МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____ к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 «Кібербезпека»

на тему: **ОРГАНІЗАЦІЯ ЗАХИСТУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ**

Студент групи СЗД-41, Гресько Олексій Сергійович _____

Науковий керівник: к.т.н. Шуклін Герман Вікторович _____

Нормоконтроль: Гребенніков Асаді Болдхоягович _____

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н., доц. Г.В. Шуклін
«_____» _____ 2022р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Гресько Олексію Сергійовичу

1. Тема роботи: Організація захисту електронного документообігу

Затверджена наказом по університету від «16» лютого 2022 р. № 22

2. Термін здачі студентом оформленої роботи «____» _____ 2022 р.

3. Об'єкт дослідження: процеси створення систем захисту електронного документообігу.

4. Предмет дослідження: методи та засоби захисту електронного обігу документів на об'єкті інформаційної діяльності.

5. Мета роботи: підвищення якості методичного забезпечення в технології захисту інформації в системі електронного документообігу.

6. Перелік питань, які мають бути розроблені:

1. Аналіз існуючих підходів до комплексного захисту систем електронного документообігу на підприємстві.
2. Системи електронного документообігу та забезпечення захисту інформації від несанкціонованого втручання.
3. Розробка та реалізація політики безпеки в системі електронного документообігу.
4. Застосування технологій криптографічного захисту інформації для убезпечення системи електронного документообігу.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу:

презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____ 2022 р.

Науковий керівник _____ Шуклін Г.В.

Завдання прийняв до виконання _____ Гресько О.С.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів бакалаврської роботи	Примітка
1.	Уточнення постановки завдання	До 04.04.2022	Виконано
2.	Аналіз науково-технічної літератури	До 25.04.2022	Виконано
3.	Системи електронного документообігу та забезпечення їх безпеки	До 06.05.2022	Виконано
4.	Розробка та реалізація політики безпеки в СЕД	До 13.05.2022	Виконано
5.	Застосування технологій криптографічного захисту інформації для убезпечення СЕД	До 25.05.2022	Виконано
6.	Перевірка роботи на плагіат+Передзахист	До 01.06.2022	
7.	Захист роботи	13.06.22-21.06.22	
8.	Випуск	30.06.2022	

Студент _____ Гресько О.С.

Керівник бакалаврської роботи _____ Шуклін Г.В.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

АРМ – Автоматизоване робоче місце
АС – Автоматизована система
АЦСК – Акредитований центр сертифікації ключів
ВОЛЗ – Волоконно-оптична лінія зв'язку
ДСТУ – Державний стандарт України
ЕЦП – Електронний цифровий підпис

ІБ – Інформаційна безпека
ІТС – Інформаційно-телекомунікаційна система
КС – Комп’ютерна система
КСЗІ – Комплексна система захисту інформації
КЗІ – Криптографічний захист інформації
КЗЗ – Комплекс засобів захисту
КЦД – Конфіденційність, цілісність, доступність
ЛОМ – Локальна обчислювальна мережа
МЕ – Міжмережевий екран
НД – Нормативний документ
НСД – Несанкціонований доступ
ОС – Операційна система
ПБ – Політика безпеки
СЕД – Система електронного документообігу
ТЗІ – Технічний захист інформації
ЦЗО – Центральний засвідчувальний орган
ЦСК – Центр сертифікації ключів
ЦКУ – Цивільний кодекс України
CMP – Certificate Management Protocol
DLP – Data Lost Protection / Data Leak Prevention
ISO/IEC – International Organization for Standardization / International Electrotechnical Commission
OCSP – Online Certificate Status Protocol
TSP – Time-Stamp Protocol

ВСТУП

Однією з загальновизнаних тенденцій сучасності є трансформація суспільства з індустріального в постіндустріальне, що відбувається в умовах посилення процесів глобалізації, зростання нематеріального виробництва та ринків послуг на основі досягнень науково-технічного прогресу, зокрема, завдяки масштабному, глибинному та динамічному втіленню інформаційно-

комунікаційних технологій в майже всі сфери життєдіяльності особи, суспільства та держави.

Провідні країни світу ще у минулому столітті ставили за мету забезпечення переходу до нового етапу розвитку людства — інформаційного суспільства, яке сприяє становленню відкритого демократичного суспільства та дозволяє:

✓ підвищити національну конкурентоспроможність за рахунок розвитку людського потенціалу, насамперед у високоінтелектуальних сферах суспільного виробництва;

✓ забезпечити належну якість життя громадян за рахунок економічного зростання та надання рівного якісного доступу до інформації.

Саме тому, одним із важливих і першорядних завдань України є розвиток інформаційного суспільства, яке орієнтоване на інтереси громадян. У той же час, впровадження новітніх інформаційних технологій несе потенційні загрози несанкціонованого втручання в роботу комп'ютерних систем, у відповідні процеси та порушення конфіденційності, цілісності та авторства інформації, тому вкрай необхідна відповідна реакція на зазначені виклики у вигляді: розробки методологій, стандартів, впровадження технічних рішень і подібне.

Актуальність теми. Разом із зростанням та втіленням нових технологій у різні процеси бізнесу, держави та власного життя, через велику кількість кібератак та вразливостей, зростає небезпека під час їх використання, яка полягає у несанкціонованому доступу до інформації, порушенні роботоздатності систем та подібних можливих діях.

Україна має власні, відомі у всьому світі, наукові розробки у сфері кібернетики, які стали підґрунтям для становлення інформаційного суспільства, впровадження концепції та програми інформатизації; створення різноманітних інформаційних систем та технологій, засобів криптографічного та технічного захисту інформації.

З кожним днем зростає кількість осіб, яка активно долучається до процесів створення, використання та розвитку світових та національних інформаційних ресурсів та технологій. Ці процеси, їхня динаміка та інші передумови

демонструють, що вітчизняна сфера інформаційних технологій знаходиться в стадії активного становлення та безпосередньо інтеграції в світовий інформаційний простір, будучи фундаментом для розвитку інформаційного суспільства в державі.

Однією із найефективніших форм створення, накопичення і обміну інформацією та її використання у процесі управлінської діяльності є саме технологія електронного документообігу. Тому актуальним завданням в Україні є розвиток інфраструктури електронного документообігу та взаємодії суб'єктів інформаційних відносин. Паперовий документообіг вже активно втрачає свою актуальність, оскільки необхідність вручну формувати, обробляти та зберігати документи, контролювати їх рух та життєвий цикл, виконання також істотно підвищує трудові, матеріальні та фінансові витрати будь-якої установи або підприємства.

Системи електронного діловодства і документообігу можуть сприяти створенню нової організаційної культури в органах влади, зробивши роботу виконавців більш цивілізованою, цікавою і значимою. Інформаційні технології дозволяють їм фактично спільно опрацьовувати та вирішувати більш широкий спектр поточних та стратегічних завдань.

Втім, ступінь розбудови системи інформаційної та кібернетичної безпеки, зокрема, на рівні окремих підприємств, установ та організацій є недостатньою і не відповідає потенціалу та можливостям України.

Постає необхідність невідкладного вдосконалення захисту не тільки окремих елементів електронного документообігу а його системи у цілому з урахуванням зростання кількості та небезпеки кібернетичних атак.

Наведене зумовлює актуальність проблематики, необхідність додаткового дослідження вказаних питань, а відтак вибір теми.

Мета дослідження полягає у системному аналізі сучасного стану створення та впровадження технологій захисту електронного документообігу у корпоративних мережах, визначенні ступеню нормативного та технологічного забезпечення цих процесів, визначенні перешкод у реалізації державної політики

електронного урядування та розробці пропозицій щодо їх вирішення й удосконалення.

З огляду на мету дослідження, його **основними завданнями** є:

- вивчення та аналіз сучасного стану нормативного забезпечення та технологічної бази у сфері створення та впровадження захищених систем електронного документообігу;

- дослідження засобів та технологій забезпечення конфіденційності, цілісності та безперервної доступності електронного документообігу, зокрема сутності та побудови системи електронного цифрового підпису;

- розробка певних пропозицій щодо методологічного забезпечення за тематикою досліджуваних питань.

Об’єктом дослідження є технології та процеси створення та вдосконалення, забезпечення безпечного функціонування систем електронного документообігу в розподілених корпоративних мережах.

Предметом цього дослідження є сукупність інженерно-технічних принципів, методів та засобів що мають бути використані для комплексного захисту електронного документообігу, включаючи методи електронного цифрового підпису.

Методи дослідження випливають з вимог системного та об’єктивного аналізу явищ суспільного життя та міждисциплінарного підходу до поставлених завдань. Дослідження проведено на основі таких наукових методів: емпіричного – спостереження та порівняння; теоретичного: застосування методів формальної логіки, порівняльного аналізу і синтезу, моделювання, статистичного. При написанні кваліфікаційної роботи використано теоретичні та практичні здобутки вітчизняних та зарубіжних дослідників та провідних розробників систем та засобів інформаційної та кібернетичної безпеки.

1 СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ТА ЗАБЕЗПЕЧЕННЯ ЇХ БЕЗПЕКИ

1.1. СЕД як засіб ефективного управління сучасним підприємством

Функціонування підприємства у сучасних реаліях є неможливим без ефективної системи управління. А під поняттям управління мається на увазі вплив для спонукання дій для досягнення певних цілей, але так само і прийнятті відповідальності за результативність цього. Управління здійснює наступні функції: планування, організація, мотивація, контроль і координація.

Останнім часом з'явилася ще така управлінська функція, як бенчмаркінг – знаходження ноу-хау, або що одні можуть робити краще за інших, опрацювання цього та удосконалення, після яких може бути впровадження нових методів роботи. Різні дослідники, експерти вважають, що подібна функція є важливою складовою успіху підприємства в сучасному світі.

Управління – складна сукупність з багатьох різновекторних процесів. Система управління складається з самостійних, проте взаємопов'язаних підсистем: керуючої і керованої. Керуюча підсистема має компоненти, що впливають на ресурси і колективи людей іншої підсистеми. До іншої, тобто керованої, підсистеми входять такі елементи, які відповідають за процеси безпосередньо створення матеріальних і духовних благ, надання будь-яких послуг. Зв'язок між цими підсистемами здійснюється через інформацію, що є основою вироблення нових рішень в управлінні.

Науково-технічна революція у суспільному виробництві ускладнила процеси керування економікою, потребує значних матеріальних і фінансових витрат, незважаючи на інші необхідні ресурси. Це першочергово пов'язано з розвитком науки і техніки, через що почали з'являтися сучасні технології і нові методи виробництва продукції. Внаслідок цього стаються постійні зміни цих процесів, і системи управління на підприємстві загалом. Важливу роль має швидке збільшення номенклатури виробів. Останні роки зростання номенклатури набагато збільшиться, що ускладнить системи управління. Зміни

складу продукції та стрімке зростання змінюваності виробів ускладнює різні функції управління на підприємстві.

Сьогодні на ринках у всьому світі переважає конкуренція, що є причиною для розширення асортименту та якості продукції, покращення асортименту продукції, отримання додаткових зусиль, отримання значних фінансових ресурсів для маркетингу та роботи НДДКР. Ці процеси дуже ускладнюють роботу менеджера (керівної ділянки підприємства), задаючи планку «виживання» на ринку. Це все вимагатиме обробки великого обсягу інформації за мінімальний час.

Саме на вирішення зазначених завдань спрямоване впровадження у різні компанії систем автоматизації, які забезпечують підвищення ефективності та вирішення завдань менеджменту, частина з них зазначена у таблиці 1.1.

По суті, сучасна автоматизована система – це комплекс програмно-апаратних засобів, що використовуються для управління фінансовими, матеріальними та людськими ресурсами підприємства.

В загальному випадку система управління ресурсами – це саме сукупність програмних, технічних, інформаційних, лінгвістичних та організаційно-технологічних методів та цілеспрямованих дій кваліфікованого персоналу, і ця сукупність призначена вирішенню завдань планування та управління базою ресурсів підприємства.

У свідомості сучасних людей ефективне управління корпоративними ресурсами є цінним процесом управління організацією загалом. З того часу підвищення ефективності управління ресурсами підприємства на основі систем управління ресурсами стало одним із безпосередніх шляхів покращення ділової активності в цілому.

Таблиця 1.1

Основні методи та функції управління

Методи та функції управління		
Адміністративні (організаційно-розпорядчі)	***Економічні***	***Соціально-психологічні***

1. Формування структури органів управління	1.Техніко-економічний аналіз та обґрунтування	1. Соціальний аналіз та соціальне планування
2.Створення та затвердження організаційних норм та нормативів (накази, правила, інструкції)	2. Формування економічних норм та нормативів	2. Формування морально-психологічного клімату на підприємстві
3. Планування організаційно-технічних заходів і контроль їх виконання	3. Розробка показників економічного розвитку та оцінка відповідності	3. Стимулювання підвищення кваліфікації
4. Підбір та розстановка кадрів	4. Ціноутворення	4. Соціальний розвиток колективу
5. Визначення посадових обов’язків та функцій.	5. Матеріальне стимулювання	5. Моральне заохочення
6. Договірна робота		6. Участь співробітників в управлінні підприємством

Впровадження нових систем управління ресурсами підприємства, як і інші істотні перетворення на ньому, є непростим і зазвичай стресовим процесом.

Однією з таких важливих систем управління є ERP (англ. *Enterprise Resource Planning* – планування ресурсів підприємства) системи, які можуть автоматизувати майже всі домени діяльності сучасного підприємства будь-яких масштабів та розмірів. Це може бути обробка замовлень, прогнозування, управління закупівлями і збутом, контроль процесів виробництва, планування обсягів сировини, диспетчеризація, бухгалтерський облік, управління фінансами, менеджмент персоналу, контроль якості, взаємодія з системами авто-управління виробничих технологій, підтримка штрих-кодування тощо.

Можна вважати, що виконання таких та інших функцій управління ресурсами пов’язане з обміном інформацією у вигляді документів тощо, різновидом ERP систем є системи електронного документообігу (СЕД).

Законом України «Про електронні документи та електронний документообіг» визначено, що електронний документ – це інформація, зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, склад та порядок розміщення яких визначається законодавством. Він може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного

документа є відображення даних у ньому електронними засобами чи на папері у формі, зрозумілій людині.

Досвід провідних підприємств свідчить, що втілення СЕД дозволяє вирішити багато проблем та опрацювати різні завдання, які має керівництво підприємства, вирішити визначені завдання в управлінні, досягти цілей тощо (рис. 1.1).

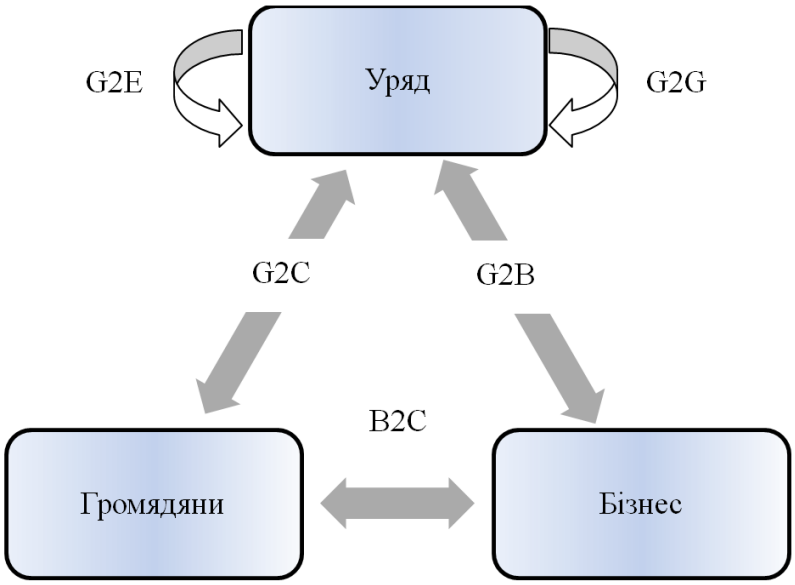

Рис. 1.1. Схема електронної взаємодії держави, бізнесу та громадян

Зокрема, надання електронним урядом послуг бізнесу (G2B, *Government to business*) та громадянам (G2C, *Government-to-Citizen*) дає змогу 24/7 в онлайн висвітлювати інформацію про діяльність державних органів та отримувати необхідні послуги. Це все можливо саме через інтеграцію інформаційних систем та автоматизації процесів інформаційного обміну між цими системами.

