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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Петкевічуса Яніса Вікторовича*

академічної групи *125-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка вимог та рекомендацій для управління інформаційною безпекою в системах електронного документообігу організації*

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

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Петкевічусу Янісу Вікторовичу*** **академічної групи** ***125-19-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка вимог та рекомендацій для управління інформаційною безпекою в системах електронного документообігу організації***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № 350-с

Розділ	Зміст	Термін виконання
Розділ 1	Правові аспекти захисту інформації та управління інформаційною безпекою	29.03.2023
Розділ 2	Комплексний захист інформації як компонент інформаційного забезпечення. Виконати аналіз основних аспектів захисту інформації в СЕД в Україні, розглянути та проаналізувати особливості захисту електронного документообігу	24.05.2023
Розділ 3	Визначити вартість впровадження розробленої СЕД на прикладі умовного підприємства.	09.06.2023

Завдання видано _____ Мєшков В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 09.01.2023р.

Дата подання до екзаменаційної комісії: 09.06.2023р.

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

РЕФЕРАТ

Пояснювальна записка: 115 с., 1 рис., 5 табл., 4 додатка, 48 джерел.

Об'єкт дослідження: управління інформаційною безпекою в системах електронного документообігу.

Мета роботи: підвищення рівня інформаційної безпеки при роботі в СЕД.

Методи дослідження: системний аналіз, методи порівняння, структурний аналіз та спостереження.

У спеціальній частині дана характеристика управлінню інформаційною безпекою в СЕД. У роботі досліджена система управління інформаційною безпекою в системах електронного документообігу. Проведено аналіз основних аспектів захисту інформації в СЕД в Україні, розглянуто та проаналізовано особливості захисту електронного документообігу.

Запропоновано для управління інформаційною безпекою в СЕД впровадити на підприємстві систему управління інформаційною безпекою згідно з рекомендаціями міжнародного стандарту ISO/IEC 27001 та використання в організаціях правил забезпечення захисту інформації в та інформаційно-телекомунікаційних системах та порядку здійснення електронного документообігу та інших правил і інструкцій.

В економічному розділі визначено вартість впровадження розробленої СЕД на прикладі умовного підприємства.

Практичне значення роботи полягає в управлінні інформаційною безпекою в СЕД в організаціях різного типу.

Результати здійснених у роботі досліджень можуть бути використані в управлінні інформаційною безпекою в системах електронного документообігу.

Новизна дослідження полягає в запропонованій СУІБ саме в СЕД.

СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ABSTRACT

Explanatory note: 115 pp., 1 pic., 4 table, 4 app, 48 sources.

Object of research: information security management in systems electronic document management.

Objective: increase the level of information security when working in EDMS.

Research methods: systematic analysis, comparison methods, structural analysis and monitoring.

In the special part of the characteristics of information security management in EDMS. This paper is devoted to control system security electronic document management systems. The analysis of the main aspects of the protection of information in EDMS in Ukraine, reviewed and analyzed the security features of electronic document management.

Proposed for information security management in EDMS to introduce the system in the company information security management in accordance with the recommendations of the international standard ISO/IEC 27001 and use in organizations the rules of protection of information in information and telecommunication systems and procedure of electronic document management and other rules and regulations.

In the economic section identifies the cost of implementing the EDMS is developed on the example of the conventional enterprise.

The practical value of the work lies in information security management in the EDMS in different kinds of organizations.

The results accomplished in the research can be used in the management of information security in electronic document management systems.

Scientific novelty of the research lies in the proposed ISMS in the EDMS.

ELECTRONIC DOCUMENT MANAGEMENT SYSTEM, MANAGEMENT SYSTEM AND INFORMATION SECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

АСЕД – автоматизована система електронного документообігу;

АЦСК – акредитований центр сертифікації ключів;

ВК – відкритий ключ;

ЕД – електронний документ;

ЕДО – електронний документообіг;

ЕП – електронна печатка;

ЕЦП – електронний цифровий підпис;

ІР – інформаційний ресурс;

ІС – інформаційна система;

ІСЕД – інтегрована система електронного документообігу;

ІТС – інформаційно-телекомунікаційна система;

КЗЗІ – комплексні засоби захисту інформації;

КЗІ – криптографічний захист інформації;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОК – особистий ключ;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПСВК – посилений сертифікат відкритого ключа;

СВК – сертифікат відкритого ключа;

СЕД – система електронного документообігу;

СЗІ – служба захисту інформації;

СКД – система контролю доступу;

СКУД – система контролю і управління доступом;

ТЗІ – технічний захист інформації;

ЦСК – центр сертифікації ключів.

ЗМІСТ

с.

ВСТУП 8

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 11

1.1 Правові аспекти електронного документообігу в Україні 11

1.2 Складові інформаційної безпеки в Україні 16

1.3 Правові аспекти захисту інформації та управління інформаційною безпекою 19

1.4 Основні поняття та визначення 21

1.5 Висновки за розділом 33

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА 35

2.1 Комплексний захист інформації як компонент інформаційного забезпечення 35

2.2 Стандартний набір загроз та перелік зловмисників 44

2.3 Захист в системах електронного документообігу 62

2.3.1 Забезпечення безпечного доступу 63

2.3.2 Розмежування прав користувача 64

2.3.3 Конфіденційність 64

2.3.4 Забезпечення достовірності документів 65

2.3.5 Протоколювання дій користувачів 66

2.4 Організація СУІБ в системах електронного документообігу 68

2.5 Правила забезпечення захисту інформації в інформаційно-телекомунікаційних системах де використовується СЕД 79

2.6 Порядок здійснення електронного документообігу в організації 83

2.7 Інструкція адміністратора безпеки при роботі з СЕД 88

2.8 Правила роботи в ІТС 92

2.9 Інструкція управління паролями 97

2.10 Висновки за розділом 99

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ 100

3.1 Визначення поточних витрат 100
3.2 Розрахунок витрат на необоротні активи 103
3.3 Визначення економічного ефекту 103
3.4. Висновки за розділом 104
ВИСНОВКИ 105
ПЕРЕЛІК ПОСИЛАНЬ 106
ДОДАТОК А 112
ДОДАТОК Б 113
ДОДАТОК В 114
ДОДАТОК Г 115

ВСТУП

Актуальність. Створення розвиненого і захищеного інформаційного середовища є умовою розвитку суспільства та держави. Останнім часом в світі відбуваються якісні зміни у процесах управління, зумовлені інтенсивним впровадженням сучасних інформаційних технологій.

Впровадження системи електронного документообігу, дозволяє придбати величезну гнучкість в обробці і зберіганні інформації і змушує бюрократичну систему компанії працювати швидше і з більшою віддачою. У той же час, СЕД породжує нові ризики, і зневаги захистом обов'язково призведе до нових загроз конфіденційності.

Останні роки попит на системи електронного документообігу збільшувався і, за прогнозами експертів, ця тенденція продовжиться.

Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже зросла. Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої організації. Як наслідок, в багатьох з них все більше уваги приділяється проблемам захисту інформації та пошуку шляхів її вирішення.

Значний вклад в розвиток СЕД та управління інформаційною безпекою в системах електронного документообігу в Україні внесли Клименко І.В., Дурняк Б.В., Круковський М. Ю., Хорев А.А., Матвієнко О.В., Домарев В.В., Нестеренко О.В. та інші.

Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних витрат. Сукупність внутрішніх і зовнішніх інформаційних загроз створює передумови для порушення безпечного функціонування систем будь якої організації.

Таким чином, після проведення аналізу основних аспектів захисту інформації в СЕД в Україні, та особливостей захисту електронного документообігу, дана характеристика управлінню інформаційною безпекою в

СЕД, та досліджена система управління інформаційною безпекою в системах електронного документообігу.

Саме розробка рекомендацій щодо створення системи управління інформаційною безпекою в СЕД є актуальним науковим завданням яке має теоретичне та практичне значення.

Метою роботи є підвищення рівня інформаційної безпеки при роботі в системах електронного документообігу.

Для досягнення мети дипломної роботи були поставлені окремі завдання:

– проаналізувати основні аспекти захисту інформації в СЕД в Україні а саме: правові аспекти електронного документообігу та захисту інформації та управління інформаційною безпекою в Україні;

– проаналізувати особливості захисту електронного документообігу та комплексний захист інформації як компонент інформаційного забезпечення;

– проаналізувати стандартний набір загроз та перелік зловмисників при роботі в СЕД та захист в системах електронного документообігу, а саме: забезпечення безпечного доступу, розмежування прав користувача конфіденційність, забезпечення достовірності документів та протоколювання дій користувачів;

– запропонувати для управління інформаційною безпекою в СЕД вимоги та рекомендації по створенню системи управління інформаційною безпекою;

– запропонувати використання в організаціях правил забезпечення захисту інформації в інформаційно-телекомунікаційних системах, порядку здійснення електронного документообігу, інструкції адміністратора безпеки при роботі з СЕД, правил роботи в ІТС та інструкції по управлінню паролями.

Об’єкт дослідження: управління інформаційною безпекою в системах електронного документообігу.

Методи дослідження: системний аналіз, методи порівняння, структурний аналіз та спостереження.

Запропоновано для управління інформаційною безпекою в СЕД впровадити на підприємстві систему управління інформаційною безпекою згідно з рекомендаціями міжнародного стандарту ISO/IEC 27001 та використання в організаціях правил забезпечення захисту інформації в та інформаційно-телекомунікаційних системах та порядку здійснення електронного документообігу та інших правил і інструкцій.

Практичне значення роботи полягає в управлінні інформаційною безпекою в СЕД в організаціях різного типу.

Результати здійснених у роботі досліджень можуть бути використані в управлінні інформаційною безпекою в системах електронного документообігу.

Новизна дослідження полягає в запропонованій СУІБ саме в СЕД .

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Правові аспекти електронного документообігу в Україні

Для запровадження електронного документообігу в Україні перед органами влади, передусім, постало завдання зі створення нормативно-правової бази, що забезпечує його здійснення шляхом належної організації відповідних процесів та дотримання вимог до оформлення документів, уніфікації систем організаційно-розпорядчої документації, розроблення єдиної державної системи діловодства, єдиної державної системи документаційного забезпечення управління тощо. Це також мало стати основою для врегулювання відносин між суб'єктами в таких якісно нових сферах діяльності, як електронна комерція, електронна торгівля, подання електронної звітності, надання електронних (адміністративних) послуг через спеціалізовані інформаційні системи та загальнодоступні мережі, зокрема Інтернет.

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про телекомунікації", "Про обов'язковий примірник документів", "Про Національний архівний фонд та архівні установи" та інші.

Наприклад, два базових закони України: "Про електронні документи та електронний документообіг", та "Про електронні довірчі послуги". При цьому слід зазначити, що положення другого з цих законів відповідають вимогам Директиви 1999/93/ЕС Європейського Парламенту та Ради Європи від 13 грудня 1999 року "Про систему електронних підписів, що застосовується в межах Співтовариства". З прийняттям зазначених законів за умови дотримання певних вимог електронний цифровий підпис було прирівняно за правовим статусом до власноручного підпису (печатки), встановлено основні організаційно-правові засади використання електронного документа та застосування ЕДО.

Законом України "Про електронні документи та електронний документообіг", регулюються відносини, пов'язані з відправленням, передаванням та одержанням електронного документа. Зокрема, відправлення та передавання електронного документа здійснюються автором або посередником в електронній формі за допомогою засобів інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ. При цьому електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про його одержання, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами ЕДО. Перевірка цілісності електронного документа проводиться шляхом перевірки справжності накладеного на нього електронного цифрового підпису.

На виконання зазначених законів Кабінет Міністрів України прийняв низку постанов, які конкретизували врегулювання відносин у цій сфері, зокрема:

– "Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу";

– "Про затвердження Порядку акредитації центру сертифікації ключів";

– "Про затвердження Положення про центральний засвідчувальний орган";

– "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності";

– "Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади";

– "Про затвердження Порядку обов'язкової передачі документованої інформації".

Зазначені постанови поряд з іншим спрямовані на створення і розвиток в Україні інфраструктури відкритого ключа (англ. PKI - Public Key Infrastructure) для забезпечення використання електронного цифрового підпису, насамперед

створення її суб'єктів – центрального засвідчувального органу та контролюючого органу, а також засвідчувальних центрів. Створення й забезпечення діяльності інших суб'єктів цієї інфраструктури – центрів сертифікації ключів, у тому числі й акредитованих центрів сертифікації ключів, здійснюється представниками бізнесу.

Затверджений Постановою Кабінету Міністрів України "Типовий порядок здійснення електронного документообігу в органах виконавчої влади" встановлює загальні правила документування в органах влади управлінської діяльності в електронній формі і регламентує виконання дій з електронними документами з моменту їх створення або одержання до відправлення чи передачі до відповідного архіву. При цьому всі інші дії з електронними документами виконуються в органі влади згідно з вимогами до дій з документами на папері, передбаченими інструкцією з діловодства цього органу. Дія Типового порядку поширюється на всі електронні документи, що створюються або одержуються органом влади.

При цьому кожен державний орган влади, орган місцевого самоврядування, підприємство, установа або організація незалежно від форми власності конкретизує для своїх потреб загальні правила документування в електронній формі і регламентує виконання дій з електронними документами згідно з законодавством.

Орган влади здійснює ЕДО лише за умови використання надійних засобів електронного цифрового підпису (ЕЦП), що має бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації (КЗІ), одержаним на ці засоби від Адміністрації Держспецзв'язку, та наявності посилених сертифікатів відкритих ключів (ПСВК) у своїх працівників – підписувачів. При цьому ЕДО здійснюється органом влади через спеціальні телекомунікаційні мережі або телекомунікаційні мережі загального користування, а відправлення електронних документів через телекомунікаційні

мережі загального користування здійснюється за рішенням керівника цього органу.

Згідно із законодавством система електронного документообігу (СЕДО) органу влади повинна відповідати вимогам нормативно-правових актів у сфері захисту інформації. Зокрема, це стосується положень Закону України "Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" та Постанови Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".

Створення архівів електронних документів, подання їх до архівних установ України та зберігання в цих установах здійснюється в порядку, визначеному законодавством. Зокрема, наказом Державного комітету архівів України було затверджено "Порядок зберігання електронних документів в архівних установах".

Іншими рішеннями уряду, нормативно-правовими актами і нормативними документами центральних органів виконавчої влади було врегульовано ще низку юридичних, організаційних і технічних питань, але на сьогодні нагальні проблеми у цій сфері поки що вирішені не повністю.

Основою для врегулювання питань діловодства стала Постанова Кабінету Міністрів України "Про затвердження Примірної інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади". Примірна інструкція визначає порядок ведення загального діловодства, а її положення поширюються на всю службову документацію, в тому числі створювану за допомогою персональних комп'ютерів. Комп'ютерні (автоматизовані) технології обробки документної інформації повинні відповідати вимогам державних стандартів, а також зазначеної інструкції.

Згідно з Примірною інструкцією відповідальність за організацію діловодства в установі несе керівник установи. Ведення діловодства відповідно до вимог державних стандартів, цієї Примірної інструкції та інструкцій з

діловодства установ покладається на управління справами, загальні відділи, канцелярії або секретарів.

При цьому основним завданням діловодної служби є встановлення єдиного порядку документування і роботи з документами в установі на основі використання сучасної комп'ютерної техніки, автоматизованої технології роботи з документами та скорочення кількості документів.

Низка положень Примірної інструкції певною мірою вже закладала основу для впровадження в установах СЕДО. Зокрема, в них зазначалося, що механізація і автоматизація діловодних процесів є обов'язковою умовою раціональної організації діловодства в кожній установі, засобом підвищення продуктивності і здешевлення управлінської праці і повинна здійснюватися на основі впорядкованої системи документування управлінської діяльності, уніфікації та скорочення кількості форм використовуваних документів. Крім того, ці заходи вживаються на всіх етапах діловодного процесу: підготовки документів, їх копіювання, оперативного зберігання і транспортування, контролю за виконанням тощо, а засоби механізації і автоматизації діловодних процесів мають бути сумісними і передбачати можливість об'єднання в єдину систему.

У Примірній інструкції також зазначено, що комплекс технічних засобів повинен забезпечувати збирання і передачу інформації, її запис на машинні носії, введення інформації в персональний комп'ютер, виведення результатів, її обробку у формі машино- або відеограм, сумісність з іншими інформаційними системами, а також можливість об'єднання в єдину інтегровану систему. При цьому під час впровадження нових технологій роботи з документами необхідно враховувати:

– доцільність упровадження технічних засобів;

– можливість придбання технічних засобів у певні терміни;

– наявність придатних приміщень;

– необхідність залучення спеціалістів до обслуговування техніки

тощо.

Відповідальність за ефективність використання механізованої і автоматизованої технології роботи з документами несе керівник установи.

Опрацювання документів в установі здійснюється за типовими схемами відповідно для вхідних, внутрішніх і вихідних документів. Зокрема, при опрацюванні вхідного документа виділяються такі етапи: отримання, попередній розгляд, реєстрація, доповідь керівництву, організація виконання – призначення виконавців та постановка завдань, здійснення діловодного контролю за перебігом та наслідками виконання, закінчення справи (кінцеве оформлення) та направлення на зберігання.

Усі дії з електронним документом, якщо це не стосується специфіки їх створення або одержання до відправлення чи передачі до архіву, виконуються в установах згідно з вимогами до дій з документами на папері, передбаченими інструкціями з діловодства цих органів.

1.2 Складові інформаційної безпеки в Україні

За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку.

Від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління з використанням інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього і зовнішніх ринків. Використання інформаційних технологій визначає структуру і якість озброєнь, необхідний рівень їх достатності, ефективність дій збройних сил. Спроможність ідентифікувати науково-технічні та екологічні проблеми, здійснювати моніторинг їх розвитку і прогнозування наслідків безпосередньо залежать від ефективності використовуваної інформаційної інфраструктури.

