Київський національний торговельно-економічний університет

Кафедра кібернетики та системного аналізу

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Моделі економічної безпеки та захисту інформації в електронному бізнесі»

Студента 2 курсу, 1м групи,

спеціальності
051 «Економіка»

_____
підпис студента

Поляничко Павло Павлович

спеціалізації
«Економічна кібернетика»

Науковий керівник
Кандидат фізико-математичних наук, доцент

_____
підпис керівника

Баннікова Світлана Олександрівна

Гарант освітньої програми
доктор фізико-математичних наук, професор

_____
підпис керівника

Гамалій Володимир Федорович

Київ 2018

Київський національний торговельно-економічний університет

Факультет обліку, аудиту та інформаційних систем
Кафедра кібернетики та системного аналізу
Спеціальність 051 «Економіка»
Спеціалізація «Економічна кібернетика»

Затверджую
Зав. кафедри _____Роскладка А. А.
«05»листопада 2017р.

Завдання
на випускну кваліфікаційну роботу (проект) студенту

Поляничко Павлу Павловичу

1. Тема випускної кваліфікаційної роботи (проекту)
«Моделі економічної безпеки та захисту інформації в електронному бізнесі»
Затверджена наказом ректора від *«02» жовтня 2017 р. № 3035*
2. Строк здачі студентом закінченої роботи *15 листопада 2018 року*
3. Цільова установка та вихідні дані до роботи
Мета роботи: дослідження концептуальних моделей для захисту інформації і забезпечення безпечної і безперебійної роботі підприємств сфери електронної комерції.
Об'єкт дослідження: процеси захисту інформації.
Предмет дослідження: моделі економічної безпеки і методи захисту електронного бізнесу.
4. Перелік графічного матеріалу_____
_____
_____

5. Консультанти по роботі із зазначенням розділів, за якими здійснюється консультування:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Баннікова С. О.	05.11.2017 р.	05.11.2017 р.
2	Баннікова С. О.	05.11.2017 р.	05.11.2017 р.
3	Баннікова С. О.	05.11.2017 р.	05.11.2017 р.

6. Зміст випускної кваліфікаційної роботи (проекту) (перелік питань за кожним розділом)

ВСТУП

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ ЕЛЕКТРОННОГО БІЗНЕСУ

1.1. Українське законодавство в сфері забезпечення безпеки інформації

1.2. Кібербезпека як один з ключових напрямів захисту важливих даних для електронного бізнесу

1.3 «Білі хакери» - сучасний тренд технологій безпеки

Висновки до розділу 1

РОЗДІЛ 2. АНАЛІЗ СУЧАСНИХ СПОСОБІВ ЗАХИСТУ ПІДПРИЄМСТВ ЕЛЕКТРОННОГО БІЗНЕСУ

2.1.Сучасні загрози і аспекти для захисту інформації

2.2.Види захисту інформації

2.3.Система управління інформаційною безпекою(СУІБ) як необхідна складова електронного бізнесу

Висновки до розділу 2

РОЗДІЛ 3. РОЗРОБКА МОДЕЛІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

3.1. Інструменти, методи та технології розробки моделі СУІБ

3.2. Ключові елементи для захисту інформації

3.3. Програмна реалізація

Висновки до розділу 3

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

7. Календарний план виконання роботи

№ пор.	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1	*Вибір теми випускної кваліфікаційної роботи*	*01.10.2017*	*01.10.2017*
2	*Розробка та затвердження завдання на випускну кваліфікаційну роботу*	*05.11.2017*	*05.11.2017*
3	*Вступ*	*01.04.2018*	
4	*Розділ 1. Теоретичні основи захисту інформації у сфері електронного бізнесу*	*01.05.2018*	
5	*Розділ 2. Аналіз сучасних способів захисту підприємств електронного бізнесу*	*20.06.2018*	
6	*Підготовка статті у збірник наукових статей магістрів*	*15.09.2018*	
7	*Розділ 3. Розробка моделі системи управління інформаційною безпекою*	*01.10.2018*	
8	*Висновки*	*01.11.2018*	
9	*Здача випускної кваліфікаційної роботи на кафедру науковому керівнику*	*15.11.2018*	
10	*Попередній захист випускної кваліфікаційної роботи*	*22.11.2018*	
11	*Виправлення зауважень, зовнішнє рецензування випускної кваліфікаційної роботи*	*25.11.2018*	
12	*Представлення готової зшитої випускної кваліфікаційної роботи на кафедру*	*31.11.2018*	
13	*Публічний захист випускної кваліфікаційної роботи*	*За розкладом роботи ЕК*	

8. Дата видачі завдання «05» листопада 2017 р.

9. Керівник випускної кваліфікаційної роботи (проекту)

Баннікова С.О.
(прізвище, ініціали, підпис)

10. Гарант освітньої програми Гамалій В.Ф.
(прізвище, ініціали, підпис)

11. Завдання прийняв до виконання студент-дипломник

Поляничко П. П.
(прізвище, ініціали, підпис)

12. Відгук керівника випускної кваліфікаційної роботи (проекту)

____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

Керівник випускної кваліфікаційної роботи (проекту)
__________________ 15.11.2018 р.
(підпис, дата)

13. Висновок про випускну кваліфікаційну роботу (проект)

Випускна кваліфікаційна робота (проект) студента ______________________
(прізвище, ініціали)
може бути допущена до захисту в екзаменаційній комісії.

Гарант освітньої програми__________________________Гамалій В.Ф.______
(підпис, прізвище, ініціали)

Завідувач кафедри __________________________________Роскладка А.А.___
(підпис, прізвище, ініціали)
«_____»__________________2018 р.

Анотація

В даній роботі розглянуто методи і моделі захисту інформації електронного підприємства, сучасні тренди і загрози в сфері економічної безпеки, загальні методи створення систем управління інформаційною безпекою. Визначено основні небезпеки і способи протидії при створенні СУІБ. Було розглянуто основні методи захисту інформації і убезпечення діяльності підприємств електронного бізнесу.

Було розроблено модель системи управління інформаційною безпекою. В роботі описано інструменти, ключові елементи для захисту інформації, використані при розробці моделі а також найважливіші складові для підтримки безпечної роботи підприємств електронної комерції.

Ключові слова: електронний бізнес, захист інформації, системи управління інформаційною безпекою, економічна безпека.

Anotation

This thesis is addressed to the development of automated approaches for information security management system, general methods for solving problems of information and economic security for e-business. The main methods for protection enterprise activity are reviewed. Basic methods of information protection and existing option for creation information security management system are reviewed.

Model of information security management system for e-business was created. This thesis describes tools, key elements for protection information used in the development model of information security management system and the most important constituents of this system is described.

Keywords: e-business, information protection, information security management system, economic security.

ЗМІСТ

ВСТУП

Важко переоцінити роль інформації у сучасному житті. Кожну хвилину ми отримуємо десятки повідомлень в месенжерах. Наша стрічка новин в соціальних мережах постійно оновлюється, показуючи новини з різних куточків світу. Важливість інформації проявляється не лише у нашому приватному житті, а й у бізнесі. Важко уявити сучасний бізнес без баз даних, у яких знаходяться дані про постачальника, ціни та опції товарів і послуг, маркетингові акції, системи спілкування з клієнтами, контролю дистрибуції та виробництва. Зауважимо, що усі ці засоби мають зв'язок з інтернетом, де ми маємо одну з найбільщ небезпечних загроз для сучасного підприємства – кіберзлочини.

Прикладом кіберзлочину та масштабів його дії може бути вірус Petya, який у жовтні 2017 року паралізував 90% інфраструктури країни. І надалі в Україні економічна загроза постійно зростає, що пов'язано із зростанням кіберзлочинів на 2,5 тисячі на рік і як засіб правового захисту у 2017 році було відкрито 4,5 тисячі кримінальних проваджень.

Розглядаючи детальніше поняття кіберзлочину стає зрозумілою його неоднорідність, адже сюди можна віднести як DDOS атаку на сайт з метою вимагання грошей за його розблокування, так і викрадення персональних даних клієнтів фінансових установ, інформації що становить комерційну таємницю, наприклад, умови договорів з контрагентами, персональні данні топ-менеджменту компанії, данні про нові товари та послуги, а також маркетингові заходи.

Виходячи з усього цього, в епоху тотальної прозорості виникає необхідність убезпечити важливу інформацію для компанії від сторонніх осіб. Результатом протидії цієї нової загрози стало створення комплексних систем захисту інформації(КСЗІ), які максимально ускладнюють доступ до неї та її витік. Вони являють собою не лише технічні та програмні засоби, а й організаційно-правові норми для здійснення роботи з інформацією у компанії, які полягають у створенні ролей з правом доступу, регламентування правил

додавання зміни і розповсюдження інформації, використання зовнішніх накопичувачів даних.

Поруч з такими високотехнологічними засобами інформаційної безпеки а також класичними засобами безпеки (криптографічний захист інформації) з'явились інші спеціалісти, так звані етичні або білі хакери (на мережевому сленгі «white hat hackers»). Їхня робота полягає не у здійсненні кіберзлочинів, як звичайні хакери, а у взаємодії з компаніями –виробниками ПО, а також підприємствами для знаходження слабких місць у доступу до інформації і способів їх вирішення.

Підсумовуючи все вище сказане, варто зазначити актуальність кібербезпеки, зокрема створення систем захисту економіки та бізнесу, адже сьогодні ми живемо в час, коли найбільшою цінністю є інформація, а враховуючи те що кількість користувачів глобальної мережі інтернет невпинно зростає, ми можемо говорити про зростання загроз, пов'язаних із незаконним отриманням чи викраденням даних як фізичних осіб так і компаній, які проводять свою комерційну діяльність в інтернеті.

На сучасному етапі розвитку підприємництва збільшується важливість у створенні комплексних систем захисту інформації, що максимально зменшує загрозу для інформації підприємства. При цьому, така система поєднує у собі організаційно-правову основу, технічні і програмні засоби, розмежування доступу та оновлення програмного забезпечення і особливо діяльність, пов'язану із хмарними сервісами.

Мета дипломної роботи є дослідження та аналіз існуючих моделей і систем захисту інформації та створення нової моделі комплексної системи захисту інформації.

Об'єктом дослідження є методи реалізаціїбезпеки підприємства.

Предметом дослідження є практичні засоби створення систем захисту інформації.

Відповідно до мети було поставлено такі **завдання:**

1. Дослідити теоретичні та методологічні основи захисту інформації в інтернеті.
2. Розглянути існуючі моделі та системи захисту інформації
3. Дослідити моделі поняття електронного бізнесу.
4. Створити модель системи захисту інформації в електронному бізнесі.

Аналіз останніх досліджень і публікацій. Поняття «інформаційної безпеки» розглядали Близнюк І.М., Братель О.Р., Бондаренко В.О., Бучило І.Л., Горбатюк О.М., Гуцалюк О.М., Ляшенко О.М., Камлик М.І., Козаченко Г.В., Остроухов В.В., Пономарьов В.П., Стрельцов А.А., Расторгуєв С.П., Цимбалюк В.Л., Чубарук Т.І., Щербина В.М

.

Розділ 1

1.1. Українське законодавство в сфері забезпечення безпеки інформації

Для розгляду засобів і способів захисту інформації варто спочатку ознайомитись із українським законодавством у цій сфері а саме які способи захисту нам дозволені законодавцем. Для цього звернемось до таких законодавчих актів і нормативних документів, як:

- Закон України «Про інформацію» від 02.10.1992 № 2657-XII
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
- Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI
- Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
- Постанова Кабінету міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 р. №1893
- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
- НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
- НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу
- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Закон України «Про інформацію» у 1 статті визначає поняття захист інформації та інформації як «захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї; інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді…».При цьому у статті 6 зауважується, що «. Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації,

одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя»

У розділі 2 статті 21 розглядається поняття доступу до інформації і з'являється поняття інформації з обмеженим доступом. «1.За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. 2.Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.», а в наступній статті детально описується що вважається інформацією з обмеженим доступом «1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. 2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень…4. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

5-1) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов'язковому оприлюдненню відповідно до закону;

{ Частину четверту статті 21 доповнено пунктом 5-1 згідно із Законом N 1405-VIII (1405-19) від 02.06.2016 }

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.»

Виходячи з усього цього ми отримуємо перший спосіб захисту інформації (організаційно-правовий) виділення важливої інформації у категорію інформація з обмеженим доступом.

У законі України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР регламентуються поняття захисту інформації між суб'єктами правовідносин. В особливості розглядаються поняття, блокування витоку та знищення інформації, криптографічний захист інформації «…вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо», а також комплексна система захисту інформації «взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації»

Держава у статті 8 регламентує системи обробки даних з обмеженим доступом, які повинні бути оброблятись із застосуванням комплексної системи

захисту інформації з підтвердженою відповідністю, підтвердження здійснюється за результатами державної експертизи.

Отже, держава на законодавчому рівні розробила спосіб захисту інформації – визначення її як інформації з обмеженим доступом. Також регламентовано створення програмних засобів для її захисту і обов'язкові правила стандартизації та сертифікації ПО.

1.2. Кібербезпека як один з ключових напрямів захисту важливих даних для електронного бізнесу

У попередньому пункті ми розглядали регламентовані державою організаційно-правові норми захисту інформації, також поняття конфіденційної інформації і комплексних систем захисту інформації. Для подальшого захисту інформації від кіберзлочинів необхідно детально розглянути поняття комплексних систем захисту інформації, які повинні проходити державну стандартизацію, а також інформацію яка підлягає захисту. Відповідно до Положення «Про державну експертизу в сфері криптографічного захисту інформації» об'єктами експертизи виступають «засоби та методи, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ; звіти про наукові дослідження і розробки, результати тематичних досліджень, інші результати наукової та науково-технічної діяльності у сфері КЗІ; криптографічні алгоритми та протоколи; алгоритми, протоколи, засоби та системи генерації, тестування та розподілу ключових даних; криптографічні системи, засоби та обладнання КЗІ, програмно-технічні комплекси центрів сертифікації ключів, надійні засоби електронного цифрового підпису (далі - криптографічні засоби);положення державних і міждержавних програм та проектів державного значення в частині, що стосується КЗІ.

1.6. Експертиза є обов'язковою або добровільною. Обов'язковій експертизі підлягають: засоби та методи, призначені для розробки,

дослідження, виробництва та випробувань засобів криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом; криптографічні алгоритми та криптографічні протоколи, які планується визначити як такі, що рекомендовані для використання або як національні стандарти; алгоритми, протоколи, засоби та системи генерації, тестування та розподілу ключів; криптосистеми, засоби й обладнання криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, програмно-технічні комплекси центрів сертифікації ключів, які передбачають акредитацію, надійні засоби електронного цифрового підпису; криптосистеми, засоби та обладнання КЗІ іноземного виробництва, які підлягають експортному контролю; результати тематичних досліджень.»

Розглядаючи підприємства сфери електронного бізнесу, варто зазначити що електронний бізнес і електронна комерція поняття різні, проте електронний бізнес включає у себе електронну комерцію ,а також електронний документообіг, більшість із них мають спеціалізоване програмне забезпечення для управління клієнтами, виробництвом(за потреби),персоналом(підготовкою та навчанням).Сучасне програмне забезпечення все частіше переходить на хмарні технології, що створюю загрозу витоку даних при їх передачі/отриманні а також можливість стороннього підключення. Розглядаючи кібербезпеку підприємств в мережі Інтернет, варто звернути увагу і загрози і засоби захитсу держави.

За оцінками експертів, щорічні втрати світової економіки в результаті дій кіберзлочинців можуть досягати 500 мільярдів дол. США, в той час, як, наприклад, річний ВВП Швейцарії в 2017 році оцінюється в 659 мільярдів доларів США [1]. У таблиці 1.1 наведено найгучніші інциденти з витоку інформації у США, можна побачити що найбільшу шкоду становить людський фактор.