Завданнями проекту впровадження сучасних програмно-технічних засобів для автоматизації процесів обробки документів, як правило, є реалізація наступних задач, функцій та цілей (рис. 1.2 і 1.3):

Рис. 1.2. Функції документообігу

1. Новий рівень керованості підприємством завдяки скороченню часу на управлінські рішення, розробку наказів та розпоряджень, їх узгодження, підвищення виконавської дисципліни загалом. Для вирішення цього завдання СЕД реалізують певні функції, такі як:

✓ Забезпечення єдиного сховища документів з відповідною політикою доступу;

✓ Процеси збору, накопичення, узагальнення інформації щодо всіх документів, які обробляються та зберігаються на підприємстві, включаючи стан та терміни опрацювання;

✓ Забезпечення контролю за виконанням вимог, наказів, планових завдань, окремих доручень шляхом надання керівному складу своєчасної та достовірної інформації щодо актуального стану справ без проведення зайвих нарад, телефонних дзвінків тощо;

✓ Формування оперативної і якісної аналітичної інформації (зведених відомостей) щодо актуальної статистики роботи з документами (без

спотворення), включаючи обсяг опрацьованих документів середнього часу, що витрачений для цього окремими виконавцями або підрозділами.

2. Якість роботи підприємства збільшується через скорочення часу опрацювання запитів (такі, як, наприклад, узгодження та пошук необхідних документів), через швидке надання відповідей, меншу кількість помилок під час обробки і так далі. Відповідно цього, СЕД реалізують наступні функції:

✓ Можливість створення шаблонів документів;

✓ Забезпечення одночасного доступу кільком виконавцям для редагування документів (тобто усунення зайвого пересилання між ними, що точно спрощує можливість несанкціонованого доступу до цих документів);

✓ Підготовка авто-звітів і передача їх відповідальним виконавцям.

Серед основних результатів щодо впровадження СЕД можна виділити:

✓ Налагодження системи контролю реалізації бізнес-процесів;

✓ Високий рівень взаємодії співробітників через безпосередньо поліпшення умов та якості їх роботи, зменшення багатьох рутинних процесів;

✓ Забезпечення належного рівня виконавської дисципліни та відповідальності за виконання дорученої роботи;

✓ Нові можливості та передумови щодо впровадження системи прозорого контролю доступу до інформаційних ресурсів підприємства, менеджмент цього контролю;

✓ Збільшення ефективності використання інформації, швидкий доступ до неї (що можливо через класифікацію документів та різні системи пошуку, ведення історії та журналювання роботи);

✓ Структуроване зберігання документів, зручна каталогізація та виключення дублікатів.

Рис. 1.3. Цілі СЕД у системі управління

Стратегічними перевагами впровадження СЕД можна вважати:

1. Підвищення продуктивності та якості роботи. Це може бути важливим фактором надання переваги компанії серед клієнтів та партнерів. Зокрема, за допомогою реєстрації документів, призначенні завдань, спрощенню отримання відповідних звітів та подібним перевагав СЕД, виконавці можуть набагато швидше надати керівництву пропозиції щодо актуальних проблем та завдань.

2. Хороша мобільність та адаптація підприємства до будь-яких нових умов та змін, завдяки аналітичній інформації та оперативній реакції на зовнішні впливи через управлінські рішення, що зменшує стресовий період від цих змін, дає нові перспективи для розвитку і загалом може утримати підприємство від краху.

3. Своєчасне виявлення та усунення проблем у взаємодії керівництва, виконавців, партнерів та будь-яких структурних підрозділів.

Серед основних функцій СЕД слід виділити:

✓ Створення або прийом електронних документів (наприклад через сканування паперових документів);

✓ Зберігання та редагування цих електронних документів;

- ✓ Гибке управління рухом та циклом життя документів;
- ✓ Автентифікація користувачів в системі;
- ✓ Розділ прав користування.

Технологічною основою побудови СЕД при територіально рознесеному розміщенні підприємства є, зазвичай, мережі загального користування, які можуть забезпечити пропускну здатність згідно тарифів та умов користування. Прикладом такої мережі можуть бути мережі стеку протоколів TCP/IP. В цілому, використання СЕД підвищує ефективність та якість роботи працівників, їх зацікавленість у роботі через усунення рутинних задач тощо (використання шаблонів, зручний пошук і так далі). Зменшує витрати часу та інших ресурсів (матеріальних та людських), забезпечує компактність та швидкість роботи з інформацією.

Можна зазначити деякі переваги впровадження та використання СЕД:

- ✓ - швидкий та дешевий безпаперовий документообіг;
- ✓ - поліпшення процедури підготовки та обліку документів, їх цілісність, конфіденційність, авторство і неспростовність;
- ✓ - криптозахист інформації (електронних документів тощо), що дає можливість передачі відкритими каналами зв’язку;
- ✓ - зменшення фінансових ризиків через поліпшення конфіденційності обміну документами;
- ✓ - менше витрата ресурсів за рахунок задіяння електронного архіву;
- ✓ - можливість оперативного пошуку електронних документів, зручного та швидкого їх перегляду, навіть визначення юридичної сили цих документів завдяки ЕЦП;
- ✓ - проста але захищена та дієва процедура підписання договорів та подачі будь-якої фінансової звітності;
- ✓ - надійний та швидкий обмін документами з партнерами, незалежно від місцезнаходження адресанта та адресата.

Проте, застосування несе деякі нові відповідні ризики несанкціонованого втручання в роботу СЕД, порушення конфіденційності, цілісності та доступності

інформаційних ресурсів, що може викликати значні фінансові та матеріальні збитки. Через це аналіз інформаційних загроз безпеці у територіально розподілених корпоративних мережах, визначення певних методів та засобів захисту – актуальна задача.

1.2. Вимоги щодо нормативного та технологічного забезпечення побудови СЕД

Система електронного документообігу за суттю є автоматизованою системою (АС) обробки інформації. Слід зазначити, що у загальному випадку будь яка АС відповідно до вимог державних стандартів, перш за все, характеризується апаратною, програмною платформами, прикладним програмним забезпеченням, технологіями обробки інформації, нормативно-правовим забезпеченням та інформацією, що підлягає обробці.

Нормативно-правову базу створення та функціонування СЕД утворюють Закони України, Укази Президента України, постанови та розпорядження Кабінету Міністрів України, прикази міністерств та відомств, що прийняті в межах відповідних повноважень, державні стандарти та технічні регламенти.

Слід зауважити, що вимоги наведених нормативно-правових та нормативно-технічні актів та документів є обов’язковими для виконання органами державної влади та управління, державними установами тощо.

Щодо приватних підприємств, за винятком банківських установ, у майже всіх випадках, під час створення СЕД та розробки політики використання, вони самостійно визначають вимоги до систем електронного документообігу. Винятком є ситуації, коли в таких системах передбачається обробка державної інформації з обмеженим доступом або задіяння державних інформаційних ресурсів, чи будь-якої іншої інформації, захист якої гарантується та контролюється державою.

Банківські установи також додатково регламентуються нормативними актами національного регулятора – у Випадку України, це є постанови Національного банка України (НБУ).

Ще існують стандарти міжнародних організацій, таких як Міжнародна організація зі стандартизації (МОС, англ. ISO), Міжнародна електротехнічна комісія (МЕК, англ. IEC), Міжнародний союз електрозв'язку (МСЕ, англ. ITU), вони не є обов'язковими, проте переважно мають рекомендаційний характер та навіть певні технічні рішення, недотримання яких може спричинити проблеми у впровадженні або проблеми несумісності.

Основними та загальновизнаними вимогами до СЕД вважаються наступні:

Масштабованість. Система бажано повинна підтримувати будь-яку адекватну кількість користувачів та документів, здатність СЕД змінювати потужність та об'єм даних має визначатись тільки загальними можливостями апаратної та програмної платформ.

Розподіленість. Архітектурні рішення таких систем мають підтримувати взаємодію з розподіленими системами, тобто мати можливості для роботи з документами в територіально-розподілених організаціях.

Модульність. Такі системи мають складатись з окремих модулів, які можна інтегрувати між собою, бажано при необхідності замінити якийсь з цим модулів, забезпечити можливість поетапного впровадження компонентів СЕД або лише часткового, для виконання лише певного спектру задач документообігу.

Відкритість. Подібна система повинна мати відкриті інтерфейси для зручної інтеграції, сумісності, доповнення та можливого доопрацювання з іншими програмними та апаратними системами, комплексами та рішеннями.

Автоматизація документообігу здійснюється через певні автоматизовані функції, поєднані за призначенням у типові ***функціональні комплекси (підсистеми)***, що можуть включати***:***

- ✓ підготовку документів комп'ютерними засобами;
- ✓ зберігання, реєстрацію документів в електронному архіві;

- ✓ ведення цього архіву та організацію доступу до його інформації;
- ✓ зручний контроль виконавчої діяльності, журналювання;
- ✓ проектування руху документів та подібний обмін даними;
- ✓ підтримку формування аналітичної та статистичної звітності;
- ✓ створення та ведення нормативно-довідкової інформації;
- ✓ адміністрування, каталогізація, класифікація;

Через проектування СЕД багатьма різними світовими та вітчизняними компаніями, які є незалежними між собою, через відсутність загальновизнаних стандартів та протоколів, також через неузгодженість роботи систем виникають певні проблеми при взаємодії систем документообігу, інтеграції між одна до одної. Наприклад, різні формати подання даних, різні методи та технології їх обробки дуже часто призводить до несумісності. Проте це іноді дає конкурентоспроможність та альтернативні варіанти з певними перевагами відносно потреб.

Електронний документообіг обслуговується певним програмним забезпеченням (англ. *Enterprise Document Management Systems - EDMS*). Одними з найважливіших характеристик СЕД фахівці, як правило, вважають такі:

- ✓ – сумісність з програмною платформою;
- ✓ – типи документів, з якими працює система;
- ✓ – певні можливості масштабування;
- ✓ – максимальна кількість користувачів; кількість рівнів структур, які відображають внутрішню організацію підприємства;
- ✓ – можливість роботи без жорсткої фіксації маршрутів;
- ✓ – засоби визначення маршрутних схем для документів;
- ✓ – можливості контролю за проходженням документів, повідомлення про порушення проходження та повідомлення посадових осіб;
- ✓ – підтримка роботи з кількома версіями документа (контроль версій)
- ✓ – можливості інтеграції та сумісності зі сторонніми додатками;
- ✓ – налаштування та відповідність потребам замовника;
- ✓ – засоби регламентації доступу, криптозахисту, надійність системи.

Існують певні принципи, на яких засновані процеси організації збору й обробки облікової та управлінської інформації на підприємстві. Виділяють деякі загальні принципи побудови СЕД:

1) в організаційному аспекті:

a. реєстрація документів відповідно до регламенту, контроль їх цілісності та конфіденційності, обробка документів в різних ситуаціях;

b. просте і мінімальне внесення змін до структурних зв'язків підприємства у СЕД при фактичній зміні цих зв'язків;

c. різні альтернативні варіанти зв'язку та можливості працювати із зовнішніми підрозділами та установами в структурі у випадку втрати зв'язку;

2) в інформаційному аспекті:

a. можливість інтегрувати дані, які підтримуються та використовуються підрозділами та установами в процесі взаємодії, додаткова можливість виконувати локально певні базові функції в локальному при порушенні зв'язку;

b. відповідність певним технологіям, що функціонують в органах держвлади;

3) в алгоритмічному та апаратному аспектах:

a. алгоритми та функціонування повинні максимально відповідати міжнародним та національним стандартам і рекомендаціям стосовно інтерфейсів, засобів, мережевих протоколів, систем управління базами даних і подібним;

b. забезпечення резервування, дублювання, дзеркалювання та взаємозамінності певних технічних засобів в усій системі, що є необхідною складовою надійності та бажано безперервного функціонування системи у критичні моменти;

c. принципи архітектури системи загалом мають дозволяти розширення та заміну будь-яких програмних або технічних засобів, доповнення та оновлення їх функцій без порушення функціонування системи;

4) в технологічному аспекті:

a. управління та планування здійснюється відносно виробничих процесів взаємодії центральних та місцевих органів влади, тобто створюються і обробляються документи;

b. легкого та швидке налагодження або зміна процесів відносно технологій обробки або потреб, бажано при збереженні рівня продуктивності системи та її надійності загалом;

c. не змінюється режим праці певних спеціалістів при впровадженні інтегрованої системи електронного документообігу (ІСЕД);

5) у нормативно-правовому аспекті:

a. дотримання різних нормативно-правових актів щодо застосування електронного документообігу і ЕЦП.

Принципи створення інформаційних СЕД та загальні вимоги до подібних систем:

- ✓ – *системність* – структурних елементів системи, зв'язки між якими забезпечують її цілісність і можливість взаємодії з іншими системами;
- ✓ – *відкритість* – можливість оновлення функцій системи без порушення порядку її функціонування;
- ✓ – *сумісність* – можливість взаємодіяти з іншими системами, завдяки інформаційно-технологічним інтерфейсам;
- ✓ – *стандартизація та уніфікація* – використання стандартизованих та рекомендованих варіантів, уніфікованих рішень при створенні системи;
- ✓ – *ефективність* – результати роботи системи задовольняють певні критерії відносно витрачених ресурсів.

Як можна помітити, ключовим принципом є принцип економії, який можна досягти шляхом раціональних підходів в організації системи звітності, розвитку прогресивних її форм, автоматизації бізнес-процесів, управління документообігом.

Реалізація цього принципу можлива також за раціонально організованого

електронного документообігу, який націлений на забезпечення економії матеріалів та інших ресурсів.

З погляду закону та права важливо визначити, чи прийнято нормативно-правові акти, що регулюють впровадження електронного документообігу та забезпечують відповідну юридичну силу цього документообігу згідно світових тенденцій.

1.3. Організаційно-технологічні підходи щодо впровадження СЕД

Виходячи з нормативних документів за питань захисту інформації, процеси захисту мають відбуватися одночасно з побудовою технології або через впровадження систем захисту у вже існуючі технології – перший підхід, звичайно, є більш ефективним через кращу сумісність. Тому подивимось на процеси впровадження та створення СЕД детальніше.

Основні підходи, принципи створення та впровадження типового електронного документообігу аналогічні до впровадження будь-якого комплексного IT-рішення для управління бізнесом. Відповідно, реалізація проекту залежать від організаційної, економічної та технологічної потужності.

Організаційна потужність – керування проекту, його підтримка. Проблеми такого характеру зазвичай пов’язані саме із людським фактором, наприклад: слабкою мотивацією робітників до роботи з новими системами та рішеннями, поганим рівнем їх комп’ютерної грамотності та обізнаності, помилковим визначенням та постановкою завдань, що постають перед системою.

Економічна – це фінансові ресурси, переваги та ефект від впровадження системи, що можуть бути поступовими.

Технологічні – складність створення якісної інфраструктури, проблеми сумісності, питання розробки, впровадження нових технологій тощо.

Тому задля ефективного впровадження СЕД необхідно:

- зацікавленість керівництва та всіх відповідальних у такому рішенні;
- розробка концепції та плану впровадження СЕД, формування групи;
- тісна і постійна співпраця із ІТ-фахівцями;
- чіткий менеджмент та розподіл обов’язків та повноважень в групі;
- пілотний проект для відпрацювання автоматизації бізнес-процесів;
- постійні процеси навчання та вдосконалення знань співробітників.

Для автоматизації процесів документообігу, необхідним є аналіз документообігу підприємства, що ґрунтується на виявленні проблемних ділянок, їх покращенні і оптимізації руху документів в системі. Подібний аналіз може відбуватися за такими етапами:

1. аналіз СЕД на підприємстві;
2. вивчення структури документообігу;
3. оптимізація взаємодії наявної моделі документообігу.