Таким чином, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки в усіх сферах та на всіх рівнях.

У зв'язку з цим слід виділити такі її рівні:

– законодавчий та нормативно-правовий – закони, нормативно-правові акти, тощо;

– адміністративний – дії загального характеру, що вживаються органами виконавчої влади;

– процедурний – конкретні процедури забезпечення інформаційної безпеки;

– програмно-технічний – конкретні технічні заходи забезпечення інформаційної безпеки.

Проблема ефективного забезпечення безпеки інформації в державі передбачає вирішення таких масштабних задач, як:

– розроблення теоретичних основ забезпечення безпеки інформації;

– створення системи органів та структур, відповідальних за безпеку інформації;

– вирішення та автоматизація проблем керування захистом інформації;

– створення нормативно-правової бази, що регламентує рішення всіх задач забезпечення безпеки інформації;

– налагодження виробництва засобів програмно-технічного захисту інформації; організація підготовки відповідних фахівців та ін.

Серед основних принципів державної політики у сфері забезпечення інформаційної безпеки можна зазначити:

– держава формує програму інформаційної безпеки, що поєднує зусилля державних організацій і комерційних структур у створенні єдиної системи інформаційної безпеки;

– держава здійснює контроль за створенням і використанням засобів захисту інформації за допомогою їхньої обов'язкової сертифікації і ліцензування діяльності в області захисту інформації;

– обмеження доступу до інформації є виключення з загального принципу відкритості інформації і здійснюється тільки на основі законодавства;

– відповідальність за зберігання, засекречення і розсекречення інформації персоніфікується;

– доступ до інформації, а також обмеження доступу, здійснюються з обліком обумовлених законом прав власності на цю інформацію;

– держава формує нормативно-правову базу, що регламентує права, обов'язки і відповідальність усіх суб'єктів, що діють в інформаційній сфері;

– юридичні і фізичні особи, що збирають, нагромаджують і обробляють персональні дані і конфіденційну інформацію, несуть відповідальність перед законом за їх зберігання і використання;

– держава проводить протекціоністську політику, що підтримує діяльність вітчизняних виробників засобів інформатизації і захисту інформації, і здійснює заходи для захисту внутрішнього ринку від проникнення на нього неякісних засобів інформатизації й інформаційних продуктів;

– держава прагне до відмовлення від закордонних інформаційних технологій для інформатизації органів державної влади і управління по мірі створення конкурентоздатних вітчизняних інформаційних технологій і засобів інформатизації.

Відповідно до вищеназваних принципів і положень забезпечення інформаційної безпеки держави необхідно вирішити наступні ключові проблеми:

– розвиток науково-практичних основ інформаційної безпеки, що відповідають сучасній геополітичній ситуації та умовам політичного і соціально-економічного розвитку держави;

– формування законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, у тому числі розробка регламенту інформаційного

обміну для органів державної влади, підприємств, нормативного закріплення відповідальності посадових осіб і громадян за дотримання вимог інформаційної безпеки;

– розробка механізмів реалізації прав громадян на інформацію;

– формування системи інформаційної безпеки, що є складовою частиною загальної системи національної безпеки країни;

– розробка сучасних методів і технічних засобів, що забезпечують комплексне рішення задач захисту інформації;

– розробка критеріїв і методів оцінки ефективності систем і засобів інформаційної безпеки і їх сертифікація;

– комплексне дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально-психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією.

Базовим елементом інформаційного середовища органів державної влади є інформаційна інфраструктура, що являє собою єдність наступних компонентів, тобто системи сервісного обслуговування елементів інфраструктури:

– виробництва інформаційних продуктів;

– доставки їх до споживача;

– виробництва засобів виробництва інформаційних продуктів та їх доставки;

– виробництва інформаційних технологій;

– накопичення і збереження інформаційного продукту або інформаційного ресурсу.

1.3 Правові аспекти захисту інформації та управління інформаційною безпекою

Відповідно до мети дипломної роботи у відповідності з темою та завданням, в роботі розглядається питання щодо управління інформаційною безпекою в системах електроного документообігу. Також слід зазначити що це

питання можна розкласти на складові: інформаційна безпека, система управління інформаційною безпекою, системи електроного документообігу та безпека в системах електроного документообігу. А оскільки системи електроного документообігу є однією із складових загальної ІТС організації, то також слід додати ще й складову про захист інформації в інформаційно-телекомунікаційних системах. З цією метою можно навести перелік основних документів, що було розглянуто в роботі:

Закони України:

- Закон України "Про інформацію"
- Закон України "Про телекомунікації"
- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"
- Закон України "Про державну таємницю"
- Закон України "Про захист персональних даних"
- Закон України "Про електронний цифровий підпис"
- Закон України "Про електроні документи та електронний документообіг"
- Закон України Про доступ до публічної інформації"

Постанови КМУ:

- Постанова Кабінету міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 №373

Нормативні документи в галузі технічного захисту інформації та стосовно створення і функціонування КСЗІ:

- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
- 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 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній 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

Міжнародні стандарти ISO/IEC серії 27000:

ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary (на стадії FDIS)

ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management

В даній роботі використовувалися переважно лише перші три стандарти цієї серії, більш повний перелік стандартів та їх проектів наведено в додатку А цієї роботи.

1.4 Основні поняття та визначення

В законі України «Про електронні документи та електронний документообіг», що встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів та поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів, наведено ряд основних термінів та визначень:

адресат - фізична або юридична особа, якій адресується електронний документ;

дані - інформація, яка подана у формі, придатній для її оброблення електронними засобами;

посередник - фізична або юридична особа, яка в установленому законодавством порядку здійснює приймання, передавання (доставку), зберігання, перевірку цілісності електронних документів для задоволення власних потреб або надає відповідні послуги за дорученням інших суб'єктів електронного документообігу;

обов'язковий реквізит електронного документа - обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили;

автор електронного документа - фізична або юридична особа, яка створила електронний документ;

суб'єкти електронного документообігу - автор, підписувач, адресат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу.

електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

електронний документообіг (обіг електронних документів) - сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Для ідентифікації автора електронного документа може використовуватися електронний підпис.

Накладанням електронного підпису завершується створення електронного документа.

Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом.

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.

Оригіналом електронного документа вважається електронний примірник документа з обов’язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України "Про електронний цифровий підпис"

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії.

Перевірка цілісності електронного документа може проводитися шляхом перевірки електронного цифрового підпису.

Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

У разі неможливості зберігання електронних документів на електронних носіях інформації протягом строку, встановленого законодавством для відповідних документів на папері, суб'єкти електронного документообігу повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством. Якщо неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у вигляді копії документа на папері (у разі відсутності оригіналу цього документа на папері). При копіюванні електронного документа з електронного носія інформації обов'язково здійснюється перевірка цілісності даних на цьому носії.

При зберіганні електронних документів обов'язкове додержання таких вимог:

- інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

- має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

- у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Суб'єкти електронного документообігу можуть забезпечувати додержання вимог щодо збереження електронних документів шляхом використання послуг посередника, у тому числі архівної установи, якщо така установа додержується вимог цієї статті. Створення архівів електронних

документів, подання електронних документів до архівних установ України та їх зберігання в цих установах здійснюється у порядку, визначеному законодавством. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання (Наказ Міністерства юстиції України 11.11.2014 № 1886/5)

Суб'єкти електронного документообігу, які здійснюють його на договірних засадах, самостійно визначають режим доступу до електронних документів, що містять конфіденційну інформацію, та встановлюють для них систему (способи) захисту.

В інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять державні інформаційні ресурси, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до законодавства.

ЗУ “Про захист інформації в інформаційно-телекомунікаційних системах”, який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, дає наступні визначення:

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації - фізична або юридична особа, якій належать права на інформацію;

власник системи - фізична або юридична особа, якій належить право власності на систему;

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

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

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

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;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Закон України “Про електронний цифровий підпис”, який визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису, дає наступні визначення термінів:

електронний підпис - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

електронний цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

засіб електронного цифрового підпису - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

особистий ключ - параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

відкритий ключ - параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

засвідчення чинності відкритого ключа - процедура формування сертифіката відкритого ключа;

сертифікат відкритого ключа - документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;

посилений сертифікат відкритого ключа - сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

акредитація - процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;

компрометація особистого ключа - будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

блокування сертифіката ключа - тимчасове зупинення чинності сертифіката ключа;

підписувач - особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;

послуги електронного цифрового підпису - надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені цим Законом;

надійний засіб електронного цифрового підпису - засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється у порядку, визначеному законодавством.

Суб'єктами правових відносин у сфері послуг електронного цифрового підпису є:

- підписувач;
- користувач;
- центр сертифікації ключів;

- акредитований центр сертифікації ключів;
- центральний засвідчувальний орган;
- засвідчувальний центр органу виконавчої влади або іншого державного органу (далі - засвідчувальний центр);
- контролюючий орган.

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами - суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

Інші юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, сформованим

центром сертифікації ключів, а також використовувати електронний цифровий підпис без сертифіката ключа.

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, які користуються електронними цифровими підписами без сертифіката ключа, визначається суб'єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах.

Функції контролюючого органу здійснює спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

Контролюючий орган перевіряє дотримання вимог цього Закону центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів.

Стандарт ISO / IEC 27001 “Інформаційні технології - Методи захисту - Системи менеджменту інформаційної безпеки – Вимоги” був розроблений з метою встановити вимоги для створення, впровадження, підтримки функціонування і безперервного поліпшення системи менеджменту інформаційної безпеки. Визнання необхідності системи менеджменту інформаційної безпеки є стратегічним рішенням організації. На створення та впровадження системи менеджменту інформаційної безпеки організації впливають потреби і цілі організації, вимоги з безпеки, які застосовуються організаційні процеси, розмір і структура організації. Всі ці фактори впливу очікувано змінюються протягом тривалого часу.

Система менеджменту інформаційної безпеки спрямована на збереження конфіденційності, цілісності та доступності інформації за рахунок застосування процесів управління ризиками і забезпечує впевненість зацікавлених сторін у тому, що ризики управляються належним чином.

Важливим є те, що система менеджменту інформаційної безпеки становить частину процесів організації і вбудована в загальну структуру управління, і, таким чином, питання інформаційної безпеки враховуються при розробці процесів, інформаційних систем та засобів управління.

Передбачається, що система менеджменту інформаційної безпеки буде змінюватися відповідно до потреб організації.

Стандарт ISO / IEC 27001 може використовуватися як самою організацією, так і зовнішніми сторонами для оцінки здатності організації відповідати власним вимогам з інформаційної безпеки.

Система менеджменту інформаційної безпеки (СМІБ) включає в себе політики, процедури, керівництва та відповідні ресурси і завдання, колегіально керованих організацією з метою захисту її інформаційних активів. СМІБ є системний підхід до розробки, впровадження, функціонування, моніторингу, аналізу, забезпечення і поліпшення інформаційної безпеки організації для досягнення бізнес-цілей. Вона ґрунтується на оцінці ризиків і рівнях прийнятності ризиків організації, встановлених таким чином, щоб результативно обробляти ризики і управляти ними. Аналіз вимог до захисту інформаційних активів і застосування засобів управління для забезпечення захисту цих інформаційних активів відповідно до ситуації, вносить свій внесок в успішну реалізацію СМІБ. Наступні фундаментальні принципи також сприяють успішній реалізації СМІБ:

- усвідомлення необхідності забезпечення інформаційної безпеки;
- призначення відповідальності за інформаційну безпеку;
- пов'язування зобов'язань керівництва з інтересами зацікавлених сторін;
- підвищення значення соціальних цінностей;
- оцінка ризику, яка визначає відповідні засоби управління для забезпечення прийнятних рівнів ризику;
- безпеку, як невід'ємний елемент інформаційних мереж і систем;
- активне попередження і виявлення інцидентів інформаційної безпеки;
- забезпечення комплексного підходу до управління інформаційною безпекою;
- постійна переоцінка рівня інформаційної безпеки та внесення змін при необхідності.

Інформація - це актив, який, подібно до інших важливих активів, є істотним для бізнесу організації і, отже, повинен бути відповідним чином захищен. Інформацію можна зберегти в різних формах, в тому числі: цифровий (наприклад, файли, що зберігаються на електронних або оптичних носіях), на матеріальних носіях (наприклад, папері), а також прихованої - у формі знань співробітників. Інформація може передаватися різними засобами, включаючи: кур'єрів, електронні та голосові засоби зв'язку. Яка б форма або які б кошти не використовувалися для передачі інформації, вона завжди повинна бути відповідним чином захищена.

У багатьох організаціях інформація залежить від інформаційно-комунікаційних технологій. Ці технології часто - суттєвий елемент в організації, який полегшує створення, обробку, зберігання, передачу, захист і утилізацію інформації.

Інформаційна безпека включає в себе три основних компоненти:

конфіденційність, можливість застосування і цілісність. Інформаційна безпека забезпечується застосуванням та управлінням відповідними заходами забезпечення безпеки, які охоплюють широкий діапазон загроз з метою гарантувати стійкий успіх бізнесу і мінімізувати вплив інцидентів інформаційної безпеки.

Інформаційна безпека досягається за допомогою виконання відповідного набору засобів управління, сформованого в ході обраного процесу ризик-менеджменту і керованого через СМІБ, включаючи політики, процеси, процедури, організаційні структури, програмне та технічне забезпечення для захисту виявлених інформаційних активів. Ці кошти управління повинні бути визначені, впроваджені, контролюватися, аналізуватися і поліпшуватися, якщо необхідно, щоб гарантувати досягнення встановленого рівня інформаційної безпеки та бізнес-цілей. Очікується, що відповідні кошти управління інформаційної безпеки будуть вбудовані в бізнес-процеси організації.

1.5 Висновки за розділом

Базовий елемент будь СЕД - документ, всередині системи це може бути файл, а може бути запис в базі даних. Говорячи про захищений документообіг, часто мають на увазі саме захист документів, захист тієї інформації, яку вони в собі несуть. У цьому випадку все зводиться до хоча і не простої задачі захисту даних від несанкціонованого доступу.

Але тут є велика помилка, адже мова йде саме про захист системи, а не тільки про захист даних всередині неї. Це означає, що потрібно захистити також її працездатність, забезпечити швидке відновлення після ушкоджень, збоїв і навіть після знищення. Система - це як живий організм, мало захистити тільки вміст його клітин, необхідно захистити також зв'язок між ними і їх працездатність. Тому до захисту системи електронного документообігу необхідний комплексний підхід, який передбачає захист на всіх рівнях СЕД. Починаючи від захисту фізичних носіїв інформації, даних на них, і закінчуючи організаційними заходами.

Таким чином, необхідно захищати, по-перше, апаратні елементи системи. Це комп'ютери, сервери, елементи комп'ютерної мережі та мережеве обладнання (як активне - маршрутизатори, switch'і і т.д., так і пасивне - кабелі, розетки і т.д.). Необхідно передбачити такі загрози, як поломка устаткування, доступ зловмисника до обладнання, відключення живлення і т.д.

По-друге, захист необхідних файлів системи. Це файли програмного забезпечення та бази даних, рівень між апаратними пристроями системи і логічними елементами системи і фізичними складовими. В іншому випадку з'являється можливість впливу зловмисником або зовнішніми обставинами на файли СЕД, не проникаючи в систему, тобто як би зовні. Наприклад, файли бази можуть бути скопійовані зловмисником або пошкоджені в результаті збою операційної системи або обладнання.

По-третє, саме собою, необхідно захищати документи і інформацію, що знаходяться всередині системи.

Використовуючи такий підхід, можна побудувати систему, захищену на всіх рівнях від загроз на кожному рівні. Можливо, виглядає трохи

параноїдально, та й вартість такого захисту може зрівнятися з вартістю самої СЕД, тому завжди потрібно шукати розумний баланс між безпекою та вартістю.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Комплексний захист інформації як компонент інформаційного забезпечення

Об’єктами захисту в системі є інформація, що обробляється в ній, та програмно-технічне забезпечення, яке призначене для обробки цієї інформації.

Для забезпечення захисту інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах повинні обов’язково виконуватися наступні процедури:

автентифікація – процедура встановлення належності користувачеві інформації в системі (далі – користувач) пред’явленого ним ідентифікатора;

ідентифікація – процедура розпізнавання користувача в системі, як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред’явленого ідентифікатора повинні блокуватися.

Передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

Порядок підключення систем, в яких обробляється конфіденційна і таємна інформація, до глобальних мереж передачі даних визначається законодавством.

Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято власником (розпорядником) інформації.

Комплексність підходу до захисту інформації є рішення в рамках єдиної концепції двох або більшої кількості різнопланових завдань.

Сучасна система захисту інформації повинна включати структурну, функціональну і часову комплексність. Структурна комплексність припускає забезпечення необхідного рівня захисту у всіх елементах системи обробки інформації.

Функціональна комплексність означає, що методи захисту повинні бути направлені на всі виконувані функції системи обробки інформації.

Часова комплексність припускає безперервність здійснення заходів щодо захисту інформації як в процесі безпосередньої її обробки, так і на всіх етапах життєвого циклу об'єкту обробки інформації.

