW" prefWidth="109.0" text="CD-RW"** />  
 </**columns**>  
 </**TableView**>  
 <**Button fx:id="btnGenerate" layoutX="49.0" layoutY="319.0" mnemonicParsing="false" onAction="#generateOnAction" prefWidth="75.0" text="Generate"** />  
 <**Button fx:id="btnExit" layoutX="225.0" layoutY="319.0" mnemonicParsing="false" onAction="#exitOnAction" prefWidth="75.0" text="Exit"** />  
 <**Button fx:id="btnBack" layoutX="138.0" layoutY="319.0" mnemonicParsing="false" onAction="#backOnAction" prefWidth="75.0" text="Back"** />  
</**Pane**>

sample.fxml

*<?***xml version="1.0" encoding="UTF-8"***?>  
  
<?***import javafx.scene.control.Button***?>  
<?***import javafx.scene.control.Label***?>  
<?***import javafx.scene.control.PasswordField***?>  
<?***import javafx.scene.control.TextField***?>  
<?***import javafx.scene.layout.ColumnConstraints***?>  
<?***import javafx.scene.layout.GridPane***?>  
<?***import javafx.scene.layout.Pane***?>  
<?***import javafx.scene.layout.RowConstraints***?>*<**GridPane alignment="center" hgap="10" vgap="10" xmlns="http://javafx.com/javafx/9.0.1" xmlns:fx="http://javafx.com/fxml/1" fx:controller="sample.Controller"**>  
 <**rowConstraints**>  
 <**RowConstraints** />  
 <**RowConstraints** />  
 </**rowConstraints**>  
 <**columnConstraints**>  
 <**ColumnConstraints** />  
 <**ColumnConstraints** />  
 </**columnConstraints**>  
 <**Pane prefHeight="172.0" prefWidth="308.0"**>  
 <**Label layoutX="14.0" layoutY="31.0" text="ID"** />  
 <**Label layoutX="14.0" layoutY="78.0" text="Password"** />  
 <**TextField fx:id="txtID" layoutX="73.0" layoutY="27.0" prefHeight="25.0" prefWidth="184.0"** />  
 <**Button fx:id="btnOkay" layoutX="73.0" layoutY="120.0" mnemonicParsing="false" onAction="#accessButtonAction" prefHeight="25.0" prefWidth="78.0" text="Okay"** />  
 <**Button fx:id="btnCancel" layoutX="179.0" layoutY="120.0" mnemonicParsing="false" onAction="#cancelButtonAction" prefWidth="78.0" text="Cancel"** />  
 <**PasswordField fx:id="txtPassword" layoutX="73.0" layoutY="74.0" prefHeight="25.0" prefWidth="184.0"** />  
 </**Pane**>  
</**GridPane**>