При виборі таких систем керівництву підприємства необхідно точно визначити завдання, які вирішуються зараз, та які будуть вирішуватися за допомогою СЕД. Далі потрібно проаналізувати різні рішення на ринку, наприклад, відносно критеріїв, що вже були згадані раніше, можливо звернутися до фахівців та експертів, які допоможуть визначити найкращий варіант згідно задач та сфери діяльності. Пріоритетні завдання та конкретні умови функціонування підприємства також є досить значними факторами під час визначення та оцінки варіантів СЕД від різних виробників.

Відносно захисту інформації, існують вимоги, що встановлені законом в інформаційно-телекомунікаційних системах та визначені Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі – системах), що затверджені постановою Кабінету Міністрів України від 29.03.2006 року № 373 (далі – Правила).

Встановлено, що захисту в системі підлягає:

- відкрита інформація, яка належить до державних інформаційних ресурсів, або про суб'єктів владних повноважень, військових

формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації" (далі - конфіденційна інформація);
- службова інформація та інформація, яка становить державну або іншу передбачену законом таємницю (далі - таємна інформація);
- інформація, вимога щодо захисту якої встановлена законом.

У приватному підприємстві цей перелік може бути доповнений відомостями, що становлять комерційну таємницю.

Під час обробки в системі, відкрита інформація повинна зберігати цілісність (тобто бути під захистом від несанкціонованих модифікації чи знищення). Знищити або модифікувати цю інформацію повинні лише ідентифіковані, автентифіковані та авторизовані користувачі, що мають відповідні повноваження, інші спроби мають бути заблоковані.

Щодо службової та таємної – необхідно забезпечити захист від несанкціонованого та неконтрольованого ознайомлення або іншим операцій (модифікації або знищення, копіювання, передачі тощо). Доступ так само має надаватися тільки ідентифікованим, автентифікованим та авторизованим користувачам.

Згідно з Правилами у системі здійснюється обов'язкова фіксація:

- результатів ідентифікації та аутентифікації;
- виконання будь-яких операцій стосовно інформації;
- будь-яких несанкціонованих дій;
- надання або позбавлення права доступу чи модифікації даних;
- перевірки цілісності інформації.

Аналіз цих даних здійснює виключно адміністратор безпеки – окрема людина, яка має певні повноваження та доступ до реєстраційних даних, також

вона має права на коригування прав інших користувачів, контроль, збір та обробка даних здійснюється автоматично.

Передача таємних та службових даних між системами має бути у зашифрованому вигляді або лише захищеними каналами зв'язку, згідно з вимогами законодавства. Перераховані вимоги становлять певну основу для фундаментальних заходів безпеки СЕД, що будуть розглянуті в наступних розділах.

Висновки до 1 розділу

Згідно тенденцій сучасності та завдяки досягненням науково-технічного прогресу, відбувається багато процесів, серед яких масштабне та динамічне втілення нових технологій в усі сфери суспільства, зокрема кожної особи, держави та світу загалом. Особливо втілення інформаційних технологій та технологій зв’язку.

Традиційні технології та підходи у створенні та обробці інформації значно програють новим, це добре помітно, коли є необхідність збереження, верифікації, обробки, редагування, створення та передачі документів в підприємстві, в державних установах або у повсякденному житті людини. З методів роботи із повністю паперовими документами значна більшість підприємств та людей давно відмовилась, але досі дуже часто цей цикл включає розроблення документа в електронному вигляді, створення паперової копії для підпису, пересилання паперової копії з підписом, розгляд паперової копії та перенесення її знову до електронного вигляду. Це все потребує багато зайвих ресурсів, часу, є достатньо неефективним трудомістким процесом. Тому можливо захищені СЕД невдовзі займуть місце у системі опрацювання документів підприємств та держави, згодом і взагалі більшості документообігу, початок розвитку цих процесів вже можна спостерігати у нових проектах України щодо державного документообігу.

СЕД сприяють створенню нової організаційної культури в секторі реальної економіки. З огляду на поступове впровадження технологій електронного урядування можливо, стверджувати, що застосування на підприємствах України покращує в цілому покращує інвестиційну привабливість держави та утворює нові можливості для взаємодії громадян та суб'єктів господарювання з органами державної влади.

На поточний час в державі прийнята низка нормативно-правових актів, що регламентують порядок організації захищеного СЕД, правовий статус і відносини з використання ЕЦП, але недосконаліть механізму їх впровадження, слабка матеріально-технічна база, відсутність стандартів та форматів СЕД, занадто складна методологічна база побудови захищених систем гальмують розвиток такого процесу.

Тому уявляється доцільним дослідити у наступних розділах методологічні аспекти створення захищених СЕД.

2 РОЗРОБКА ТА РЕАЛІЗАЦІЯ ПОЛІТИКИ БЕЗПЕКИ В СЕД

2.1. Розробка політики інформаційної безпеки

Інформаційні ресурси підприємства являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів. Потенційно можливий несприятливий вплив є загрозою інформаційній безпеці.

Захист інформації, що обробляється в комп’ютерних системах (КС), полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації

спрямовано на забезпечення безпеки оброблюваної інформації і КС в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і ресурсів системи, що їх реалізує. Сукупність взаємоузгоджених та взаємодоповнюючих заходів, що забезпечує захист інформації в КС, отримала назву комплексної системи захисту інформації (КСЗІ).

Певна частина проблем забезпечення інформаційної безпеки може бути розв’язана шляхом неухильного дотримання нормативних вимог та реалізації організаційних заходів. Деякі загрози, що є зовнішніми по відношенню до КС, можуть бути нейтралізовані або блоковані лише шляхом застосування спеціальних методів та засобів, які реалізують технології технічного та криптографічного захисту інформації.

Концептуальні засади щодо забезпечення інформаційної безпеки на підприємстві мають бути оформлені у вигляді окремого документу – політики безпеки (ПБ), що має бути затверджений на рівні керівництва.

Політика безпека безпеки в КС за суттю є методологічною основою реалізації сукупності заходів щодо захисту інформаційних ресурсів підприємства та регламентує принципі та підходи щодо їх впровадження.

Найбільш важливою частиною політики безпеки є правила розмежування доступу (англ. *access mediation rules*), що регламентують умови доступу користувачів і процесів до пасивних об'єктів.

Виходячи з цього несанкціонований доступ (НСД)до інформації (англ. *unauthorized access to information*) визначається як доступ до інформації, здійснюваний з порушенням правил розмежування доступу.

ПБ застосовується розробниками систем та комплексів захисту в КС, власниками та користувачами КС у плані забезпечення безпеки комп’ютерної системи (англ. *computer system security*) та захисті інформації від загроз несанкціонованого доступу.

При цьому під захистом інформації в КС розуміється діяльність, яка спрямована на забезпечення безпеки оброблюваної інформації та КС в цілому і дозволяє запобігти або ускладнити можливість реалізації потенційних і реальних

(перспективних) загроз, а також знизити величину потенційних збитків внаслідок реалізації цих загроз. Захист інформації повинен забезпечуватись на всіх стадіях життєвого циклу КС, на всіх технологічних етапах обробки інформації і в усіх режимах функціонування. Життєвий цикл КС включає розробку, впровадження, експлуатацію та виведення з експлуатації.

Залежно від принципів побудови та умов застосування нормативні документи розрізняють КС трьох класів: 1 – окрема персональна електронно-обчислювальна машина - ПЕОМ; 2 – локальна обчислювальна мережа - ЛОМ; 3 – локальні обчислювальні мережі, що підключені до глобальних обчислювальна мереж, включаючи Інтернет.

З урахуванням вимог щодо пріоритетів у захисті інформації КС поділяють на підкласи:

- ✓ «К» – у системі висуваються підвищені вимоги до захисту від загроз конфіденційності інформації;
- ✓ «Ц» – відповідає підвищеним вимогам до захисту від загроз цілісності інформації;
- ✓ «Д» – для систем з підвищеними вимогами до захисту від загроз доступності інформації;
- ✓ «КЦ» – підвищені вимоги до захисту від загроз конфіденційності і цілісності інформації;
- ✓ «КД» – підвищені вимоги до захисту від загроз конфіденційності і доступності інформації;
- ✓ «ЦД» – підвищені вимоги до захисту від загроз цілісності і доступності інформації;
- ✓ «КЦД» – підвищені вимоги до захисту від загроз конфіденційності, цілісності і доступності інформації.

Політика безпеки комп’ютерної системи включає в себе певну низку концептів та складових політики безпеки. Під концептами в концептуальних евристиках розуміються узагальнені елементи проблеми і відносини між ними.

Під концептами політики безпеки розуміються узагальнені і найбільш важливі елементи (технічні, програмні, організаційні тощо) щодо забезпечення рішення проблеми безпеки інформації і ресурсів комп'ютерної системи (далі безпеки КС). Такі концепти формуються вибором із множини шляхів рішення проблеми безпеки КС суттєво важливих та формування на цій основі узагальнених, найбільш важливих, результативних послуг безпеки (елементів проблеми) і відносин між ними (пріоритетність, вагомість, залежність від інших послуг безпеки, вплив певних послуг безпеки на інші щодо їх обов'язкової необхідності, сумісності чи несумісності тощо).

При такому підході і в такій постановці задачі елементами (концептами) політики безпеки КС можуть бути:

- ✓ створення та забезпечення функціонування комплексу засобів захисту (КЗЗ), комплексної системи захисту інформації КС, проведення випробувань КЗЗ;
- ✓ формування профілю захищеності інформації КС на основі стандартних профілів для обраного класу і підкласу КС;
- ✓ створення нових об'єктів доступу, визначення функцій і механізмів доступу, концепції побудови диспетчера доступу, атрибутів доступу та забезпечення їх сталості;
- ✓ забезпечення безперервного захисту та блокування несанкціонованого доступу;
- ✓ застосування безпечних архітектур КС, середовищ розробки КС, послідовності розробки КС, середовища функціонування КС;
- ✓ опрацювання нормативної документації КС, включаючи експлуатаційну, з питань безпеки тощо;
- ✓ застосування критеріїв експертної оцінки захищеності інформації КС від несанкціонованого доступу та інші.

Таким чином, складовими політики безпеки КС є часткові політики і послуги безпеки, реалізацією яких забезпечується розв'язок проблеми інформаційної безпеки в КС.

Забезпечення політики безпеки досягається шляхом виконання положень нормативних документів НД ТЗІ, певних принципів, концепцій, системних основ тощо щодо забезпечення рішення проблеми безпеки та реалізації політики безпеки КС.

Під час розробки політики безпеки в КС базовими визначаються наступні послуги безпеки:

- ✓ функціональні послуги безпеки КС;
- ✓ гарантії послуг безпеки КС;
- ✓ послуги безпеки стандартних профілів захищеності інформації КС.

Виходячи з цих положень далі розкриємо сутність заходів з забезпечення безпеки СЕД, як прикладної системи у рамках захищеної КС.

Політика безпеки в СЕД визначає стратегію організації в області захисту інформації в системі, а також пріоритетність вирішення проблем та ресурси, які керівництво вважає за доцільне виділити для цього.

Визначення політики інформаційної безпеки (ІБ) у загальному випадку повинне зводитися до наступних практичних кроків:

1. Визначення переліку керівних документів і стандартів в області ІБ, а також основних положень політики ІБ, включаючи:
   - ✓ керування доступом до засобів обчислювальної техніки, програм та даних;
   - ✓ антивірусний захист;
   - ✓ питання резервного копіювання;
   - ✓ проведення ремонтних і відбудовних робіт;
   - ✓ інформування про інциденти в області ІБ.

2. Визначення підходів до керування ризиками: чи є достатнім базовий рівень захищеності або потрібно проводити повний варіант аналізу ризиків.

3. Сертифікація на відповідність стандартам в області ІБ.

Для побудови системи захисту інформації необхідно визначити границі системи, для якої повинен бути забезпечений режим інформаційної безпеки.

Система керування інформаційною безпекою (система захисту інформації), відповідно, повинна будуватися саме в цих границях.

Опис границь системи, для якої повинен бути забезпечений режим інформаційної безпеки, рекомендується виконувати за наступним планом.

1. Аналіз структури організації. Опис існуючої структури й змін, які передбачається внести у зв'язку з розробкою або модернізацією СЕД.

2. Вивчення розміщення засобів обчислювальної техніки, оргтехніки й підтримуючої інфраструктури. Модель ієрархії засобів обчислювальної техніки.

3. Визначення ресурсів СЕД, що підлягають захисту.

4. З’ясування технології обробки інформації й розв'язувані завдання. Для розв'язуваних завдань повинні бути побудовані моделі обробки інформації в термінах ресурсів.

У результаті проведення робіт повинен бути створений документ, у якому:

- ✓ зафіксовані границі й структура системи;
- ✓ перераховані ресурси, що підлягають захисту;
- ✓ наведена система критеріїв для оцінки їх цінності.

Мінімальним вимогам до режиму інформаційної безпеки відповідає базовий рівень. Звичайною областю використання цього рівня є типові проектні рішення. Існує ряд стандартів і специфікацій, у яких розглядається мінімальний (типовий) набір найбільш ймовірних загроз, таких як віруси, збої встаткування, несанкціонований доступ тощо.

У випадку, коли порушення ІБ можуть мати важкі наслідки, базовий рівень вимог до режиму інформаційної безпеки є недостатнім. Для того, щоб сформулювати додаткові вимоги, необхідно:

- ✓ визначити цінність ресурсів;
- ✓ до стандартного набору додати список загроз, актуальних для досліджуваної інформаційної системи;
- ✓ оцінити ймовірності загроз;
- ✓ визначити рівень вразливості ресурсів.

Політика ІБ будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації. Існують різні підходи до оцінки ризиків. Вибір підходу залежить від рівня вимог, встановлених на підприємстві щодо режиму інформаційної безпеки, характеру прийнятих в увагу загроз (спектра впливу загроз) і ефективності потенційних контрзаходів.

Процес оцінки ризиків включає кілька кроків.

1. Ідентифікація ресурсу й оцінювання його кількісних показників (визначення негативного впливу).

2. Оцінювання загроз.

3. Оцінювання вразливостей.

4. Оцінювання існуючих і перспективних засобів забезпечення.

5. Оцінка ризиків.

На підставі оцінки ризиків вибираються засоби, що забезпечують необхідний рівень інформаційної безпеки.

Ресурси, значимі для нормальної роботи підприємства, що й мають певний ступінь вразливості, вважаються підданими ризику, якщо стосовно них існує деяка загроза.

При оцінюванні ризиків враховуються потенційні негативні впливи від небажаних подій і показники значимості розглянутих вразливостей і загроз для цих ресурсів. Ризик характеризує небезпеку для СЕД.

Ціль оцінки ризиків полягає у визначенні характеристик ризиків для інформаційної системи і її ресурсів. На основі таких даних можуть бути обрані необхідні засоби керування інформаційною безпекою.

Ризик залежить від показників цінності ресурсів, ймовірності реалізації загроз для ресурсів і ступеня легкості, з якого уразливості можуть бути використані при існуючих або планованих засобах забезпечення інформаційної безпеки. Таким чином, при оцінюванні ризиків враховуються: цінність ресурсів, значущість загроз, ефективність існуючих і планованих засобів захисту.

Показники ресурсів або потенційний негативний вплив на діяльність організації можна визначати декількома способами: кількісними (наприклад, на

основі вартості), якісними (можуть бути побудовані на використанні таких понять, як, помірний, середній або надзвичайно небезпечний), або комбінацією двох попередніх.

Питання про те, як провести границю між припустимими й неприпустимими ризиками, вирішується власником інформації (бізнесу). Очевидно, що розробка політики безпеки вимагає врахування специфіки конкретних підприємств.

На підставі політики ІБ формується план захисту, який реалізується на процедурному й програмно-технічному рівнях.