Склад комплексної системи захисту визначається на основі вивчення усіх інформаційних процесів та потоків системи телекомунікацій і, як наслідок, розробці такої моделі загроз, щоб забезпечити мінімізацію втрат. На основі

моделі загроз має бути розроблена та запроваджена концепція та політика інформаційної безпеки органів державної влади та створена комплексна система захисту інформації, які мають забезпечувати такі функції:

конфіденційність інформації – властивість інформації, коли неавторизовані особи, які не мають доступу до інформації, не можуть розкрити зміст цієї інформації;

цілісність інформації – властивість інформації, яка полягає в тому, що вона не може бути змінена навмисно або випадково користувачем чи процесом. А також властивість, яка полягає в тому, що жодний з її компонентів не може бути усунений, модифікований або доданий з порушенням політики безпеки;

доступність – властивість ресурсу системи (інформації), яка полягає в тому, що авторизований користувач може отримати доступ до ресурсу тільки із заданим змістом та якістю;

спостережливість – властивість ресурсу інформаційної технології, що дозволяє реєструвати всі дії користувачів, здійснювати доступ поіменно, відповідно до ідентифікаторів та повноважень, а також реагувати на ці дії з метою мінімізації можливих втрат в системі, що здійснюється також за рахунок застосування криптографічного захисту інформації (КЗІ).

До складу КЗЗІ входять заходи і засоби, які реалізують способи, методи, механізми захисту інформації від:

– витоків технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань, акустоелектричних і інших каналів;

– несанкціонованих дій і несанкціонованого доступу до інформації, які можуть здійснюватися шляхом підключення до апаратури і ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування помилковій інформації, застосування заставних пристроїв або програм, використання комп'ютерних вірусів і т.п.;

– спеціального впливу на інформацію, який може здійснюватися

– шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної інформаційної системи склад, структура і вимоги до КЗЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи (АС) і умовами її експлуатації.

Однією з вимог забезпечення захисту інформації в АС є те, що обробка конфіденційної інформації повинна здійснюватись з використанням захищеної технології, яка містить програмно-технічні засоби захисту і організаційні заходи, які забезпечують виконання загальних вимог з захисту інформації. Загальні вимоги передбачають:

– наявність переліку конфіденційної інформації, яка підлягає автоматизованій обробці; у разі потреби можлива її класифікація в межах категорії за цільовим призначенням, ступенем обмеження доступу окремої категорії користувачів і іншими класифікаційними ознаками;

– наявність відповідального підрозділу, якому надаються повноваження щодо організації і впровадження технології захисту інформації, контролю за станом захищеності інформації;

– створення КСЗІ, яка являє собою сукупність організаційних і інженерно-технічних заходів, програмно-апаратних засобів, направлених на забезпечення захисту інформації під час функціонування АС;

– розробку плану захисту інформації в АС;

– наявність атестату відповідності КСЗІ в АС нормативним документам із захисту інформації;

– можливість визначення засобами КСЗІ декількох ієрархічних рівнів повноважень користувачів і декількох класифікаційних рівнів інформації;

– обов'язковість реєстрації в АС всіх користувачів і їх дій щодо конфіденційної інформації;

– можливість надання користувачам тільки за умови службової необхідності санкціонованого і контрольованого доступу до конфіденційної інформації, яка обробляється в АС;

– заборона несанкціонованій і неконтрольованій модифікації конфіденційної інформації в АС;

– здійснення за допомогою СЗІ обліку вихідних даних, отриманих під час рішення функціональної задачі, у формі віддрукованих

– документів, які містять конфіденційну інформацію, відповідно до керівних документів;

– заборона несанкціонованого копіювання, розмноження, розповсюдження конфіденційної інформації, в електронному вигляді;

– забезпечення за допомогою СЗІ контролю за санкціонованим копіюванням, розмноженням, розповсюдженням конфіденційної інформації, в електронному вигляді;

– можливість здійснення однозначної ідентифікації і аутентифікації кожного зареєстрованого користувача;

– забезпечення КСЗІ можливості своєчасного доступу зареєстрованих користувачів АС до конфіденційної інформації.

Приведені вимоги є базовими і застосовуються при захисті інформації від несанкціонованого доступу (НСД) у всіх типах АС.

Отже, зважаючи на викладене вище, доступ до інформації у суб'єктивному розумінні – це гарантована державою можливість фізичних, юридичних осіб і державних органів вільно одержувати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законних інтересів інших громадян, прав та інтересів юридичних осіб.

Провівши оцінку необхідності захисту інформації від НСД, можна судити про складність КСЗІ, оцінити вірогідність погроз, що проявляються, на інформаційну систему, а також сформувати модель порушника, після чого слід приступити до формування захисних заходів.

Спираючись на вимоги із захисту інформації від НСД, можна привести основні принципи захисних заходів від НСД в АС.

Принцип перший – обґрунтованість доступу. Даний принцип полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню “форму допуску” для отримання інформації потрібного ним рівня конфіденційності, і ця інформація необхідна йому для виконання його виробничих функцій. У сфері автоматизованої обробки інформації як користувачі можуть виступати активні програми і процеси, а також носії інформації різного ступеня складності. Тоді система доступу припускає визначення для всіх користувачів відповідного програмно-апаратного середовища або інформаційних і програмних ресурсів, які будуть їм доступні для конкретних операцій.

Принцип другий – достатня глибина контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів АС, які відповідно до принципу обґрунтованості доступу слід розділяти між користувачами.

Принцип третій – розмежування потоків інформації. Для попередження порушення безпеки інформації, яке, наприклад, може мати місце при записі секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, не призначеним для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах і лініях зв'язку, необхідно здійснювати відповідне розмежування потоків інформації.

Принцип четвертий – чистота повторно використовуваних ресурсів. Даний принцип полягає в очищенні ресурсів, що містять конфіденційну інформацію, при їх видаленні або звільненні користувачем до перерозподілу цих ресурсів іншим користувачам.

Принцип п’ятий – персональна відповідальність. Кожен користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту, а також за випадкові або умисні дії, які можуть привести до несанкціонованого ознайомлення з конфіденційною інформацією, її

спотворенню або знищенню, або виключенню можливості доступу до такої інформації законних користувачів.

Принцип шостий – цілісності засобів захисту. Даний принцип має на увазі, що засоби захисту інформації в АС повинні точно виконувати свої функції відповідно до перерахованих принципів і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і дії на процеси в системі.

При розгляді питань безпеки інформації в АС завжди говорять про наявність "бажаних" станів системи. Ці стани описують "захищеність" системи. Поняття "захищеності" принципово не відрізняється від інших властивостей технічної системи, наприклад "надійної роботи". Особливістю поняття "захищеність" є його тісний зв'язок з поняттям "загроза" (те, що може бути причиною виведення системи із захищеного стану). Виділяються три компоненти, що пов'язані з порушенням безпеки системи:

"загроза" – зовнішнє відносно системи джерело порушення властивості "захищеність";

"об'єкт атаки" – частина системи, на яку діє загроза;

"канал дії" – середовище перенесення зловмисної дії.

Інтегральною характеристикою, що об'єднує всі ці компоненти, є політика безпеки – якісний/якісно-кількісний вираз властивостей захищеності в термінах, що представляють систему. Опис політики безпеки повинен включати і враховувати властивості загрози, об'єкта атаки та каналу дії.

За означенням, під політикою безпеки інформації розуміється набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосований до організації, автоматизованої системи, операційної системи, послуги, що реалізується системою (набору функцій) для забезпечення захисту від певних загроз.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації. Для кожної автоматизованої системи політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама автоматизована система може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій автоматизованій системі буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси автоматизованої системи, що потребують захисту, зокрема встановлювати категорії оброблюваної в ній інформації. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Методи мають такий зміст:

перешкоди – фізичної перешкоди доступу зловмиснику до інформації, що захищається;

керування доступом – захист інформації шляхом регулювання використання всіх ресурсів комп'ютерної інформаційної системи;

маскування – захисту інформації шляхом її криптографічного закриття;

регламентація – захист інформації, що створює такі умови автоматизованої обробки, зберігання й передачі інформації, що захищається, за яких можливості несанкціонованого доступу до неї зводилися б до мінімуму;

примушення – захист, за якого користувачі й персонал системи змушено дотримувати правил обробки, передачі й використання інформації, що захищається, під загрозою матеріальної, адміністративної або карної відповідальності;

спонукання – захист, який спонукує користувача й персонал системи не порушувати встановлений порядок за рахунок дотримання моральних і етичних норм, які склалися;

Розглянуті методи забезпечення безпеки реалізуються на практиці шляхом застосування різних засобів захисту, таких, як технічні, програмні, організаційні, законодавчі й морально-етичні. До основних засобів захисту, які використовуються для створення механізму забезпечення безпеки, належать такі:

Технічні засоби реалізуються у вигляді електричних, електромеханічних та електронних пристроїв. Уся сукупність технічних засобів поділяється на апаратні й фізичні.

Програмні засоби являють собою програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

Організаційні засоби – це організаційно-технічні й організаційно-правові заходи, які здійснюються в процесі створення та експлуатації обчислювальної техніки, апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи апаратури на всіх етапах їх життєвого циклу.

Морально-етичні засоби реалізуються у вигляді різних норм, які склалися традиційно або складаються в міру поширення обчислювальної техніки й засобів зв'язку в суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчі заходи.

Законодавчі засоби захисту визначаються нормативно-правовими актами, якими регламентуються норми та правила користування, обробки й передачі інформації обмеженого доступу. За порушення цих правил встановлюються відповідальність.

Захист інформації в системі обробки інформації повинен ґрунтуватися на наступних основних принципах:

- системності;

- комплексності;

- безперервності захисту;

- розумної достатності;

- гнучкості керування й застосування;

- відкритості алгоритмів і механізмів захисту;

- простоти застосування захисних заходів і засобів.

Системний підхід до захисту комп'ютерних систем припускає необхідність обліку всіх взаємозалежних, взаємодіючих і мінливих у часі елементів, умов і факторів, суттєво значимих для розуміння й вирішення проблеми забезпечення безпеки. При створенні системи захисту необхідно враховувати всі слабкі, найбільш уразливі місця системи обробки інформації, а також характер, можливі об'єкти й напрямки атак на систему з боку порушників, шляхи проникнення в розподілені системи й несанкціонованого доступу до інформації. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення й несанкціонованого доступу до інформації, але й з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеки.

2.2 Стандартний набір загроз та перелік зловмисників

Відповідно до п. 6.1.2.9 НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», за результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об'єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003. Модель загроз для інформації та модель порушника рекомендується оформляти у вигляді окремих документів (або поєднаних в один документ) плану захисту.

Відповідно до розділу 4 “Загрози для інформації в АС” НД ТЗІ 1.4-001-2000 “Типове положення про службу захисту інформації в автоматизованій системі”

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;
- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
- збої і відмови у роботі обладнання та технічних засобів АС;
- наслідки помилок під час проектування та розробки компонентів АС

(технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

- помилки персоналу (користувачів) АС під час експлуатації;
- навмисні дії (спроби) потенційних порушників.

Необхідно визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію, тобто на порушення яких властивостей вони спрямовані (конфіденційності, цілісності та доступності інформації), а також порушення спостережності та керованості АС.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);
- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);
- неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);
- наслідки некомпетентного застосування засобів захисту;

- інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

- порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);

- порушення режимів функціонування АС (обладнання і ПЗ);

- впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

- використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

- використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;

- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

- несанкціоноване копіювання носіїв інформації;

- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");

- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

- впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ

до критичної інформації (наприклад, аналізаторів безпеки мереж);

- інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

- на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості АС);

- джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

- можливі способи здійснення загроз.

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної АС. Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;

- категорії осіб, з числа яких може бути порушник;

- припущення про кваліфікацію порушника;

- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;

- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

- нанесення збитків шляхом знищення матеріальних та інформаційних

цінностей.

Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами АС, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

- третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

- четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

За рівнем знань про АС усіх порушників можна класифікувати як таких, що:

- володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

- володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;

- володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників можна класифікувати як таких, що:

- використовують виключно агентурні методи одержання відомостей;

- використовують пасивні технічні засоби перехоплення інформаційних сигналів;

- використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

- використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії можуть класифікуватись:

- без одержання доступу на контрольовану територію організації (АС);

- з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

- з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;

- з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

- з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

Ці рекомендації враховано та наведено в таблицях 2.1 – 2.4

Таблиця 2.1 – Класифікація рівнів загроз

Рівень загрози	Пояснення
Антропогені	
1	Низький. Недостатня кваліфікація особи в поєднанні з відсутністю доступу до інформаційного ресурсу.
2	Середній. Недостатня кваліфікація особи в поєднанні з наявністю доступу до інформаційного ресурсу.
3	Високий. Достатня кваліфікація особи в поєднанні з наявністю доступу до інформаційного ресурсу.
Техногенні та стихійні	
1	Низька ймовірність.
2	Середня ймовірність.
3	Висока ймовірність.

Таблиця 2.2 –Джерела загроз

Позначення	Джерело загрози	Рівень загрози
Антропогенні		
АВн1	технічний персонал, обслуговуючий приміщення, у яких знаходиться.	1
АВн2	персонал, що безпосередньо працює з АС, але не має доступу лише до інформації в межах матриці доступу.	2
АВн3	персонал, що безпосередньо працює в АС та має доступ до інформації	3
АЗв1	будь які особи, що знаходяться за межами КЗ	1
АЗв2	відвідувачі	2
АЗв3	Хакери	2
АЗв4	кримінальні структури	2
АЗв5	Конкуренти	3
Техногенні		
Т1	засоби зв'язку (телефон, Інтернет)	1
Т2	мережі інженерних комунікацій (система опалення, каналізації, водопостачання, заземлення, вентиляції, кондиціонування)	2
Т3	допоміжні засоби (відеоспостереження, сигналізація, протипожежна система)	2
Т4	неякісні технічні засоби обробки інформації (робочі станції, сервер, комутатор, маршрутизатор, система кабелів, принтери, багатофункціональні пристрої)	3
Т5	неякісні програмні засоби обробки інформації (операційна система, ПЗ для роботи з БД клієнтів, ПЗ для бухгалтерського обліку)	3
Стихійні		
С1	Пожежа	3
С2	Урагани та повені	2
С3	Інші форс-мажорні обставини	1

Таблиця 2.3 – Специфікація порушника

Позначення	Ознаки порушника	Рівень загрози
1	2	3
За мотивами		
Мт1	Самоствердження	1
Мт2	Безвідповідальність	2
Мт3	корисливий інтерес	3

За кваліфікацією		
К1	не має інформації щодо системи захисту	1
К2	знає особливості систем захисту на об'єкті	2
К3	знає структуру, функції та механізми систем захисту інформації	3
За часом		
Ч1	в неробочій час	1
Ч2	під час функціонування підприємства	2

продовження таблиці 2.3

Ч3	в будь-який час	3
За місцем		
М1	без доступу до контрольованої зони	1
М2	з доступом до контрольованої зони, але без доступу до приміщень	2
М3	усередині приміщень, але без доступу до АС	3
М4	від робочих станцій співробітників компанії	4

Таблиця 2.4 – Модель порушника

Специфікація порушника	Загроза							
	АВн1	АВн2	АВн3	АЗв1	АЗв2	АЗв3	АЗв4	АЗв5
Мотив	1,2,3	2,3	2,3	1,3	1,3	1,3	1,3	1,3
Кваліфікація	1	2,3	2,3	1	1	1	1	1
Час дії	3	2	2	3	2	3	3	3
Місце дії	2	3	3	1	2	2	2	2
Підсумок	12	15	15	9	9	10	10	10

Оскільки загрози для системи електронного документообігу досить стандартні і можуть бути класифіковані в такий спосіб.

Загроза цілісності – пошкодження і знищення інформації, спотворення інформації - як й не навмисне в разі помилок і збоїв, так і зловмисне.

Загроза конфіденційності - це будь-яке порушення конфіденційності, в тому числі крадіжка, перехоплення інформації, зміни маршрутів слідування.

Загроза працездатності системи - всілякі загрози, реалізація яких призведе до порушення або припинення роботи системи; сюди входять як умисні атаки, так і помилки користувачів, а також збої в обладнанні та програмному забезпеченні.

Захист саме від цих загроз в тій чи іншій мірі повинна реалізовувати будь-яка система електронного документообігу. При цьому, з одного боку, впроваджуючи СЕД, впорядковуючи і консолідуючи інформацію, збільшуються ризики реалізації загроз, але з іншого боку, як це не парадоксально, впорядкування документообігу дозволяє вибудувати більш якісну систему захисту.

Джерел загроз в нашому небезпечному світі не мало: це і низький рівень кваліфікації деяких системних адміністраторів, і техніка, яка має властивість ламатися в самий не підходящий момент, і форс-мажорні обставини, які рідко, але все ж відбуваються. І навіть якщо сервери не постраждають від пожежі, що сталася в будівлі, будьте впевнені - їх неодмінно заллють водою пожежники, що приїдуть гасити пожежу.

В цілому ж, можна виділити кілька основних групп зловмисників: легальні користувачі системи, адміністративний IT-персонал, зовнішні зловмисники.

Спектр можливих злодіянь легальних користувачів досить широкий - від скріпок в апаратних частинах системи до умисної крадіжки інформації з корисливою метою. Можлива реалізація погроз в різних класах: загрози конфіденційності, загрози цілісності.

Користувач системи - це потенційний зловмисник, він може свідомо чи несвідомо порушити конфіденційність інформації.

Особлива група - це адміністративний IT-персонал або персонал служби IT-безпеки. Ця група, як правило, має необмежені повноваження і доступ до сховищ даних, тому до неї треба поставитися з особливою увагою. Вони не тільки мають великі повноваження, але і найбільш кваліфіковані в питаннях безпеки та інформаційних можливостей. Не так важливий мотив цих злочинів,

чи був це корисливий умисел або помилка, від якої ніхто не застрахований, результат один - інформація або загубилася, або набула розголосу. Згідно з численними дослідженнями, від 70 до 80% втрат від злочинів припадають на атаки зсередини.

Набір зовнішніх зловмисників суто індивідуальний. Це можуть бути і конкуренти, і партнери, і навіть клієнти.