№ з/п	*Інцидент*	*Кількість потерпілих*	*Збитки (дол.)*
1	Витік даних про ветеранів та військовослужбовців США	28,7 млн.	45 млрд.
2	Викрадено ноутбук співробітника Natiowide Building Society	11 млн.	1,5 млрд.
3	Крадіжка диску з приватною інформацією клієнтів Dai Nippon Printing	8,64 млн.	1,2 млрд.
4	З медичного центру викрадено ноутбук з персональними картками лікарів та пацієнтів	1,8 млн.	367 млн.
5	З офісу Affiliated Computer Services викрадено ноутбук з даними клієнтів	1,4 млн.	320 млн.
6	Фірма-підрядник Texas Guaranteed загубила леп-топ з даними клієнтів	1,3 млн.	237 млн.
7	Пропав лептоп з автомобіля співробітника Boeing	382 тис.	147 млн.
8	З офісу страхової компанії CS Stars пропав ноутбук з іменами, адресами та номерами соцстрахування робітників Нью-Йорка	540 тис.	84 млн.
9	Співробітник бухгалтерської фірми Hancock Askew втратив ноутбук з персональними даними клієнтів	401 тис.	73 млн.
10	В медичному центрі Vassar Brothers зник лептоп та резервний диск з медичними картками пацієнтів	257 тис.	47 млн.

Таблиця 1.1. Інциденти з витоку інформації у США (За даними ComputerWorld/Україна)

Більшість менеджерів і власників підприємства розглядають кібезагрози лише як зовнішній фактор(стороннє підключення до каналу передачі, злам і викрадення даних).При цьому найбільше джерело небезпеки для підприємства це його персонал. Сторонньому спеціалісту треба великий пласт часу для розшифрування і викрадення даних, при цьоу працівники підприємства мають можливість як переслати чи вивести дані(на зовнішній носій),так і запустити вірус на ПО з зовнішніх носіїв чи через електронну пошту.Можливий варіант коли через недостатню підготовленість і обізнаність людина може нанаести шкоду компанії і безпеці важливих даних.

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

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

Виходячи з наведених даних варто вказати, що при створенні КСЗІ одним з нафважливіших моментів виступає як створення ролей користувачів, їх рівнів доступу і можливих дій у системі так і навчання персоналу що до користування системою і підключення сторонніх пристроїв.

У 2012 році американська компанія, розробник антивірусного програмного забезпечення McAfee, що належить Intel Corporation, виступила спонсором у створенні глобального звіту про стан світової кібербезпеки [3].Рейтинг встановили по 5-бальній системі. Узагальнені данні наведено у таблиці 1.2

Практично всі фахівці кожної з 27 країн, які були опитані в ході складання звіту, одностайно зійшлися у тому, що для підвищення ефективності боротьби з кіберзлочинністю необхідний глобальний обмін інформацією. Крім того, всі вони відзначили необхідність не просто забезпечення обміну інформацією, а саме його оперативність та швидкість у прийняті управляючих рішень.[2]

Рейтинг	**Країна**
5	–
4,5	Фінляндія, Ізраїль, Швеція
4	Данія, Естонія, Франція, Німеччина, Нідерланди, Іспанія, Великобританія, США
3,5	Австралія, Австрія, Канада, Японія
3	Китай, Італія, Польща, Росія
2,5	Бразилія, Індія, Румунія
2	Мексика

Таблиця 1.2 Рейтинг безпеки країн

Європейське агентство з мережевої та інформаційної безпеки (англ.: European Network and Information Security Agency – ENISA) у своїй «Програмі надійності та захисту ключової інформаційної інфраструктури» (англ.: Cisco International Internship Program – CIIP), як і експерти, які були залучені Security & Defence Agenda, також наполягає на необхідності налагодження співпраці з метою гарантій узгодженості характерних методик кіберборотьби [4].

Виходячи із даного дослідження можна створити перелік ключових позицій для забезпечення кібербезпеки як України в цілому так і українських підприємств у сфері електронного бізнесу[4]:

- визначення адекватного механізму, в основному у вигляді суспільно-партнерства, який дозволить приватним та державним зацікавленим

сторонам обговорювати та затверджувати політики, пов’язані з проблемою кібербезпеки;

- планування та визначення необхідних політик та регулюючих механізмів, чітке позначення ролей, прав та відповідальності для приватного та державного сектора у сфері протидії кіберзлочинності;
- визначення ключових інформаційних інфраструктур, у тому числі – основних активів, сервісів та взаємозалежностей;
- підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;
- доказ необхідності нової програми освіти в якій робиться акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки;

Отже, в сфері кібербезпеки важливим є не лише створення програмних засобів для захисту, а й державне приватне партнерство, яке у свою чергу підвищить ефективність і оперативність прийнятих дій, а також дозволить системно реагувати на загрози.При цьому слід зазначити важливість як криптографічного захисту, так і організаційно-правові аспекти безпеки на підприємстві, адже одна з найбільших небезпек- дії персоналу.

1.3. «Білі хакери» - сучасний тренд технологій безпеки

Електронний бізнес для захисту своїх даних використовує організаційно-правові, технологічні і технічні засоби. При цьому в сучасному світі з’явилась можливість використовувати «білих хакерів». Найчастіше їх називають «white-hat hackers» (білі капелюхи), або етичні хакери.

Етичні хакери швидко стають важливою частиною зброї архітектури корпоративної безпеки підприємства. Так звані "білі шапки" - щоб відрізнити їх від своїх шкідливих чорних капелюхів - все більше виконують роль за тестом проникнення. По мірі загрози змінюються набори етичних хакерів, що

охоплюють соціальну інженерію, соціальні мережі та споживацькі мобільні технології.[5] У статті 21 серпня 2017 року cbsnews опублікувала 2 розмови з білими хакерами. У ній [6]“Білі хакери" - це хороші хлопці, які платять компанії, щоб зламати їхні системи та знаходити недоліки, перш ніж вони будуть експлуатуватися кібер-злочинцями або "Чорними капелюхами".CBS News подорожував в Мумбаї, Індія, щоб познайомитись із одним із найкращих у світі хакерів з білого шару, Сандеп Сінгх, більш відомий своїм онлайн-іменем "Geekboy".

Індія виникла як провідна держава в кібервійні. “Білі хакери" повідомляють про більше вразливостей для компаній звідси, ніж хакери де-небудь у світі. "Geekboy" з гарячими компаніями, такими як Microsoft, Facebook, Twitter, Uber і AirBnb, з гарними намірами. І він отримує за це добре - компанії пропонують високу оплату людям, які знаходять вразливі місця в своїх системах, які вони можуть потім виправляти.

Такі компанії, як Убер, набирають цю допомогу. Сандеп відправився з Індії в Лас-Вегас, щоб конкурувати з найкращими хакерами у світі для HackerOne, хаккатону, де хакерські хакери шукають уразливості в компаніях, що співпрацюють. Убер був однією з компаній, які відкрили себе для хакерів у конкурсі. Мелані Енсіг, який керує кібербезпекою для Убер, вважає, що ці програми стимулюють хакерських комах. "Найголовніше пам'ятати про те, що хтось завжди намагається зламати ваш продукт, незалежно від того, чи знаєте ви це чи ні", це насправді є наступним поколінням захисту ".

Наприклад, в 1983 році група, яка називає 414, проникли в дослідницьку установу з ядерної зброї в штаті Лос-Аламос в Нью-Мексико, але вони не зловживали та не продавали привілейовану інформацію. ФБР спіймав їх, але судді виконували поблажливість через відсутність хакерів злочинного наміру, і вони не отримали жодного часу в тюрмі. У кінцевому підсумку Winslow став мережевим інженером, який частково працював над посиленням стандартів кібербезпеки. Злочини 414-х років змусили законодавців розробляти

конкретні положення щодо комп'ютерних злочинів, які не існували на початке 1980-х років. Але, мабуть, більш помітно, що Уїнслоу може вважатись - якщо не попередником - хабарництвом. Незрозуміло, хто вперше застосував терміни "біла капелюшка" та "чорна шапка", хоча культурний натяк на фільми раннього західного періоду та їх явне сприйняття доброго проти зла очевидні. Але ідея санкціонованого викрадення існувала до Winslow: згідно з 1981 роком The New York Times, компанія Timesharing National CSS Inc. заохочувала співробітників втручатися в свої системи, щоб знайти слабкі місця або помилки. У 2001 році для IBM Systems Journal, infosec експерт C.C. Палмер визначив роботу білих капелюхів як "етичний злодій" і пояснив, що американські військові часто займаються цим, щоб знати свої вразливі дані.[7]

Висновки до розділу 1

Отже відповідно до Положення «Про державну експертизу в сфері криптографічного захисту інформації» об’єктами експертизи виступають 1.засоби та методи, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ; 2. звіти про наукові дослідження і розробки, результати тематичних досліджень у сфері КЗІ; 3.криптографічні алгоритми та протоколи; алгоритми, протоколи, засоби та системи генерації, тестування та розподілу ключових даних; 4. криптографічні системи, засоби та обладнання КЗІ, 5.програмно-технічні комплекси центрів сертифікації ключів, 6.надійні засоби електронного цифрового підпису; 7.положення державних і міждержавних програм та проектів у частині, що стосується КЗІ.

РОЗДІЛ 2

2.1.Сучасні загрози і аспекти для захисту інформації

Електронний бізнес являє собою поєднання електронної комерції і електронного документообігу, що за умови швидкої інформатизації суспільства призводить до загрози витоку даних, їх зміни видалення та модифікації, чи підключення до каналів зв'язку сторонніх осіб. Та поруч з цим більшість сучасного бізнесу як класичного так і електронного переходить на хмарні рішення-в хмарних середовищах встановлюють ПО і знаходяться бази даних. З економічної точки зору це зручніше, так як дозволяє зекономити кошти на необхідні техніку та ПО, при цьому з'являється загроза викрадення даних з хмарних сервісів або ж їх перехоплення при передачі/отриманні. Класичні криптографічні способи для захисту інформації поступово стають менш ефективними, що при збільшення часу виконання операцій вимагає нового рішення.

Зважаючи, що заходи забезпечення ІБ в організації спрямовуються головним чином на те, щоб не допустити збитків від втрати інформації, правомірно перш за все сконцентрувати увагу на визначенні загроз – сукупності умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства та держави в цілому в інформаційній сфері.[8] Передумовою появи загроз ІБ є як об'єктивні (недосконаліть засобів захисту), так і суб'єктивні фактори (промислове шпигунство, карні елементи, несумлінні співробітники тощо).

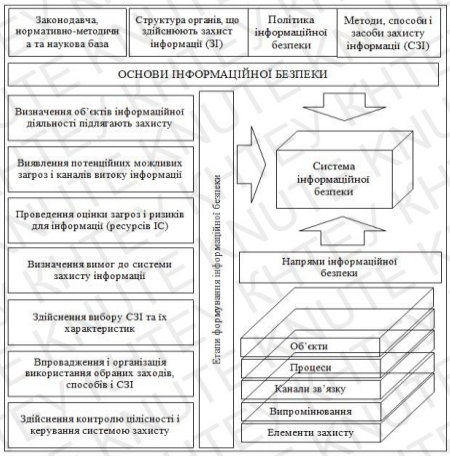

Рис. 2.1. Основи, етапи та напрями формування ІБ

Природа походження загроз ІБ може бути при цьому випадковою (збоїв, помилки, побічні впливи тощо), або навмисною (злочинні дії соціуму), табл.2.1.

ТИП ЗАГРОЗИ		Причини або спонукальні мотиви
Навмисні загрози	**Ненавмисні загрози**	
Розкрадання носіїв інформації	–	Прагнення використовувати конфіденційну інформацію (КІ) у своїх цілях
Застосування програмних пасток	–	
–	Несправність апаратури, що може ініціювати несанкціоноване зчитування ІР	Недостатня кваліфікація обслуговуючого персоналу, застосування несертифікованих технічних засобів
Використання програм «троянський кінь»	–	Завдання збитків шляхом НСД в інформаційну систему (ІС)
Помилки в програмах обробки інформації	–	Завдання збитків шляхом внесення програмних закладок у процесі розробки програмних систем
Впровадження комп'ютерного вірусу	–	Руйнування ІС з метою завдання збитків
–	Помилки в програмах обробки інформації	Застосування несертифікованого програмного продукту
–	–	Недотримання персоналом вимог ІБ, порушення технологічної послідовності роботи з ІС
Помилкова комутація в мережі ЕОМ	–	З метою створення каналу для витоку КІ
–	Помилкова комутація в мережі ЕОМ	НКВ обслуговуючого персоналу
–	Паразитне електромагнітне випромінювання (ЕМВ)	Недостатнє урахування вимог безпеки на етапі проектування ІС або її створення
–	Перехресні наведення за рахунок ЕМВ	
Примусове ЕМВ	–	Вивід з ладу ІС з метою завдання збитків
Використання акустичних випромінювань	–	Одержання конфіденційної інформації
Копіювання за допомогою візуального і слухового контролю	–	
Маскування під користувача, підбор паролю	–	Несанкціоноване втручання в роботу системи в злочинних цілях
–	Помилка в роботи оператора	Недостатня кваліфікація, застосування несертифікованого ПЗ
–	Помилки користувача	Використання недостатнього захисту
Помилки програміста: опис, перекручування програмного захисту, розкриття кодів, паролів	–	З метою добування особистої вигоди або завдання збитків
Помилки технічного персоналу: опис і перекручування схем захисту, помилкова комутація	–	–
–	Помилки персоналу: перекручування схем захисту, помилкова комутація	Недостатня кваліфікація обслуговуючого персоналу, порушення технології

Таблиця 2.1. Типи загроз інформаційній безпеці в інформаційних системах

Засобами реалізації загроз як правило є: шкідливе та потенційно небезпечне ПЗ (computer virus; worm; trojan horse; rootkit; spyware тощо), Internet-шахрайство (phishing, carding, pharming, sms phishing тощо), несанкціонований доступ (НСД) до ІР та ІС (hacking, deface), DoS та DDoS-атаки тощо. За наслідками своєї дії загрози ІБ спрямовані на порушення *конфіденційності, цілісності та доступності до інформації* (рис.2). Оцінку можливих актуальних загроз ІБ в організації доцільно починати з аналізу джерел загроз, обумовлених різними факторами.

Рис. 2.2 Ознаки загроз конфіденційності, цілісності та доступності інформації

Джерелами загроз можуть виступати: *людина, технічні пристрої, моделі, алгоритми, програми; технологічні схеми обробки; зовнішнє середовище.* Прикладом цьому можуть слугувати статистичні дані, оприлюднені аналітичним центром компанії InfoWatch. Фахівці компанії стверджують, що останнім часом більше половини інцидентів, зафіксованих в компаніях, а саме біля 65,4%, пов'язані з внутрішніми порушниками. При цьому витік інформації відбувається з їх вини або по необережності. Причиною більше 32% витоку інформації на ОІД стають зовнішні зловмисники. У 51,2% випадків винуватцями витоків інформації були нинішні та колишні робітники – 48,9% і 2,3% відповідно. Тобто, як видно, нині саме людський фактор є одним з основних чинників ризику з точки зору ІБ організації.[9-11]

В контексті ситуаційного підходу процедуру оцінювання ймовірної реалізації загроз доцільно починати з актуальних загроз із ряду відомих класифікацій загроз [12 – 17] щодо вибраної організації (рис.3).