2.2. Критерії захисту інформації. Формування профілю захисту

Згідно стандарту ДСТУ ISO/IEC 27001, власники та користувачі КС (включаючи такі, що реалізують функції СЕД) мають бути впевнені, що протягом всього їх життєвого циклу забезпечується належний рівень безпеки інформації, яка обробляється, зберігається і передається. Оцінка безпеки інформації в КС (англ. *information security evaluation*) це процес, метою якого є визначення відповідності стану безпеки інформації в КС встановленим вимогам.

Для формалізації вимог з безпеки у НД ТЗІ використовуються критерії оцінки захищеності (англ. *security evaluation criteria*) такі шкали оцінки (сукупність вимог), що використовуються для оцінки ефективності функціональних послуг безпеки і коректності їх реалізації в оцінюваній ІТС.

При цьому, для оцінки ефективності гарантійних послуг безпеки і коректності їх реалізації в оцінюваній КС використовуються критерії оцінки гарантії безпеки (англ. *criterion estimation guarantee safety*) - сукупність вимог (шкала) оцінки.

Множина критеріїв оцінки, що характеризує конкретний (бажаний або досягнутий) стан інформаційної безпеки в КС.

На рис. 2.1 наведена структура критеріїв захисту інформації в КС. Наведена класифікація корисна у плані спрощення процедури вибору переліку функцій, які повинен реалізовувати комплекс засобів захисту до проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Законом України «Про інформацію» визначено, що основними видами інформаційної діяльності є одержання, використання, поширення, захист та зберігання інформації. Одержання, використання, поширення, захист та зберігання документованої здійснюється у порядку, передбаченому цим Законом та іншими законодавчими актами в галузі інформації.

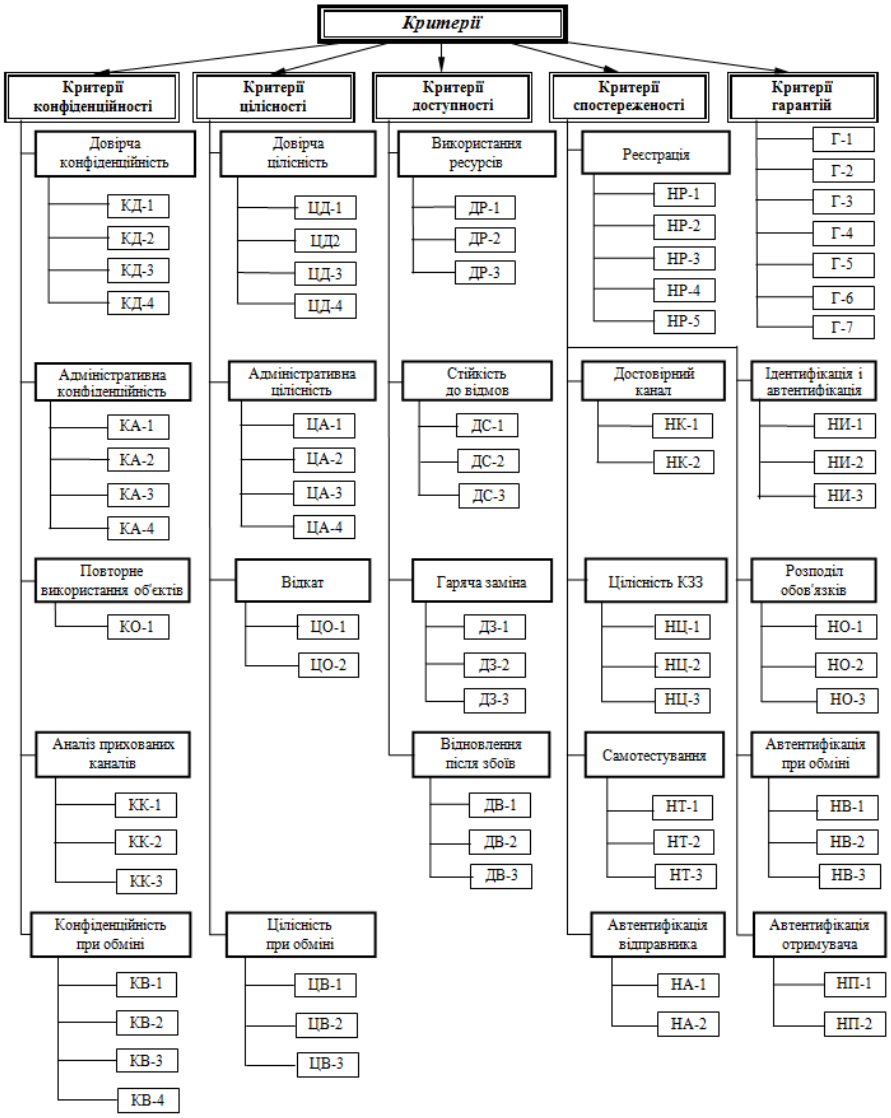

Рис. 2.1. Структура критеріїв згідно НД ТЗІ 2.5-004-99

Об’єкти захисту уточнені у «Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», що затверджені Постановою Кабінету Міністрів України № 373 від 29.03.2006. Захисту в системі, згідно пункту 4 згаданих Правил, підлягає:

- ✓ відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється

в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- ✓ конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі - конфіденційна інформація).

Крім того, пункт 13 цих Правил встановлює, що 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.

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.

Особливої уваги заслуговує порядок захисту на підприємстві інформації про особу. як сукупності документованих відомостей про особу. По-перше, це обумовлено повсюдним застосуванням персональних даних під час приймання на роботу, укладання різного роду договорів, опрацювання фінансових документів тощо. По-друге, захист персональних даних має свої нормативні, організаційні та технічні відмінності від захисту, наприклад, державної або комерційної таємниці.

Персональні дані за режимом доступу є інформацією з обмеженим доступом.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Оператори обробки персональних даних повинні обробляти інформацію відповідно до існуючого законодавства.

Беручи до уваги вищенаведені тези, потенційні загрози безпеки інформації та згідно з вимогами нормативних документів НД ТЗІ 2.5-005-99 і НД ТЗІ 2.5-

004-99, для автоматизованих систем класів «1» (відокремлених або підключених до захищених мереж), «2» та «3», які обробляють та передають персональні дані пропонуються для реалізації нижче наведені (таблиця 2.1) функціональні профілі захисту (ФПЗ).

Виходячи з даних, наведених у таблиці, можливо зрозуміти, яким чином посилюється система захисту залежно від умов застосування СЕД, що підлягає захисту. Зауважимо, що відповідно до вимог НД ТЗІ 3.7-003-05 інформаційно-телекомунікаційна система у відповідних випадках може розглядатися як інтегрована, тоді комплексну систему захисту для неї пропонується створювати шляхом поєднання комплексних систем захисту інформації окремих її елементів.

Зокрема, якщо у територіально-розподіленій СЕД наявні елементи у вигляді автоматизованих систем класів АС-1 і АС-2, то загальну комплексну систему захисту інформації доцільно розглядати, як поєднання відповідних підсистем – захищених віддалених АРМ та локальних обчислювальних мереж.

Реалізація наведених профілів захищеності може бути забезпечена підсистемами захисту інформації, які дозволяють суттєво підвищити рівень інформаційної безпеки у будь яких комп’ютерних мережах, включаючи СЕД.

Зокрема, це стосується підсистем: антивірусного захисту, розмежування доступу (захисту від НСД), мережного екранування, виявлення вторгнень у мережу, аналізу захищеності та виявлення вразливостей, протидії витоку інформації (англ. *Data Lost Protection/Data Leak Prevention - DLP*), криптографічного захисту інформації.

Таблиця 2.1

Рекомендовані ФПЗ для систем що обробляють персональні дані

Клас автом	**Критерії**			
	Конфіденційності	**Цілісності**	**Дост.**	**Спостереженості**

атизованої системи	**Адміністративна конфіденційність**	**Довірча конфіденційність**	**Повторне використання об'єктів**	**Конфіденційність при обміні**	**Адміністративна цілісність**	**Довірча цілісність**	**Відкат**	**Цілісність при обміні**	**Стійкість до відмов**	**Реєстрація**	**Ідентифікація і автентифікація**	**Достовірний канал**	**Розподіл обов'язків**	**Цілісність КЗЗ**	**Самотестування**	**Автентифікація при обміні**
АС-1 Окрема	КА-1		КО-1							НР-2	НИ-2	НК-1	НО-1	Ц-1	НТ-1	
АС-1 у ЗТМ	КА-1		КО-1	КВ-1	ЦА-1			ЦВ-1		НР-2	НИ-2	НК-1	НО-1	Ц-1	НТ-1	
АС-2	КА-2	КД-2	КО-1	КВ-1	ЦА-2	ЦД-1	ЦО-1	ЦВ-1		НР-2	НИ-2	НК-1	О-2	НЦ-2	НТ-2	
АС-3	КА-2	КД-2	КО-1	КВ-1	ЦА-2	ЦД-1	ЦО-1	ЦВ-1	ДС-1	НР-2	НИ-2	НК-1	О-2	НЦ-2	НТ-2	НВ-1

Сучасний ринок систем та засобів захисту інформації пропонує широкий спектр різноманітних засобів, які можна віднести до визначеного переліку підсистем. Їх застосування повинно ґрунтуватися на чіткому розумінні переваг та недоліків перед іншими, знанні принципів побудови, здатності поєднувати у єдину несуперечливу систему захисту та інших характеристиках.

Різні аспекти побудови підсистеми криптографічного захисту інформації будуть окремо проаналізовані у розділі 3. У наступному розділі проаналізуємо особливості застосування інших підсистем захисту, що застосовуються для забезпечення як відкритої, так і інформації з обмеженим доступом.

2.3 Сучасні методи та технології технічного захисту інформації в СЕД

Перераховані у попередньому розділі підсистеми захисту, а саме: антивірусного захисту, розмежування доступу (захисту від НСД), мережного екранування, виявлення вторгнень у мережу, аналізу захищеності та виявлення вразливостей, а також *DLP* системи згідно законодавства відносяться до систем та засобів технічного захисту інформації, а тому на них поширюється вимоги НД ТЗІ. Уявляється доцільним більш детально проаналізувати принципи їх побудови, функціонування та застосування.

Зауважимо, що ядром сучасних систем захисту інформації, які застосовуються у державному та приватному секторах суспільного виробництва, переважно виступають операційні системи (ОС), що мають вбудований комплекс засобів захисту, оцінений за критеріями ТЗІ. Це з одного боку, надає впевненість власникам СЕД та їх користувачам у оперативній підтримці з боку розробників у багатьох випадках виникнення кіберінцидентів комп'ютерних мережах. З іншого застосування атестованих ОС надає можливість побудувати довірену систему розмежування доступу, надання повноважень легальним користувачам, а також забезпечити реєстрацію подій у системі та ведення відповідного журналу подій. Функціональний профіль перевіреної ОС зазвичай є основою для формування функціонального профілю захисту комп'ютерної мережі (системи).

У багатьох випадках необхідно виключити можливість проникнення у локальну мережу деякої протиправної (пропаганда насильства, війни тощо). З зазначеною метою використовуються контент-фільтр – апаратний пристрій або програмне забезпечення, що обмежує проходження через нього веб-контенту (англ. *Content-control software* або *web filtering software*) та не дозволяє отримати доступ до певних сайтів або послуг мережі Інтернет. Система дозволяє блокувати веб-сайти з вмістом, що не призначені для перегляду.

Контент-фільтр працює по статистичному принципу, тобто підраховує заздалегідь певні слова тексту і визначає категорію, до якої відноситься вміст сайту.

Фільтрація в багатьох випадках відбувається на рівні запитів по протоколу HTTP. Для цього URL запитаного сайту звіряється з чорним списком за допомогою списків певних мовних конструкцій - виразів. Такі списки необхідно регулярно оновлювати, захист з їх допомогою вважається малоефективним. Більш просунуті є методи розпізнавання образів і обробки природної мови. Для класифікації сайтів за деякою ознакою (наприклад, «пиратский сайт») текст запитуваної сторінки аналізується на кількість різних ключових слів (наприклад, «безкоштовно», «скачати» тощо) та інші властивості тексту, які

використовуються для обчислення ймовірності попадання в небезпечну категорію. Якщо ця ймовірність перевищує заданий рівень (наприклад, 90%), доступ до сторінки блокується.

Найпростіші програми дозволяють ввести слова, пошук яких буде вести система вручну. Найскладніші пристрої вже мають великий словник і припускають вже готову базу посилань, які вже класифіковані. Як правило, до складних пристроїв виробники забезпечують періодичне оновлення бази посилань. Ті веб-сайти, які не були розпізнані автоматично, переглядає людина і привласнює категорію сайту вручну. Головна вимога до програм контент-фільтрів – забезпечення належної швидкодії класифікації.

Забезпечення безпеки периметру локальної мережі від несанкціонованого проникнення, а точніше точок доступу до глобальних мереж здійснюється за наступними основними способами: за допомогою прокси-серверів та мережевих екранів, а також шляхом забезпечення побудови *VPN* з використанням методів шифрування.

Проксі (англ. *proxy)* сервер у комп'ютерній мережі це програма, яка є посередником між комп'ютером і web-серверами та забезпечує передачу запитів браузерів і інших програм в Інтернет та отримання відповідей та передачу у зворотній бік.

При використанні локального проксі-сервера браузер не звертається до web-серверів в Інтернет безпосередньо, а посилає запит на скачування web-сторінок, картинок і файлів проксі-сервера. Цей сервер звертається в Internet за певними файлами і потім передає їх на певний комп'ютер. У локальній мережі проксі-сервер забезпечує доступ в Інтернет комп'ютерів локальної мережі через єдине підключення.

При цьому проксі-сервер може виконувати кілька завдань, а саме:

- ✓ Захист від стеження і забезпечення схоронності переданих даних;
- ✓ Блокування проходження небажаної інформації (реклами) або відвідування небажаних сайтів;
- ✓ Обмеження і підрахунок Інтернет-трафіку;

- ✓ Кешування (тимчасове збереження) інформації, що проходить з Інтернету до браузеру. Завдяки кешуванню проксі-сервер дозволяє суттєво прискорити відображення сторінок браузером і істотно знизити трафік;
- ✓ Кешування запитів до *DNS*-серверів.

Таким чином проксі-сервер дозволяє певним чином захистити локальну мережу від стеження за нею. Також за його допомогою можна обмежувати доступ до ресурсів завдяки застосуванню «чорного списку» сайтів (*URL - Uniform Resource Locator* - фільтрація), на які проксі-сервер не пускатиме користувачів (або певну їх частину, або в певний час тощо).

Мережевий екран є програмним або програмно-апаратним засобом, що здійснює відповідно до заданих правил контроль і фільтрацію мережевого трафіку, який проходить через нього. Замість поняття мережевий екран застосовують також інші терміни, які запозичені відповідно з німецької та англійської мов: брандмауер (нім. *Brandmauer*) або файрвол (англ. *Firewall*).

Серед завдань, які вирішують міжмережеві екрани, основним є захист сегментів мережі або окремих хостів від несанкціонованого доступу з використанням вразливих місць в протоколах або в програмному забезпеченні, встановленому на комп'ютерах мережі. Міжмережеві екрани пропускають або забороняють трафік, порівнюючи його характеристики з заданими шаблонами.

Найбільш поширене місце для установки міжмережевих екранів - межа периметра локальної мережі для захисту внутрішніх хостів від атак ззовні. Однак атаки можуть починатися і з внутрішніх вузлів - в цьому випадку, якщо атакується хост розташований в тій же мережі, трафік не перетне кордон мережевого периметра, і міжмережевий екран не буде задіяний. Тому в даний час міжмережеві екрани розміщують не тільки на кордоні, але і між різними сегментами мережі, що забезпечує додатковий рівень безпеки.