Також можна зазначити, що останнім часом все більше помітне відхилення понять в області захисту даних: кажучи про інформаційну безпеку, багато, в першу чергу, мають на увазі захист від вірусів і хакерів. Але якщо попросити фахівців з безпеки розповісти про те, що їх хвилює, з'ясується, що найбільшу стурбованість викликають дії "інсайдерів" (співробітників компанії). Це показали і щорічний звіт ФБР Computer Crime and Security Survey, і Global Information Security Survey компанії Ernst & Young.

Так, за даними цих досліджень, збиток від необережних і неправомірних дій співробітників в кілька разів перевищує обсяг завданої шкоди від дій вірусів і хакерських атак. І це незважаючи на те, що, згідно зі звітом Computer Crime and Security Survey, кількість інцидентів з вини зовнішніх і внутрішніх порушників приблизно однакова.

Цей результат цілком закономірний. Хоча зовнішніх зловмисників дійсно значно більше, але, по-перше, вони менше мотивовані. Відкинувши мале число найманих професіоналів, ми отримаємо величезну масу школярів і студентів, які просто з цікавості пробують викачані утиліти, не переслідуючи якихось певних цілей і часом навіть не знаючи, що робити з отриманою інформацією. По-друге, їм протистоять потужні і зрілі технології периметрового захисту, тобто зовнішньому зловмисникові потрібна велика кваліфікація, щоб подолати всі ці бар'єри.

У внутрішнього порушника, особливо якщо його дії свідомі, а не є помилкою, стимулів може бути більше: від банальної образи до матеріальної вигоди в разі підкупу з боку конкурентів. А можливостей - не в приклад більше. Він вже є легальним користувачем мережі, має доступ в тому числі і до

конфіденційних ресурсів організації, може користуватися корпоративними додатками і робочою в них даними на законних підставах.

Будувати систему захисту від зовнішнього ворога набагато простіше. Це добре відомий і вже вторований шлях. Будь-хто з нас готовий почати перераховувати необхідні засоби захисту. Крім того, займаючись побудовою цього рубежу оборони, ми не впливаємо на працездатність нашої інформаційної системи. Всі бізнес-додатки працюють нормально, ціна помилки адміністрування - за великим рахунком, лише короткочасна відсутність доступу в Інтернет.

Захист від внутрішнього ворога складніше і вимагає великих зусиль. Вона складається з забезпечення безпеки самих додатків і грамотного адміністрування, яке перш за все має на увазі під собою наявність чітких привілеїв співробітників компанії на доступ до ресурсів інформаційної системи (в сформульованому вигляді - це політика безпеки).

Дані привілеї повинні бути достатні для забезпечення нормальної роботи і в той же час мінімальні з точки зору доступу і можливості маніпулювання інформацією.

І часто при появі такого завдання, проблем бачиться більше, ніж рішень.

Перераховувати їх можна довго, проблеми чіпляються один за одного. Наприклад, незахищеність ряду додатків змушує нас використовувати додаткові засоби захисту. Однак ці кошти потрібно не тільки придбати і правильно впровадити, але і супроводжувати. І якщо з процесом впровадження зазвичай проблем не виникає (справляються або штатні фахівці, або найняті консалтингові компанії), проблеми виникають потім, в процесі адміністрування системи. Адже управління засобами захисту здійснюється найчастіше окремо від вже використовуваних в компанії, в тому числі і штатних механізмів. А це означає, що рано чи пізно (в залежності від масштабу інформаційної системи) настає момент, коли налаштування системи захисту і налаштування штатних механізмів починають розходитися.

Розбіжність відбувається ще й тому, що відсутні процедури, які регламентують внесення змін до інформаційної системи і в настройки механізмів безпеки. А внести зміни в реальні настройки системи набагато простіше і швидше, ніж оформити їх. Та й набрати номер адміністратора або забігти до нього по шляху простіше, ніж написати заявку. В результаті - в заданий момент часу практично неможливо відтворити реальну картину того, що відбувається, неможливо відповісти на питання: "Чому до певного ресурсу мають доступ ці користувачі та групи користувачів?". Втрачається історія всіх вироблених змін, і вже не можна визначити - правильно чи неправильно сконфігуровані, нехай навіть найдосконаліші, механізми захисту.

Ціна помилки за неправильне адміністрування вимірюється або наданням користувачеві необґрунтовано великих компетенцій (а так само - створенням величезної уразливості в інформаційній системі), або обмеженням необхідного йому в якийсь момент доступу (при цьому, можливо, зривається виконання завдань організації).

До речі, серед цих варіантів не може бути вибраний кращий.

Існують два шляхи вирішення зазначених проблем: впровадження системи централізованого управління та впровадження системи обліку налаштувань і змін в настройках інформаційної системи.

Але універсальна консоль управління всіма додатками не рятує, оскільки не дає відповідь на питання - на якій підставі, хто і як повинен приймати рішення про те, які зміни потрібні.

Для упорядкування діяльності з адміністрування на підприємстві рано чи пізно виробляються регламенти та інші документи, що описують правила роботи і взаємодії всіх суб'єктів інформаційної системи.

Але вирішити цю проблему тільки організаційними методами не вдається. Виною всьому нестача і недостатня кваліфікація адміністраторів, перевантаженість фахівців і, найголовніше - відсутність механізмів перевірки фактичного стану справ. Все це призводить до того, що навіть при наявності

деякої формальної системи управління контроль над інформаційною системою і питаннями безпеки даних в ній все одно втрачається.

До речі, часом просте збільшення штату IT-підрозділу і підрозділу інформаційної безпеки лише поглиблюють проблеми. У цих структурах, в свою чергу, з'являються підрозділи, що спеціалізуються на окремих підсистемах, взаємодія структур порушується ще більше.

Усвідомлюючи всю складність вирішення завдання, а так само відсутність інструментів, фахівці з інформаційної безпеки часто зволікають з вирішенням цієї проблеми.

За великим рахунком, для управління будь-якої складної системою необхідно створити жорсткий, але простий регламент обслуговування системи і забезпечити контроль за тим, щоб настройки системи змінювалися відповідно до цього регламенту.

Стосовно до забезпечення безпеки інформаційної системи (ІС) це можна представити в такий спосіб:

1 Мати в наявності документ, в якому повинно бути чітко описано, хто і на якій підставі повинен мати доступ до ресурсів інформаційної системи.

2 Мати єдину точку взаємодії співробітників організації з інформаційною системою, через яку вони зможуть формулювати свої побажання на надання доступу до тих чи інших ресурсів ІС.

3 Мати інструменти контролю правильності налаштувань ІС.

Розробками такого роду останнім часом займається кілька великих корпорацій. Свої рішення пропонують Oracle і IBM, "Інформзахист", які мають свою систему комплексного управління безпекою (КУБ).

Особливість пропонованих рішень в тому, що в них з'єднуються не працюють окремо технічний і організаційний підходи до управління безпекою.

При впровадженні таких систем передбачається, що організація вже має сформульовану політику безпеки. Ця політика разом з інформацією про ІС служить надалі фундаментом системи управління.

Для опису інформаційної системи зазвичай необхідно знати наступне.

– Перелік інформаційних ресурсів. Під ресурсом можуть розумітися конкретні сервери і папки на них, експлуатовані додатки, обладнання та навіть сегменти мережі.

– Відповідальний за безпеку цих ресурсів. Це можуть бути власники ресурсів, голови підрозділів, куратори з боку служби безпеки та інші.

– Відповідальний за адміністрування цих ресурсів.

– Як ресурси інформаційної системи взаємопов'язані між собою. Часом для нормальної роботи програми необхідний комплекс налаштувань - від налаштувань самого додатка до комутаційного обладнання. Адже навіть якщо ми виконаємо всі настройки, але забудемо прописати дозволяє правило на внутрішньому межсетевом екрані, рішення всієї задачі буде зірвано.

– Штатна структура компанії. Який доступ і до яких ресурсів має співробітник, що займає на певну посаду.

На базі отриманої інформації система управління вибудовує ідеальну модель ІС. Цей момент можна вважати стартовим в роботі системи управління безпекою.

Відтепер усі спілкування з питань змін у налаштуваннях інформаційної системи починає відбуватися через спеціалізовану систему документообігу, що входить до складу системи управління безпекою.

До речі, від зарубіжних аналогів вітчизняну систему КУБ відрізняє спеціальний транслятор, який дозволяє долати мовний бар'єр і надає можливість кожному працювати зі зрозумілими йому термінами: менеджменту компанії - з термінами "співробітник", "посада", ІТ-фахівцям - з термінами типу "обліковий запис "," права доступу "і т. п.

Заявка на зміну доступу, складена в системі управління безпекою, буде перевірена на несуперечливість вимогам політики безпеки, узгоджена з власниками ресурсів і спрямована на виконання адміністраторам.

Виявляти невідповідність моделі ІС і її поточного стану системи управління безпекою дозволяють агенти-сенсори. Такі агенти регулярно

стежать за всіма пов'язаними з безпекою ІС настройками операційних систем, додатків, засобів захисту, мережевого обладнання.

Під невідповідністю системи управління безпекою ІС підприємства слід розуміти або невиконані адміністратором необхідних дій по адмініструванню інформаційної системи, які дії, вчинені ним в обхід прийнятого і затвердженого в організації порядку. Наприклад, надання зайвих повноважень якого-небудь користувачеві або неправомірне обмеження користувача в правах.

Інформація про невідповідності тут же надходить в служби безпеки і в службу ІТ. Адже кожне з них пов'язане з тим, що хтось із співробітників або набуває права на доступ до ресурсів ІС, або втрачає їх. Це означає, що він може отримати зайву інформацію або позбутися доступу до необхідних йому відомостей. А це, як ми вже відзначали, рівнозначно неприпустимо, оскільки таїть загрозу безпеці або ж призводить до зриву виконання бізнес-завдань.

Наявність в системі документообігу механізму архівації заявок на зміни доступу до інформаційної системи дозволить в будь-який момент зрозуміти, хто має доступ до ресурсів інформаційної системи і хто запитував надання цього доступу.

Використання описаного підходу до управління інформаційною безпекою - це серйозні зміни в звичному ритмі роботи інформаційної системи.

Але витрачені зусилля з лишком окупляться. Вигоди від впровадження систем управління безпекою очевидні. І перш за все це підвищення захищеності ІС, оскільки відтепер всі вироблені зміни налаштувань будуть контролюватися і проводитися в точній відповідності з політикою інформаційної безпеки організації. Додатковим бонусом буде скорочення витрат на супутній управління документообіг.

Крім того, після впровадження подібної системи управління забезпечення інформаційної безпеки перестає бути долею, відповідальністю і обов'язком тільки вузьких фахівців. В управлінні інформаційною системою починає дійсно активно брати участь менеджмент організації: адже саме вони тепер формують вимоги до налаштувань за допомогою механізму заявок.

Наприклад, попередній аналіз основних принципів побудови СЕД з метою виявлення особливостей побудови системи захисту інформації від несанкціонованого доступу в СЕД показав, що при її побудові необхідно враховувати наступні загрози неведені в таблиці 2.5:

Таблиця 2.5 – Перелік основних загроз та особливості і моделі захисту

Опис загрози	Особливості і моделі захисту
Протиправні дії адміністратора системи.	Один системний адміністратор не повинна мати всі адміністраторськими повноваженнями (різні адміністраторські повноваження повинні бути делеговані різним системним адміністраторам). Системним адміністраторам не надається права читання документів, не призначених для них. Системні адміністратори можуть тільки видаляти такі документи.
Необережні дії адміністратора системи.	Протоколювання дій адміністратора. Організаційні заходи.
Запуск троянської програми на сервері і передача з її допомогою даних на комп'ютер зловмисника.	Закриття з'єднання з мережею доступу до ресурсів комп'ютера, що не дозволить перенести троянську програму на сервер. Замкнута програмне середовище операційної системи, що не дозволяє встановлювати нові програмні компоненти без підтвердження адміністративних повноважень. Адміністративні заходи проти зловмисників всередині організації.
Запуск троянської програми на комп'ютері-клієнті і передача з її допомогою даних на комп'ютер зловмисника.	Замкнута програмне середовище операційної системи. Адміністративні заходи проти зловмисників всередині організації. Технічні обмеження на мережеві операції, наприклад, локальний міжмережевий екран.
Модифікація вихідного коду серверного та клієнтського ПЗ розробниками.	Збірка в організації Замовника.
Модифікація виконуваного коду на сервері.	Замкнуте програмне середовище операційної системи.
Модифікація виконуваного коду на комп'ютері-клієнті.	Замкнуте програмне середовище операційної системи.
Доступ до даних на сервері в	Розміщення сервера в окремому приміщенні, що

обхід системи, безпосередньо з інтерфейсу сервера.	охороняється.
Доступ до даних на сервері в обхід системи по мережі через мережеві диски.	Закриття з'єднання з мережею доступу до ресурсів комп'ютера.
Доступ до даних на сервері в обхід системи по протоколу сервера системи (мається на увазі підключення до сервера спеціальною програмою, а не АРМ клієнта).	Система розмежування доступу на сервері (на рівні серверної БД). Мережева ідентифікація и аутентіфікація.
Доступ до даних на сервері з мережних протоколах використовуваного серверного ПЗ без підключення до сервера системи.	Дозвіл мережевого доступу тільки по використовуваному порту. Заборона на мережеві підключення засобами СУБД.
Перехоплення мережевого трафіку і його аналіз з метою несанкціонованого доступу.	Шифрування трафіку засобами операційної системи або додатковими засобами.
Доступ сторонніх до клієнтського комп'ютера і читання даних з локального кеша в разі, коли комп'ютер не в системі.	Адміністративні заходи: заборона залишати робоче місце без блокування робочої станції (в термінології NT), закріплення комп'ютерів за користувачами. Технічні заходи: чистка тимчасових директорій при виході з програми.
Доступ сторонніх до клієнтського комп'ютера і робота з даними в разі, коли комп'ютер в системі.	Адміністративні заходи: заборона залишати робоче місце без блокування робочої станції (в термінології NT).
Перезавантаження сервера з метою виклику відмови в обслуговуванні.	Обмежити доступ до сервера з метою перевантаження. Дана загроза не веде до несанкціонованого доступу.
Перехоплення мережевого трафіку і підміна користувача, що працює на клієнтському комп'ютері.	Шифрування трафіку ключами, створюваними тільки на час сеансу. Підписування кожного переданого пакета ЕЦП працюючого користувача.
Перехоплення мережевого трафіку і підміна сервера.	Шифрування трафіку ключами, створюваними тільки на час сеансу. Підписування кожного переданого пакета ЕЦП працюючого користувача.
Вхід в систему користувача з правами, що перевищують його власні.	Ідентифікація и аутентифікація засобами операційної системи, або за допомогою додаткових засобів. Збереження в таємниці системних імен та паролів.

	Використання технічних засобів ідентифікації и аутентифікації (апаратні ключі). Обов'язкова наявність у адміністраторів системи окремих системних імен та паролів для адміністративних дій та звичайної роботи.
Робота з даними, що не відповідають рівню доступу користувача.	Реалізація мандатного контролю доступу на сервері.

Зазвичай, передбачається робота системи тільки в локальних закритих мережах, так що комп'ютер зловмисника може бути тільки в локальній мережі.

Протиправні дії адміністратора системи можуть бути одними з найважчих і руйнівних за своїми наслідками. У зв'язку з цим необхідно приділяти підвищену увагу заходам щодо захисту від таких дій.

Крім погроз, перерахованих в таблиці, необхідно відзначити проблеми, пов'язані з Web-доступом - відкритість мереж і «тонкість» клієнта, що значно обмежує можливості шифрування і аутентифікації (зокрема - непридатність (або мала застосовність) апаратних засобів аутентифікації). Внаслідок цього, працювати з конфіденційною інформацією через Web рекомендується тільки в разі крайньої необхідності.

2.3 Захист в системах електронного документообігу

Не зупиняючись на засобах захисту комп'ютерних мереж, мережевих пристроїв і операційних систем з їх файловими система, що представляють окрему тему, розглянемо більш докладно засоби, інтегровані в самі СЕД.

Будь-яка СЕД, що претендує на звання «захищена», повинна як мінімум передбачити механізм захисту від основних її загроз: забезпечення збереження документів, забезпечення безпечного доступу, забезпечення достовірності документів та протоколювання дії користувачів.

СЕД повинна забезпечити збереження документів від втрати і псування і мати можливість їх швидкого відновлення. Статистика невблаганна, в 45% випадків втрати важливої інформації припадають на фізичні причини (відмова апаратури, стихійні лиха і т.п.), 35% обумовлені помилками користувачів і

менш 20% - дією шкідливих програм і зловмисників. Опитування аналітичної компанії Deloitte Touche, показало, що більше половини всіх компаній стикалися з втратою даних протягом останніх 12 місяців. 33% таких втрат призвели до серйозного фінансового збитку. Представники половини компаній, які пережили втрату даних, заявляють, що причиною інциденту став саботаж або недбале ставлення до правил інформаційної політики компанії, і тільки 20% респондентів повідомили, що інтелектуальна власність їх компаній захищена належним чином. Всього 4% опитаних заявило, що їх роботодавці звертають належну увагу на інформаційну політику компанії. Що стосується СЕД, то в ефективності її захисту впевнене тільки 24% учасників опитування.

Так, наприклад, СЕД, в основі своїй використовують бази даних Microsoft SQL Server або Oracle, вважають за краще користуватися засобами резервного копіювання від розробника СУБД (в даному випадку Microsoft або Oracle). Інші ж системи мають власні підсистеми резервного копіювання, розроблені безпосередньо виробником СЕД. Сюди слід також віднести можливість відновлення не тільки даних, але і самої системи в разі її пошкодження.

2.3.1 Забезпечення безпечного доступу

Саме забезпечення безпечного доступу зазвичай все розуміють під безпекою СЕД, ніж часто обмежують поняття безпеки систем. Безпечний доступ до даних усередині СЕД забезпечується аутентифікацією і розмежуванням прав користувача.