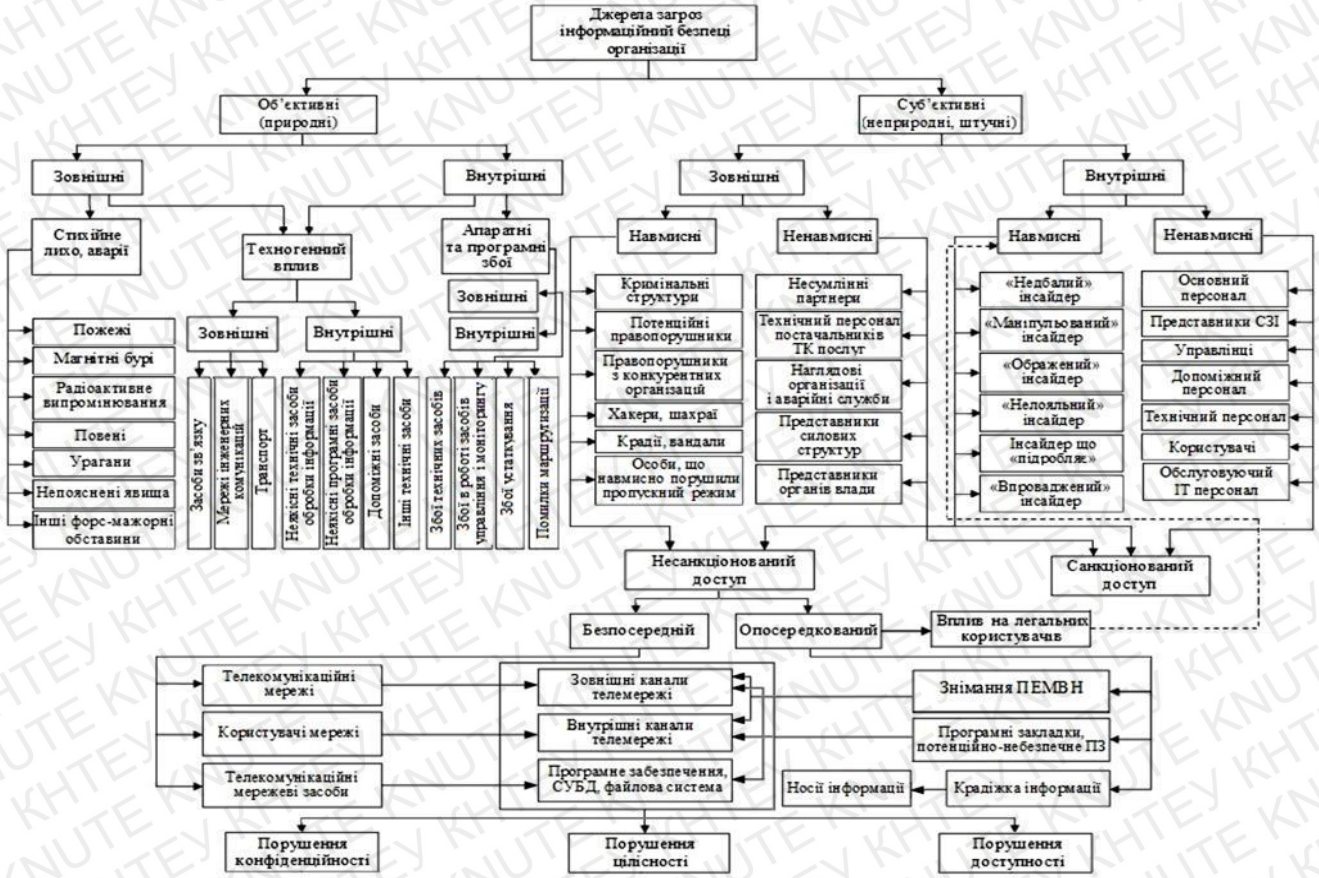

Рис. 2.3. Класифікація загроз за видами ознак та можливі цілі їх прояву

Загалом інформація пронизує всі сфери життя суспільства, створюючи нову основу розвитку економіки, культури і взагалі нову характеристику соціуму. Вивченням питання інформаційної безпеки займалися такі вчені, як С. Ф. Гуцу, Б. А. Кормич, А. І. Марущак,О. А. Сороківська [17-20].Класичними чинниками економічної безпеки країни, за визначенням О. А. Кулініч, є «активізація попиту і відповідна за обсягами та структурою реакція пропозиції» [21, с. 59-60].Учений під класичними чинниками економічної безпеки розуміє чинники сталого економічного зростання, які досліджує через вивчення та порівняння зростання внутрішнього попиту, зміни його структури за секторами та верствами населення. Живко З. Б. та Керницькою М. І.

проаналізовано чинники позитивного та негативного, прямого та опосередкованого впливу у різних сферах безпеки, зазначено роль індикаторів і чинників економічної безпеки, визначено та досліджено суть соціально-економічної безпеки [22, с. 14-15].Кавун С. В. визначає життєвий цикл економічної безпеки підприємства та досліджує основні рівні економічної безпеки підприємства [23, с. 17-18].Усі економічно розвинуті країни світу використовують переваги інформаційних технологій у виробничій, комерційній та банківських сферах. Це пояснюється тим, що традиційні методи не дозволяють зорієнтуватись в сучасному інформаційному потоці і проаналізувати динамічні процеси економічної діяльності підприємства. Швидше за все розвиваються технології, по'вязані з глобальною комп'ютерною мережею Інтернет, що призвело до появи таких нових категорій, як електронна торгівля, електронний бізнес, електронний уряд та ін.[19, с. 32] Не викликає сумніву і той факт, що між рівнем економічної безпеки і інформаційною складовою існує пряма залежність. Як показує практика, будь-яка акція, спрямована проти господарюючого суб'єкта, розпочинається зі збору інформації, саме тому питання інформаційної безпеки давно ввійшли до головних пріоритетів практично всіх великих підприємств. Усе більше керівників розуміють, наскільки небезпечною може бути інсайдерська інформація, системи обробки інформації і дії співробітників, які беруть участь у діяльності підприємства [25].

Для регулювання економічної безпеки на підприємстві створюється служба інформаційної безпеки, що має виявляти і наочно демонструвати власникам підприємства весь спектр загроз в інформаційній сфері. Завдання керівників служби переконати, що протистояти загрозам можна тільки на основі створення і упровадження ефективних систем захисту інформації [18].

Виділимо найпоширеніші види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій:

– відсутність регламентованого доступу до файлів даних;

– вільне втручання в програмне забезпечення;

– відсутність протоколювання змін у програмному забезпеченні;

– відсутність регламентації користувачів інформації;

– відсутність дублювання важливих документів на документальних носіях даних;

– часті удосконалення одного і того ж програмного забезпечення різними особами;

– відсутність схем інформаційного забезпечення рівнів управління;

– наявність непідзвітних посадових осіб у системі управління тощо [24, 26-28].

Створюючи системи захисту на підприємстві, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту. Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки. У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями [25]:

1) розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;

2) організація і здійснення конкретних видів діяльності із захисту інформації;

3) експлуатація технічних засобів захисту інформації;

4) аудит і контроль функціонування системи інформаційної безпеки підприємства [29,с. 131]

Способи захисту інформації передбачають використання певного набору засобів. Для запобігання втрати та витоку таємних даних використовуються засоби:

- фізичні;
- апаратні;
- програмні;
- апаратно-програмні;
- законодавчі;
- криптографічні та організаційні методи.

Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об’єктів. Вони реалізуються на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, що захищаються.

Апаратні засоби захисту – це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв’язку тощо.

Програмні засоби захисту, які вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

Апаратно-програмні засоби захисту – це засоби, які основані на синтезі програмних та апаратних засобів.

Законодавчі засоби – комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, що охороняються, і визначають міру відповідальності за втрату або крадіжку секретної інформації.

Організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу [32]

2.2.Види захисту інформації

Найпоширенішим засобом захисту інформації є шифрування.На сьогоднішній день існує багато алгоритмів шифрування, серед яких зустрічаються достатньо вдалі та широко використовувані, що розроблені не тільки спецслужбами, а й приватними особами. Їх опис можна знайти у багатьох наукових джерелах [34, 37, 39,40, 41, 42, 46-49].

Взагалі "криптографія" – грецьке слово, що походить від слів kryptos (таємний, схований) та graphy(запис) і включає методи і засоби забезпечення перетворення даних з метою маскування (шифрування) змісту інформації для гарантування конфіденційності та цілісності, а криптоаналіз, відповідно, орієнтований на зламування шифротекстів (шифрів).

Галузі застосування криптографії: безпечний зв'язок: веб-трафік: HTTPS, бездротовий трафік: 802.11i WPA2 (WEP), GSM, Bluetooth; шифрування файлів на диску: EFS, TrueCrypt; захист контенту (DVD, Blu-Ray): CSS, AACS; аутентифікація користувачів тощо.

Шифротекст є даними, представленими в зашифрованій формі і мають прихований семантичний зміст, який утворюються після шифрування (криптографічного перетворення) відкритого тексту (з неприхованим семантичним змістом). Зародження криптографії почалося з глибокої давнини, з якої до нас дійшов ряд систем шифрування, які швидше за все

з'явилися одночасно з писемністю в 4 тис. до н. е. Методи секретного переписування були винайдені незалежно в багатьох стародавніх суспільствах (Єгипет, Шумер, Китай).Шифрування – оборотне перетворення даних, з метою приховання інформації, дешифрування –зворотній процес, що полягає у відновленні первинних (до шифрування) даних. Проте, у сучасній літературі [18] можна знайти інші визначення: під шифруванням розуміється синтез процесів зашифрування і розшифрування, а от дешифрування – це відновлення вхідного тексту без знання ключа (тобто, це процес злому шифру – криптоаналіз). Єдиної думки сьогодні не існує, можливу дану ситуацію виправить прийняття національного стандарту у галузі криптографії. Крім забезпечення конфіденційності ДІР, криптографія застосовується для розв'язання таких задач, як:

− перевірка справжності (автентифікація).Одержувач може встановити відправника, а зловмисник не може під нього маскуватися;

− цілісність. Отримувач може перевірити несанкціоновану модифікацію в тексті, а зловмисник не може видати підробний текст за справжній;

− не заперечення авторства. Відправник не може в подальшому заперечувати відсилання даних.

У сучасній криптографії можна виділити такі базові розділи:

1) Симетрична (з секретним ключем) криптографія;

2) Асиметрична (з відкритим ключем) криптографія;

3) Квантова криптографія.

Симетрична криптографія [38, 45, 51] – це сукупність криптографічних методів, у яких використовується один секретний ключ для зашифрування і розшифрування.

Асиметрична криптографія [38, 45, 51] – це сукупність криптографічних методів, у яких використовуються роздільні ключі для

реалізації процесу зашифрування і розшифрування – відкритий і секретний. У таких методах секретність повідомлень ґрунтується на складності обчислення ключа за деякою функціонально залежною від нього інформацією, що передається, як правило, різними каналами зв'язку.

Квантова криптографія [35, 36, 44, 50] – наука, що вивчає методи захисту систем зв'язку і базується на постулатах квантової механіки, об'єкти якої (здебільшого це фотони, хоча, в принципі, можуть використовуватись і інші носії) забезпечують процеси безпечної передачі інформації.

Криптосистема – це алгоритм плюс усі можливі відкриті тексти, шифротексти і ключі. Алгоритм вважається обчислювально безпечним (чи, як іноді називають, криптостійкими), якщо він не може бути зламаний (розкритий) з використанням доступних обчислювальних ресурсів зараз чи у майбутньому [38, 43]. З огляду на це, для визначення обчислювальної стійкості використовують потужні сучасні GRID системи, та інші обчислювальні мережі (які, до речі, є загальнодоступними в мережі Інтернет і приєднатися до них може будь-який користувач).

Гібридна криптосистема – криптосистема, що базується на методах асиметричної і симетричної криптографії, при цьому криптографічна система з відкритим ключем задіюється тільки для управління загальними ключами, які потім використовуються в традиційних криптосистемах із секретним ключем.

Під комбінованою криптографічною системою захисту інформації у даній роботі будемо розуміти сукупність взаємопов'язаних компонентів, серед яких елементи симетричної, асиметричної і квантової криптографії, спрямованих на забезпечення захищеної передачі ДІР.

Виходячи із [43, 45] можна сформулювати основні принципи криптографії:

1) Принцип рівної міцності захисту. На шляху від одного законного власника до іншого ДІР можуть захищатись різними способами в залежності від загроз, що виникають. Так утворюється ланцюг захисту ДІР з ланками різного типу. Противник прагне знайти найслабкішу ланку, щоб з найменшими витратами добратися до інформації. Законні власники повинні враховувати це у своїй стратегії захисту ДІР криптографічними методами: безглуздо робити якусь ланку дуже міцною, якщо є слабкіші ланки.

2) Принцип доцільності захисту. На сучасному рівні технічного розвитку засоби зв'язку, засоби перехоплення повідомлень, а також засоби захисту ДІР вимагають занадто великих витрат. Тому, існує проблема співвідношення вартості ДІР, витрат на їх захист та витрат на її здобування. Перш ніж захищати ДІР криптографічними методами, треба відповісти на два питання:

– Чи отримає противник внаслідок атаки ДІР, що будуть більш цінними, ніж вартість самої атаки?

– Чи є ДІР, які захищає її власник, більш цінними, ніж вартість захисту? Відповідь на ці два питання визначає доцільність захисту й вибір підходящих засобів криптографічного захисту.

3) Принцип використання ключа. Розробка хорошого шифру – справа надзвичайно трудомістка. Тому, бажано збільшити термін життя цього шифру і використовувати його для шифрування якнайбільшої кількості повідомлень. Але при цьому виникає небезпека, що противник вже зламав шифр і вільно читає шифровані повідомлення. Саме тому в сучасних шифрах використовують ключі. Ключем в криптографії називають змінюваний елемент шифру, який застосовується для шифрування конкретного повідомлення. При цьому вважають, що сам шифр (крім ключа) є відомим противнику і доступним для вивчення. Оригінальність подання повідомлення забезпечується тільки періодично змінюваним ключем. Знання ключа

дозволяє швидко та просто відновити початковий текст. Без знання ключа дешифрування тексту має бути практично недосяжним.

4) Принцип стійкості шифру. Здатність шифру протидіяти різноманітним атакам на нього називається стійкістю шифру. З математичної точки зору проблема отримання строго доведених оцінок стійкості для будь-якого шифру ще не вирішена. Ця проблема відноситься до проблем нижніх оцінок обчислювальної складності задачі, ще нерозв'язаних математично. Тому, стійкість конкретного шифру оцінюється шляхом різноманітних спроб його зламування, а отримані результати оцінюють в залежності від кваліфікації криптоаналітиків, що атакують цей шифр.

5) Принцип Керкхоффса. Стійкість сучасного шифру має визначатись, в першу чергу, ключем. Зміст цього принципу полягає в тому, що захищеність інформації не повинна залежати від таких чинників, які важко змінити при появі загрози. При використанні ключів законним власникам ДІР легше перешкоджати противнику, оскільки міняти їх можна досить часто. Щоправда, тепер перед законними власниками виникає інша задача – як таємно обмінятись ключами перед тим, як обмінюватись шифрованими повідомленнями.

6) Принцип використання різноманітних шифрів. Не існує єдиного шифру, що підходить до всіх випадків. Вибір шифру залежить від особливостей інформації (може мати різний характер, тобто бути документальною, телефонною, телевізійною, комп'ютерною тощо), від цінності інформації, від обсягів інформації, від потрібної швидкості її передачі, від тривалості захисту ДІР (державні та військові таємниці зберігаються десятками років, біржеві – декілька годин), від можливостей зловмисника (можна протидіяти окремій особі, можна протидіяти потужній державній структурі), а також від можливостей власників ДІР.