Фільтрація трафіку за допомогою міжмережевого екрану здійснюється на основі набору попередньо визначених правил, які називаються *RULESET*. При цьому міжмережевий екран представляється як послідовність фільтрів, що

обробляють інформаційний потік. Кожен з фільтрів забезпечує виконання окремого правила. Послідовність правил в наборі істотно впливає на продуктивність брандмауера. Наприклад, багато міжмережевих екранів послідовно порівнюють трафік з правилами до тих пір, поки не буде знайдено відповідність. Для таких міжмережевих екранів, правила, які відповідають найбільшій кількості трафіку, слід розташовувати якомога вище в списку, збільшуючи тим самим продуктивність.

Існує два принципи обробки трафіку. Перший принцип говорить: «Що явно не заборонено, то дозволено». В даному випадку, якщо міжмережевий екран отримав пакет, який не потрапляє ні під одне правило, то він передається далі. Протилежний принцип - «Що явно не дозволено, то заборонено» - гарантує набагато більшу захищеність, так як він забороняє весь трафік, який явно не дозволено правилами. Однак, цей принцип обертається додатковим навантаженням на адміністратора.

В кінцевому рахунку, міжмережеві екрани виконують над вхідним трафіком одну з двох операцій: пропустити пакет далі (*allow*) або відкинути пакет (*deny*). Деякі міжмережеві екрани мають ще одну операцію - *reject*, при якій пакет відкидається, але відправнику повідомляється про недоступність сервісу, доступ до якого він намагався отримати. На противагу цьому, при операції *deny* відправник не інформується про недоступність сервісу, що є більш безпечним.

Брандмауер дозволяє здійснювати фільтрацію тільки того трафіку, який він здатний "розуміти". В іншому випадку, він втрачає свою ефективність, оскільки не здатний прийняти рішення про те, що робити з нерозпізнаним трафіком. Існують протоколи, такі як TLS, SSH, IPsec і SRTP, що використовують шифрування, щоб приховати вміст, через що їх трафік неможливо проаналізувати. Також, деякі протоколи, такі як OpenPGP і S/MIME, шифрують дані прикладного рівня, через що фільтрувати трафік на підставі інформації, що міститься на даному мережевому рівні стає неможливо. Ще одним прикладом обмеженості аналізу міжмережевих екранів є тунелювання трафіку, якщо міжмережевий екран «не розуміє» використаного механізму тунелювання. У цих

випадках, правила конфігурації *RULESET* на міжмережевому екрані повинні явно визначати, що робити з трафіком, який вони не можуть проінтерпретувати.

Розрізняють наступні типи міжмережевих екранів (рис. 2.2): керовані комутатори, пакетні фільтри, шлюзи сеансового рівня, посередники прикладного рівня, інспектори стану.

Керовані комутатори іноді зараховують до класу міжмережевих екранів, так як вони здійснюють фільтрацію трафіку між мережами або вузлами мережі. Однак вони працюють на канальному рівні і поділяють трафік в рамках локальної мережі, а значить не можуть бути використані для обробки трафіку з зовнішніх мереж (наприклад, з Інтернету).

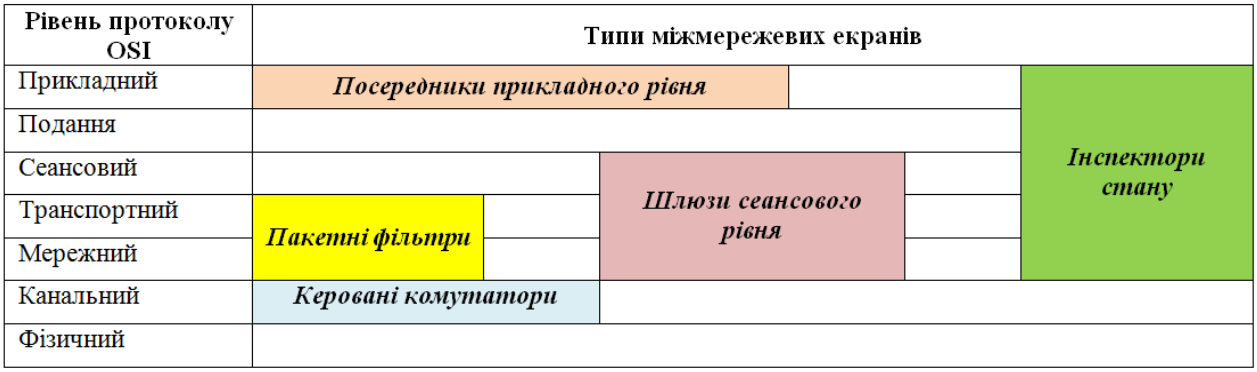

Рис. 2.2. Класифікація міжмережевих екранів

Пакетні фільтри функціонують на мережевому рівні і контролюють проходження трафіку на основі інформації, що міститься в заголовку пакетів. Багато міжмережевих екранів даного типу можуть оперувати із заголовками протоколів і більш високого, транспортного, рівня (наприклад, TCP або UDP). Пакетні фільтри залишаються найпоширенішим типом. Дана технологія реалізована в переважній більшості маршрутизаторів і навіть в деяких комутаторах.

При аналізі заголовка мережевого пакету можуть використовуватися такі параметри: IP-адреси джерела і одержувача, тип транспортного протоколу, поля

службових заголовків протоколів мережевого і транспортного рівнів, порт джерела і одержувача.

Шлюзи сеансового рівня виключають пряму взаємодію зовнішніх хостів з вузлом, розташованим в локальній мережі, виступаючи в якості посередника (англ. *Proxy*), який реагує на всі вхідні пакети і перевіряє їх допустимість на підставі поточної фази з'єднання. Шлюз сеансового рівня гарантує, що жоден мережевий пакет не буде пропущений, якщо він не належить раніше встановленому з'єднанню.

Як тільки приходить запит на встановлення з'єднання, в спеціальну таблицю поміщається відповідна інформація (адреси відправника і одержувача, використовувані протоколи мережевого і транспортного рівня, стан з'єднання тощо). У разі, якщо з'єднання встановлено, пакети, що передаються в рамках даної сесії, будуть просто копіюватися в локальну мережу без додаткової фільтрації. Коли сеанс зв'язку завершується, відомості про нього видаляються з даної таблиці. Тому всі наступні пакети, «хто вдає» пакетами вже завершеного з'єднання, відкидаються.

Так як міжмережевий екран даного типу виключає пряму взаємодію між двома вузлами, шлюз сеансового рівня є єдиною сполучним елементом між зовнішньою мережею і внутрішніми ресурсами. Це створює враження того, що на всі запити з зовнішньої мережі відповідає шлюз, і робить практично неможливим визначення топології мережі, що захищається. Крім того, так як контакт між вузлами встановлюється тільки за умови його допустимості, шлюз сеансового рівня запобігає можливості реалізації DoS-атаки, властивої пакетним фільтрам.

Незважаючи на ефективність цієї технології, вона має серйозний недолік: як і у всіх перерахованих вище класів міжмережевих екранів, у шлюзах сеансового рівня не реалізується перевірка вмісту поля даних, що дозволяє зловмисникам передавати «троянських коней» в мережу, що захищається.

Посередники прикладного рівня, також, як і шлюзи сеансового рівня, виключають пряму взаємодію двох вузлів. Однак, функціонуючи на

прикладному рівні, вони здатні «розуміти» контент переданого трафіку. Міжмережеві екрани, які реалізують цю технологію, містять кілька додатків-посередників (англ. *Application proxy*), кожне з яких обслуговує свій прикладний протокол. Такий міжмережевий екран здатний виявляти в переданих повідомленнях і блокувати неіснуючі або небажані послідовності команд, що часто означає DoS-атаку, або забороняти використання деяких команд (наприклад, тих що дають можливість користувачу записувати інформацію на FTP сервер).

Інспектори стану (англ. *Stateful inspection*) поєднують кращі властивості перерахованих вище типів міжмережевих екранів використовується для захисту корпоративних мереж і має низку переваг. Вони здійснюють фільтрацію трафіку з мережевого по прикладний рівень забезпечуючи високу продуктивність і захищеність. Даний тип міжмережевих екранів дозволяє контролювати: кожен переданий пакет - на основі таблиці правил, кожну сесію - на основі таблиці станів, кожен додаток - на основі розроблених посередників.

Заходи протидії DDoS-атакам можна розділити на пасивні і активні, а також на превентивні і реакційні. Нижче наведено короткий перелік основних методів.

Запобігання. Профілактика причин, що спонукають тих чи інших осіб організовувати і зробити DDoS-атаки.

Адекватні заходи. Застосовуючи технічні та правові заходи, потрібно якомога активніше впливати на джерела і організатора DDoS-атаки.

Програмне забезпечення. На ринку сучасного програмного і апаратного забезпечення існує і таке, яке здатне захистити малий та середній бізнес від слабких DDoS-атак.

Фільтрація. Блокування трафіку, що виходить від атакуючих машин. Ефективність цих методів знижується в міру наближення до об'єкта атаки і підвищується в міру наближення до атакуючої машині. В цьому випадку фільтрація може бути шляхом використання міжмережевих екранів.

Використання міжмережевих екранів блокує конкретний потік трафіку, але не дозволяє відокремити «хороший» трафік від «поганого».

Зворотний DDOS - перенаправлення трафіку, що використовується для атаки, на атакуючого. При достатній потужності атакується сервера дозволяє не тільки успішно відбити атаку, але і вивести з ладу сервер атакуючого.

Усунення вразливостей. Дана міра націлена на усунення помилок в системах і службах.

Нарощування ресурсів. Абсолютного захисту, природно, не дає, але є хорошим фоном для застосування інших видів захисту від DDoS-атак.

Розосередження. Побудова розподілених і дублювання систем, які не припиняють обслуговувати користувачів, навіть якщо деякі їх елементи стануть недоступні через DoS-атаки.

Ухилення. Відведення безпосередньої мети атаки (доменного імені або IP-адреси) подалі від інших ресурсів, які часто також піддаються впливу разом з безпосередньою метою атаки.

Активні заходи у відповідь. Вплив на джерела, організатора або центр управління атакою, як техногенними, так і організаційно-правовими засобами.

Використання обладнання для відображення DDoS-атак. Наприклад, DefensePro® (Radware), SecureSphere® (Imperva), Периметр (МФІ Софт), Arbor Peakflow®, Riorey, Impletec iCore і від інших виробників.

Придбання сервісу по захисту від DDoS-атак. Вважається актуальним в разі перевищення пропускної спроможності мережевого каналу.

Висновки до 2 розділу

Детальний аналіз вихідних даних щодо побудови інформаційно-телекомунікаційної системи (СЕД) надає можливість сформувати політику інформаційної безпеки та визначити вимоги до системи захисту та функціональний профіль захищеності.

Завдяки наявному переліку систем та засобів, що отримали позитивний експертний висновок існує реальна можливість сформувати перелік засобів, за допомогою якого можливо побудувати систему захисту СЕД, яка відповідатиме визначеному профілю захисту.

За результатами проведеного порівняльного аналізу 20 антивірусних продуктів, що мають експертні висновки (ДОДАТОК Б) були визначені найбільш ефективні за співвідношенням ціна/ функціональність засоби. Завдяки кращим характеристикам «Ідентифікація і автентифікація», «Розподіл обов'язків та використання ресурсів» можуть бути запропоновані до використання наступні антивіруси: "ESET Mail Security для Microsoft Exchange Server версії 4.5.X (EMSEx) " та "ESET File Security для Microsoft Windows Server версії 6.0.X (EFSW) ".

Єдиною проблемою, що не може бути розв’язана в умовах застосування тільки засобів технічного захисту інформації залишається забезпечення конфіденційності та авторства документів під час їх передавання мережами загального користування.

Розв’язку наведеної проблеми присвячене дослідження розділу 3.

3 ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ УБЕЗПЕЧЕННЯ СЕД

3.1. Завдання та функції підсистеми криптографічного захисту інформації. Аналіз загроз безпеки інформації в СЕД

Створення територіально розподілених корпоративних мереж шляхом об’єднання локальних мереж за допомогою відкритої мережі підвищує ризики реалізації загроз інформаційної безпеки двох основних типів:

• несанкціонованого доступу до внутрішніх ресурсів корпоративної локальної мережі, одержуваний зловмисником в результаті несанкціонованого входу в цю мережу;

• несанкціонованого доступу до корпоративних даних в процесі їх передачі по відкритій мережі.

Наслідком реалізації наведених загроз може бути порушення конфіденційності, цілісності та доступності інформації, а також спостережності відповідних процесів.

Забезпечення безпеки інформаційної взаємодії локальних мереж і окремих комп'ютерів через відкриті мережі, зокрема через мережу Інтернет, можливо шляхом ефективного вирішення наступних завдань:

• захист підключених до відкритих каналах зв'язку локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища;

• захист інформації в процесі її передачі по відкритих каналах зв'язку.

Як вже зазначалося у попередньому розділу, для захисту локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища зазвичай використовують мережеві екрани (МЕ), що підтримують безпеку інформаційної взаємодії шляхом фільтрації двостороннього потоку повідомлень, а також виконання функцій посередництва при обміні інформацією. МЕ розташовують на стику між локальної та відкритою мережею. Для захисту

окремого віддаленого комп'ютера, підключеного до відкритої мережі, на цьому комп'ютері встановлюють програмне забезпечення (ПЗ) мережевого екрану, і такий мережевий екран називається персональним.

Захист інформації в процесі її передачі по відкритих каналах заснований на використанні віртуальних захищених мереж VPN. Віртуальною захищеною мережею VPN (англ. *Virtual Private Network*) називають об'єднання локальних мереж і окремих комп'ютерів за допомогою відкритого зовнішнього середовища передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку даних, які обробляються.

Віртуальна захищена мережа *VPN* утворюється шляхом застосування віртуальних захищених каналів зв'язку, що побудовані на базі відкритих каналів зв'язку загальнодоступної мережі. Ці віртуальні захищені канали зв'язку називають тунелями *VPN*. Мережа *VPN* дозволяє за допомогою тунелів *VPN* з'єднати центральний офіс, офіси філій, бізнес-с нами Офіси партнерів і віддалених користувачів і безпечно передавати інформацію через Інтернет.

Оскільки, у багатьох випадках, реалізація віртуальних приватних мереж забезпечується шляхом застосування засобів та методів криптографічного захисту інформації, то уявляється доцільним розглянути питання щодо безпеки саме криптографічного захисту інформації.

Зауважимо, що у науковій літературі та публікаціях поняття криптосистема іноді ототожнюється з крипто алгоритмом та описом його застосування. У рамках дослідження під поняттям ***криптосистема*** переважно розуміється визначення введене Положенням про порядок здійснення криптографічного захисту інформації в Україні, яке затверджене Указом Президента України від 22.05.1998 № 505 [15], а саме: криптографічна система (***криптосистема***) - сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та (або) передається.

Організація захищеного інформаційного обміну за допомогою двох засобів КЗІ наведена на рисунку 3.1.

На наведеній схемі засіб КЗІ (або шифратор), до складу якого входить генератор потокового шифру та функція *f* його додавання до бітів відкритого повідомлення. У переважній більшості випадків функція додавання є звичайною бітовою операцією «Виключне АБО», що позначається символом ⊕ При цьому, правило додавання таке: 0⊕0=1⊕1=0 та 0⊕1=1⊕0=1.