Для спрощення будемо називати процеси встановлення особи користувача і процеси підтвердження легітимності користувача на ту чи іншу дію або інформацію одним терміном - аутентифікацією, розуміючи під ним весь комплекс заходів, що проводяться як на вході користувача в систему, так і постійно протягом його подальшої роботи.

Тут необхідно загострити увагу на методах аутентифікації. Найпоширеніший з них, звичайно, парольний. Основні проблеми, які сильно знижують надійність даного способу - це людський фактор. Навіть якщо змусити користувача використовувати правильно згенерований пароль, в

більшості випадків його можна легко знайти на папірці в столі або під клавіатурою, а особливо «талановиті» зазвичай прикріплюють її прямо на монітор.

Найстаріший з відомих світу способів аутентифікації - майновий. Свого часу повноваження власника скрині підтверджувалися ключами, сьогодні прогрес пішов далеко вперед, і повноваження користувача підтверджуються спеціальним носієм інформації. Існує безліч рішень для майнової аутентифікації користувача: це всілякі USB-ключі, смарт-карти, «таблетки» магнітні картки, в тому числі використовуються і дискети, і CD. Тут також не виключений людський фактор, але зловмисникові необхідно також отримати сам ключ і дізнатися PIN-код.

Максимально надійний для проведення ідентифікації та подальшої аутентифікації спосіб - біометричний, при якому користувач ідентифікується за своїми біометричними даними (це може бути відбиток пальця, сканування сітківки ока, голос). Однак в цьому випадку вартість рішення вище, а сучасні біометричні технології ще не настільки досконалі, щоб уникнути помилкових спрацьовувань або відмов.

Ще один важливий параметр аутентифікації - кількість чинників, що враховуються. Процес аутентифікації може бути однофакторний, двофакторний та т.д. Також можливе комбінування різних методів: парольного, майнового та біометричного. Так, наприклад, аутентифікація може проходити за допомогою пароля і відбитка пальця.

2.3.2 Розмежування прав користувача

У будь-якій системі обов'язково повинно бути передбачено розмежування прав користувача - і чим гнучкіше і детальніше, тим краще. Нехай буде потрібно більше часу на налаштування, але в підсумку ми отримаємо більш захищену систему. Розмежування прав всередині системи технічно влаштовують по-різному: це може бути повністю своя підсистема, створена розробниками СЕД, або підсистема безпеки СУБД, яку використовує СЕД. Іноді їх розробки комбінують використовуючи свої розробки і підсистеми

СУБД. Така комбінація краще, вона дозволяє закрити мінуси підсистем безпеки СУБД, які також мають «дірки».

2.3.3 Конфіденційність

Величезною перевагою для конфіденційності інформації мають криптографічні методи захисту даних. Їх застосування дозволять не порушити конфіденційність документа навіть в разі його попадання в руки стороннього особи. Не варто забувати, що будь-який криптографічний алгоритм має таку властивість як криптостійкість, тобто і його захисту є межа. Немає шифрів, які не можна було б зламати - це питання тільки часу і коштів. Ті алгоритми, які ще кілька років тому вважалися надійними, сьогодні вже успішно демонстративно зламуються. Тому для збереження конфіденційності переконайтеся, що за час, витрачений на злом зашифрованою інформацією, вона безнадійно застаріє або кошти, витрачені на її злом, перевершать вартість самої інформації.

Крім того, не варто забувати про організаційні заходи захисту. Якою би ефективною криптографія не була, ніщо не завадить третій особі прочитати документ, наприклад, стоячи за плечем людини, який має до нього доступ. Або розшифрувати інформацію, скориставшись ключем який валяється в столі співробітника.

2.3.4 Забезпечення достовірності документів

Сьогодні основним і практично єдиним пропонованим на ринку рішенням для забезпечення достовірності документа є електронно-цифровий підпис (ЕЦП). Основний принцип роботи ЕЦП заснований на технологіях шифрування з асиметричним ключем. Тобто ключі для шифрування і розшифровки даних різні. Є «закритий» ключ, який дозволяє зашифрувати інформацію, і є «відкритий» ключ, за допомогою якого можна цю інформацію розшифрувати, але з його допомогою неможливо «зашифрувати» цю інформацію. Таким чином, власник «підпису» повинен володіти «закритим» ключем і не допускати його передачу іншим особам, а «відкритий» ключ може поширюватися

публічно для перевірки автентичності підпису, отриманого за допомогою «закритого» ключа.

Для наочності ЕЦП можна уявити як дані, отримані в результаті спеціального криптографічного перетворення тексту електронного документа. Воно здійснюється за допомогою так званого «закритого ключа» - унікальної послідовності символів, відомої тільки відправнику електронного документа. Ці «дані» передаються разом з текстом електронного документа його одержувачу, який може перевірити ЕЦП, використовуючи так званий «відкритий ключ» відправника - також унікальну, але загальнодоступну послідовність символів, однозначно пов'язану з «закритим ключем» відправника. Успішна перевірка ЕЦП показує, що електронний документ підписаний саме тим, від кого він виходить, і що він не був модифікований після накладання ЕЦП.

Таким чином, підписати електронний документ з використанням ЕЦП може тільки власник «закритого ключа», а перевірити наявність ЕЦП - будь-який учасник електронного документообігу, який отримав «відкритий ключ», відповідний «закритому ключу» відправника. Підтвердження належності «відкритих ключів» конкретним особам здійснює засвідчує центр - спеціальна організація або сторона, якій довіряють всі учасники інформаційного обміну. Звернення в засвідчують центри дозволяє кожному учаснику переконатися, що наявні у нього копії «відкритих ключів», які належать іншим учасникам (для перевірки їх ЕЦП), дійсно належать цим учасникам.

Більшість виробників СЕД вже мають вбудовані в свої системи, власноруч розроблені або партнерські кошти для використання ЕЦП, як, наприклад, в системах Megapolis. Документообіг, АСКОД та OPTIMA-WorkFlow і el-Dok за умови використання додаткового програмного забезпечення.

2.3.5 Протоколювання дій користувачів

Протоколювання дій користувачів – важливий пункт в захисті електронного документообігу. Його правильна реалізація в системі дозволить відстежити всі неправомірні дії і знайти винуватця, а при оперативному

втручанні навіть зупинити спробу неправомірних або завдаючих шкоди дій. Така можливість обов'язково має бути присутня в самій СЕД. Крім того, додатково можна скористатися рішеннями сторонніх розробників і партнерів, чиї продукти інтегровані з СЕД. Говорячи про партнерські рішеннях, перш за все мова йде про СУБД і сховищах даних, будь-який подібний продукт великих розробників, таких як Microsoft або Oracle, наділений цими засобами. Також не варто забувати про можливості операційних систем з протоколювання дій користувачів і рішеннях сторонніх розробників в цій області.

Основне проблемне місце при організації захисту СЕД, як відзначають більшість розробників систем захисту, це не технічні засоби, а лояльність користувачів. Як тільки документ потрапляє до користувача, конфіденційність цього документа по відношенню до користувача вже порушена. Технічними заходами в принципі неможливо запобігти витоку документа через цього користувача. Він знайде безліч способів скопіювати інформацію, від збереження його на зовнішній носій до банального фотографування документа за допомогою камери, вбудованої в стільниковий телефон. Основні засоби захисту тут - це організаційні заходи щодо обмеження доступу до конфіденційних документів і роботи з самим користувачем. Він повинен розуміти ступінь своєї відповідальності, яку несе перед організацією і законом.

Основна відмінність в системах захисту - це алгоритми, що застосовуються в шифруванні і ЕЦП. На жаль, поки питання захищеності систем документообігу тільки починає цікавити кінцевих користувачів і розробників відповідно. Практично всі системи мають пральний аутентифікацией і розмежуванням доступу користувачів. Деякі з них мають також можливості інтеграції з Windows-аутентифікації, що дає можливість користуватися додатковими засобами аутентифікації, підтримуваними Windows. Не всі з перерахованих рішень мають свою криптографічний захист - шифрування документів або ЕЦП. У ряді продуктів це можливо тільки за допомогою додаткових коштів сторонніх розробників.

Підхід до захисту електронного документообігу повинен бути комплексним. Необхідно тверезо оцінювати можливі загрози і ризики СЕД і величину можливих втрат від реалізованих загроз. Як вже говорилося, захисту СЕД не зводиться тільки лише до захисту документів і розмежування доступу до них. Залишаються питання захисту апаратних засобів системи, персональних комп'ютерів, принтерів і інших пристроїв; захисту мережного середовища, в якому функціонує система, захист каналів передачі даних і мережевого устаткування, можливе виділення СЕД в особливий сегмент мережі. Комплекс організаційних заходів грають роль на кожному рівні захисту, але їм, на жаль, часто нехтують. Але ж тут і інструктаж, і підготовка звичайного персоналу до роботи з конфіденційною інформацією. Погана організація може звести до нуля всі технічні заходи, які-б досконалі вони не були.

2.4 Організація СУІБ в системах електронного документообігу

Проаналізована нормативно-правова база в Україні не дає чітких інструкцій щодо управління інформаційною безпекою в СЕД, а підхід до захисту інформації в цих системах пропонує організаціям створити службу захисту інформації, використання КСЗІ і електронного цифрового підпису.

Для організації на підприємстві системи управління інформаційною безпекою саме в системах електронного документообігу, можна за основу взяти підхід створення СУІБ згідно з рекомендаціями міжнародного стандарту ISO/IEC 27001:2013.

Цей стандарт приймає модель «Плануй-Виконуй-Перевіряй-Дій» («Plan-Do-Check-Act»), надалі ПВПД (PDCA), яку застосовують для структуризації всіх процесів СУІБ. Рисунок 2.1 ілюструє, яким чином СУІБ, використовуючи як вхідні дані вимоги інформаційної безпеки та очікування зацікавлених сторін, за допомогою необхідних дій і процесів виробляє вихідні дані інформаційної безпеки, що відповідають цим вимогам та очікуванням.

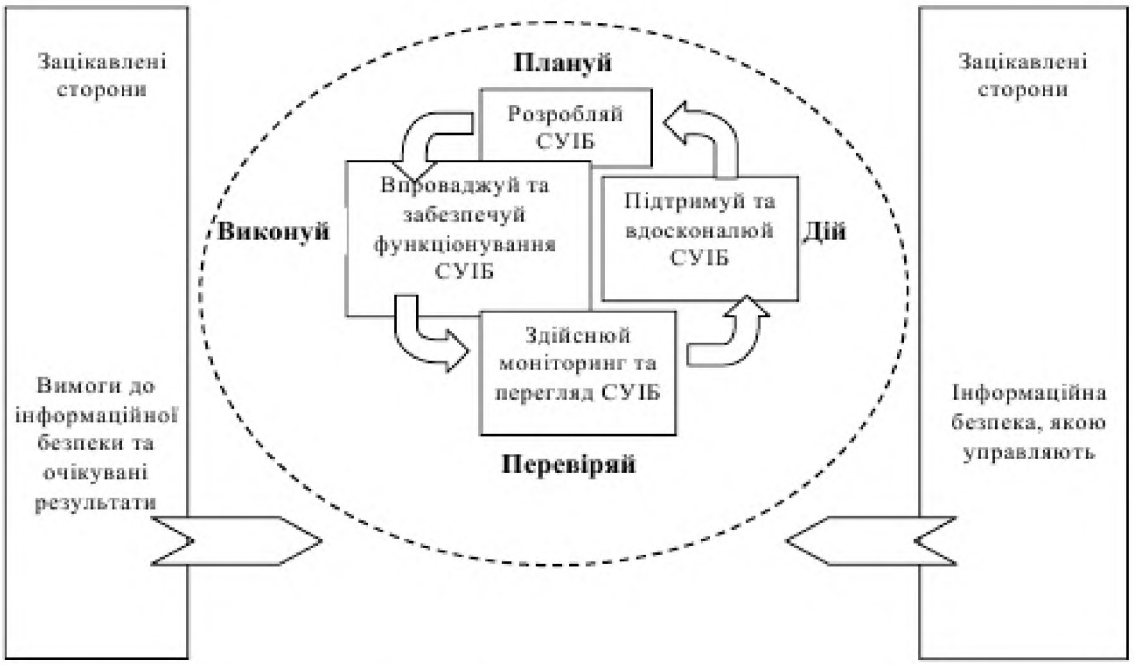

Рисунок 2.1 – модель ПВПД (PDCA), застосована до процесів СУІБ

Організація повинна розробляти, впроваджувати, забезпечувати функціонування, здійснювати моніторинг, переглядати, підтримувати та вдосконалювати задокументовану СУІБ в контексті загальної бізнес-діяльності організації і ризиків, з якими вона стикається.

Процес, використаний для цього стандарту, базується на моделі ПВПД (PDCA), яку наведено на рисунку 2.1.

Відповідно зі стандатом можна встановити наступні вимоги щодо СУІБ в СЕД.

Політика інформаційної безпеки щодо використання СЕД повинна бути затверджена керівництвом, видана і доведена до відома всіх співробітників організації, а також сторонніх організацій, які працюють з СЕД.

Політика інформаційної безпеки організації щодо використання СЕД повинна бути піддана аналізу і перегляду через задані проміжки часу або при появі істотних змін характеристик цілей безпеки.

Керівництво організації повинно постійно підтримувати заданий рівень інформаційної безпеки щодо використання СЕД шляхом впровадження системи

менеджменту, а також шляхом розподілу обов'язків і відповідальності персоналу за її забезпечення.

Дії по забезпеченню інформаційної безпеки в СЕД повинні координуватися представниками різних підрозділів організації, що мають відповідні функції та посадові обов'язки.

Обов'язки персоналу щодо забезпечення інформаційної безпеки пов’язаної з використанням СЕД повинні бути чітко визначені.

Керівництво організації повинно визначати умови конфіденційності або виробляти угоди про нерозголошення інформації відповідно до цілей захисту інформації при роботі в СЕД і регулярно їх переглядати.

Порядок організації та управління інформаційною безпекою в СЕД та її реалізація (наприклад, зміна цілей і заходів управління, політики, процесів і процедур забезпечення інформаційної безпеки) повинні бути піддані незалежній перевірці (аудиту) через певні проміжки часу або при появі істотних змін в способах реалізації заходів безпеки.

Перед наданням доступу стороннім організаціям до інформації та засобів її обробки в СЕД в процесі діяльності організації необхідно визначати можливі ризики для інформації і засобів її обробки та реалізовувати відповідні їм заходи безпеки.

Угоди зі сторонніми організаціями, які працюють з СЕД організації повинні містити всі вимоги безпеки, що включають в себе правила доступу до процесів обробки, передачі інформації або до управління інформацією або засобами обробки інформації організації, а також і в разі придбання додаткових програмних продуктів або організації сервісного обслуговування засобів обробки інформації.

Опис усіх важливих активів що обробляються в СЕД організації повинна бути складена і актуалізована.

Правила безпечного використання інформації та активів в СЕД, повинні бути визначені, задокументовані та впроваджені.

Інформація в СЕД повинна бути класифікована виходячи з правових вимог, її конфіденційності, а також цінності і критичності для організації.

Відповідно до прийнятої в організації системою класифікації повинна бути розроблена і реалізована сукупність процедур маркування та обробки інформації в СЕД.

Перевірка всіх кандидатів на постійну роботу, підрядників і користувачів третьої сторони повинна бути проведена відповідно до законів, інструкціями та правилами етики, з урахуванням вимог бізнесу, характеру інформації, до якої буде здійснено їх доступ, і передбачуваних ризиків.

Співробітники, підрядники та користувачі третьої сторони повинні узгодити і підписати умови свого трудового договору, в якому встановлені їх відповідальність і відповідальність організації щодо інформаційної безпеки в СЕД.

Керівництво організації повинно вимагати, щоб співробітники, підрядники та користувачі третьої сторони були ознайомлені з правилами і процедурами забезпечення заходів безпеки при роботі з СЕД відповідно до встановлених вимог.

Всі співробітники організації і, при необхідності, підрядники та користувачі сторонніх організацій повинні проходити відповідне навчання і перепідготовку з метою регулярного отримання інформації про нові вимоги правил і процедур організації безпеки при роботі з СЕД, необхідних для виконання ними посадових функцій.

До співробітників, які вчинили порушення вимог безпеки при роботі в СЕД, повинна бути застосована дисциплінарна практика, встановлена в організації.

Права доступу до інформації та СЕД співробітників, підрядників і користувачів третьої сторони повинні бути анульовані або уточнені після закінчення дії трудового договору (звільнення).

Для захисту зон, де є фізичний доступ СЕД, повинні бути використані периметри охоронюваних зон (бар'єри, такі як стіни, прохідні, обладнані

засобами контролю входу по ідентифікаційним карткам, або, де передбачений, контроль співробітника реєстраційної стійки).

Місця доступу, такі як зони прийому, відвантаження матеріальних цінностей та інші місця, де неавторизовані особи можуть проникнути в приміщення, повинні бути під контролем і, по можливості, повинні бути ізольовані від СЕД, щоб уникнути несанкціонованого доступу.

Устаткування СЕД має бути розміщено і захищено так, щоб зменшити ризики від впливу навколишнього середовища і можливості несанкціонованого доступу.

Устаткування СЕД необхідно захищати від перебоїв в подачі електроенергії і інших збоїв, пов'язаних з відмовами в забезпеченні допоміжних послуг.

Силові та телекомунікаційні кабельні мережі, по яких передаються дані або підтримуються інформаційні послуги, необхідно захищати від перехоплення інформації або пошкодження.

Має проводитися належне регулярне технічне обслуговування обладнання для забезпечення його безперервної працездатності і збереження.

Всі компоненти обладнання, які містять носії даних, повинні бути перевірені з метою упевнитися в тому, що будь-які конфіденційні дані і ліцензійне програмне забезпечення було видалено або скопійовано безпечним чином до їх утилізації (списання).