2.3.Система управління інформаційною безпекою(СУІБ) як необхідна складова електронного бізнесу

Пошук підприємствами засобів комплексного захисту інформації привів до розробки систем управління інформаційною безпекою(СУІБ).Дані системи являють собою організаційний стандарт який включає в себе в цілому моменти обмеження доступу до інформації такі як наприклад авторизація та ідентифікація клієнтів, розмежування прав доступу, можливостей обробки інформації(редагування чи видалення).

Для ефективної роботи такої системи необхідною умовою є створення на управлінському рівні документів які організовують порядок обробки інформації, підключення зовнішніх носіїв даних та вводу-виводу даних із сховища. Даний стандарт також регламентує використання криптографічного захисту інформації а також електронний цифровий підпис (ЕЦП).

Нагадаємо що криптографічний захист інформації це спосіб захисту інформації шляхом її шифрування. Схематично принцип криптографічного захисту показано на рисунку 2.1

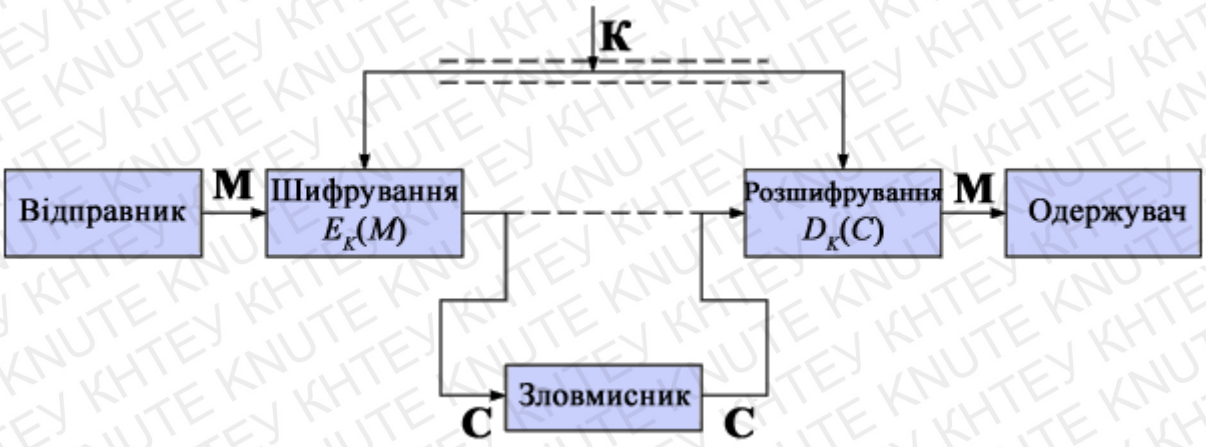

Рис.2.4 Криптографічний захист інформації

Що ж до електронного цифрового підпису, то це вид електронного підпису який використовується для захисту електронних документів, і являє собою вид електронного підпису отриманого криптографічним перетворенням даних

який додається до набору даних і може підтвердити його цілісність і підтверджувати відправника. Даний спосіб захисту накладається за допомогою особистого ключа та перевіряється відкритим ключем. Одним із програмних продуктів ,що реалізують цей спосіб захисту інформації є засіб електронного цифрового підпису «CryptoLibV2»,який включає у себе:

- бібліотеки взаємодії Avtor Cryptographic Provider.
- допоміжне програмне забезпечення.
- високорівневі бібліотеки інтеграції

Даний програмний продукт виконує наступні завдання:

- генерацію особистих ключових даних згідно ДСТУ 4145-2002 і PKCS#1 RSA Cryptography Standard;
- імпорт/експорт даних;
- створення і перевірку ЕЦП на блок даних довільної довжини;
- обчислення ґеш-кодування-функції згідно з ГОСТ 34.311-95;
- шифрування/розшифрування даних відповідно до ДСТУ ГОСТ 28147:2009;
- виготовлення імітовставки з використанням криптографічного алгоритму ДСТУ ГОСТ 28147:2009;
- шифрування/розшифрування повідомлень відповідно до PKCS#1 RSA Cryptography Standard;
- обчислення ґеш-кодування-функції згідно з міжнародними алгоритмами SHA1 і SHA-256 згідно з ДСТУ ISO/IEC 10118-3:2005;
- шифрування і виготовлення MAC з використанням міжнародних алгоритмів TDES і AES згідно з ISO/IEC 18033.

На сьогодні це один із засобів криптографічного захисту основна спеціалізація якого ЕЦП, який можна використовувати для захисту інформації, та інтеграції з іншими програмними продуктами організації.

Отже, для комплексного захисту інформації у компанії можливо використовувати як окремі програмні засоби так і спеціалізоване програмне забезпечення. Та для його ефективної роботи необхідна реалізація системи управління інформаційною безпекою, я яка являє собою організаційні норми з розподілу прав доступу і можливостей обробки інформації.

Висновки до розділу 2

Важко переоцінити важливість захисту даних підприємства в сучасних умовах, особливо врахувавши перехід підприємств у сферу електронного бізнесу. За таких умов на головне місце для компаній виходить потреба у безпеці їх комерційних даних, як результат- створення програмних засобів для регулювання доступу, шифрування та секретної передач даних

Наслідком цього стала розробка управлінської концепції систем управління інформаційною безпекою, яка максимально убезпечує данні від витоку «зсередини», та створення комплексної системи захисту інформації, яка являється не лише організаційно-правовим, а й апаратним, програмним і технологічним засобом обмеження доступу до інформації, яка включає як прості засоби захисту (ідентифікація, авторизація, ролі доступу) , так і максимально технологічні засоби (ЕЦП, криптографічний захист).

РОЗДІЛ 3. РОЗРОБКА МОДЕЛІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

3.1. Інструменти, методи та технології розробки моделі СУІБ

Серед засобів захисту інформації особливе місце належить системам управління інформаційною безпекою(СУІБ)і комплексної системи захисту інформації(КСЗІ).Система управління інформаційною безпекою являється частиною системи управління, вужчим з двох понять і розглядає в своїй основі лише організаційні і програмні аспекти доступ до інформації, а комплексна система захисту інформації розглядає нормативно-правові, організаційні, інженерно-технічні та програмні засоби.

Виходячи з цього варто вказати, що КСЗІ доцільно використовувати як всю систему в цілому так і її компоненти, перший варіанти необхідний у великих підприємствах, виходячи з великої кількості ресурсів, а, для малих підприємств рішенням є як використання компонентів КСЗІ так і створення чи купівля спеціалізованих систем захисту інформації чи хмарних рішень.

СУІБ включає в себе організаційно-правові моменти:

- визначення бізнес-процесів
- організація надання доступу
- захист інформації паролем
- контроль доступу до даних
- захист мереж
- автентифікація користувача
- ідентифікація користувача
- криптографічний захист інформації
- ЕЦБ(електронний цифровий підпис)

Комплексні системи захисту інформації включають в себе 5 рівнів

1. Прикладний та програмний

1.1.Аудит та моніторингу

1.2.Засоби антивірусного захисту

1.3.Ідентифікація і автентифікація

1.4.Розмежування доступу

2. Мережевий

2.1.Системи відслідковування втручань

2.2.Міжмережеві екрани

2.3.Віртуальні приватні мережі

2.4.Програмні засоби аналізу захищеності

3. Апаратний

3.1.Контроль портів вводу-виводу

3.2.Засоби блокування пристроїв

3.3.Апаратні ключі

4. Криптографічний

5. Організаційний

5.1.Організація правил доступу

5.2.Регламентування обробки, зовнішнього вводу-виводу інформації

На сьогодні стандартом створення СУІБ є ISO/IEC 27001:2005, який являє собою управлінські норми і заснований на процесах аналізу і оцінки ризиків, показників захищеності і заходів захисту. На основі цього стандарту виникають етапи організації СУІБ:

1. Визначення БП(бізнес-процесів) що підлягають захисту
2. Створення політики безпеки
3. Визначення аналіз та оцінка ризиків
4. Створення процедур СУІБ
5. Імплементація системи управління
6. Сертифікація СУІБ

Автентифікація являє собою перевірку і підтвердження аспектів інформаційної взаємодії, використовують її за умови коли загрозу може

нести не лише 3 сторона а й безпосередній учасник взаємодії. При транзакціях даний спосіб захисту ознаає перевірку цілісності з'єднання, обмеження повторної передачі даних і вчасної передачі даних. Часто ідентифікацію також називають автентифікацією хоча перше означає підтвердження однієї із сторін спілкування.На сьогодні існує 4 найпоширеніших способи автентифікації

- Паролі чи PIN-коди
- Одноразовий пароль
- CHAP
- Callback

Персональні ідентифікаційні номери (Паролі чи PIN-коди) – це інформація яку знає користувач та інший учасник взаємодії, одноразовий пароль- значення яке використовується для підтвердження особи лише 1 раз(наприклад при реєстрації на сайт).

CHAP – спосіб автентифікації на основі унікального запиту та секретної відповіді, типовим прикладом є секретне запитання у банку, також часто банківську установи використовують останній засіб- Callback. Його суть полягає у здійсненні телефонного дзвінка з серверу з метою запиту підтвердження дій.[52]

Також для підтвердження особи відправника чи створювача документів використовується цифровий підпис. Цифровий підпис являє собою два алгоритми один із яких обчислює, а інший- перевіряє підпис. При цьому якщо обчислення підпису може робити лише автор, то алгоритм перевірки доступний для кожного.

З метою перевірки модифікацій повідомлення використовують хеш-функції, так як їх відносно легко обчислити та майже неможливо розшифрувати, існує 4 типи.

- MD2 - найповільніша, оптимізована для 8-бітових машин

- MD4-найшвидша, оптимізована для 32-бітних машин. Не так давно зламана
- MD5-найбільш поширена з сімейства MD-функцій. Схожа на MD4, але засоби підвищення безпеки роблять її на 33% повільніше, ніж MD4. Забезпечує цілісність даних. Вважається безпечною
- SHA (Secure Hash Algorithm)- створює 160-бітове значення хеш-функції з вихідних даних змінного розміру. Запропоновано NIST і прийнята урядом США як стандарт. Призначена для використання в стандарті DSS

В суті електронного підпису створення контрольного значення(хеш-значення), отримувач перевіряє отримане з ключа значення і з повідомлення, і якщо вони ідентичні то повідомлення не піддавалось зміні і було відправлене підтвердженим відправником. На сьогодні найпоширеніші 4 алгоритми цифрового підпису:

1. DSA (Digital Signature Authorization) Алгоритм з використанням відкритого ключа для створення електронного підпису, але не для шифрування. Секретне створення хеш-значення і публічна перевірка її - тільки одна людина може створити хеш-значення повідомлення, але будь-хто може перевірити її коректність. Заснований на обчислювальній складності взяття логарифмів в кінцевих полях.
2. RSA Запатентована RSA електронний підпис, що дозволяє перевірити цілісність повідомлення та особистість особи, що створила електронний підпис. Відправник створює хеш-функцію повідомлення, а потім шифрує її з використанням свого секретного ключа. Одержувач використовує відкритий ключ відправника для розшифровки хеша, сам розраховує хеш для повідомлення, і порівнює ці два хеша.

3. MAC (код аутентифікації повідомлення) Електронний підпис, що використовує схеми хешування, аналогічні MD або SHA, але хеш-значення обчислюється з використанням, як даних повідомлення, так і секретного ключа.
4. DTS (служба електронних тимчасових міток) Видає користувачам тимчасові мітки, пов'язані з даними документа, криптографічних стійким чином.[52]

На сьогодні головним засобом захисту є криптографічний захист(шифрування).Не дивлячись на те що досить багато про даний спосіб захисту інформації було сказано у попередніх розділах варто розглянути детальніше алгоритми шифрування.

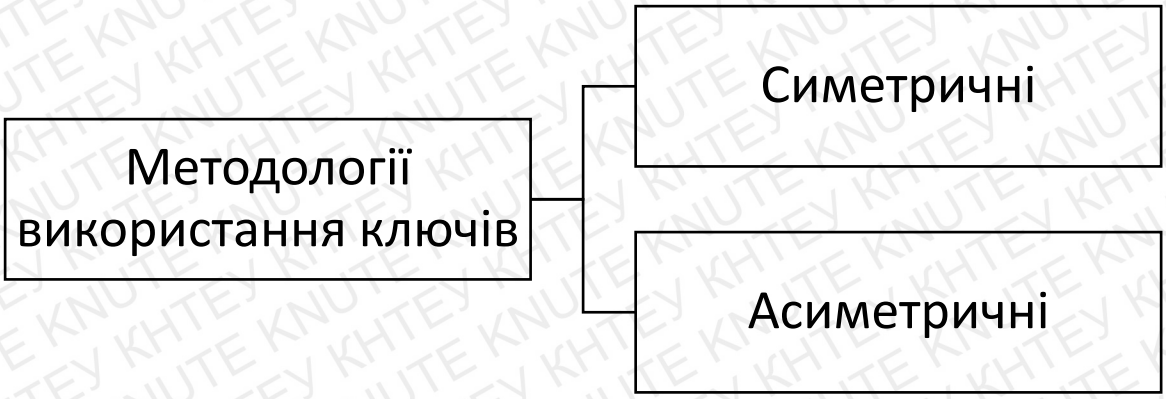

Рис 3.1 Методологія використання ключів

Різниця між симетричною і асиметричною методологією полягає у тому, що при симетричній методології використовується один ключ для шифрування і розшифрування симетричного алгоритму шифрування, при

цьому ключ передається обом користувачам до передачі даних. У асиметричній методології для шифрування даних використовується алгоритми симетричного шифрування і симетричні ключі, після цього використовуються методи асиметричного шифрування і асиметричні ключі для шифрування симетричного ключа. Результатом є два взаємопов'язаних асиметричних ключі, при цьому симетричний ключ зашифрований одним асиметричним ключем розшифровується іншим ключем. За цих умов один асиметричний ключ повинен бути переданий власникові, а інший – відповідальному за зберігання ключів (CA-сертифікатного центру ключів) до початку їх використання.

Для більш детального розгляду криптографічного захисту розглянемо алгоритми шифрування, поділяють їх на 2 категорії:

- Симетричні
- Асиметричні

Симетричні використовують одинакові алгоритми для шифрування і розшифрування. На сьогодні найпоширенішими з них являються 13 :

DES (Data Encryption Standard) Популярний алгоритм шифрування, використовуваний як стандарт шифрування даних урядом США. Шифрується блок з 64 біт, використовується 64-бітовий ключ (потрібно тільки 56 біт), 16 проходів.

Може працювати в 4 режимах:

· Електронна кодова книга (ECB-Electronic Code Book) - звичайний DES, використовує два різних алгоритмів.

· Ланцюговий режим (CBC-Cipher Block Chaining), в якому шифрування блоку даних залежить від результатів шифрування попередніх блоків даних.

· Зворотній зв'язок по виходу (OFB-Output Feedback), використовується як генератор випадкових чисел. Зворотній зв'язок по шифратору (CFB-Cipher

Feedback), використовується для отримання кодів аутентифікації повідомлень.

3-DES або потрійний DES 64-бітний блоковий шифратор, використовує DES 3 рази з трьома різними 56-бітними ключами. Досить стійкий до всіх атак

Каскадний 3-DES Стандартний потрійний DES, до якого доданий механізм зворотного зв'язку, такий як CBC, OFB або CFB. Дуже стійкий до всіх атак.

FEAL (швидкий алгоритм шифрування) Блоковий шифратор, використовується як альтернатива DES. Розкритий, хоча після цього були запропоновані нові версії.