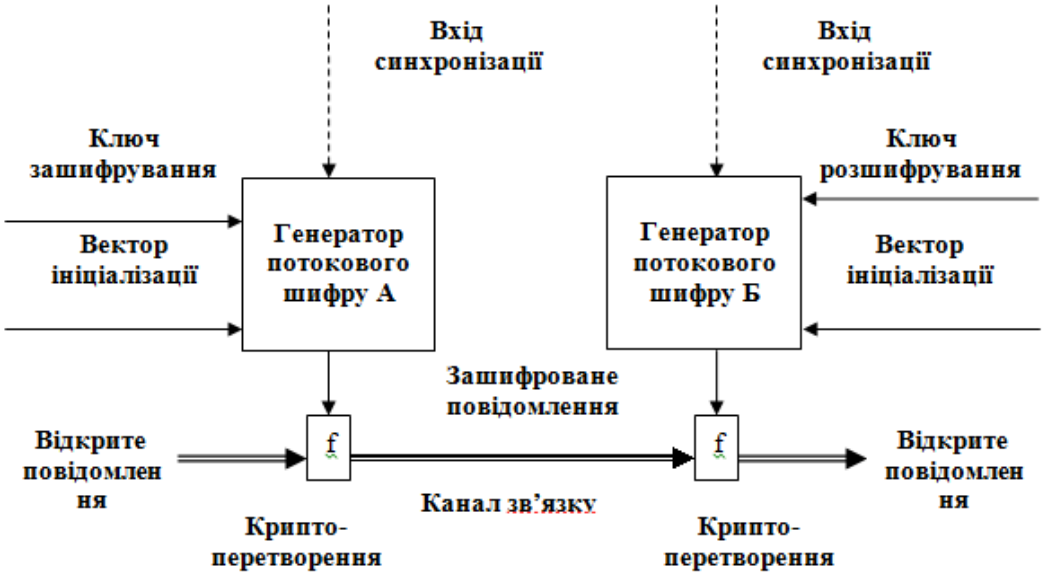

Рис. 3.1. Схема системи захищеного інформаційного обміну

Сучасна шифрувальна техніка українського виробництва характеризується малими габаритами і вагою, високою швидкістю шифрування, надійним захистом інформації (рис. 3.2 - 3.4).

Шифратор “Топаз-8000” (рис. 3.2) використовується для передачі даних в захищеному вигляді по телефонних мережах загального користування. Швидкість шифрування інформації до 115 Кбіт/сек. Виріб включається між комп'ютером (інтерфейс USB 1.1 або USB 2.0) і модемом (через з'єднувач DB-9 інтерфейсу RS-232).

Рис. 3.2. Шифратор для систем передачі даних «Топаз-8000»

Шифратор для систем передачі даних Д-300 (рис. 3.3) шифрує потоки даних із швидкістю 2 Мбіт/сек. Дана апаратура має розвинену вбудовану систему діагностики технічного стану і тестування працездатності.

Рис. 3.3. Шифратор цифрових потоків Д-300

Апаратно-програмний комплекс «Пелена» (рис. 3.6) призначений для криптографічного захисту конфіденційної інформації у відомчих (корпоративних) мережах, побудованих на базі технологій IP (протокол IP v.4). Інтерфейси комплексу відповідають рекомендаціям Ethernet IEEE 802.3-2002 100Base-TX/FX. Швидкість обробки інформації до 70 Мбіт/сек.

Рис. 3.4. Шифратор протоколу IP «Пелена»

Незалежно від призначення, експлуатаційних і технічних характеристик перераховані шифрувальні засоби об'єднує головна властивість: їх функціонування визначається алгоритмами захисту інформації – криптографічними перетвореннями відкритих повідомлень, які реалізовані програмним або апаратним способом.

Під зловмисником будемо розуміти аналітика, який має певні знання в області криптографії, оснащений деякими технічними та програмними засобами. Метою зловмисника є пошук вразливості в криптосистемі для створення технології подолання її «захисних бар'єрів».

Для криптосистем нормативно визначені чотири рівні можливостей атакуючої сторони, найбільш небезпечними для комерційних підприємств є порушники другого рівня, що добре знає особливості побудови і функціонування комплексів захисту інформації, використовує хакерські програмні засоби та найбільш потужні комп’ютери та забезпечений підтримкою потужної бізнес-структури.

Для державних підприємств, що можуть обробляти інформацію з обмеженим доступом доцільно орієнтуватися на порушника системи безпеки третього типу, який має у своєму розпорядженні наукові, технічні та фінансові можливості спеціальної служби однієї з провідних країн світу.

Загрози криптосистеми характеризують загальні можливості потенційного зловмисника при порушенні конфіденційності та імітозахищеності (цілісності, достовірності повідомлень) захищеного інформаційного обміну, а не конкретні методи (алгоритми) їх здійснення.

Особливо слід підкреслити, що важкість можливих наслідків для безпеки системи посилюється у випадку одночасної реалізації декількох загроз. Підтвердженням автентичності документа є підпис уповноваженої особи.

Окремо, слід звернути увагу, що у випадку паперовий технологій документообігу підпис документу відповідальною особою переслідує дві цілі: по-перше, необхідно надати одержувачеві можливість переконатися в істинності повідомлення, шляхом звіряння підпису з деяким зразком.

По-друге, особистим підписом забезпечується юридично значуща гарантія авторства документа (така, що може бути представлена як доказ в суді). Останній аспект особливо важливий при укладанні договорів, складанні довіреностей, зобов'язань тощо.

Якщо підробити підпис людини на папері дуже непросто, а встановити авторство підпису сучасними криміналістськими методами – технічна деталь, то з підписом електронного документа справа інша.

Використовуючи можливості програм – редакторів текстів, будь-який користувач комп'ютера може модифікувати послідовність бітів, які представляють вихідний документ.

Значне поширення в діловому світі електронних форм подання документів, електронних банківських операцій і електронної торгівлі зумовило актуальність проблеми встановлення автентичності і авторства документів в безпаперових технологіях.

Важливо відзначити, що ця проблема виникає не тільки внаслідок дій потенційних зловмисників.

Сучасні системи електронного документообігу характеризуються масовістю інформаційного обміну, що призводить до виникнення ненавмисних помилок при роботі операторів.

Виявлення подібних випадків є гарантією правильного функціонування організацій, що використовують електронний документообіг.

Підсистема безпеки системи електронного документообігу повинна захищати її легальних користувачів від таких зловмисних дій (рис. 3.5).

Небезпеку для систем документообігу становлять наступні загрози:

1. Відмова користувача А від відправленого документу.

2. Модифікація користувачем Б прийнятого документу і спроба стверджувати, що він прийнятий саме у такому вигляді.

3. Підробка – створення користувачем Б фіктивного документу і спроба стверджувати, що він надісланий конкретною посадовою особою.

4. Підроблення – втручання зловмисника в роботу системи зв'язку з метою прихованої модифікації документів, що передаються.

5. Маскування (імітація) - відправлення документів від імені легального користувача мережі, що не відправляє їх.

6. Повтор документів, що раніше передавались. Не дивлячись на те, що вживаються всі можливі заходи захисту від повторів, саме на цей метод припадає більшість випадків незаконного зняття і витрати грошей в системах електронних платежів. Дійовим методом захисту від повтору є використання імітовставки і облік вхідних повідомлень.

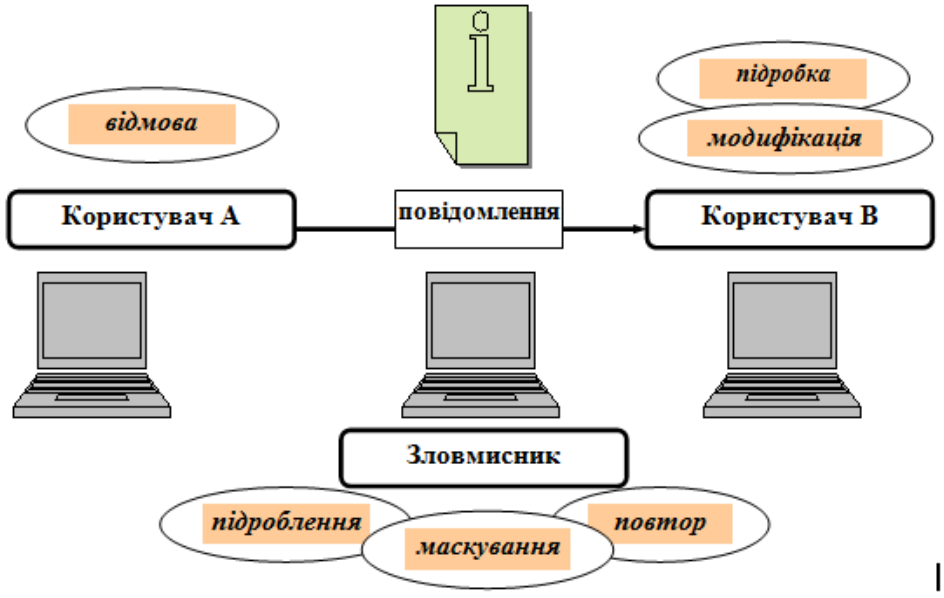

Рис. 3.5. Загрози безпеки документообігу

Для забезпечення ефективного захисту від модифікації, підробки і маскування у сучасних захищених мережах використовуються цифрові

сигнатури, що спеціально сформовані за допомогою криптографічних перетворень послідовності символів, які залежать від секретного ключа і вихідних повідомлень. Вказані механізми мають бути далі досліджені окремо.

3.2. Побудова захищених мереж на базі вітчизняних засобів шифрування

Захищені телекомунікаційні мережі забезпечують виконання багатьох завдань в державному та комерційному секторах для обміну інформацією з обмеженим доступом, управління підпорядкованими підрозділами та наявними ресурсами (включаючи сектор оборони та національної безпеки держави), здійснення різного роду технологічних операцій, таких, наприклад, як банківські операції в електронному вигляді тощо.

Захист конфіденційності інформації в цих мережах забезпечується шляхом застосування комплексу нормативно-правових та організаційно-технічних заходів та заходів, у т.ч. тих, що реалізують методи криптографічного перетворення інформації – шифрування.

Наявність значної кількості різних за призначенням та архітектурою побудови мереж не робить менш актуальною проблему побудови новітніх швидкісних багатофункціональних мереж, безпека яких гарантується застосуванням надійних сучасних засобів КЗІ.

Створенню нової мережі передує етап формування вихідних вимог щодо базових принципів її побудови та умов надання послуг конфіденційного зв’язку. Розглянемо підходи щодо визначення вимог більш детально.

По-перше, слід зазначити, що певним чином архітектура мережі, як сукупність принципів її побудови та забезпечення безпеки функціонування визначається так званою первинною транспортною мережею. Саме спосіб передавання сигналів в цій мережі (радіо, супутниковий, кабельний цифровий або аналоговий, синхронна або пакетна передача тощо) визначає певні обмеження щодо застосування технологій криптографічного захисту інформації.

Оброблення інформації з обмеженим доступом в територіально розподілених корпоративних СЕД потребує застосування захищеної транспортної мережі або побудови так званої віртуальної приватної мережі (англ. *Virtual Private Network - VPN*), яка відповідає визначеним вимогам щодо криптографічного захисту інформації.

Перший підхід може бути реалізований шляхом застосування Національної системи конфіденційного зв'язку (НСКЗ), яка відповідає підвищеним вимогам щодо забезпечення конфіденційності інформації у мережах шифрованого зв'язку, які призначені для передачі службової інформації, у плані їх архітектури (принципів, методів, способів побудови та функціонування) і забезпечення безпеки, зокрема, у частині безпеки управління ключами.

Можливість застосування цього підходу обмежується топологією мережі НСКЗ, що переважно охоплює лише обласні центри. Крім того, вартість користування мережею НСКЗ може не відповідати фінансовим можливостям підприємства.

Саме тому уявляється доцільним розглянути основні підходи до побудови власної мереж шифрованого зв'язку. Слід зазначити, що вдалий проект мережі шифрованого зв'язку поєднує високій рівень керованості мережею, високу пропускну здатність ї, головне безпеку функціонування у штатних умовах та у випадках несанкціонованого втручання в їх роботу або надзвичайних подій, що обумовлені техногенними або природними катастрофами та військовими діями.

Перш за все, звернемо увагу, мережі пакетної обробки та передачі відкритої інформації, що побудовані за допомогою комунікаційних протоколів стеку TCP/IP (включаючи, мережу Інтернет) можуть бути ефективно використані для забезпечення основних вимог щодо побудови мереж шифрованого зв'язку із застосуванням відповідних засобів КЗІ.

Зокрема, захищені мережі стеку протоколів TCP/IP, що побудовані за принципом абонентського шифрування, отримали назву віртуальних приватних мереж (англ. *Virtual Private Network – VPN*)/ Проектування *VPN* мереж передбачає декілька етапів (Таблиця 1):

- ✓ Визначення вимог (профілю безпеки) щодо захисту інформації у мережі залежно від її цінності;
- ✓ Визначення режимів роботи захищеної *VPN*, номенклатури необхідних засобів криптографічного захисту інформації, системи генерації та управління ключами;
- ✓ Опрацювання схеми резервування як інструменту забезпечення доступності на випадок збоїв та відмов обладнання;
- ✓ Реалізація основних організаційних, нормативно-правових та інженерно-технічних заходів.

Проектування системи захисту IP-трафіку, зазвичай, починається з формулювання задуму (концептуальне проектування) і закінчується розробкою і затвердженням проекту системи захисту IP-трафіку.

Задум повинен визначати об'єкт захисту, його структуру, основні загрози та принципи побудови системи захисту.

У певному сенсі концептуальне проектування системи захисту можна розглядати як пошук компромісу між функціоналом технічних рішень і обсягом організаційних заходів при заданих обмеженнях на властивості системи захисту (заданих, наприклад, вимогами).

При збільшенні функціоналу технічних рішень збільшується вартість первинних вкладень в той час як витрати на реалізацію організаційних заходів розподіляються практично рівномірно на весь період експлуатації.

Варіант графічної ілюстрації задуму для захищеної мережі представлений на рис. 3.6.

Визначення профілю безпеки здійснюється на основі загальних критеріїв безпеки, викладених в нормативному документі "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" НД ТЗІ 2.5-004-99 з урахуванням вимог до мережі, основних її функцій, результатів обстеження інформаційних і телекомунікаційних об'єктів ІТС.

Зазвичай розглядається кілька варіантів побудови системи технічних засобів, які забезпечують реалізацію заданого профілю. Серед розглянутих варіантів може вибиратися в якомусь сенсі оптимальний варіант, наприклад, за критерієм ефективності використання коштів для забезпечення вимог по заданому профілю і комплексу сервісів захисту.

Таблиця 3.1

Етапи життєвого циклу захищеної VPN

№	Назва етапу	Зміст заходів етапу
1.	Проектування мережі зв’язку	Визначення: − профілю безпеки мережі; − основних організаційних, нормативно-правових і інженерно-технічних заходів; − номенклатури засобів ТЗІ та КЗІ.
2.	Планування роботи мережі зв’язку	Розробка: − схеми захищеної VPN; − документів з забезпечення безпеки застосування VPN, включаючи правила користування засобами КЗІ та поводження з ключами до них. Підготовка витягів з плану зв’язку для кожного вузлу мережі (окремого засобу КЗІ).
3.	Розгортання ЦГКД	Інсталяція програмно-апаратного комплексу Центра генерації ключових даних та забезпечення його функціонування згідно з вимогами щодо безпеки.
4.	Авторизація IP-шифраторів в ЦГКД	Формування та запис авторизаційної інформації в ЦГКД, IP-шифратори та відповідні носії ключової інформації (НКІ).
5.	Генерація ключових даних в ЦГКД	Генерація ключових даних та запис на НКІ. Упаковка ключових документів.
6.	Розгортання центра управління (ЦУ) VPN	Інсталяція програмно-апаратного комплексу ЦУ VPN. Забезпечення зв’язності IP-шифраторів з ЦУ VPN

7.	Конфігурування IP-шифраторів	Введення профілів налаштувань IP-шифраторів згідно з документами плану захищеної VPN
8.	Розгортання захищеної VPN	Доставка IP-шифраторів та НКІ на вузли мережі. Перевірка стану. Налаштування локальної мережі. Тестування роботи тунелів.

Значною мірою ефективність використання коштів залежить від вибору засобів КЗІ, на основі яких має бути створена VPN, зокрема, у таблиці 3.2 наведені деякі шифратори вітчизняного виробництва, які встановленим порядком отримали експертні висновки щодо їх відповідності вимогам з криптографічного захисту конфіденційної інформації.