Устаткування, інформацію або програмне забезпечення допускається виносити з приміщення організації тільки на підставі відповідного дозволу.

Операційні процедури повинні документуватися, підтримуватися і бути доступними для всіх авторизованих користувачів.

Зміни в конфігураціях СЕД повинні бути контрольованими.

Обов'язки та сфери відповідальності повинні бути розмежовані з метою зниження можливостей несанкціонованої або ненавмисної модифікації, або нецільового використання активів в СЕД організації.

Засоби розробки, тестування та експлуатації повинні бути розмежовані з метою зниження ризику несанкціонованого доступу або зміни операційної системи.

Повинна бути забезпечена впевненість в тому, що заходи управління інформаційною безпекою в СЕД, які підтверджують договір про надання послуг сторонньої організації, реалізовані, функціонують і підтримуються сторонньою організацією.

Необхідно регулярно проводити моніторинг, аудит і аналіз послуг, звітів та актів, які забезпечуються сторонньою організацією.

Зміни при наданні послуг із забезпечення безпеки в СЕД, включаючи впровадження і вдосконалення існуючих вимог, процедур і заходів забезпечення інформаційної безпеки в СЕД, повинні бути керованими з урахуванням оцінки критичності систем і процесів бізнесу, а також результатів переоцінки ризиків.

Необхідно здійснювати прогнозування, моніторинг і коригування потреби потужності системи для забезпечення необхідної її продуктивності.

Повинні бути визначені критерії прийняття нових і модернізованих інформаційних СЕД, нових версій програмного забезпечення, а також проведено тестування систем в процесі їх розробки та прийняття.

Повинні бути реалізовані заходи по виявленню, запобіганню проникненню і відновленню після впливу шкідливого коду, а також повинні бути встановлені процедури забезпечення відповідного оповіщення користувачів.

Там, де дозволено використання мобільного коду, конфігурація системи повинна забезпечувати впевненість у тому, що авторизований мобільний код функціонує відповідно до чітко визначеної політикою безпеки, а виконання операції з використанням неавторизованого мобільного коду буде попереджено.

Резервні копії інформації в СЕД повинні створюватися, перевірятися і тестуватися на регулярній основі відповідно до прийнятих вимог резервування.

Мережі повинні бути адекватно керованими і контрольованими з метою захисту від загроз і підтримки безпеки систем і додатків, що використовують мережу, включаючи інформацію, передану по мережах.

Заходи забезпечення безпеки, рівні обслуговування для всіх мережевих послуг і вимоги управління повинні бути визначені і включені в будь-який договір про онлайнових службах незалежно від того, чи надаються ці послуги своїми силами або сторонньою організацією.

Для управління знімними носіями інформації повинні існувати відповідні процедури.

Носії інформації, коли в них більше немає необхідності, повинні бути надійно і безпечно утилізовані за допомогою формалізованих процедур.

Для забезпечення захисту інформації від несанкціонованого розкриття або неправильного використання необхідно встановити процедури обробки та зберігання інформації.

Системна документація щодо СЕД повинна бути захищена від несанкціонованого доступу.

Повинні існувати формалізовані процедури, вимоги і заходи контролю, що забезпечують захист обміну інформацією при використанні зв'язку всіх типів.

Між організацією і сторонніми організаціями повинні бути укладені угоди щодо обміну інформацією та програмним забезпеченням.

Носії інформації повинні бути захищені від несанкціонованого доступу, неправильного використання або пошкодження під час їх транспортування за межами території організації.

Інформація, яка використовується в електронному обміні повідомленнями, повинна бути захищена належним чином.

Вимоги і процедури повинні бути розроблені і впроваджені для захисту інформації, пов'язаної з взаємодією систем бізнес-інформації.

Інформація, яка використовується в трансакціях в режимі реального часу (on-line), повинна бути захищена для запобігання неповній передачі,

неправильній маршрутизації, несанкціонованого зміни повідомлень, несанкціонованого розголошення, несанкціонованого копіювання або повторного відтворення повідомлень.

Інформація, яку надає через загальнодоступну систему, повинна бути захищена від несанкціонованої модифікації.

Повинні бути забезпечені ведення і зберігання протягом певного періоду часу журналів аудиту, які реєструють дії користувачів, позаштатні ситуації і події інформаційної безпеки, з метою допомоги в майбутніх розслідуваннях і проведенні моніторингу контролю доступу.

Повинні бути встановлені процедури, що дозволяють вести моніторинг і регулярний аналіз результатів моніторингу використання коштів обробки інформації.

Засоби реєстрації та інформація журналів реєстрації повинні бути захищені від втручання і несанкціонованого доступу.

Дії системного адміністратора та системного оператора повинні бути зареєстрованими.

Несправності СЕД повинні бути зареєстровані, проаналізовані і усунені.

Годинники всіх відповідних систем обробки інформації в межах організації або зони, що охороняється повинні бути синхронізовані з допомогою єдиного джерела точного часу.

Політика контролю доступу до СЕД повинна бути встановлена і задокументована з урахуванням потреб бізнесу і безпеки інформації.

Повинна бути встановлена формалізована процедура реєстрації та зняття з реєстрації користувачів СЕД для надання та скасування доступу до системи і послуг.

Надання і використання привілеїв має бути обмеженим і контрольованим.

Надання паролів має бути контрольованим за допомогою формалізованого процесу управління.

Керівництво повинно періодично здійснювати перегляд прав доступу користувачів, використовуючи формалізований процес. Користувачі повинні дотримуватися правил безпеки при виборі і використанні паролів.

Користувачі повинні забезпечувати відповідний захист обладнання, залишеного без нагляду.

Повинні бути прийняті правила «чистого екрану» для СЕД.

Користувачам слід надавати доступ тільки до тих послуг, по відношенню до яких вони спеціально були авторизовані.

Для контролю доступу віддалених користувачів повинні бути застосовані відповідні методи аутентифікації.

Автоматична ідентифікація обладнання повинна розглядатися як засіб аутентифікації з'єднань, здійснюваних з певних місць і з певним обладнанням.

Фізичний і логічний доступ до портів конфігурації і діагностики повинен бути контрольованим.

У мережах повинні бути застосовані принципи поділу груп інформаційних послуг, користувачів та інформаційних систем.

Підключення користувачів до спільно використовуваних мереж, особливо до тих, які виходять за територію організації, необхідно обмежувати відповідно до політики контролю доступу та вимогами бізнес-додатків.

Повинні бути впроваджені засоби управління і контролю маршрутизації в мережі з метою виключити порушення правил контролю доступу для бізнес-додатків, що викликаються сполуками і потоками інформації.

Контроль доступу до СЕД повинен бути забезпечений безпечною процедурою реєстрації.

Всі користувачі повинні мати унікальні ідентифікатори (ID) тільки для персонального використання, а для підтвердження заявленої особистості користувача повинні бути вибрані відповідні методи аутентифікації.

Системи управління паролями повинні бути інтерактивними і забезпечувати високу якість паролів.

Використання системних утиліт, які можуть подолати засоби контролю операційних систем і додатків, необхідно обмежувати і строго контролювати.

Необхідно забезпечити завершення сеансів зв'язку після певного періоду бездіяльності.

Обмеження часу з'єднання повинно бути використано для забезпечення додаткової безпеки.

Доступ до інформації і функцій прикладних систем користувачів і обслуговуючого персоналу повинен бути наданий тільки відповідно до певними політиками контролю доступу.

Системи, що обробляють важливу інформацію, повинні мати виділену (ізольовану) обчислювальну середу.

Необхідно мати в наявності формалізовану політику для захисту від ризиків при використанні переносних пристроїв.

Для роботи в дистанційному режимі необхідно розробити і реалізувати політику, оперативні плани і процедури.

У формулюваннях вимог бізнесу для нових інформаційних систем або вдосконалення існуючих повинні бути деталізовані вимоги безпеки.

Вхідні дані для додатків повинні бути піддані процедурі підтвердження з метою встановлення їх достовірності.

Для виявлення спотворень (помилок або навмисних дій) при обробці інформації в вимоги до функцій додатків повинні бути включені вимоги щодо виконання контрольних перевірок.

Повинні бути визначені вимоги для забезпечення автентичності та захисту цілісності повідомлень в додатках, а також реалізовані відповідні засоби контролю.

Дані, що виводяться з програми, необхідно піддавати перевірці на коректність, щоб забезпечити впевненість у тому, що обробка інформації виконана правильно.

Повинні бути розроблені та впроваджені правила використання криптографічних засобів захисту інформації.

Для реалізації організацією криптографічних методів захисту повинна бути використана система управління ключами.

Необхідно уникати модифікацій пакетів програм, а всі необхідні зміни повинні підлягати суворому контролю.

Можливості для витоку інформації повинні бути попереджені.

Необхідно отримувати своєчасну інформацію про технічні вразливості використовуваних СЕД, оцінювати небезпеку таких вразливостей і вживати відповідних заходів щодо усунення пов'язаного з ними ризику.

Про випадки порушення інформаційної безпеки слід повідомляти по відповідних каналах управління негайно, наскільки це можливо.

Всі співробітники, підрядники та користувачі сторонніх організацій, що користуються СЕД та послугами, повинні негайно повідомляти про будь-які помічені або можливі порушення безпеки в системах чи послугах.

Повинні бути встановлені відповідальність керівництва та процедури, що дозволяють забезпечити швидке, ефективне та послідовне реагування на інциденти інформаційної безпеки при роботі з СЕД.

Повинні бути визначені механізми, що дозволяють вести моніторинг і реєстрацію інцидентів інформаційної безпеки в СЕД за типами, обсягами і цінами.

На випадок, якщо інцидент інформаційної безпеки може привести до судового розгляду (цивільній або кримінальній) проти особи або організації, інформація повинна бути зібрана, збережена і представлена згідно з правилами оформлення доказів, викладених у відповідних документах.

Повинен бути розроблений і підтриманий керований процес забезпечення безперервності бізнесу в усій організації з урахуванням вимог інформаційної безпеки при роботі з СЕД, необхідних для забезпечення безперервності бізнесу організації.

Події, які можуть стати причиною переривання бізнес-процесів, повинні бути пов'язані з оцінками ймовірності і ступеня впливу таких переривань, а також з їх наслідками для інформаційної безпеки.

Повинні бути розроблені та впроваджені плани для підтримки або відновлення роботи і забезпечення доступності інформації на необхідному рівні та в потрібні терміни після переривання або відмови критичних бізнес-процесів.

Повинна бути створена єдина структура планів безперервності бізнесу, що дозволяє забезпечити несуперечність всіх планів для послідовного виконання всіх вимог до інформаційної безпеки і для розстановки пріоритетів при тестуванні і обслуговуванні.

Плани щодо забезпечення безперервності бізнесу при використанні СЕД повинні підлягати регулярному перегляду та оновленню з метою забезпечити їх актуальність і ефективність.

Все застосовні норми, встановлені законодавством і виконавчими органами влади, вимоги договірних зобов'язань і порядок їх виконання слід чітко визначити, документувати і підтримувати на актуальному рівні для СЕД організації.

Повинні бути впроваджені відповідні процедури для застосування законодавчих, регулюючих і контрактних вимог до використовуваних матеріалів з урахуванням прав на інтелектуальну власність, а також прав на використання програмних продуктів, які є предметом приватної власності.

Важливі облікові записи організації повинні бути захищені від втрати, руйнування і фальсифікації відповідно до вимог, встановлених законами, документами органів виконавчої влади, контрактами і вимогами бізнесу.

Захист даних і конфіденційність персональної інформації в СЕД повинні бути забезпечені відповідно до вимог законів, нормативних актів і, де це може бути застосовано, відповідно до положень контрактів.

Засоби криптографічного захисту повинні бути використані відповідно до законів, нормативними актами та відповідними угодами.

Керівники повинні забезпечити, щоб всі процедури безпеки в їх сфері відповідальності були виконані правильно і відповідали політикам і стандартам безпеки.

СЕД слід регулярно перевіряти на відповідність вимогам стандартів безпеки.

Вимоги і процедури аудиту, що включають в себе перевірки СЕД, необхідно ретельно планувати і погоджувати, щоб звести до мінімуму ризик переривання бізнес-процесів.

Доступ до інструментальних засобів аудиту СЕД необхідно захищати для запобігання будь-якій можливості їх неправильного використання або компрометації.

2.5 Правила забезпечення захисту інформації в інформаційно-телекомунікаційних системах де використовується СЕД

Захисту в системі підлягає наступна інформація, яка обробляється в СЕД:

- відкрита інформація;
- конфіденційна інформація;
- службова інформація;
- інша інформація, вимога щодо захисту якої встановлена законом.

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

Забезпечення захисту в системі таємної інформації, яка не становить державну таємницю, та конфіденційної інформації здійснюється згідно з вимогами до захисту службової інформації, якщо інше не передбачено законом.

Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються розпорядником інформації, якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

У системі здійснюється обов'язкова реєстрація:

- результатів ідентифікації та автентифікації користувачів;

- результатів виконання користувачем операцій з обробки інформації;

- спроб несанкціонованих дій з інформацією;

- фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

- результатів перевірки цілісності засобів захисту інформації.

Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки).

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.

Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

Передача службової і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації.

Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації, яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято розпорядником інформації.

Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

У разі коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі.

План захисту інформації в системі містить:

- завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

- визначення моделі загроз для інформації в системі;

- основні вимоги щодо захисту інформації та правила доступу до неї в системі;

- перелік документів, згідно з якими здійснюється захист інформації в системі;

- перелік і строки виконання робіт службою захисту інформації.

Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту.

У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.

У системі, яка складається з кількох інформаційних та (або) телекомунікаційних систем, ці Правила можуть застосовуватися до кожної складової частини окремо.

2.6 Порядок здійснення електронного документообігу в організації

Цей порядок встановлює загальні правила документування в організації в електронній формі і регламентує виконання дій з електронними документами з моменту їх створення або одержання до відправлення чи передачі до архіву.

Усі інші дії з електронними документами виконуються в організації згідно з вимогами до дій з документами на папері, передбаченими інструкцією з діловодства організації.

Дія цього порядку поширюється на всі електронні документи, що створюються або одержуються організацією.

Особливості роботи з електронними документами, що містять інформацію з обмеженим доступом, яка є власністю держави, визначаються спеціальними нормативно-правовими актами.

Організація здійснює електронний документообіг лише за умови використання надійних засобів електронного цифрового підпису, що повинне бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, одержаним на ці засоби від Адміністрації Держспецзв'язку, та наявності посилених сертифікатів відкритих ключів у своїх працівників - підписувачів.

Організація здійснює електронний документообіг через спеціальні телекомунікаційні мережі або телекомунікаційні мережі загального користування. При цьому відправлення організацією електронного документа

через телекомунікаційні мережі загального користування здійснюється за рішенням керівника цієї організації.

Система електронного документообігу організації повинна відповідати вимогам нормативно-правових актів у сфері захисту інформації.

Відповідальність за організацію здійснення електронного документообігу на підприємстві несе його керівник, якщо інше не встановлено відповідними документами.

Електронні документи, що надходять на адресу організації, приймаються відповідною службою діловодства або особою централізовано.

Електронний документ, що надійшов на адресу організації, підлягає відхиленню у разі:

- відсутності у адресата надійних засобів електронного цифрового підпису;

- надходження не за адресою;

- зараження вірусом;

- негативного результату перевірки на цілісність і справжність усіх накладених на нього електронних цифрових підписів.

При цьому відправнику у встановлений строк надсилається відповідне повідомлення.

Зазначена процедура для електронного документа відповідає процедурі повернення документа на папері.

Кожен одержаний адресатом електронний документ перевіряється на зараження його вірусом.

Кожен одержаний адресатом електронний документ перевіряється на цілісність і справжність усіх накладених на нього електронних цифрових підписів, включаючи ті, що накладені (проставлені) згідно із законодавством як аналоги печатки (далі - електронні печатки). При цьому необхідно, щоб:

- кожен електронний цифровий підпис був підтверджений з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

- особистий ключ підписувача відповідав відкритому ключу, зазначеному у сертифікаті;

- на час перевірки був чинним посилений сертифікат відкритого ключа акредитованого центру сертифікації ключів та/або посилений сертифікат відкритого ключа відповідного засвідчувального центру.

Попередній розгляд електронного документа здійснюється у його візуальній формі.

Визначення, чи потребує електронний документ обов'язкового розгляду керівником або іншими співробітниками відповідно до функціональних обов'язків, необхідності його реєстрації, а також встановлення строків виконання цього документа структурними підрозділами чи безпосередніми виконавцями здійснюється у тому ж порядку, що й для документів на папері.

Вхідні, внутрішні та вихідні електронні документи реєструються в одній системі разом з відповідними документами на папері.

Реєстрація вхідних електронних документів здійснюється у тому ж порядку, що й вхідних документів на папері. Для забезпечення реєстрації, обліку, пошуку і контролю виконання вхідного електронного документа заповнюється реєстраційно-контрольна картка в електронній формі.

Після реєстрації вхідного електронного документа адресат у встановлений строк надсилає відправнику повідомлення за відповідною формою про його прийняття і реєстрацію.

Для фіксування резолюції щодо виконання вхідного електронного документа складається відповідний внутрішній електронний документ "Резолюція" за підписом відповідної посадової особи, про що зазначається в реєстраційно-контрольній картці.

Контроль за виконанням та оперативним використанням наявної в електронних документах інформації здійснюється в тому ж порядку, що й для документів на папері.

Оформлення і реєстрація електронних документів, що складаються в організації, за винятком особливостей їх підписання або затвердження, здійснюється у тому ж порядку, що й для документів на папері.

До візуальної форми подання електронного документа за складом та розміщенням реквізитів встановлюються ті ж вимоги, що й для документа на папері.