IDEA (міжнародний алгоритм шифрування) 64-бітний блоковий шифратор, 128-бітовий ключ, 8 проходів. Запропоновано недавно; хоча до цих пір не пройшов повної перевірки, щоб вважатися надійним, вважається більш кращим, ніж DES

Skipjack Розроблено АНБ в ході проектів уряду США "Clipper" і "Capstone". До недавнього часу був секретним, але його стійкість не залежала тільки від того, що він був секретним. 64-бітний блоковий шифратор, 80-бітові ключі використовуються в режимах ECB, CFB, OFB або CBC, 32 проходу

RC2 64-бітний блоковий шифратор, ключ змінного розміру. Приблизно в 2 рази швидше, ніж DES. Може використовуватися в тих же режимах, що і DES, включаючи потрійне шифрування. Конфіденційний алгоритм, власником якого є RSA Data Security

RC4 Потоковий шифр, байт-орієнтована, з ключем змінного розміру. Приблизно в 10 разів швидше DES. Конфіденційний алгоритм, яким володіє RSA Data Security

RC5 Має розмір блоку 32, 64 або 128 біт, ключ з довжиною від 0 до 2048 біт, від 0 до 255 проходів. Швидкий блоковий шифр. Алгоритм, яким володіє RSA Data Security

CAST 64-бітний блоковий шифратор, ключі довжиною від 40 до 64 біт, 8 проходів. Невідомо способів розкрити його інакше як шляхом прямого перебору.

Blowfish. 64-бітний блоковий шифратор, ключ змінного розміру до 448 біт, 16 проходів, на кожному проході виконуються перестановки, залежні від ключа, і підстановки, залежні від ключа і даних. Швидше, ніж DES. Розроблений для 32-бітових машин

Пристрій з одноразовими ключами Шифратор, який не можна розкрити. Ключем (який має ту ж довжину, що і шифровані дані) є наступні 'n' біт з масиву випадково створених біт, що зберігаються в цьому пристрої. У відправника і одержувача є однакові пристрої. Після використання біти руйнуються, і наступного разу використовуються інші біти.

Потокові шифри Швидкі алгоритми симетричного шифрування, зазвичай оперують бітами (а не блоками біт). Розроблені як аналог пристрою з одноразовими ключами, і хоча не є такими ж безпечними, як воно, принаймні практичні.[52]

Асиметричні алгоритми використовують для шифрування симетричного ключа, використовується 2 різних ключі, один відомий а інший таємний. Зазвичай для розшифрування використовують обидва ключі, та інформація зашифрована одним ключем може бути розшифрована лише іншим ключем.

Основні алгоритми:

1. RSA
2. ECC
3. Ель-Гамаль

RSA Популярний алгоритм асиметричного шифрування, стійкість якого залежить від складності факторизації великих цілих чисел.

ECC (криптосистема на основі еліптичних кривих) Використовує алгебраїчну систему, яка описується в термінахточок еліптичних кривих, для реалізації асиметричного алгоритму шифрування. Є конкурентом по відношенню до інших асиметричним алгоритмам шифрування, так як при еквівалентній стійкості використовує ключі меншої довжини і має велику продуктивність. Сучасні його реалізації показують, що ця система набагато ефективніша, ніж інші системи з відкритими ключами. Його продуктивність приблизно на порядок вище, ніж продуктивність RSA, Діффі-Хеллмана і DSA. [52]

Ель-Гамаль. Варіант Діффі-Хеллмана, який може бути використаний як для шифрування, так і для електронного підпису.

3.2. Ключові елементи для захисту інформації

Базуючись на даному стандарті необхідно проаналізувати процеси в компанії, загрози для безпеки інформації підприємства. В нашому випадку ми розглядаємо підприємство яке надає аутсорсингові послуги в сфері маркетингу і продажів – створення сайтів, реклами і глобальній мережі і соціальних мережах, зовнішній відділ продажів і обслуговування клієнтів, контроль якості. Основними активами що підлягають захисту є дані працівників та клієнтів компанії, CRM система, а також електронна переписка.

Схематично структура підприємства показана на рисунку 3.2

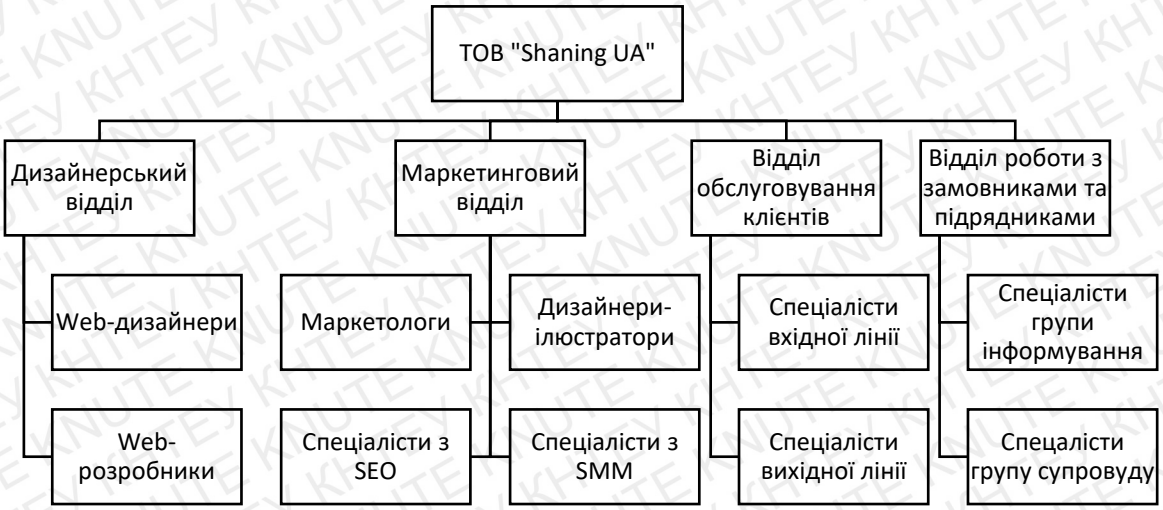

Рисунок 3.2. Структура підприємства

Наступним етапом є розгляд процесів компанії, а також необхідного доступу для різних спеціальностей працівників. Для максимального контролю за інформаційними ресурсами працівник заходить із свого персонального чи робочого комп’ютера на віддалений робочий стіл

Спочатку розглянемо процеси взаємодії із замовниками

Процес складається з декількох етапів:

1. Перший контакт із клієнтом
2. Інформування про компанію, запрошення в офіс.
3. Обговорення специфіки діяльності клієнта, підготовка комерційної пропозиції
4. Обговорення ключових моментів, підписання договору.
5. Виконання договірних зобов’язань сторонами, підготовка звітної документації по обговореним строкам(місяць, квартал, півріччя, рік).
6. Вирішення конфліктних і спірних питань, зміна умов договору(за потреби), зміна обов’язків, регламентів діяльності пов’язана із бажанням замовника, форс-мажорні ситуації, розірвання договору.

За перші 3 пункти відповідальний спеціаліст групи інформування, за четверти, п’ятий і шостий етап відповідальний спеціаліст групи супроводу. Виходячи з даної інформації для убезпечення інформації від витоку інформації спеціалісти групи супроводу не повинні бачити інформацію про те хто привів клієнта у компанію(замість персональних даних спеціаліста групи інформування код).Також необхідно прописати порядок роботи спеціалістів групи супроводу з електронною пошту, адже через неї зловмисник може відправити вірус.

Наступним етапом роботи підприємства і замовника є обговорення його представлення в глобальній мережі Інтернет, що включає в себе аудит сайту, аккаунтів і рекламних кампаній у соціальних мережах та налаштування рекламних кампаній в пошукових системах із аналізом семантичного ядра.

На цьому етапі роботи із клієнтом працює спеціаліст групи супроводження, маркетолог і дизайнер компанії, а також спеціалісти з SEO і SMM.Найважливішою інформацією на даному етапі є «Клієнтська карта» та анкета клієнта у якій він відповідає на 117 про свій бізнес, для детальної розробки «Клієнтської карти».

«Клієнтська карта» включає в себе 4 розділи. В першому детально прописані типажі клієнтів замовника, їх інтереси і цінності. Другий розділ містить детальну інформацію про товари і послуги для них що пропонує клієнти, їх ключові конкурентні переваги. Наступний розділ регламентує канали продажів і комунікації із клієнтами, регламент спілкування, скрипти продажів, також тут обумовлюється питання дизайну усіх рекламних матеріалів, фірмові кольори шрифти та логотип. Четвертий розділ регламентує звітність між замовником і виконавцем, звітні періоди і дати підготовки документів, форму їх подачі та відповідальних осіб. Також у даному розділі вказуються ключові показники важливі для клієнта.(рис 3.3)

Рис 3.3 Клієнтська карта

Усі ці данні зберігаються на хмарних серверах і передаються через десктопні чи мобільні додатки тому за їх безпеку відповідальність несе сервіс зберігання, та постає необхідні в обов'язковій змінні всіх паролів щомісяця та створенні центру з управління паролями їх створенням, блокуванням та заміною.

Після детальної опрацювання «Клієнтської карти» представником відділу супроводження і замовником формуються технічні завдання на сторінку компанії в мережі інтернет, семантичне ядро для рекламних компаній, вимоги до таргетованої реклами та ретаргетингу, правила ведення, а також матеріал і дизайн постів, у соціальних мережах. На цьому етапі відбувається тісна взаємодія представників дизайнерського і маркетингового відділів, тому для запобігання витоку інформації кожному проекту присвоюється унікальний ідентифікатор і працівник бачить лише код, що ускладнює витік інформації. Також варто вказати що для перенесення інформації на сторонній пристрій необхідний спеціальний ключ доступу, який є лише у працівників відділу роботи з замовниками та керівництва. Для усіх документів і усіх працівників

розроблений електронний цифровий підпис як спосіб підтвердження відправника.

Останнім етапом до проектної роботи є підготовка зведеного звіту для замовника. Зведений звіт це документ який включає в себе інформацію про компанію-замовника та його товари, цільові аудиторії клієнтів і їх детальний опис, канали продажів і комунікації з цільовою аудиторією, регламент роботи працівників ТОВ "Shaning UA" (ТОВ «Шайнінг Україна») з клієнтами замовника, додатково вказуються моменти для коригування усіх заходів компанії відносно останній розділ прописує форми подачі звітів, їх аналітичне і графічне представлення, терміни подачі на підпис відповідальним особам та звітні періоди.

Таким чином, ТОВ "Shaning UA" це компанія головною цінністю якою виступає як інформація у формі приватного листування працівник-замовник, працівник-працівник так і бази даних із списком замовників, працівників, проектів і проектних рішень. При цьому особливе місце у безпеці необхідно виділити брифінгу із 117 запитань для замовника та «Клієнтської карти» так як інформація у них є цілковитою власністю замовника і передається компанії на умовах комерційної таємниці. Загроза викрадення чи зміни інформації у базах даних стосується хмарного сховища, і основною небезпекою у цьому випадку є внутрішній персонал компанії. Для захисту у цьому випадку було створено схему ролей і прав доступу до різних категорій інформації та доступу до них.

3.3. Програмна реалізація

Для реалізації моделі системи захисту електронного бізнесу створимо програму що буде перевіряти дані для входу в програму і в залежності від активованої адміністратором ролі буде показувати дані по проектам. Для створення програмного засобу використаємо програмне середовище Visual Studio 2017 та СУБД MS SQL.

В основі програми знаходиться база даних у якій виділено:

1. Ролі користувачів і їх данні на вхід
2. Дозволені дії для різних ролей
3. Список проектів
4. Список клієнтів
5. Коди персоналу
6. Клієнтська карта

Процес роботи програми починається із входу у систему, на цьому рівні програма перевіряє відповідність логіну та паролю, а також чи активований користувач. У випадку невідповідності даних на екран виводиться повідомлення.

Наступним етапом відкривається основний екран залежно від ролі користувача.

Ролі користувача

1. Адміністратор системи безпеки
2. Керівник підприємства/відділу/групи
3. Спеціалісти групи інформування/супроводу
4. Розробники
5. Дизайнери/Ілюстратори
6. Спеціалісти SEO/SMM

Виходячи з цього списку варто зазначити що адміністратор служби безпеки відповідальний лише за питання створення зміни та видалення профілів користувачів у системи та означення їх ролей. В категорії працівників підприємства робочий екран має 4 основних області показників:

1. Операційна діяльність
2. Планові завдання
3. Економічні показники
4. Звіти

Меню для інших ролей разом із коротким описом наведено на рис 3.4

спеціаліст групи інформування	План заходів - включає в себе плани всіх заходів для знаходження клієнтів
	Поточні заходи - планові заходи
	Клієнти - показує заявки від нових клієнтів, їх короткий опис
	Кошторис - інформує про фінансові частини заходів,створює документи на оплату оренди, полграфічних послуг та ін
працівник групи супроводу	Завдання - показує заплановані зустрічі і етапи роботи із кліжентами на найближчий вибаний період(за умовчуваня м 1 тиждень)
	Проекти - карта проектів
	Клієнти - відображає список поточних клієнтів працівника
	Фінансові результати - показує фінансові показники доступних проектів
Розробники	Планові завдання - відображає завдання на потчний тждень із строками
	Проекти- відображає дані доступних проектів
	Зв'язок з працівником групи супроводу(відповідно до проекту)
Дизайнери/Ілюстратори	Дизайн-завдання - заплановані проектом дизайн-концепції
	Завдання від працівників проекту - додаткові графічні матерали по проектам
	Проекти - карта проекту
	Зв'язок з працівником групи супроводу(відповідно до проекту)
Спеціалісти SEO/SMM	Рекламні компанії виводить список усіх рекламних компаній спеціаліста
	Проекти -карта проекту
	Зв'язок з дизайнером/ілюстратором(відповідно до проекту)
	Зв'язок з працівником групи супроводу(відповідно до проекту

Рисунок 3.4 Опис меню для ролей в системи EntGuard

В основі бази даних програми таблиця із списком проектів та довідник клієнтів. В подальшій діяльності використовуються таблиці такі як Клієнтська карта(client_card), довідник заходів і приміщень , список зареєстрованих клієнтів, список працівників.

Першочерговим є авторизація у програмі (рис 3.5), як бачимо відсутнє меню реєстрації, адже її виконує адміністратор вносячи дані працівника до системи доступу програми, наведено на рис. 3.6

При авторизації програма перевіряє введені дані і в залежності від активної ролі завантажує робочу область.

В робочій області адміністратора програми відслідковуються усі зареєстровані користувачі та їх дані, є можливість створювати та видаляти користувачів.

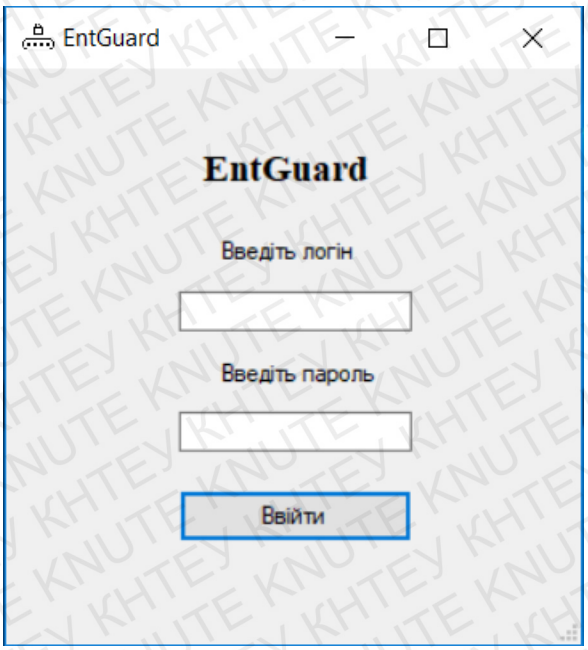

Рис 3.5 Форма реєстрації

Рис 3.6. Робоча область адміністратора програми

Що ж до робочих областей працівників то одна з них, а саме робоча область працівника групи супроводу відображена на рис. 3.7.На ній відображено відкритий пункт «Планова діяльність». В даному пункті

фіксуються усі заплановані заходи а зустрічі з можливими клієнтами, а також є можливість додати нові заходи. Також є можливість фільтрації по даті.