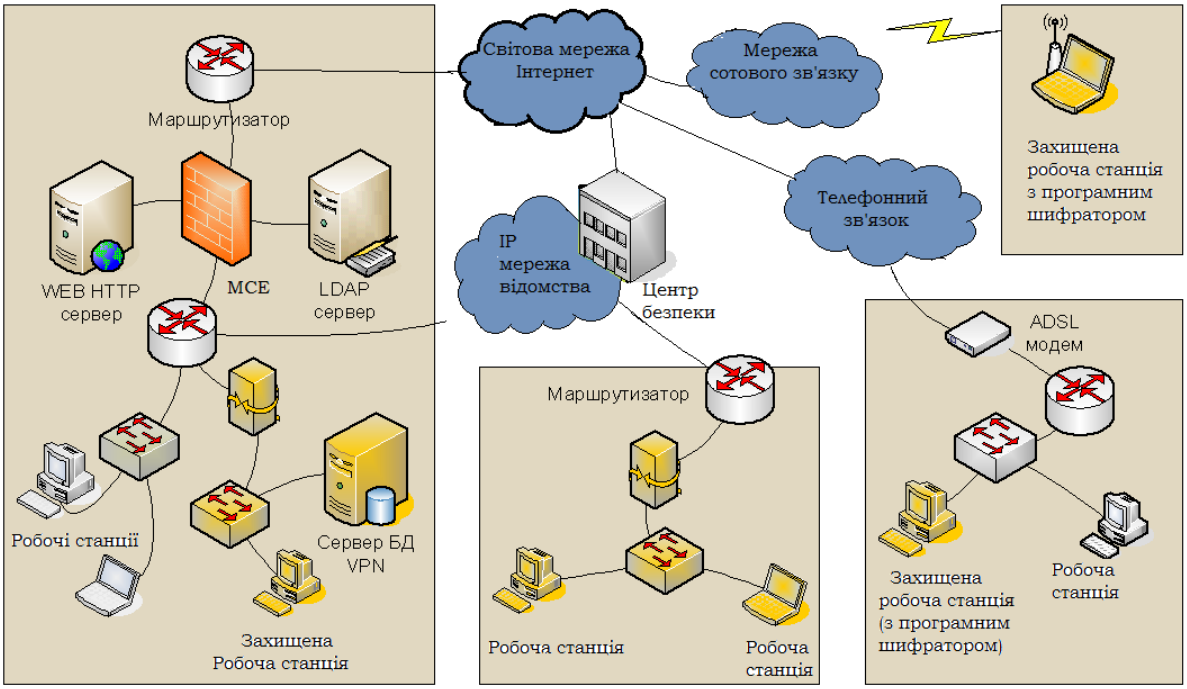

Рис. 3.6. Варіант побудови захищеної мережі

У таблиці використані наступні скорочення: АШ – Абонентське шифрування, КШ – Канальне шифрування, ЕЦП – Електронно цифровий підпис, TCP/IP- Стек протоколів, Е1 – основний потік 2048 кб/с, ”А” –ТОВ ”Автор”, ”К” – ТОВ ”НТВ Криптон”, ”Т” – ТОВ ”Трител”

Таблиця 3.2

Шифратори потокового типу для захисту конфіденційної інформації

№	Умовне найменування	Тип	Характеристики	Заявлена швидкість	Фірма
1.	”CryptoIP-459”	АШ, КШ, ЕЦП	TCP/IP, IEEE 802.3, НК- смарт карта	266 Мбит/с	А
2.	”CryptoIP-448”	АШ, КШ, ЕЦП	TCP/IP , IEEE 802.3, НК- смарт карта	6 Мбит/с	А
3.	”Оникс-200”	КШ	TCP/IP, IEEE 802.1Q, НК-МКД	94 Мб/с	К
4.	”Д-300”	КШ	E1, ITU-T, G703, G704, G706 НК-MKD	2048 Кб/с	К
5	”Пелена” В371-Е	КШ	TCP/IP, IEEE 802.3-2002 100Base-TX/FX, НК- ISO 7816	70 Мб/с	Т
6	”Гном” В271-Е	АШ	TCP/IP, IEEE 802.1Q , НК- ISO 7816	30 Мб/с	Т

Вибір шифраторів залежить від конкретних умов їх застосування, тому у рамках роботи не розглядається.

До складу системи захисту мережі входять власне IP-шифратори з урахуванням, що на кожен об'єкт, що захищається (сегмент об'єкта) виділяється один або більше IP-шифраторів в залежності від необхідного рівня доступності та пропускної здатності окремих елементів структури мережі.

IP-шифратори можуть використовуватися як абонентські пристрої. Таке їх використання є кращим, оскільки забезпечує можливість адресного визначення прав доступу і відповідальності за використання ресурсів захищеної мережі, більш ефективного вирішення питань блокування несанкціонованого доступу.

Один або кілька IP-шифраторів, використовуваних на одному об'єкті, можуть входити до складу комплексу засобів захисту (КЗЗ) на об'єкта інформаційної діяльності. При цьому, IP-шифратори можуть стати доповненням (увійти до складу) наявної КСЗІ. Якщо відповідну КСЗІ ще належить створити, то її доцільно будувати з урахуванням забезпечуваних IP-шифратором функцій безпеки. Використання IP-шифраторів, як і інших засобів КЗІ, в багатьох випадках дозволяє зменшити розмірність зон, послабити вимоги до КСЗІ і знизити загальні витрати на побудову КСЗІ об'єкта.

Визначення номенклатури засобів криптографічного захисту інформації здійснюється на основі розроблених технічних рішень, результатів обстеження об'єктів захисту з урахуванням необхідної пропускної спроможності інформаційних напрямків і вимог щодо забезпечення необхідного рівня доступності сервісів захищеної VPN.

Режими роботи захищеної VPN визначаються залежно від умов її застосування.

Всі елементи захищеної VPN в кожен момент часу можуть працювати в одному з трьох доступних режимів:

- ✓ Режим симетричної ключової системи та попереднього розподілу ключів.
- ✓ Режим асиметричною ключової системи з використанням центру сертифікації ключів (ЦСК).

За необхідності режим роботи VPN може бути змінений. Перехід з одного режиму в інший може бути обумовлений змінами умов функціонування самої мережі або зовнішніх умов (особливі ситуації). При виборі режиму роботи захищеної VPN враховуються особливості роботи VPN в кожному режимі.

3.3 Методи та засоби формування та перевірки ЕЦП

Електронний цифровий підпис (ЕПЦ) – це блок інформації, який логічно поєднаний з файлом даних автору і захищає файл від модифікації. Електронний цифровий підпис є якісно новим етапом в розвитку сучасного документообігу.

Сертифікат відкритого ключа у стандарті X.509 містить наступні дані:

- ✓ найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);
- ✓ позначку, що сертифікат виданий в Україні;
- ✓ унікальний реєстраційний номер сертифіката ключа;
- ✓ основні дані (реквізити) підписувала-власника особистого ключа;
- ✓ дату і час початку та закінчення строку чинності сертифіката;
- ✓ відкритий ключ;
- ✓ найменування криптоалгоритму, що використовується власником особистого ключа;
- ✓ інформацію про обмеження використання підпису.

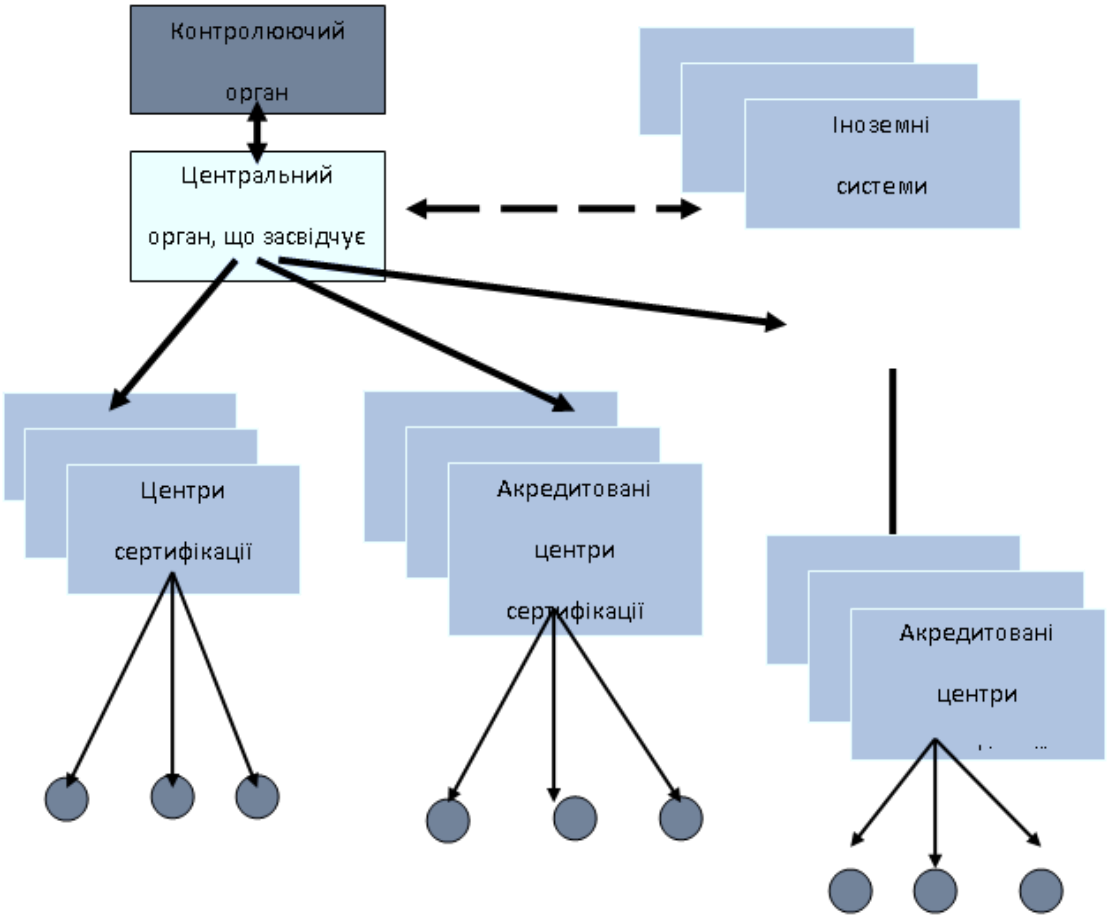

Рис. 3.7. Структура системи електронного цифрового підпису

Сертифікат ключа підпису в електронному вигляді, підписаний секретним ключем ЦСК, направляється користувачеві ключа підпису і вноситься (по його бажанню) до реєстру сертифікатів ключів підписів ЦСК.

Засвідчення чинності відкритого ключа здійснюється шляхом формування сертифіката відкритого ключа – документа, що видається центром сертифікації ключів. Посилений сертифікат відкритого ключа видається акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Сертифікат ключа містить найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру); зазначення, що сертифікат виданий в Україні; унікальний реєстраційний номер сертифіката ключа; основні дані (реквізити) підписувача – власника особистого ключа; дату і час початку та закінчення строку чинності сертифіката; відкритий

ключ; найменування криптографічного алгоритму, що використовується власником особистого ключа; інформацію про обмеження використання підпису.

В даний час існують наступні пристрої зберігання особистого ключа – дискети, смарт-карти, e-token тощо. Найбільш захищений спосіб зберігання закритого ключа - зберігання на смарт-картці. Для того, щоб використовувати смарт-карту, користувачеві необхідно не тільки її мати, але й ввести PIN-код, тобто, виходить двофакторна автентифікація.

Особистий ключ ЕЦП формується на основі випадкових чисел, які генеруються датчиком випадкових чисел, а відкритий - обчислюється з особистого ключа так, щоб отримати другий з першого було неможливо.

Особистий ключ генерується виходячи з вимог, встановлені алгоритмом криптографічного перетворення індивідуально для кожного клієнта. Збереження конфіденційності цієї інформації повністю залежить від клієнта. Клієнт повинен самостійно забезпечити безпеку зберігання і використання особистого ключа щоб уникнути підробки його ЕЦП іншими особами.

При підписанні електронного документу його початковий зміст не змінюється, а додається блок даних - ЕЦП. Отримання цього блоку можна розділити на два етапи:

На першому етапі за допомогою спеціальної математичної функції – функції хешування обчислюється так званий «відбиток повідомлення» (англ. *message digest*). Цей відбиток має такі особливості:

- ✓ фіксовану довжину, незалежно від довжини повідомлення;
- ✓ унікальність відбитку для кожного повідомлення;
- ✓ неможливість відновлення повідомлення по його відбитку.

Таким чином, якщо документ був модифікований, то зміниться і його відбиток, що відобразиться при перевірці ЕЦП.

На другому етапі відбиток документу шифрується за певного алгоритму і особистого ключа автора. Розшифрувати ЕЦП і отримати початковий відбиток,

який відповідатиме документу, можна тільки використовуючи сертифікат відкритого ключа автора.

Управління розподілом ключів не може бути відокремлене від процесу підтримки відкритих ключів так само, як використання тільки пари ключів для шифрування не може гарантувати надійного інформаційного обміну.

За даними останніх досліджень впровадження технологій шифрування з відкритими ключами на корпоративному рівні без використання цифрових сертифікатів представляється малоефективним. Внаслідок необхідності сертифікатів, що підтверджують особу власника відкритого ключа, керування сертифікатами є невід'ємною частиною системи з відкритими ключами.

Для зменшення довжини ЕЦП використовують хеш функцію.

Асиметричні схеми цифрового підпису спираються на обчислювально складні завдання, для підвищення їх криптостійкості потрібно збільшувати довжину ключів.

Розподіл ключів - найвідповідальніший процес в управлінні ключами. До нього висуваються наступні вимоги: оперативність та точність розподілу, надійність розподілу ключів.

✓ Механізм запиту-відповіді, коли один з абонентів включає в свої повідомлення елемент, що неможливо передбачити (запит). Дії другого абонента полягають в наперед обумовленій модифікації запиту та додавання його до своїх повідомлень. Недоліком такого методу є можливість встановлення закономірності запит-відповідь та необхідність попереднього встановлення правил модифікації запиту.

✓ Механізм часової відмітки - "часовий штемпель", що передбачає фіксацію часу для кожного повідомлення. В такому випадку кожен користувач може визначити точний час створення повідомлення.

В реальних інформаційних системах, наприклад, в системах оплати платіжними картками, використовується саме механізм додавання часової відмітки, причому часовий інтервал може становити від одної до декількох

хвилин. Таким чином, задача управління ключами зводиться до пошуку такого протоколу розподілу ключової інформації, який забезпечує:

- ✓ можливість відмови від центру розподілу ключів;
- ✓ взаємна верифікація учасників сеансу зв'язку;
- ✓ підтвердження достовірності сеансу механізмом запиту-відповіді з використанням програмних чи апаратних засобів;
- ✓ використання при обміні ключами мінімальної кількості повідомлень.

Програмно-технічні комплекси центрів сертифікації ключів призначені для забезпечення реалізації центром сертифікації ключів регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів ЦСК, надання послуг фіксування часу, надання користувачам засобів ЕЦП та шифрування, а також засобів генерації особистих і відкритих ключів.

3.4. Розробка пропозиції щодо забезпечення безпеки СЕД

На поточний час у державному та приватному секторах використовується декілька систем, які мають експертні висновки щодо їх відповідності вимогам НД ТЗІ. Підтримка цих продуктів з боку вітчизняних розробників програмних систем створює позитивне підґрунтя для їх впровадження практичного застосування. У той же час, існує проблема вибору найбільш придатної системи для цілей конкретних підприємств та, головне, визначення критеріїв такого вибору.

В якості критеріїв можуть бути обрані універсальні характеристики програмних систем, зокрема, функціональність; продуктивність, масштабуємість, інтегрованість, ліцензійна/ цінова політика, складність та вартість масштабування, вимоги до апаратних та програмних платформ тощо.

Специфічним критерієм у нашому випадку є досягнутий рівень інформаційної безпеки, що реалізується вбудованим КЗЗ.

Залежно від умов застосування, необхідно визначити вагові показники критеріїв та здійснити експертну оцінку (внутрішніми консультанти або незалежними експертами) ступеню відповідності кожної системи електронного документообігу кожному критерію (таблиця 3.3).