Підписання або затвердження електронного документа здійснюється шляхом накладення на нього електронних цифрових підписів відповідних посадових осіб. На момент накладення останнього електронного цифрового підпису технологічно та/або організаційно забезпечується проставлення у створеному електронному документі дати і його реєстраційного номера.

У разі непідписання або незатвердження електронного документа керівником чи іншою посадовою особою реєстрація цього документа скасовується, а його виконавець інформується про відхилення документа.

Проставлення електронної печатки на електронний документ здійснюється згідно із законодавством. При цьому зазначена процедура виконується лише після підписання або затвердження електронного документа.

Адресування електронних документів здійснюється з додержанням тих же вимог, що й для документів на папері.

На кожний внутрішній та вихідний електронний документ заповнюється реєстраційно-контрольна картка в електронній формі.

Перед відправленням вихідного електронного документа проводиться перевірка його цілісності та справжності усіх накладених на нього електронних цифрових підписів з додержанням тих же вимог, що й для вхідних документів.

У разі порушення цілісності вихідного електронного документа або непідтвердження справжності накладеного на нього електронного цифрового підпису (підписів) його реєстрація скасовується, а виконавець інформується про відхилення документа.

Вихідні електронні документи відправляються адресатам службою діловодства оба відповідальною особою централізовано у встановлений строк після їх одержання від структурних підрозділів - виконавців.

Електронний документ вважається одержаним адресатом з часу надходження відправнику повідомлення про його прийняття і реєстрацію.

У разі неодержання від адресата протягом встановленого строку повідомлення про прийняття і реєстрацію або про відхилення електронного документа відправник вживає додаткових заходів з використанням інших засобів зв'язку для одержання від адресата відповідного повідомлення.

У разі одержання від адресата повідомлення про відхилення електронного документа відправником вживаються заходи для усунення причин відхилення і забезпечення повторного відправлення цього документа. Якщо таке повідомлення одержане від адресата, який не має надійних засобів цифрового електронного підпису, цьому адресату надсилається відповідний документ на папері.

Підтвердження факту одержання від адресата повідомлення щодо електронного документа відправником не здійснюється.

Реєстраційний номер, дата і час реєстрації електронного документа адресатом, зазначені у його повідомленні, фіксуються відправником у реєстраційно-контрольній картці.

Погодження електронного документа здійснюється шляхом накладення на нього електронного цифрового підпису посадової особи.

Зауваження і пропозиції до поданого електронного документа (у разі наявності) фіксуються в окремому електронному документі, на який накладається електронний цифровий підпис посадової особи.

Порядок внутрішнього погодження електронних документів у системі електронного документообігу організації затверджується його керівником, якщо інше не встановлено законодавством.

Строк зберігання електронних документів повинен бути не меншим від строку, встановленого для відповідних документів на папері.

2.7 Інструкція адміністратора безпеки при роботі з СЕД

1 Загальні положення

1.1 Інструкція регулює відносини між адміністратором безпеки, користувачами і розробниками, що виникають при:

- експлуатації та розвитку ІТС та СЕД;
- формуванні та використанні даних, повідомлень, баз даних, інформаційних ресурсів на основі створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження і надання користувачеві документованої інформації в ІТС та СЕД;
- при створенні, впровадженні та експлуатації нових інформаційних технологій в ІТС та СЕД.

1.2 Цілі адміністрування ІТС та СЕД досягаються забезпеченням і підтримкою в ІТС та СЕД:

- підсистем управління доступом, реєстрації та обліку, забезпечення цілісності програмно-апаратної середовища, що зберігається, обробляється і передається по каналах зв'язку інформації;
- доступності інформації (стійке функціонування ІТС та СЕД і її підсистем);
- конфіденційності інформації, що зберігається, обробляється і передається по каналах зв'язку інформації.

1.3 Захист ІТС та СЕД є комплексом організаційних і інженерно-технічних заходів, спрямованих на виключення або суттєве утруднення протиправних дій відносно ресурсів ІТС та СЕД.

1.4 Адміністратор безпеки є відповідальною посадовою особою організації, уповноваженим на проведення робіт з захисту інформації і підтримці досягнутого рівня захисту ІТС та СЕД і її ресурсів на етапах експлуатації та модернізації.

1.5 Адміністратор безпеки ІТС та СЕД призначається наказом по організації. Кількість адміністраторів безпеки ІТС та СЕД залежить від структури і призначення ІТС та СЕД (кількості серверів, робочих станцій

мережі, їх розташування), характеру і кількості вирішуваних завдань, режиму експлуатації, організації чергування.

1.6 Адміністратор безпеки керується в своїй практичній діяльності положеннями законів, нормативних та інших актів України та організаційно-розпорядчими документами організації.

1.7 Адміністратор безпеки несе відповідальність відповідно до чинного законодавства за розголошення інформації, що захищається, що стала йому відомою у відповідності з родом роботи, і заходів, прийнятих щодо захисту ІТС та СЕД.

1.8 Вимоги адміністратора безпеки, пов'язані з виконанням ним своїх функцій, є обов'язковими для виконання всіма користувачами ІТС та СЕД.

1.9 Інструкція не регламентує питання захисту і охорони будівель і приміщень, в яких розташована ІТС та СЕД, питання забезпечення фізичної цілісності компонентів ІТС та СЕД, захисту від стихійних лих (пожеж, повеней та ін.), Збоїв в системі енергопостачання, а також заходи забезпечення безпеки персоналу та заходи, прийняті при виникненні в ІТС та СЕД позаштатних ситуацій.

2 Права і обов'язки адміністратора безпеки

2.1 Права адміністратора безпеки

Адміністратор безпеки має право:

- відключати від мережі користувачів, які здійснили НСД де захищаються СЕД або які порушили інші вимоги з безпеки інформації;

- брати участь в будь-яких перевірках ІТС та СЕД;

- забороняти встановлення на серверах і робочих станціях ІТС позаштатне програмне і апаратне забезпечення.

2.2 Обов'язки адміністратора безпеки

Адміністратор безпеки повинен:

- знати досконало як застосовуються інформаційні технології;

- брати участь в контрольних і тестових випробуваннях і перевірках СЕД;

- вести контроль за процесом резервування і дублювання важливих ресурсів ІТС та СЕД;

- брати участь у прийманні нових програмних засобів;

- уточнювати в установленому порядку обов'язки користувачів ІТС та СЕД з підтримки рівня захисту ІТС та СЕД;

- вносити пропозиції щодо вдосконалення рівня захисту;

- аналізувати дані журналу обліку роботи ІТС та СЕД з метою виявлення можливих порушень вимог захисту;

- оцінювати можливість і наслідки внесення змін до складу ІТС та СЕД з урахуванням вимог НД щодо захисту, готувати свої пропозиції;

- забезпечити доступ до інформації, що захищається користувачам ІТС та СЕД згідно їх прав доступу при отриманні оформленого відповідним чином дозволу;

- забороняти і негайно блокувати спроби зміни програмно-апаратної середовища ІТС та СЕД без узгодження порядку введення нових (відремонтованих) технічних і програмних засобів і засобів захисту ІТС та СЕД;

- забороняти і негайно блокувати застосування користувачам мережі програм, за допомогою яких можливі факти несанкціонованого доступу до ресурсів ІТС та СЕД;

- негайно доповідати начальнику відділу безпеки про всі спроби порушення захисту ІТС та СЕД;

- аналізувати стан захисту ІТС і її окремих підсистем;

- контролювати фізичну схоронність коштів і устаткування ІТС та СЕД;

- контролювати стан засобів і систем захисту та їх параметри і критерії;

- контролювати правильність застосування користувачами мережі засобів захисту;

- надавати допомогу користувачам в частині застосування засобів захисту від несанкціонованого доступу та інших засобів захисту, що входять до складу ІТС та СЕД;

- не допускати установку, використання, зберігання і розмноження в ІТС та СЕД програмних засобів, не пов'язаних з виконанням функціональних завдань;

- своєчасно аналізувати журнал обліку подій, що реєструються засобами захисту, з метою виявлення можливих порушень;

- в період профілактичних робіт на робочих станціях і серверах ІТС та СЕД знімати при необхідності засоби захисту ІТС та СЕД з експлуатації з обов'язковим забезпеченням збереження інформації;

- не допускати до роботи на робочих станціях і серверах ІТС сторонніх осіб;

- здійснювати періодичні контрольні перевірки робочих станцій і тестування правильності функціонування засобів захисту ІТС;

- періодично надавати керівництву звіт про стан захисту ІТС та СЕД і про нештатні ситуації на об'єктах ІТС і допущених користувачами порушеннях встановлених вимог щодо захисту інформації;

- контроль за виконанням працівниками вимог нормативних документів з організації роботи з мережею Internet.

Адміністратору безпеки забороняється залишати свою робочу станцію без контролю, в тому числі в робочому стані.

Забороняється фіксувати облікові дані користувача (паролі, ідентифікатори, ключі та ін.) На твердих носіях, а також повідомляти їх кому б то не було, крім самого користувача.

2.3 Відповідальність за захист ІТС та СЕД від несанкціонованого доступу до інформації.

2.3.1 Відповідальність за захист ІТС та СЕД від несанкціонованого доступу до інформації покладається на адміністратора безпеки.

2.3.2 Адміністратор безпеки несе персональну відповідальність за якість проведених ним робіт з контролю дій користувачів при роботі в ІТС та СЕД, стан і підтримання встановленого рівня захисту ІТС та СЕД.

2.8 Правила роботи в ІТС

1 Загальні правила роботи

1.1 Робота в ІТС проводиться співробітниками підприємства з метою отримання необхідної інформації для виконання покладених на них посадових обов'язків.

1.2 Робота в ІТС підприємства проводиться за допомогою базового комп'ютера і інших додаткових пристроїв.

1.3 Запит на установку базового комп'ютера, його налаштування та встановлення мережевого програмного забезпечення здійснюється керівником підрозділу за попередньою письмовою заявкою, написаної на ім'я керівника підприємства або відповідної особи у вигляді службової записки.

1.4 Для ідентифікації користувача ІТС співробітнику видається ім'я (обліковий запис) і пароль. Ім'я та пароль необхідні для ідентифікації в ІТС підприємства і отримання доступу до ресурсів мережі (мережевих дисків, принтерів і програмами). Ім'я та пароль співробітника повинні бути унікальні в мережі. За унікальність і збереження пароля відповідає користувач. Пароль - інформація конфіденційна, конфіденційність забезпечується самим користувачем і засобами операційних систем.

1.5 Забороняється повідомляти пароль іншим користувачам ІТС і працювати під чужим паролем.

1.6 Користувачі ІТС зобов'язані ознайомитися з даними правилами.

2 Технічні норми і правила

2.1 Для кожного управління (відділу) виділено дисковий простір на сервері відповідно до поточних квот, для зберігання документів, пов'язаних з виконанням посадових обов'язків.

2.2 При вході в ІТС під своїм ім'ям і паролем відбувається автоматичне підключення мережевого диска. Залежно від того в якому відділі зареєстрований користувач буде доступний той чи інший мережевий диск. Ніхто, крім співробітників свого відділу і адміністраторів мережі, не має доступ до інформації, що зберігаються на сервері в Інтернеті.

2.3 Для обміну інформацією між відділами доступний загальний ресурс - автоматично підключається мережевий диск. Доступ до цього мережного диска мають абсолютно всі зареєстровані користувачі мережі. Зберігати документи на загальному ресурсі не рекомендується, тому що він автоматично очищається в ніч на перше число кожного місяця. За видалення інформації на ньому адміністратори мережі відповідальності не несуть.

2.4 Категорично забороняється викладати важливу інформацію на загальних ресурсах ІТС. За розміщення на загальному ресурсі мережі важливої інформації персональну відповідальність несе користувач, який виклав її.

2.5 За замовчуванням, відповідно до корпоративної політикою будь-якого знову зареєстрованому користувачеві доступ до локальних і мережевих дисководів, CD-ROM, портам USB заборонений.

2.6 Ремонтувати системи і в разі виявлення несправності будь-якого комп'ютерного та мережевого обладнання, а також при збої або несправності в роботі програмного забезпечення користувач зобов'язаний негайно повідомити у відділ технічного (програмного) забезпечення.

2.7 Підтримка і супровід встановленого системного і мережевого програмного забезпечення здійснюється відділом технічного забезпечення.

2.8 При необхідності використання нового програмного забезпечення, користувач зобов'язаний погодити його використання з начальником відділу технічного забезпечення.

2.9 На першу вимогу технічного фахівця користувач зобов'язаний звільнити комп'ютер для контролю або виконання регламентних робіт.

2.10 Всі дії, пов'язані з установкою програмного забезпечення, а також наданням доступу до конкретних ресурсів ІТС, здійснюються за попередньою письмовою заявкою, написаної на ім'я керівника організації або відповідальної особи у вигляді службової записки.

2.11 Відповідальність за працездатність клієнтського програмного забезпечення робочих станцій мережі підрозділу несуть відділи технічного і програмного забезпечення.

2.12 В ІТС підприємства встановлено обмеження на обсяг відправляється і приймається кореспонденції.

2.13 Системний адміністратор підприємства веде перелік базових комп'ютерів мережі організації. Кожен запис містить наступну інформацію:

- тип комп'ютера;
- використовувана операційна система;
- складові системного блоку (додаткові пристрої);
- модель монітора;
- IP-адреса комп'ютера;
- ресурси, які надаються іншим комп'ютерам;
- список встановленого програмного забезпечення;
- ПІБ відповідального користувача;
- дата заповнення.

2.14 В ІТС здійснюється моніторинг мережевих подій. Перелік подій, які підлягають протоколювання, визначається відділом технічного забезпечення. Отримані при цьому електронні журнали подій використовуються системним адміністратором для аналізу роботи мережі, а також можуть служити доказом неправомірних дій користувачів.

3 Права і обов'язки користувачів мережі

3.1 Користувач, який використовує носії інформації несе відповідальність за антивірусну чистоту містяться на них даних.

3.2 У разі отримання носія інформації з сумнівного джерела користувач зобов'язаний перевірити його на «віруси». Якщо у нього виникли сумніви, то він має право запросити фахівця з технічного відділу для повторної перевірки.

3.3 Користувачеві категорично забороняється відкривати підозрілі електронні листи і вкладені в них файли.

3.4 Користувач зобов'язаний негайно припинити роботу за комп'ютером, і звернеться до фахівців технічного відділу для з'ясування причин і вироблення заходів відновлення нормального функціонування корпоративної мережі в випадках:

- підозри на зараження вірусами;

- виявлення зараження вірусами;

- порушенням безпеки роботи мережі.

3.5 Кожен користувач в індивідуальному порядку відповідає за розуміння і правильне ставлення до правил безпеки систем, які вони використовують.

3.6 У програмах, що використовують парольний захист, користувачі зобов'язані вибирати якісні паролі і періодично самостійно змінювати їх.

3.7 З метою захисту від підбору системного пароля користувача накладено обмеження: при неправильному введенні пароля більше 5 раз, обліковий запис користувача блокується. Блокування може зняти тільки системний адміністратор (фахівець технічного відділу).

3.8 Для надійної і безпечної роботи основних сервісів функціонують в мережі, а також інформації користувачів, відділ технічного забезпечення зобов'язаний проводити повне або часткове резервне копіювання баз даних за планом проведення резервного копіювання.

4 Відповідальність користувачів мережі

4.1 Користувачі, які порушують нормальне (безпечне) функціонування мережі, що спричинило за собою матеріальні та моральні збитки організації, посадовим особам та користувачам мережі несуть відповідальність.

4.2 Відповідальність користувачів мережі повинна визначатися чинним законодавством і адміністративними заходами.

4.3 Адміністративні заходи повинні бути порівнянні з об'єктом відповідальності.

5 Користувачам забороняється

5.1 Самостійно переставляти і пересувати, а також підключати комп'ютерну техніку в приміщенні (в тому числі при проведенні генеральних прибирань, перестановці меблів та ін.).

5.2 Самостійно проводити встановлення, налаштування, модифікацію і тестування мережевого апаратного або програмного забезпечення.

5.3 Передавати через мережу інформацію, що ображає честь і гідність інших абонентів мережі, що містить заклики до насильства, розпалювання міжнаціональної ворожнечі, інформацію в зашифрованому вигляді, а також передавати інформацію за межі організації, якщо це не входить в посадові обов'язки користувачів.

5.4 Використовувати ресурси корпоративної мережі для здійснення будь-якого роду особистої або сторонньої комерційної діяльності.

5.5 Вчиняти будь-які дії прямо або побічно спрямовані на порушення нормальної роботи мережевого устаткування і руйнування загальних інформаційних ресурсів.

5.6 Передавати будь-кому свій пароль, працювати під чужим реєстраційним ім'ям, а так само здійснювати будь-які дії, пов'язані з отриманням паролів і реєстраційних записів.

6 Безпека і стійкість мережі

6.1 Складові безпеки мережі:

- конфіденційність - захист від несанкціонованого отримання інформації;
- цілісність - захист від несанкціонованого зміни інформації;
- доступність - захист від несанкціонованого утримання інформації і ресурсів.

Пряме чи непряме порушення однієї з даних компонент є порушенням безпеки мережі.

6.2 Відділ технічного забезпечення зобов'язаний забезпечувати і підтримувати безпеку всіх компонентів ІТС.

6.3 Відділ технічного забезпечення повинен забезпечувати антивірусний захист програмного забезпечення.

6.4 Для забезпечення стійкості і безпеки мережі відділ технічного забезпечення зобов'язаний проводити регулярні регламентні роботи.

2.9 Інструкція управління паролями

1 Правила створення парольних фраз

Парольні фрази є конфіденційною інформацією і не можуть бути розголошені, або передані кому-небудь. Відповідальність за безпечне зберігання пароля лежить на його власнику.

Обирання користувачами парольних фраз повинно автоматично перевірятися на відповідність вимогам, що пред'являються до складності пральних фраз, зазначеним в даному документі.