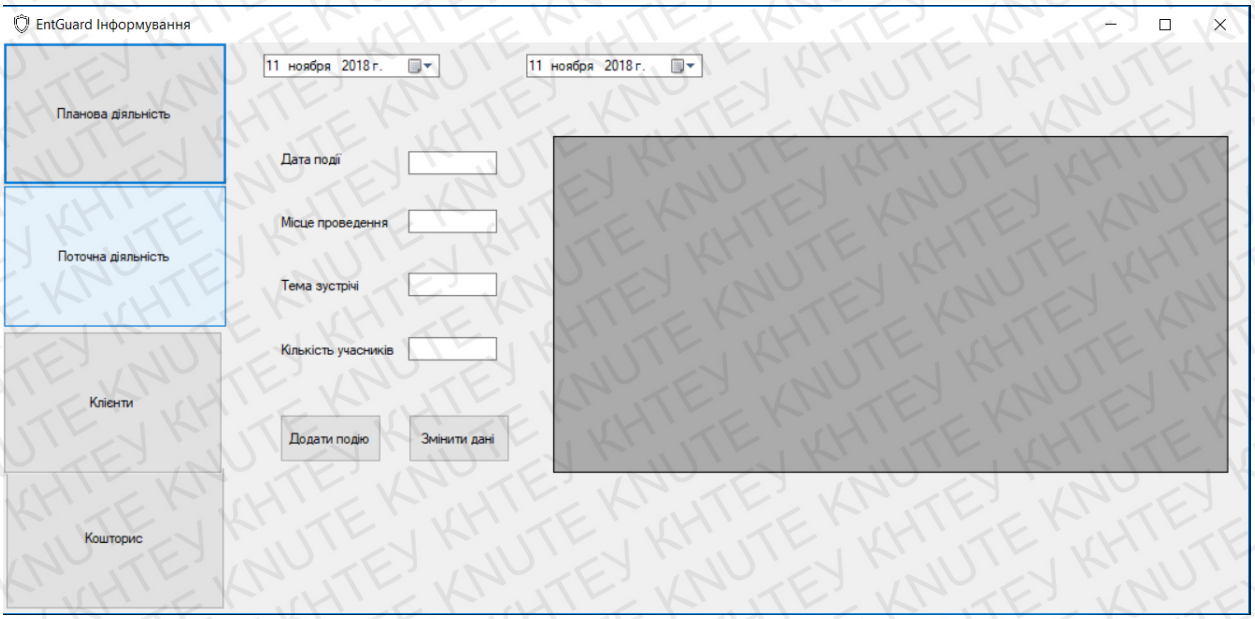

Рис 3.7 Робоча область спеціаліста групи інформування

Висновки до розділу 3

Розглядаючи підприємства сфери електронного бізнесу, варто зазначити що більшість із них мають спеціалізоване програмне забезпечення для управління клієнтами, виробництвом (за потреби) та персоналом (підготовкою та навчанням).

Сучасне програмне забезпечення все частіше переходить на хмарні технології, що створюю загрозу витоку даних при їх передачі/отриманні а також можливість стороннього підключення.

Виходячи з наведених даних варто вказати, що при створенні моделі КСЗІ одним з найважливіших моментів виступає, по-перше, створення ролей користувачів, їх рівнів доступу і можливих дій у системі, а по-друге, навчання персоналу щодо користування системою і підключення сторонніх пристроїв.

ВИСНОВКИ

Отже становлення та поширення підприємств електронного бізнесу – одна з важливих економічних тенденцій XXI століття - призводить до розробки програмних засобів, а саме систем управління інформаційною безпекою та комплексної системи захисту інформації як основного засобу забезпечення безпеки інформації в окрему випадку так і забезпечення стабільної роботи підприємства в цілому.

Без сумніву, сучасний технологічний розвиток програмного та апаратного забезпечень дозволяє мінімізувати злочинні впливи за допомогою чіткої, ефективної, а найголовніше раціональної організації доступу до інформації, та дій з ним.

Організаційні норми дозволяють обмежити можливості отримання, модифікація та розсекречення інформації за рахунок створення ролей доступу, регламентів обробки, підключення пристроїв вводу-виводу інформації.

Апаратні засоби дозволяють обмежити підключення зовнішніх носіїв даних, створити захищенні канали передачі інформації від вірусів, чи стороннього проникнення.

Що ж до програмного забезпечення то воно дозволяє використовувати такі засоби як віддалений робочий стіл, завдяки якому можна відслідковувати усі дії користувачів, а також варто зазначити криптографічні способи захисту інформації та електронний цифровий підпис.

На завершення варто сказати про те що сучасний світ швидко змінюється, а разом з ним змінюються як загрози так і засоби захисту. В останній роки все популярнішими стає захист даних з використанням білих хакерів(білі капелюхи), які являють собою висококваліфікованих програмістів, які шукають слабкі місця у програмних засобів замовника.

В поєднанні з розвитком штучного інтелекту це приведе до появи нових моделей та системи захисту інформації СЗІ.

Список використаних джерел

1. UKRINFORM. В Давосе объявили о создании Глобального центра кибербезопасности [Електронний ресурс] // – Режим доступу: https://www.ukrinform.ru/rubric-technology/2389711-v-davose-obavili-o-sozdanii-globalnogocentra-kiberbezopasnosti.html
2. ВІСНИК СХІДНОУКРАЇНСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ імені Володимира Даля № 15 (204) ч.1 2013 59 УДК 341.4 СВІТОВІ ТЕНДЕНЦІЇ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ Йона О.О., Казакова Н.Ф.
3. McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report [Електронний ресурс] // Портал : An Intel Company. – Режим доступу\www/ URL :http://www.mcafee.com/us/about/news/2012/q1/20120120-01.aspx. – Заголовок з екрану, доступ вільний,28.06.2013.
4. Безпека банківської діяльності : монографія /Казакова Н. Ф., Панфілов В. І., Скачек Л. М., Скопа О.О., Хорошко В. О. ; за ред. проф. Хорошко В. О. – К. :ПВП «Задруга», 2013. – 282 с. – ISBN 978-966-2970-82-1
5. [https://www.sciencedirect.com/science/article/pii/S1353485811700757]
6. [https://www.cbsnews.com/news/cyber-soldiers-cbsn-on-assignment/]
7. [https://online.maryville.edu/blog/can-we-learn-from-white-hat-hackers/]
8. Хмелевський Р.М. Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності // Сучасний захист інформації №4, 2016 р
9. Хмелевський Р.М. Тези. «Інформаційна безпека, як одна з основ забезпечення ефективності роботи державного управління». Матеріали міжнародної науково-технічної конференції «Сучасні інформаційнотелекомунікаційні технології» Том IV «Сучасні технології інформаційної безпеки» Київ, ДУТ. 17–20 листопада 2015 р. – С.155–158.

10. «Про Стратегію кібербезпеки України». Указ Президента України №96 / 2016 від 27 січня 2016 року. – [Електроний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/287/2015
11. Вихорев С.В., Кобцев Р.Ю. Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Защита информации. Конфидент, № 2, 2002. С.44–49.
12. Касперский Е. Основные классы угроз в компьютерном сообществе 2003 года, их причины и способы устранения // Информационный бюллетень «Jet Info». № 12 (127)/2003.
13. Классификация угроз Digital Security (Digital Security Classification of Threats). – [Електронный ресурс]. – Режим доступа: http://www.dsec.ru/products/grif/fulldesc/classification
14. Кузнецов И.Н. Учебник по информационно-аналитической работе. Информация: сбор, защита, анализ. М.: Изд. Яуза, 2001.
15. Расторгуев С. П. Философия информационной войны. – М.: Вузовская книга, 2001. – 468 с.
16. Christopher Alberts, Audrey Dorofee «OCTAVE Threat Profiles»; Software Engineering Institute, Carnegie Mellon University.
17. Гуцу С. Ф. Правові основи інформаційної діяльності : навч. посіб. / С. Ф. Гуцу. — Х. : Нац. аерокосм.ун-т «Харк. авіац. ін-т», 2009. — 48 с.
18. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б. А. Кормич ; Нац. ун-т внутр. справ. — Х., 2004. — 42 с.
19. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки /А. І. Марущак // Державна безпека України. — 2011. — № 21. — С. 92—95.

20. Сороківська О. А. Інформаційна безпека підприємства : нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. — 2010. — № 2, т. 2. — С. 32—35.
21. Кулініч О. А. Структурні чинники економічної безпеки України / О. А. Кулініч // Шлях України до економічної безпеки : матеріали наук.-практ. конф. — Х. : ХНУВС, 2007. — С. 59—63.
22. Живко З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. І. Керницька. — Львів : Ліга-Прес, 2008. — 345 с.
23. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия / С. В. Кавун // Управління розвитком. — Х. : ХНЕУ, 2008. — Вип. 6. — С. 17—21.
24. Smieliauskas W. Auditing: An International Approach / W. Smieliauskas, K. Bewley. — McGraw-Hill Ryerson Higher Education, 2006. — 800 p.
25. Иванов О. В. Информационная составляющая современных войн / О. В. Иванов // Вестн. Моск. ун-та: сер. 18 : Социология и политология. — 2004. — № 4. — С. 64—70.
26. Гришина Н. В. Организация комплексной системы защиты информации / Н. В. Гришина. — М. : Гелиос АРВ. — 2007. — 256 с.
27. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. Р. А. Калюжного. — Запоріжжя : Просвіта, 2001. — 252 с.
28. Porter B. Principles of External Auditing / B. Porter, D. Hatherly, Jon Simon. — [3rd edition]. — Wiley, 2008.— 816 p.
29. Марунич А. В. Захист інформації як основна складова економічної безпеки підприємства / А. В. Марунич // Управління розвитком. — 2014. — № 14. — С. 130—132.

30. Гордієнко С. Б. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії /С. Б. Гордієнко, О. С. Микитенко, В. Г. Данильчук // Вісник ДУІКТ. — 2013. — № 1. — С. 104—107.
31. Ясенев В. Н. Информационная безопасность в экономических системах : учеб. пособ. [Электронный ресурс] / В. Н. Ясенев. — Н. Новгород : Изд-во ННГУ, 2006. — Режим доступа :http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html.
32. Захаркін О. О. Інформаційні системи та технології у фінансових установах : конспект лекцій[Електронний ресурс] / О. О. Захаркін, М. Ю. Абрамчук, М. А. Деркач. — Суми : Вид-во СумДУ, 2007.— 80 с. — Режим доступу : http://elkniga.info/book_188.html.
33. Науково-практичний журнал « Безпека інформації» 2012 № 1 ОСОБЛИВОСТІ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ Сергій Гнатюк, Василь Кінзерявий, Андрій Охріменко Національний авіаційний університет
34. Advanced Encryption Standard (AES) [Electronic resource] : FIPS 197. — Electronic data (1 file:279 457 byte). — Gaithersburg, Maryland, USA : NIST, 2001. — Mode of access: World Wide Web. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. — Description based on screen.
35. Korchenko O. Modern quantum techno-logies of information security against cyber-terrorist attacks /O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius :Technika, 2010, Vol. 14, № 2, p. 58–69.
36. Telecommunications Networks – Current Status and Future Trends / [O. Korchenko, M. Lutskiy,79 S. Gnatyuk et al.]; edited by J. H. Ortiz. — Rijeka : InTech,2012. — 446 p.
37. Алексейчук А.Н. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на

гомоморфизмах /А.Н. Алексейчук, Л.В. Ковальчук, Е.В. Скрынник, А.С. Шевцов // Прикладная радиоэлектроника. —2008. — Т.7, № 3. — С. 203-209.

38. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах //І.Д. Горбенко, Т.О. Гріненко. – Х. : 2004. — 222 с.
39. Горбенко І.Д. Перспективний блоковий симетричний шифр «КАЛИНА». Основні положення та специфікація / І.Д. Горбенко, В.І. Долгов,Р.В. Олійников та ін. // Прикладная радиоэлектроника. — 2007. — Т. 6, № 2. — С. 195-208.
40. Кваснiков В.П. Блоковий симетричний криптоалгоритм «LUNA» / В.П. Кваснiков, В.М. Кінзерявий, С.О. Гнатюк, О.М. Кінзерявий //Захист інформації. − №3 (52). – 2011. − С. 77-87
41. Корченко О.Г. Спосіб шифрування інформації на основі шифру Файстеля / О.Г. Корченко,Є.В. Паціра, В.М. Кінзерявий, С.О. Гнатюк // Вісник інженерної академії України. – №2, 2009. – С. 117–121.
42. Корченко О.Г., Скулиш Є.Д., Горбенко Ю.І.,Пушкарьов О.І., Соловйов О.А., Коряков І.В. Сучасні системи захисту державних інформаційних ресурсів //Захист інформації. – № 4(53) 2011. – с. 5-17.
43. Корченко О.Г. Основні критерії та вимоги до побудови сучасних криптосистем / О.Г. Корченко, С.О. Гнатюк, Ю.Є. Хохлачова, А.О. Охріменко // Вісник інженерної академії України. – №3-4, 2011. – С. 77–83.
44. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк // Захист інформації. — 2010. — № 1. —С. 77–89

45. Математичні основи криптографії: навч.посібник / Г.В. Кузнецов, В.В. Фомичов, С.О.Сушко, Л.Я. Фомичова. – Д.: Національний гірничий університет, 2004. – Ч.1. – 391 с.
46. Панасенко С.П. Алгоритмы шифрования.Специальный справочник. — СПб. : БХВ-Петербург,2009 — 576 с.
47. Пат. № 45776 України, МПК H04L 9/06.Спосіб криптографічного перетворення інформації /Корченко О.Г., Паціра Є.В., Кінзерявий В.М., Гнатюк С.О.; заявник та патентовласник Націон. авіаційний ун–тет. – №u200905972; заявл. 10.06.2009; опубл. 25.11.2009,Бюл. №22.
48. Пат. № 55211 України, МПК H04L 9/06.Конвеєрний криптографічний обчислювач / Корченко О.Г., Паціра Є.В., Панасюк А.Л., Кінзерявий В.М.,Гнатюк С.О.; заявник та патентовласник Націон.авіаційний ун–тет. – № u20100641; Заявл. 19.05.2010;Опубл. 10.12.2010. Бюл. №23. – 8 с.
49. Пат. № 55213 України, МПК H04L 9/06.Конвеєрний криптографічний обчислювач / Корченко О.Г., Паціра Є.В., Панасюк А.Л., Кінзерявий В.М., Гнатюк С.О.; заявник та патентовласник Націон. авіаційний ун–тет. – № u20100644; Заявл. 19.05.2010;Опубл. 10.12.2010. Бюл. №23. – 8 с.
50. Румянцев К.Е. Квантовая криптография :принципы, протоколы, системы / К.Е. Румянцев,Д.М. Голубчиков // Всероссийский конкурс. Отбор обзорно-аналитических статей по приоритетному направлению «Информационно-телекоммуникационные системы», 2008. — 37 с.
51. Юдін О.К. Захист інформації в мережах передачі даних : Підручник / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. — К. : Видавництво «DIRECTLINE», 2009. — 714 с.

52. Алфьоров А.П., Зубов А.Ю., Кузьмін А.С., Черьомушкін А.В. Основи криптографії: Навчальний посібник. 3-тє вид., Испр. і доп. - М.: 2005. - 480с.