Таблиця 3.3

Орієнтовні критерії для оцінки СЕД

№№	Критерій	Вага	Системи електронного документообігу			
			$СЕД_1$	$СЕД_2$	…	$СЕД_N$
1.	Функціональність	W_1	E_{11}	E_{21}	…	E_{N1}
2.	Продуктивність	W_2	E_{12}	E_{22}	…	E_{N2}
3.	Масштабуємість	W_3	E_{13}	E_{23}	…	E_{N3}
4.	Вартість масштабування	W_4	E_{14}	E_{24}	…	E_{N4}
5.	Цінова політика	W_5	E_{15}	E_{25}	…	E_{N5}
6.	Фактичний рівень ІБ	W_6	E_{16}	E_{26}	…	E_{N6}

Оцінки за кожним з критеріїв, помножені на ваговий коефіцієнт цього критерію, підсумовуються. Система, яка набрала найбільшу кількість балів, є оптимальною для даної організації.

$$I_{\text{СЕД}} = ind \sum_{j=1}^{N} E_{ij} \cdot W_j \text{, де функція } ind(\dots) \text{ є номером СЕД.} \quad (3.3)$$

На поточний час вітчизняними розробниками програмних систем та засобів пропонується декілька СЕД (у т.ч. АСКОД-К, АСКОД WEB, eDocs, Мегаполіс.Документообіг-ДСК, Megapolis.DocNet), які отримали позитивні експертні висновки за результатами державної експертизи у сфері технічного захисту інформації. Ці системи вже працюють у деяких державних установах та підприємствах, тому уявляється доцільним проаналізувати досягнутий ними рівень захисту та визначити рекомендації їх подальшого вдосконалення.

З переліку технічних засобів на сайті Держспецзв'язку України можливо з'ясувати характеристики функціональних профілів захисту зазначених СЕД та

провести їх порівняльний аналіз. Для зручності дослідження дані наведені у вигляді таблиці та згруповані по критеріях (таблиця 3.4).

Умовні позначення у таблиці наступні: (-) означає відсутність у профілі зазначеного критерію, позначка (=) відповідає однаковим значенням критерію для аналізованих систем, позначення [Ц] відповідає кращий характеристиці у системи під номером Ц. Додатково, сірим кольором відтінені кращі значення критерії захисту.

За результатами порівняльного аналізу даних, що наведені у таблиці 3.4 можливо зробити наступні висновки.

Значна кількість показників по критеріях збігаються, що свідчить про однакові підходи різних розробників щодо формування моделі загроз СЕД та моделі порушника. Тобто можливо стверджувати про наявність у певному сенсі еталонної моделі.

У той же час, можливо констатувати, що найбільш потужний вбудований комплекс засобів захисту має СЕД Мегаполіс. Документообіг-ДСК, переважна кількість критеріїв якого (17) має вищий порівняно з іншими системами рівень безпеки або рівний. Ця СЕД лише за критеріями «Конфіденційність при обміні» та «Розподіл обов'язків» поступається іншим.

Оскільки зазначена СЕД була створена в інтересах побудови системи електронної взаємодії органів виконавчої влади з обміном інформацією з грифом «Для службового користування», тому її застосування на підприємством є доцільним, перш за все, у визначених законодавством випадках. Саме ця СЕД після доопрацювання за критеріями «Конфіденційність при обміні» та «Розподіл обов'язків» може бути обрана за основу для створення перспективної системи електронного документообігу у державних установах.

Слід також приділити особливу увагу СЕД АСКОД WEB та Megapolis.DocNet, що побудовані за технологією «клієнт-сервер», яка використовує лише одну копію програмного продукту, яка інсталюється на сервері, а на клієнтській частині розміщується лише браузер, за допомогою якого здійснюється перегляд та редагування документів.

Такий підхід до архітектури СЕД дозволяє уникнути проблеми «багатьох копій» на різних робочих місцях. А це, в свою чергу, є актуальним з точки зору розмежування доступу різних користувачів до певної інформації.

Нажаль, розробники перерахованих систем не надають вичерпної інформації щодо організаційних заходів щодо забезпечення інформаційної безпеки, а також технічних аспектів побудови територіально-розподілених систем на основі захищених продуктів.

Для формування пропозицій щодо убезпечення систем скористаємося результатами розробки моделі загроз, яка наведена у попередніх розділах роботи.

По-перше, слід убезпечити периметр мережі від кібернетичних втручань з боку мережі загального користування. У випадку обробки документів, що містять інформацію з обмеженим доступом, безпеку доцільно забезпечити шляхом застосування програмно-апаратних засобів потокового шифрування, які мають експертні висновки щодо їх відповідності вимогам нормативних документів з питань КЗІ.

Таблиця 3.4

Порівняльний аналіз сучасних захищених СЕД вітчизняного виробництва

Функціональні профілі безпеки							
№№	**Критерії безпеки**	**Системи ЕДО**					**Краща СЕД за критерієм**
		1.**АСКОД-К**	2.**АСКОД WEB**	3.**eDocs**	4.**Мегаполіс. Документообіг-ДСК**	5.**Megapolis.DocNet**	
Критерії конфіденційності							
1.	Довірча конфіденційність	(-)*	(-)	(-)	КД-2	(-)*	
2.	Адміністративна конфіденційність	КА-2	КА-2	КА-2	КА-2	КА-2	(=)**
3.	Повторне використання об'єктів	КО-1	КО-1	КО-1	КО-1	КО-1	(=)
4.	Конфіденційність при обміні	(-)	(-)	(-)	(-)	КВ-1	[5]
Критерії цілісності							
5.	Довірча цілісність	(-)	(-)	(-)	ЦД-1	(-)	[4]
6.	Адміністративна цілісність	ЦА-1	ЦА-1	ЦА-1	ЦА-2	ЦА-1	[4]
7.	Відкат	ЦО-1	ЦО-1	ЦО-1	ЦО-1	ЦО-1	(=)
8.	Цілісність при обміні	(-)	(-)	(-)	ЦВ-2	ЦВ-2	[4],[5]

Критерії доступності							
9.	Використання ресурсів	ДР-1	ДР-1	(-)	ДР-1	(-)	[1],[2],[[4]
10.	Стійкість до відмов	ДС-1	ДС-1	ДС-1	ДС-1	(-)	(=)
11.	Гаряча заміна	ДЗ-1	ДЗ-1	ДЗ-1	ДЗ-1	ДЗ-1	(=)
12.	Відновлення після збоїв	ДВ-1	ДВ-1	ДВ-1	ДВ-1	ДВ-1	(=)
Критерії спостереженості							
13.	Реєстрація	НР-2	НР-2	НР-2	НР-2	НР-2	(=)
14.	Ідентифікація і автентифікація	НИ-2 НИ-3	НИ-2 НИ-3	НИ-2	НИ-3	НИ-1 НИ-2	[1],[2],[4]
15.	Достовірний канал	НК-1	НК-1	НК-1	НК-1	НК-1	(=)
16.	Цілісність КЗЗ	НЦ-1	НЦ-1	НЦ-1	НЦ-2	НЦ-1	[4]
17.	Розподіл обов'язків	НО-3	НО-3	НО-3	НО-2	НО-1	[1],[2],[3]
18.	Самотестування	НТ-2	НТ-2	НТ-2	НТ-2	НТ-2	(=)
19.	Автентифікація відправника	НА-2	НА-2	НА-2	НА-2	НА-2	(=)
20.	Автентифікація отримувача	(-)	(-)	(-)	НП-2	НП-2	[4],[5]

В разі обробки відкритої, але дуже корисної для підприємства інформації кожен окремий фрагмент мережі доцільно убезпечити шляхом застосування належним чином налаштованих файерволів.

Безумовною вимогою щодо убезпечення СЕД та захисту її від шкідливих кодів є застосування системи антивірусного захисту, яка має необхідний висновок щодо їх відповідності нормативам з технічного захисту інформації, як це було зазначено у попередніх розділах.

Розмежування прав доступу до інформаційних ресурсів може бути забезпечене за допомогою відповідних механізмів атестованої операційної системи.

Висновок до 3 розділу

1. Для забезпечення конфіденційності інформації, що обробляється у системах електронного документообігу доцільно використовувати сучасні засоби шифрування стеку протоколів TCP/IP, які мають експертні висновки щодо відповідності вимогам нормативних документів з питань криптографічного захисту інформації.

2. Обов’язковим реквізитом електронного документа є електронний цифровий підпис. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа Метою застосування систем цифрового підпису є автентифікація інформації – захист учасників інформаційного обміну від нав’язування хибної інформації,

встановлення факту модифікації інформації, яка передається або зберігається, й отримання гарантії її справжності, а також вирішення питання про авторство повідомлень.

3. Правові основи для застосування електронних документів у цивільних відносинах вперше закладено Цивільним кодексом України, який прирівнює електронні документи до паперових і допускає засвідчення їх електронним підписом.

Безпека використання електронного цифрового підпису забезпечується тим, що засоби, які використовуються для роботи з ним, проходять експертизу і сертифікацію в уповноваженому державному органі, яка гарантує неможливість злому та підробки ЕЦП.

4. Проведено узагальнення основних заходів щодо побудови та забезпечення надійного функціонування захищеної мережі VPN на основі засобів КЗІ вітчизняного виробництва та визначений відповідний перелік, який може бути корисним у нагоді побудови розподіленої СЕД, у якій обробляється інформація з обмеженим доступом.

5. У рамках роботи запропоновано критерій вибору системи електронного документообігу на основі вагових показників критеріїв що мають визначатися внутрішніми консультанти або незалежними експертами.

6. За результатами порівняльного аналізу поширених захищених СЕД можливо можливо зробити висновок, що найбільш потужний вбудований комплекс засобів захисту має СЕД Мегаполіс. Документообіг-ДСК, який по 17 критеріям захищеності має порівняно з іншими системами вищий рівень безпеки або рівний.

✓ ВИСНОВКИ

Проведені в роботі дослідження направлені на покращення методичного забезпечення робіт з побудови комплексного захисту систем електронного документообігу (СЕД) на підприємстві, включаючи застосування легітимного цифрового підпису.

У ході розв’язання поставлених задач були отримані наступні результати:

- ✓ розглянуто роль та задачі нормативного регулювання у сфері захисту інформації;
- ✓ визначені пріоритети та структура побудови політики безпеки СЕД;
- ✓ проаналізовані сучасні механізми технічного захисту інформації, а також технології шифрування та формування/перевірки ЕЦП;
- ✓ запропонований підхід щодо визначення найбільш придатних складових системи захисту;
- ✓ проведено аналіз технологій побудови ЦСК.

На основі аналізу архітектури та функціональних можливостей поширеного програмно-технічного комплексу ЦСК визначені особливості його побудови та підходи щодо захисту інформації.

Проведено узагальнення основних заходів щодо побудови та забезпечення надійного функціонування захищеної мережі VPN на основі засобів КЗІ вітчизняного виробництва та визначений відповідний перелік заходів, що може бути корисним у нагоді побудови розподіленої СЕД, у якій обробляється інформація з обмеженим доступом.

У рамках роботи запропоновано критерій вибору СЕД на основі вагових показників критеріїв що можуть визначатися спеціалістами підприємства або незалежними експертами.

✓ ПЕРЕЛІК ПОСИЛАНЬ

1. Персианов В.В. Электронное офисное делопроизводство: учебник / Персианов В.В., Киреева Е.З., Казакова М.Н. Директ-Медиа, - 2016. –326с.
2. Мельник Т. Електронний документообіг та електронний підпис //Бухгалтерський облік і аудит. - 2008. - № 7. - С. 47-53.
3. Про електронні документи та електронний документообіг : Закон України від 22.05.03 р. № 851-IV.
4. Шпірко А. Запровадження та ефективне використання електронного документообігу й електронного підпису в Україні: проблеми, нові можливості, шляхи розвитку //Вісник Національного банку України. - 2005. - № 3. - С. 36-41
5. Янчева Л. Електронна комерція: організація та облік: навч.посіб. / Харківський держ. ун-т харчування та торгівлі. — Х. : ХДУХТ, 2008. — 231с
6. Брижко В. Електронна комерція: правові заходи та заходи удосконалення: монографія / Брижко В., Новицький А., Цимбалюк В., Швець М. / Науково-дослідний центр правової інформатики Академії правових наук України. — К. : НДЦПІ АПрНУ, 2008. — 149с.
7. Про електронні документи та електронний документообіг : Закон України від 22.05.03 № 851-IV.
8. Цивільний кодекс України від 16.01.2003 р. № 435-IV.
9. Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу : Постанова Кабінету Міністрів України від 26.05.04 р. № 680.
10. Голубенко О.Л. Політика інформаційної безпеки: підручник / Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є.,– Луганськ: вид-во СНУ ім.. В.Даля, 2009, - 300с.
11. Гулак Г.М., Методологія захисту інформації: навчально-методичний посібник. / Довгань О.Д., Гулак Г.М., Гринь А.К., Мельник С.В.–К.: Наук.-ви. Центр НА СБ України, 2012. – 184 с.

12. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 р. № 80/94-ВР.
13. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України 23.02.2006 року № 3475-IV
14. Шорошев В.В. Основи формування політики безпеки комп'ютерних систем, -К, Бизнес и безопасность, 2006, 141с., іл.
15. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.98 р. № 505/98.
16. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації : наказ Державної служби спеціального зв'язку та захисту інформації України від 20.07.07 р. № 141. – (Зареєстрований Міністерством юстиції України від 30.07.07 р. № 862/14129).
17. Гулак Г.М. Основи криптографічного захисту інформації : підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук, Вінниц. нац. техн. ун-т.– Вінниця : ВНТУ, 2011.– 198 с.
18. Про Національну систему конфіденційного зв'язку : *Закон України* від 10.01.2002 № 2919-III.
19. Про систему електронних підписів, що застосовується в межах Співтовариства: Директива 1999/93/ЄС Європейського парламенту та Ради від 13.12.99 р.
20. Щодо стану роботи з адаптації законодавства України до законодавства Європейського Союзу: Рішення шостого засідання Міжвідомчої координаційної ради з адаптації законодавства України до законодавства ЄС від 28.09.01 р.
21. Про електронний цифровий підпис : Закон України від 22.05.03 р. № 852-IV.
22. Про затвердження Положення про центральний засвідчувальний орган : Постанова Кабінету Міністрів України від 28.10.04 р. № 1451.
23. Про затвердження Порядку акредитації центру сертифікації ключів : Постанова Кабінету Міністрів України від 13.07.04 р. № 903.
24. Про затвердження Порядку обов'язкової передачі документованої інформації: Постанова Кабінету Міністрів України від 28.10.04 р. № 1454.

25. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності : Постанова Кабінету Міністрів України від 28.10.04 р. № 1452.
26. Про затвердження Правил посиленої сертифікації : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.05 р. № 3. – (Зареєстрований Міністерством юстиції України від 27.01.05 р. № 104/10384.
27. Про затвердження Правил проведення робіт із сертифікації засобів захисту інформації: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.007 р. № 75/91. – (Зареєстрований Міністерством юстиції України від 14.05.07 р. № 498/13765).
28. Про затвердження Положення про державну експертизу у сфері криптографічного захисту інформації : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.06.08 р. № 100. – (Зареєстрований Міністерством юстиції України від 16.07.2008 р. № 651/15342).
29. Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису : наказ Міністерства юстиції України та Державної служби спеціального зв'язку та захисту інформації України від 20.08.12 р. № 1236/5/453. – (Зареєстрований Міністерством юстиції України від 20.08.12 р. № 1398/21710).
30. Про затвердження Вимог до форматів криптографічних повідомлень : наказ Державної служби спеціального зв'язку та захисту інформації України від 18.12.12 р. № 739. – (Зареєстрований Міністерством юстиції України від 14.01.13 р. № 108/22640.Про затвердження Регламенту роботи центрального засвідчувального органу: наказ Міністерства юстиції України від 29.01.13 р. № 183/5. – (Зареєстрований Міністерством юстиції України від 30.01.13 р. № 191/22723).