При виборі парольних фраз необхідно керуватися наступними критеріями:

1 Парольні фрази повинні містити не менше двох спецсимволов, букви в різному регістрі і цифри;

2 Паролі повинні бути випадковими, тобто:

- ні з якої наявної частини парольної фрази не можна зробити припущення про решти пароля;

- маючи парольну фразу користувача А можна зробити припущення про парольну фразу користувача Б.

3 Неприпустимо зберігання парольних фраз у відкритому вигляді;

4 Неприпустимо зберігання парольних фраз в перетвореному вигляді, стійкість алгоритму перетворення якого повністю залежить від знання самого алгоритму;

5 Довжина обираних парольних фраз повинна залежати від часу використання одних і тих же паролів. Так, наприклад, для використання однієї і тієї ж парольної фрази протягом 60 днів, досить її довжини в 8 символів. У разі збільшення періоду дії парольної фрази її довжина повинна бути збільшена.

6 Довжина парольних фраз, які не передбачають свою зміну з часом, повинна бути не менше 32 символів.

2 Безпечне утримання парольних фраз

Парольні фрази не підлягають зберіганню в паперовій або електронній формах у загальнодоступних місцях.

При первинному наданні доступу до інформаційних ресурсів мережевої інфраструктури, а також при отриманні заявки на скидання пароля,

користувачеві надається первинна парольний фраза. Первинна парольний фраза задовольняє вимогам, що пред'являються до паролів даним документом, а також є тимчасовою і повинна бути змінена при першому ж вході в систему.

Парольна фраза повідомляється виключно користувачеві інформаційних ресурсів, запитів доступ.

Первинна парольна фраза може бути передана кінцевому користувачу системи у відкритій формі через електронну пошту тільки в межах корпоративної поштової системи.

3 Зміна парольних фраз

Парольна фраза повинна бути змінена в наступних випадках:

- час дії пароля минув;

- при підозрі, що пароль став відомий комусь ще;

- якщо право користування обліковим записом було передано іншому користувачу;

- в разі, якщо склад групи, що користується загальним паролем, змінився.

При первинній реєстрації користувача в системі повинна бути запрошена зміна первинної парольної фрази. Також, користувачі повинні бути сповіщені про закінчення терміну дії його пароля і необхідності встановити новий.

Обов'язкові вимоги до парольного введення:

- придушення відображення введеної парольної фрази;

- нова парольна фраза повинна вводитися двічі;

Парольне поле повинно скидатися після кожної перевірки введеної парольної фрази.

2.10 Висновки за розділом

Проаналізована нормативно-правова база в Україні не дає чітких інструкцій щодо управління інформаційною безпекою саме в СЕД, але підхід до захисту інформації в цих системах пропонує організаціям створити службу захисту інформації, використання КСЗІ і електронного цифрового підпису, відповідно із законами України: «Про електронні документи та електронний

документообіг», «Про електронні довірчі послуги» та «Про захист інформації в інформаційно-комунікаційних системах».

Для управління інформаційною безпекою в СЕД слід впровадити на підприємстві систему управління інформаційною безпекою саме в системах електронного документообігу.

Було запропоновано використання в організаціях правил забезпечення захисту інформації в інформаційно-телекомунікаційних системах та порядку здійснення електронного документообігу. Разом з цим було запропоновано додатково ряд правил та інструкцій, а саме:

- інструкція адміністратора безпеки при роботі з СЕД;
- правила роботи в ІТС;
- інструкція управління паролями;

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Збільшення об'ємів інформації призвело до відповідного росту і кількості документів, які є основними носіями інформації, тому традиційні методи роботи з документами стали малоефективними, і виникла необхідність впровадження систем електронного документообігу (СЕД), які дозволяють створювати та обробляти документи електронними засобами.

Мета – визначити вартість впровадження розробленої СЕД на прикладі умовного підприємства.

Вихідні дані:

- кількість умовних співробітників – 10 осіб, у тому числі – 3 співробітника мають право на підпис зовнішніх електронних документів;

3.1 Визначення поточних витрат

Розрахунок трудомісткості реалізації розробленої політики безпеки наведений у таблиці 3.1.

Таблиця 3.1 - розрахунок річної трудомісткості розробленої політики інформаційної безпеки відповідно до інструкції адміністратора безпеки при роботі з СЕД

№ п/п	№ стр. в інструкції	Функціональні обов'язки системного адміністратора	t, ос.-год.
1	2	3	4
1.	2.1	контроль за процесом резервування, дублювання важливих ресурсів ІТС та СЕД;	200

продовження таблиці 3.1

1	2	3	4
2.	2.2	аналіз журналу обліку роботи ІТС та СЕД з метою виявлення можливих порушень вимог захисту;	200
3.	2.3	оцінка можливості і наслідки внесення змін до складу ІТС та СЕД з урахуванням вимог НД щодо захисту;	100
4.	2.4	налаштування паролів та доступу до інформації, що надається 10 користувачам ІТС та СЕД згідно їх прав доступу при отриманні оформленого відповідним чином дозволу;	10х0,2х2=4
5.	2.5	аналіз стану захисту ІТС і її окремих підсистем;	200
6.	2.6	контроль фізичної схоронності коштів і устаткування ІТС та СЕД, та участь в їх щорічної інвентаризації;	40
7.	2.7	контроль стан засобів і систем захисту та їх параметри і критерії;	40
Всього			784

При збільшенні кількості співробітників загальна трудомісткість повинна збільшуватися. При умовних вихідних даних 784 ос.-год. підприємству буде доцільно наймати системного адміністратора на пів ставки.

Сумарні загальні витрати на заробітну плату складають:

$$Ззп = 12500 \text{ х } 1,22 \text{ х } 0,5 = 7625 \text{ грн.}$$

Вартість машинного часу роботи ПК з урахування терміну експлуатації 2 роки. Метод амортизації для ПК – регресивний, для ПЗ – прямолінійний:

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p}$$

Смч = (0,6*1,44)+(18000*0,5)/2080+(12500*0,25)/2080= 6,69 грн/год,

де $P = 0,6$ – встановлена потужність ПК, кВт;

C_e = 1,44 – тариф на електричну енергію, грн/кВт*година;

$Ф_{зал} = 18000$ – залишкова вартість ПК на поточний рік, грн.;

$Н_a$ = 0,5 – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ = 0,25 – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ =12500 грн, вартість ліцензійного програмного забезпечення, грн

F_p = 2080 годин – річний фонд робочого часу обладнання.

Витрати вартості машинного часу на впровадження функціональних обов'язків системного адміністратора:

$$З_{мч} = t \cdot С_{мч}$$

Змч=6,69*784=5244.98 грн,

Сумарні поточні витрати складають:

С=Ззп + Змч = 7625 +5244,98 = 12869,96 грн.

3.2 Розрахунок витрат на необоротні активи

При впровадженні удосконаленої інформаційній безпеки в системах електронного документообігу умовно підприємство понесе наступні витрати:

- для налаштування електронних ключем для внутрішнього документообігу - спеціалізовано програмне забезпечення вартістю 4500 грн без ПДВ;

- придбання посилених електрони ключем для 3 співробітників, що мають право для підписання зовнішніх документів – 452 х 3 = 1356 грн без ПДВ (на 1 рік);

- придбання безперебійного джерела живлення для 10 ПК - 4800 *10 = 48000 грн (придбання 1 раз на 5 років);

- витрати на придбання антивірусних програм – 1200 *10 = 12000 грн (1 на рік);

- витрати на придбання диска для зберігання електронної документації - 3500 грн (1 раз на рік)

Загальні витрати на придбання або оновлення необоротних активів складають 69356 грн. Проте більшість цих витрат умовне підприємство повинне нести щорічно.

3.3 Визначення економічного ефекту

Для розрахунку економічного ефекту від впровадження системи електронного документообігу необхідно зазначити, що 25% робочого часу співробітники підприємства витрачають на роботу з паперовими документами.

Загальні витрати на придбання, обслуговування та підтримку системи електронного документообігу складають 42000 грн/рік.

Ефект від впровадження системи електронного документообігу буде спостерігатися, якщо умовне підприємство буде отримувати чистий прибуток від основної діяльності до оподаткування більше 42000 грн.

3.4. Висновки за розділом

Виконаний розрахунок показав, що при використанні удосконаленої системи електронного документообігу вона окупиться ще в першій рік експлуатації при чистим прибутку підприємства більше 42000, якщо кількість співробітників не привісить 10 осіб. Таким характеристикам може відповідати підприємство малого бізнесу.

ВИСНОВКИ

Згідно до мети та задач роботи було зроблено наступне:

- проаналізовано правові аспекти електронного документообігу, захисту інформації та управління інформаційною безпекою в Україні;

- проаналізовано особливості захисту електронного документообігу та комплексний захист інформації як компонент інформаційного забезпечення.

- проаналізовано стандартний набір загроз та перелік зловмисників при роботі в СЕД та захист в системах електронного документообігу, а саме: забезпечення безпечного доступу, розмежування прав користувача, конфіденційність, забезпечення достовірності документів та протоколювання дій користувачів.

Проаналізована нормативно-правова база в Україні не дає чітких інструкцій по управлінню інформаційною безпекою саме в СЕД, але підхід до захисту інформації в цих системах пропонує організаціям створити службу захисту інформації, використання КСЗІ і електронного цифрового підпису, відповідно із законами України: «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги» та «Про захист інформації в інформаційно-комунікаційних системах».

Рекомендовано впровадити систему управління інформаційною безпекою саме в системах електронного документообігу. За основу, як один з варіантів, взято підхід створення СУІБ згідно з рекомендаціями міжнародного стандарту ISO/IEC 27000.

Запропоновано згідно з цим стандартом в роботі використання правил забезпечення захисту інформації в ІТС та порядок здійснення електронного документообігу.

В роботі запропоновано наступні правила та інструкції, а саме:

- інструкція адміністратора безпеки при роботі з СЕД;
- правила роботи в ІТС;
- інструкція управління паролями.

ПЕРЕЛІК ПОСИЛАНЬ

1. Гречко А.В. Основи електронного документообігу: Навч. посібник / Київський національний торговельно-економічний ун-т. – К., 2006. – 156 с.

2. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту: [Електронний ресурс] – Режим доступу: http://domarev.kiev.ua.

3. Дурняк Б. В. Семантичний захист інформації в системах документообігу. Інформаційні технології [Текст] : монографія / Б. В. Дурняк, В. І. Сабат. - Л.: Вид-во Укр. акад. друкарства, 2010. – 160 с.

4. Іванова Т.В., Піддубна Л.П. Діловодство в органах державного управління та місцевого самоврядування: підруч. – К.: – 2007. –290 с.

5. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К. ДСТСЗІ СБ України, 1999 – 16 с.

6. Зибін С.В. Захист інформації від несанкціонованого доступу в системах обробки інформації // Інформаційна безпека. – 2011. – №1.

7. Зіма І.І. Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів) / І.І. Зіма, І.М. Ніколаєв.– К.: Наука і оборона. – 1998. – № 1. – С. 56-58.

8. Клименко І.В., Линьов К.О. Система електронного документообігу в державному управлінні: Навч.-метод. посіб. – К.: Вид-во НАДУ, 2006. – 32 с.

9. Круковський М. Ю. Рішення електронного документообігу. – К.: "Азимут-Україна". 2006. – 112 с.

10. Кузьменко Б. В. Організаційно-правові та програмно-технічні засоби забезпечення інформаційної безпеки: навч. посібник. – К.: НАУ, 2008. – 164 с.

11. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України / В.А. Ліпкан– К.: Текст, 2009. – 600 с.

12. Марчук О. В Захист інформації. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 170-172.

13. Марчук О. В. Документ електронний. Енциклопедія державного управління: у 8 т. – К.: НАДУ, 2011. Т.2. Методологія державного управління. – с. 142-144.

14. Матвієнко О.В. Основи організації електронного документообігу [Текст] : навч. посіб. для студ. вищ. навч. закл. / О. В. Матвієнко, М. Н. Цивін. – К. : Центр учбової л-ри, 2008. – 111 с.

15. Нестеренко О.В. Засади забезпечення необхідного рівня інформаційної безпеки державної влади: [Електронний ресурс] – Режим доступу: http://www.nbuv.gov.ua/portal/soc_gum/nac_bez/2009_4/pdf/nesterenko.pdf.

16. Почепцов Г. Г., Чукут С. А. Інформаційна політика. – К.: Вид-во "Знання", 2008. – 665 с.

17. Рибак М.І. До питання про інформаційні війни / М.І. Рибак, А.В. Атрохов. – К.: Наука і оборона. – 2003. – № 2 – С. 65-68.

18. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99.–К.: ДСТСЗІ СБ України, 1999. - 26 с.

19. Директива 1999/93/ЕС Європейського Парламенту та Ради від 13 грудня 1999 року "Про систему електронних підписів, що застосовується в межах Співтовариства" (DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, Офіційний журнал L 013, 19/01/2000 p. 0012 – 0020. Переклад здійснено Центром перекладів актів Європейського права при міністерстві юстиції України): [Електронний ресурс] – Режим доступу: http://uazakon.com/document/spart50/inx50337.htm.

20. Про державну таємницю : Закон України від 21 січня 1994 № 3 855-XII: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

21. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 р. № 851-IV: [Електронний ресурс] – Режим доступу: http:// www.rada.gov.ua

22. Про захист інформації інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

23. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

24. Про національну систему конфіденційного зв'язку України від 10 січня 2002 № 2919-III : Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

25. Про затвердження Примірної інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади : Постанова Кабінету Міністрів України від 17 жовтня 1997 р. № 1153: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

26. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації: Постанова Кабінету Міністрів України від 4 лютого 1998 р. № 121: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

27. Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади : Постанова Кабінету Міністрів України від 10.09.2003 р. № 1433: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

28. Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу : Постанова Кабінету Міністрів України від 26 травня 2004 р. № 680: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

29. Про затвердження Порядку акредитації центру сертифікації ключів : Постанова Кабінету Міністрів України від 13 липня 2004 р. № 903: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

30. Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади : Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1453: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

31. Про затвердження Порядку обов'язкової передачі документованої інформації : Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1454: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

32. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

33. Про затвердження загальних вимог до програмних продуктів, які закуповуються або створюються на замовлення державних органів: Постанова Кабінету Міністрів України від 12 серпня 2009 р. № 869: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

34. Про затвердження нормативно-правових актів з питань функціонування електронного цифрового підпису в банківській системі України : Постанова Національного банку України від 17 червня 2010 р. № 284: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

35. Про схвалення Концепції створення багатофункціональної комплексної системи: "Електронна митниця": Розпорядження Кабінету Міністрів України від 17 вересня 2008 р. № 1236: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

36. Про погодження створення Засвідчувального центру Національного банку України : Розпорядження Кабінету Міністрів України від 6 травня 2009 р. № 483: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

37. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 13 грудня 2010 р. № 2250: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

38. Питання впровадження системи електронної взаємодії органів виконавчої влади : Розпорядження Кабінету Міністрів України від 28 грудня 2011 р. № 1363: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

39. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 р. № 141: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

40. Про затвердження Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24 липня 2007 р. № 143: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua

41. Про затвердження Правил посиленої сертифікації: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 р. № 3: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

42. Про вимоги до форматів даних електронного документообігу в органах державної влади. Формат електронного повідомлення : Наказ Міністерства освіти і науки, молоді та спорту України від 20.10.2011 № 1207: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

43. Про затвердження Технічних умов на систему електронного документообігу органу виконавчої влади : Наказ Державного департаменту з питань зв'язку та інформатизації Міністерства транспорту та зв'язку України від 7 червня 2005 р. № 70 (ТУ У 30.0-33240054-001:2005).

44. Про затвердження Порядку зберігання електронних документів в архівних установах: Наказ Державного комітету архівів України від 25 квітня 2005 р. № 49: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

45. Про затвердження Технічних специфікацій форматів представлення базових об'єктів національної системи електронного цифрового підпису: Наказ Державного комітету України з питань науки, інновацій та інформатизації та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 13 серпня 2010 р. № 8/229: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

46. Про внесення змін до деяких нормативно-правових актів : Наказ Міністерства інфраструктури України від 8 червня 2011 р. № 138 (зареєстровано в Міністерстві юстиції України 24 червня 2011 р. за № 763/19501): [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua.

47. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння".

48. Міжнородній стандарт ISO / IEC 27001 "Інформаційні технології - Методи захисту - Системи менеджменту інформаційної безпеки – Вимоги"

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	1 Розділ	24	
6	А4	2 Розділ	65	
7	А4	3 Розділ	5	
8	А4	Висновки	1	
9	А4	Перелік посилань	6	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка вимог та рекомендацій для управління інформаційною безпекою в системах електронного документообігу організації
студента групи 125-19-1
Петкевічуса Яніса Вікторовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 115 сторінках та містить 1 рисунків, 5 таблиць, 48 джерел та 4 додатка.

Об'єкт дослідження: управління інформаційною безпекою в системах електронного документообігу.

Мета роботи: підвищення рівня інформаційної безпеки при роботі в СЕД.

Методи дослідження: системний аналіз, методи порівняння, структурний аналіз та спостереження.

У спеціальній частині дана характеристика управлінню інформаційною безпекою в СЕД. У роботі досліджена система управління інформаційною безпекою в системах електронного документообігу. Проведено аналіз основних аспектів захисту інформації в СЕД в Україні, розглянуто та проаналізовано особливості захисту електронного документообігу.

Запропоновано для управління інформаційною безпекою в СЕД впровадити на підприємстві систему управління інформаційною безпекою згідно з рекомендаціями міжнародного стандарту ISO/IEC 27001 та використання в організаціях правил забезпечення захисту інформації в та інформаційно-телекомунікаційних системах та порядку здійснення електронного документообігу та інших правил і інструкцій.

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

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

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

Керівник