ДОДАТКИ

Додаток А

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.ComponentModel.Design;
using System.Security.Cryptography;
using MySql.Data.MySqlClient;

namespace EntGuard
{
   public partial class SpecSuppForm : Form
   {
      public SpecSuppForm()
      {
         InitializeComponent();
      }
      //public static string ConnectionString => ConfigurationManager.ConnectionStrings["mySql connection"].ToString();
      //MySqlConnection connection = new MySqlConnection(ConnectionString);
      MySqlConnection connection = new MySqlConnection("server='localhost';user id = 'root';password='Water2460Air';database='ent_guard'");
      MySqlCommand command;
      EventHandler Name_Click;
      EventHandler Add_Click;

      public void OpenConnection()
      {
         if (connection.State == ConnectionState.Closed)
         {
            connection.Open();
         }
      }
```

```
public void CloseConnection()
{
    if (connection.State == ConnectionState.Open)
    {
        connection.Close();
    }
}
public void ExecuteQuery(String query)
{
    try
    {
        OpenConnection();
        command = new MySqlCommand(query, connection);
        if (command.ExecuteNonQuery() == 1)
        {
            MessageBox.Show("Запит виконано");
        }
        else
        {
            MessageBox.Show("Запит не виконано");
        }
    }
    catch (Exception ex)
    {
        MessageBox.Show(ex.Message);
    }
    finally
    {
        CloseConnection();
    }
}
void CreateDataGridView(Control Parent, Point Pos, String Text)
{
    DataGridView sup = new DataGridView();
    sup.Location = Pos; //расположение
    sup.Size = new Size(600, 500); // размер
    sup.Name = Text;
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
}
void CreateDateTimePicker(Control Parent, Point Pos, String Text)
{
    DateTimePicker sup = new DateTimePicker();
    sup.Location = Pos; //расположение
    sup.Value = new System.DateTime(2018, 11, 18, 0, 0, 0, 0);
    sup.Size = new Size(125, 60); // размер
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
}
void CreateLabel(Control Parent, Point Pos, String Text)
{
    Label sup = new Label
    {
        Location = Pos, //расположение
```

```
            Size = new Size(100, 22), // размер
            Text = Text //текст
        };
        Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
    }
    void CreateTextBox(Control Parent, Point Pos, String Text)
    {
        TextBox sup = new TextBox
        {
            Location = Pos, //расположение
            Size = new Size(100, 22), // размер
            Name = Text //текст
        };
        Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
    }
    void CreateButton(Panel suppanel, Control Parent, Point Pos, String Text, String
Name )
    {
        Button sup = new Button();
        sup.Name = Name;
        sup.Text = Text;
        sup.Size = new System.Drawing.Size(51, 51);
        Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
        //

    }
    void CreateButton(Control Parent, Point Pos, String Text, String Name, EventHandler
NameClick )
    {
        Button sup = new Button();
        sup.Name = Name;
        sup.Text = Text;
        sup.Size = new System.Drawing.Size(51, 51); ;
        sup.Click += new EventHandler(Name_Click);
        //sup.MouseClick += new MouseEventHandler(Name_MouseClick);*/
        Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол

    }
    private void SupTaskbutton_Click(object sender, EventArgs e)
    {
        Suppanel.Controls.Clear();
        CreateDateTimePicker(Suppanel, new Point(10, 20),"NowDay");
        CreateLabel(Suppanel, new Point(20, 65), "Задача");
        CreateTextBox(Suppanel, new Point(120, 61), "Task");
        CreateLabel(Suppanel, new Point(20, 95), "Проект");
        CreateTextBox(Suppanel, new Point(120, 91), "Project");
        CreateLabel(Suppanel, new Point(20, 125), "Дата виконання");
        CreateTextBox(Suppanel, new Point(120, 121), "DateOfEnd");
        CreateLabel(Suppanel, new Point(20, 155), "Цільова аудиторія");
        CreateTextBox(Suppanel, new Point(120, 151), "CA");
        CreateLabel(Suppanel, new Point(20, 185), "Вартість угоди");
        CreateTextBox(Suppanel, new Point(120, 181), "Value");
```

```
        CreateDataGridView(Suppanel, new Point(300, 125), "TasksDGV");
        CreateButton(Suppanel, new Point(60, 215), "Додати задачу", "SupAddTask",
"Add_Click");
        CreateButton(Suppanel, new Point(60, 245), "Змінити задачу",
"SupChangeTask", "Change_Click");
        CreateButton(Suppanel, new Point(60, 275), "Відмінити завдання",
"SupDeleteTask", "Delete_Click");
        OpenConnection();
        string support = "SELECT * FROM project ";
        MySqlDataAdapter da = new MySqlDataAdapter(support, connection);
        DataSet ds = new DataSet();
        da.Fill(ds, "support");
        //TasksDGV.DataSource = ds.Tables["support"];
        CloseConnection();
        /*void Add_Click(object sender, EventArgs e)
        {
          insert = "INSERT INTO
idProjects,Company_idCompany,Auditory,DateContract,Cost
VALUES(Project.Text,Task.Text,CA.Text,DateOfEnd.Text,Value.Text) ";
          ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Change_Click(object sender, EventArgs e)
        {
          insert = "INSERT INTO Company_idCompany,Auditory,DateContract,Cost
VALUES(Task.Text,CA.Text,DateOfEnd.Text,Value.Text) WHERE idProjects =
Project.Text ";
          ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Delete_Click(object sender, EventArgs e)
        {
        delete = "DELETE WHERE idProjects= Project.Text ";
        ExecuteQuery(delete);
        }
        CloseConnection();*/

    }

    private void CreateButton(Panel suppanel, Point point, string v1, string v2, string v3)
    {
      throw new NotImplementedException();
    }

    private void SupProbutton_Click(object sender, EventArgs e)
    {
      Suppanel.Controls.Clear();
      CreateLabel(Suppanel, new Point(20, 65), "Проект");
      CreateTextBox(Suppanel, new Point(120, 61), "Projects");
      CreateLabel(Suppanel, new Point(20, 95), "Компанія");
      CreateTextBox(Suppanel, new Point(120, 91), "Company");
      CreateLabel(Suppanel, new Point(20, 125), "Спеціалізація");
```

```
        CreateTextBox(Suppanel, new Point(120, 121), "Specialize");
        CreateLabel(Suppanel, new Point(20, 155), "Цільова аудиторія");
        CreateTextBox(Suppanel, new Point(120, 151), "CA");
        CreateLabel(Suppanel, new Point(20, 185), "Вартість угоди");
        CreateTextBox(Suppanel, new Point(120, 181), "Value");
        CreateLabel(Suppanel, new Point(20, 215), "Термін");
        CreateTextBox(Suppanel, new Point(120, 211), "Term");
        CreateDataGridView(Suppanel, new Point(300, 125), "ProjectsDGV");
        CreateButton(Suppanel, new Point(60,250), "Додати проект","SupAddTProject",
"AddPr_Click");
        CreateButton(Suppanel, new Point(60,280), "Змінити проект",
"SupChangeProject", "ChangePr_Click");
        CreateButton(Suppanel, new Point(60,310), "Видалити проект",
"SupDeleteProject", "DeleteAdd_Click");
        OpenConnection();
        string company = "SELECT * FROM company ";
        MySqlDataAdapter da = new MySqlDataAdapter(company, connection);
        DataSet ds = new DataSet();
        da.Fill(ds, "company");
        //ProjectsDGV.DataSource = ds.Tables["company"];
        CloseConnection();
        /*void Add_Click(object sender, EventArgs e)
        {
          insert = "INSERT INTO CompanyName,Market,Auditory,Cost
VALUES(Company.Text,Specialize.Text,CA.Text,Value.Text) ";
          ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Change_Click(object sender, EventArgs e)
        {
          insert = "INSERT INTO CompanyName,Market,Auditory,Cost
VALUES(Company.Text,Specialize.Text,CA.Text,Value.Text)";
          ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Delete_Click(object sender, EventArgs e)
        {
        delete = "DELETE WHERE idPCompany= Company.Text ";
        ExecuteQuery(delete);
        }
        CloseConnection();*/

    }

    private void SupClientbutton_Click(object sender, EventArgs e)
    {
        Suppanel.Controls.Clear();
        CreateLabel(Suppanel, new Point(20, 65), "Компанія");
        CreateTextBox(Suppanel, new Point(120, 61), "Company");
        CreateLabel(Suppanel, new Point(20, 95), "Регіон розміщення");
        CreateTextBox(Suppanel, new Point(120, 91), "Region" );
        CreateLabel(Suppanel, new Point(20, 125), "Спеціалізація");
```

```
        CreateTextBox(Suppanel, new Point(120, 121), "Specialize");
        CreateLabel(Suppanel, new Point(20, 155), "Керівник");
        CreateTextBox(Suppanel, new Point(120, 151), "Director");
        CreateLabel(Suppanel, new Point(20, 185), "Ціль");
        CreateTextBox(Suppanel, new Point(120, 181), "Goal");
        CreateLabel(Suppanel, new Point(20, 215), "Термін");
        CreateTextBox(Suppanel, new Point(120, 211), "Term");
        CreateDataGridView(Suppanel, new Point(300, 125), "CompanyDGV");
        CreateButton(Suppanel, new Point(60, 250), "Додати замовника",
"SupAddComp","AddComp_Click");
        CreateButton(Suppanel, new Point(60, 280), "Змінити дані", "SupChangeComp",
"ChangeComp_Click");
        CreateButton(Suppanel, new Point(60, 310), "Видалити замовника",
"SupDeleteComp", "DeleteComp_Click");
        OpenConnection();
        string support = "SELECT * FROM project WHERE Users idUsers=1 ";
        MySqlDataAdapter da = new MySqlDataAdapter(support, connection);
        DataSet ds = new DataSet();
        da.Fill(ds, "support");
        //TasksDGV.DataSource = ds.Tables["support"];
        CloseConnection();
        /*void Add_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO
idProjects,Company_idCompany,Auditory,DateContract,Cost
VALUES(Project.Text,Task.Text,CA.Text,DateOfEnd.Text,Value.Text) ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Change_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO Company_idCompany,Auditory,DateContract,Cost
VALUES(Task.Text,CA.Text,DateOfEnd.Text,Value.Text) WHERE idProjects =
Project.Text ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Delete_Click(object sender, EventArgs e)
        {
        delete = "DELETE WHERE idProjects= Project.Text ";
        ExecuteQuery(delete);
        }
        CloseConnection();*/

    }

    private void SupFinbutton_Click(object sender, EventArgs e)
    {
        Suppanel.Controls.Clear();
        CreateLabel(Suppanel, new Point(20, 65), "Проект");
        CreateTextBox(Suppanel, new Point(120, 61), "Projects");
        CreateLabel(Suppanel, new Point(20, 95), "Компанія");
```

```
            CreateTextBox(Suppanel, new Point(120, 91), "Company");
            CreateLabel(Suppanel, new Point(20, 125), "Витрати");
            CreateTextBox(Suppanel, new Point(120, 121), "Costs");
            CreateLabel(Suppanel, new Point(20, 155), "Доходи");
            CreateTextBox(Suppanel, new Point(120, 151), "Income");
            CreateLabel(Suppanel, new Point(20, 185), "Рентабельнсть");
            CreateTextBox(Suppanel, new Point(120, 181), "Profitability");
            CreateLabel(Suppanel, new Point(20, 215), "Період у роботі");
            CreateTextBox(Suppanel, new Point(120, 211), "TermInUse");
            CreateDataGridView(Suppanel, new Point(300, 75), "FinSupDGV");
        }
    }
}
```

Додаток Б

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using MySql.Data.MySqlClient;

namespace EntGuard
{
    public partial class SpecInfoForm : Form
    {
        public SpecInfoForm()
        {
            InitializeComponent();

        }
        MySqlConnection connection = new MySqlConnection("server='localhost';user id =
'root';password='Water2460Air';database='ent_guard'");
        MySqlCommand command;
        EventHandler Name_Click;
        EventHandler Add_Click;

        public void OpenConnection()
        {
            if (connection.State == ConnectionState.Closed)
            {
                connection.Open();
            }
        }
        public void CloseConnection()
```

```
{
    if (connection.State == ConnectionState.Open)
    {
        connection.Close();
    }
}
public void ExecuteQuery(String query)
{
    try
    {
        OpenConnection();
        command = new MySqlCommand(query, connection);
        if (command.ExecuteNonQuery() == 1)
        {
            MessageBox.Show("Запит виконано");
        }
        else
        {
            MessageBox.Show("Запит не виконано");
        }
    }
    catch (Exception ex)
    {
        MessageBox.Show(ex.Message);
    }
    finally
    {
        CloseConnection();
    }
}
void CreateDataGridView(Control Parent, Point Pos, String Text)
{
    DataGridView sup = new DataGridView();
    sup.Location = Pos; //расположение
    sup.Size = new Size(600, 500); // размер
    sup.Name = Text;
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
}
void CreateDateTimePicker(Control Parent, Point Pos, String Text)
{
    DateTimePicker sup = new DateTimePicker();
    sup.Location = Pos; //расположение
    sup.Value = new System.DateTime(2018, 11, 18, 0, 0, 0, 0);
    sup.Size = new Size(125, 60); // размер
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
}
void CreateLabel(Control Parent, Point Pos, String Text)
{
    Label sup = new Label
    {
        Location = Pos, //расположение
        Size = new Size(100, 22), // размер
```

```
            Text = Text //текст
        };
        Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
    }
    void CreateTextBox(Control Parent, Point Pos, String Text)
    {
        TextBox sup = new TextBox
        {
            Location = Pos, //расположение
            Size = new Size(100, 22), // размер
            Name = Text //текст
        };
        Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
    }
    void CreateButton(Control Parent, Point Pos, String Text, String Name)
    {
        Button sup = new Button
        {
            Location = Pos, //расположение
            Size = new Size(100, 22), // размер
            Text = Text, //текст
            Name = Name,
        };
        Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
        //
    }

    private void InfoPlanbutton_Click(object sender, EventArgs e)
    {
        Infopanel.Controls.Clear();
        CreateLabel(Infopanel, new Point(20, 65), "Назва заходу");
        CreateTextBox(Infopanel, new Point(120, 61), "Task");
        CreateLabel(Infopanel, new Point(20, 95), "Розміщення");
        CreateTextBox(Infopanel, new Point(120, 91), "Location");
        CreateLabel(Infopanel, new Point(20, 125), "Дата проведення");
        CreateTextBox(Infopanel, new Point(120, 121), "DateOfExcebition");
        CreateLabel(Infopanel, new Point(20, 155), "Цільова аудиторія");
        CreateTextBox(Infopanel, new Point(120, 151), "CA");
        CreateLabel(Infopanel, new Point(20, 185), "Вартість проведення");
        CreateTextBox(Infopanel, new Point(120, 181), "Value");
        CreateDataGridView(Infopanel, new Point(300, 125), "ExcebitionDGV");
        CreateButton(Infopanel, new Point(60, 215), "Додати задачу",
"InfAddExcebition");
        CreateButton(Infopanel, new Point(60, 245), "Змінити задачу",
"InfChangeExcebition");
        CreateButton(Infopanel, new Point(60, 275), "Відмінити завдання",
"InfDeleteExcebition");
        OpenConnection();
        string support = "SELECT * FROM project ";
        MySqlDataAdapter da = new MySqlDataAdapter(support, connection);
        DataSet ds = new DataSet();
        da.Fill(ds, "support");
```

```
        //TasksDGV.DataSource = ds.Tables["support"];
        CloseConnection();
        /*void Add_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO
idProjects,Company_idCompany,Auditory,DateContract,Cost
VALUES(Project.Text,Task.Text,CA.Text,DateOfEnd.Text,Value.Text) ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Change_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO Company_idCompany,Auditory,DateContract,Cost
VALUES(Task.Text,CA.Text,DateOfEnd.Text,Value.Text) WHERE idProjects =
Project.Text ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Delete_Click(object sender, EventArgs e)
        {
        delete = "DELETE WHERE idProjects= Project.Text ";
        ExecuteQuery(delete);
        }
        CloseConnection();*/

    }

    private void InfoPotbutton_Click(object sender, EventArgs e)
    {
        Infopanel.Controls.Clear();
        CreateLabel(Infopanel, new Point(20, 65), "Захід");
        CreateTextBox(Infopanel, new Point(120, 61), "Task");
        CreateLabel(Infopanel, new Point(20, 95), "Аудиторія");
        CreateTextBox(Infopanel, new Point(120, 91), "Auditory");
        CreateLabel(Infopanel, new Point(20, 125), "Кількість контрактів");
        CreateTextBox(Infopanel, new Point(120, 121), "SumContract");
        CreateLabel(Infopanel, new Point(20, 155), "Цільова аудиторія");
        CreateTextBox(Infopanel, new Point(120, 151), "CA");
        CreateLabel(Infopanel, new Point(20, 185), "Вартість проведення");
        CreateTextBox(Infopanel, new Point(120, 181), "Value");
        CreateDataGridView(Infopanel, new Point(300, 125), "ExcebitionDGV");
        CreateButton(Infopanel, new Point(60, 215), "Додати дані заходу",
"SupAddExcebition");
        CreateButton(Infopanel, new Point(60, 245), "Внести зміни у данні",
"SupChangeExcebition");
        CreateButton(Infopanel, new Point(60, 275), "Відмінити результати заходу",
"SupDeleteExcebition");
        OpenConnection();
        string support = "SELECT * FROM project ";
        MySqlDataAdapter da = new MySqlDataAdapter(support, connection);
        DataSet ds = new DataSet();
        da.Fill(ds, "support");
```

```
        //TasksDGV.DataSource = ds.Tables["support"];
        CloseConnection();
        /*void Add_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO idProjects,Company_idCompany,Auditory,DateContract,Cost
VALUES(Project.Text,Task.Text,CA.Text,DateOfEnd.Text,Value.Text) ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Change_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO Company_idCompany,Auditory,DateContract,Cost
VALUES(Task.Text,CA.Text,DateOfEnd.Text,Value.Text) WHERE idProjects =
Project.Text ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Delete_Click(object sender, EventArgs e)
        {
        delete = "DELETE WHERE idProjects= Project.Text ";
        ExecuteQuery(delete);
        }
        CloseConnection();*/

    }

    private void InfoClientbutton_Click(object sender, EventArgs e)
    {
        Infopanel.Controls.Clear();
        CreateLabel(Infopanel, new Point(20, 65), "Компанія");
        CreateTextBox(Infopanel, new Point(120, 61), "Company");
        CreateLabel(Infopanel, new Point(20, 95), "Директор");
        CreateTextBox(Infopanel, new Point(120, 91), "Directory");
        CreateLabel(Infopanel, new Point(20, 125), "Місцезнаходження");
        CreateTextBox(Infopanel, new Point(120, 121), "Localization");
        CreateLabel(Infopanel, new Point(20, 155), "Напрям діяльності");
        CreateTextBox(Infopanel, new Point(120, 151), "Market");
        CreateLabel(Infopanel, new Point(20, 185), "Цільова аудиторія");
        CreateTextBox(Infopanel, new Point(120, 181), "Auditory");
        CreateDataGridView(Infopanel, new Point(300, 125), "CompanyDGV");
        CreateButton(Infopanel, new Point(60, 215), "Додати дані заходу",
"InfAddCompany");
        CreateButton(Infopanel, new Point(60, 245), "Внести зміни у данні",
"infChangeCompany");
        CreateButton(Infopanel, new Point(60, 275), "Відмінити результати заходу",
"InfDeleteCompany");
        OpenConnection();
        string support = "SELECT * FROM project ";
        MySqlDataAdapter da = new MySqlDataAdapter(support, connection);
        DataSet ds = new DataSet();
        da.Fill(ds, "support");
```

```
        //TasksDGV.DataSource = ds.Tables["support"];
        CloseConnection();
        /*void Add_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO idProjects,Company_idCompany,Auditory,DateContract,Cost
VALUES(Project.Text,Task.Text,CA.Text,DateOfEnd.Text,Value.Text) ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Change_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO Company_idCompany,Auditory,DateContract,Cost
VALUES(Task.Text,CA.Text,DateOfEnd.Text,Value.Text) WHERE idProjects =
Project.Text ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Delete_Click(object sender, EventArgs e)
        {
        delete = "DELETE WHERE idProjects= Project.Text ";
        ExecuteQuery(delete);
        }
        CloseConnection();*/

    }

    private void InfoFinbutton_Click(object sender, EventArgs e)
    {
        Infopanel.Controls.Clear();
        CreateLabel(Infopanel, new Point(20, 65), "Інформаційний захід");
        CreateTextBox(Infopanel, new Point(120, 61), "Task");
        CreateLabel(Infopanel, new Point(20, 95), "Розміщення");
        CreateTextBox(Infopanel, new Point(120, 91), "Localization");
        CreateLabel(Infopanel, new Point(20, 125), "Кількість контрактів");
        CreateTextBox(Infopanel, new Point(120, 121), "SumContract");
        CreateLabel(Infopanel, new Point(20, 155), "Цільова аудиторія");
        CreateTextBox(Infopanel, new Point(120, 151), "CA");
        CreateLabel(Infopanel, new Point(20, 185), "Вартість проведення");
        CreateTextBox(Infopanel, new Point(120, 181), "Value");
        CreateDataGridView(Infopanel, new Point(300, 125), "InfFinDGV");
        CreateButton(Infopanel, new Point(60, 215), "Додати дані заходу", "InfAddFin");
        CreateButton(Infopanel, new Point(60, 245), "Внести зміни у данні",
"InfChangeFin");
        CreateButton(Infopanel, new Point(60, 275), "Відмінити результати заходу",
"InfDeleteFin");
        OpenConnection();
        string support = "SELECT * FROM project ";
        MySqlDataAdapter da = new MySqlDataAdapter(support, connection);
        DataSet ds = new DataSet();
        da.Fill(ds, "support");
        //TasksDGV.DataSource = ds.Tables["support"];
```

```
        CloseConnection();
        /*void Add_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO idProjects,Company_idCompany,Auditory,DateContract,Cost
VALUES(Project.Text,Task.Text,CA.Text,DateOfEnd.Text,Value.Text) ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Change_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO Company_idCompany,Auditory,DateContract,Cost
VALUES(Task.Text,CA.Text,DateOfEnd.Text,Value.Text) WHERE idProjects =
Project.Text ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Delete_Click(object sender, EventArgs e)
        {
        delete = "DELETE WHERE idProjects= Project.Text ";
        ExecuteQuery(delete);
        }
        CloseConnection();*/

    }
  }
}
```

Додаток В

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using MySql.Data.MySqlClient;

namespace EntGuard
{
  public partial class SpecDesignForm : Form
  {
    public SpecDesignForm()
    {
      InitializeComponent();
    }
    void CreateDataGridView(Control Parent, Point Pos, String Text)
    {
      DataGridView sup = new DataGridView();
      sup.Location = Pos; //расположение
```

```
    sup.Size = new Size(600, 500); // размер
    sup.Name = Text;
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
}
void CreateDateTimePicker(Control Parent, Point Pos, String Text)
{
    DateTimePicker sup = new DateTimePicker();
    sup.Location = Pos; //расположение
    sup.Value = new System.DateTime(2018, 11, 18, 0, 0, 0, 0);
    sup.Size = new Size(125, 60); // размер
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
}
void CreateLabel(Control Parent, Point Pos, String Text)
{
    Label sup = new Label
    {
        Location = Pos, //расположение
        Size = new Size(100, 22), // размер
        Text = Text //текст
    };
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
}
void CreateTextBox(Control Parent, Point Pos, String Text)
{
    TextBox sup = new TextBox
    {
        Location = Pos, //расположение
        Size = new Size(100, 22), // размер
        Name = Text //текст
    };
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
}
void CreateButton(Control Parent, Point Pos, String Text, String Name)
{
    Button sup = new Button
    {
        Location = Pos, //расположение
        Size = new Size(100, 22), // размер
        Text = Text, //текст
        Name = Name,
    };
    Parent.Controls.Add(sup); //добавляем кнопку на родительский контрол
    //
}

private void DesignTaskbutton_Click(object sender, EventArgs e)
{
    Designpanel.Controls.Clear();
    CreateLabel(Designpanel, new Point(20, 65), "Назва проекту");
    CreateTextBox(Designpanel, new Point(120, 61), "Project");
    CreateLabel(Designpanel, new Point(20, 95), "Завдання");
    CreateTextBox(Designpanel, new Point(120, 91), "Task");
```

```
        CreateLabel(Designpanel, new Point(20, 125), "Замовник");
        CreateTextBox(Designpanel, new Point(120, 121), "Company");
        CreateLabel(Designpanel, new Point(20, 155), "Цільова аудиторія");
        CreateTextBox(Designpanel, new Point(120, 151), "Auditory");
        CreateLabel(Designpanel, new Point(20, 185), "Дата завершення");
        CreateTextBox(Designpanel, new Point(120, 181), "DateOfEnd");
        CreateDataGridView(Designpanel, new Point(300, 125), "ExcebitionDGV");
        CreateButton(Designpanel, new Point(60, 215), "Додати задачу",
"DesignAddTask");
        CreateButton(Designpanel, new Point(60, 245), "Змінити задачу",
"DesignChangeTask");
        CreateButton(Designpanel, new Point(60, 275), "Відмінити завдання",
"DesignDeleteTask");
        OpenConnection();
        string support = "SELECT * FROM project ";
        MySqlDataAdapter da = new MySqlDataAdapter(support, connection);
        DataSet ds = new DataSet();
        da.Fill(ds, "support");
        //TasksDGV.DataSource = ds.Tables["support"];
        CloseConnection();
        /*void Add_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO
idProjects,Company_idCompany,Auditory,DateContract,Cost
VALUES(Project.Text,Task.Text,CA.Text,DateOfEnd.Text,Value.Text) ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Change_Click(object sender, EventArgs e)
        {
            insert = "INSERT INTO Company_idCompany,Auditory,DateContract,Cost
VALUES(Task.Text,CA.Text,DateOfEnd.Text,Value.Text) WHERE idProjects =
Project.Text ";
            ExecuteQuery(insert);
        }
        CloseConnection();*/
        /*void Delete_Click(object sender, EventArgs e)
        {
        delete = "DELETE WHERE idProjects= Project.Text ";
        ExecuteQuery(delete);
        }
        CloseConnection();*/

    }

  }

    private void DesignProjectbutton_Click(object sender, EventArgs e)
    {
        Designpanel.Controls.Clear();
        CreateLabel(Designpanel, new Point(20, 65), "Назва проекту");
        CreateTextBox(Designpanel, new Point(120, 61), "Project");
```

```
        CreateLabel(Designpanel, new Point(20, 95), "Замовник");
        CreateTextBox(Designpanel, new Point(120, 91), "Company");
        CreateLabel(Designpanel, new Point(20, 125), "Цільова аудиторія");
        CreateTextBox(Designpanel, new Point(120, 121), "Auditory");
        CreateLabel(Designpanel, new Point(20, 155),"Виконані завдання" );
        CreateTextBox(Designpanel, new Point(120, 151), "SumTasks");
        CreateLabel(Designpanel, new Point(20, 185), "Дата отримання");
        CreateTextBox(Designpanel, new Point(120, 181), "DateOfGive");
        CreateDataGridView(Designpanel, new Point(300, 125), "ExcebitionDGV");
        CreateButton(Designpanel, new Point(60, 215), "Додати задачу",
"DesignAddProject");
        CreateButton(Designpanel, new Point(60, 245), "Змінити задачу",
"DesignChangeProject");
        CreateButton(Designpanel, new Point(60, 275), "Відмінити завдання",
"DesignDeleteProject");
      OpenConnection();
      string support = "SELECT * FROM project ";
      MySqlDataAdapter da = new MySqlDataAdapter(support, connection);
      DataSet ds = new DataSet();
      da.Fill(ds, "support");
      //TasksDGV.DataSource = ds.Tables["support"];
      CloseConnection();
      /*void Add_Click(object sender, EventArgs e)
      {
        insert = "INSERT INTO
idProjects,Company_idCompany,Auditory,DateContract,Cost
VALUES(Project.Text,Task.Text,CA.Text,DateOfEnd.Text,Value.Text) ";
        ExecuteQuery(insert);
      }
      CloseConnection();*/
      /*void Change_Click(object sender, EventArgs e)
      {
        insert = "INSERT INTO Company_idCompany,Auditory,DateContract,Cost
VALUES(Task.Text,CA.Text,DateOfEnd.Text,Value.Text) WHERE idProjects =
Project.Text ";
        ExecuteQuery(insert);
      }
      CloseConnection();*/
      /*void Delete_Click(object sender, EventArgs e)
      {
      delete = "DELETE WHERE idProjects= Project.Text ";
      ExecuteQuery(delete);
      }
      CloseConnection();*/

  }
}

      private void DesignFinbutton_Click(object sender, EventArgs e)
      {

      }
```

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

        }
    }
}
```

Додаток Г

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using MySql.Data.MySqlClient;

namespace EntGuard
{
    public partial class LoginForm : Form
    {
        public LoginForm()
        {
            InitializeComponent();
        }
        MySqlConnection connection = new MySqlConnection("server='localhost';user id =
'root';password='Water2460Air';database='entguard'");
        MySqlCommand command;

        public void OpenConnection()
        {
            if (connection.State == ConnectionState.Closed)
            {
                connection.Open();
            }
        }
        public void CloseConnection()
        {
            if (connection.State == ConnectionState.Open)
            {
                connection.Close();
            }
        }
        public void ExecuteQuery(String query)
        {
            try
            {
                OpenConnection();
                command = new MySqlCommand(query, connection);
```

```
            if (command.ExecuteNonQuery() == 1)
            {
              // MessageBox.Show("Запит виконано");
            }
            else
            {
               MessageBox.Show("Запит не виконано");
            }
         }
         catch (Exception ex)
         {
            MessageBox.Show(ex.Message);
         }
         finally
         {
            CloseConnection();
         }
      }

      private void Enterbutton_Click(object sender, EventArgs e)

      {


         if (logintextBox.Text != String.Empty && passwordtextBox.Text != String.Empty)
         {
            if (logintextBox.Text == "Art213" && passwordtextBox.Text == "water213")
            {
               //MessageBox.Show("Доброго дня Артур");
               this.Hide();
               Form MainAdmin = new MainAdmin();
               MainAdmin.Show();
            }
            else if (logintextBox.Text == "Ant213" && passwordtextBox.Text == "air213")
            {
               //MessageBox.Show("Доброго дня Артур");
               this.Hide();
               Form Specinfo = new SpecInfoForm();
               Specinfo.Show();
            }
            else if (logintextBox.Text == "Alt213" && passwordtextBox.Text == "fire213")
            {
                  //MessageBox.Show("Доброго дня Артур");
                  this.Hide();
                  Form SpecDesign = new SpecDesignForm();
                  SpecDesign.Show();
            }
            else if (logintextBox.Text == "Oks213" && passwordtextBox.Text == "elem213")
            {
               MessageBox.Show("Доброго дня Оксана");
```

```
                this.Hide();
                Form SpecSupp = new SpecSuppForm();
                SpecSupp.Show();
            }
            else
            {
                MessageBox.Show("Користувача з такими даними не зарестровано у системі");
            }
        }
        else
        {

            MessageBox.Show("Введіть дані");
        }

    }
   }
  }
}
```