МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію
Зав. кафедрою УІКБ
доктор економічних наук, доцент
_____ С.В. Легомінова
____ _____ 2020р.

До захисту
Зав. кафедрою УІКБ
доктор економічних наук, доцент
_____ С.В. Легомінова
____ _____ 2020р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему:

ПОБУДОВА СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

СТУДЕНТ Бондарчук Олександр Сергійович _____
(підпис)

КЕРІВНИК к.в.н., доцент Якименко Юрій Михайлович _____
(підпис)

НОРМОКОНТРОЛЕР к.т.н., с.н.с. Щебланін Юрій Миколайович _____
(підпис)

Київ 2020 р.

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

Освітньо-кваліфікаційний рівень - магістр
Галузь знань - «12 Інформаційні технології»
Спеціальність -«125 Кібербезпека»
Спеціалізація - «Управління інформаційною безпекою»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
д.е.н.,доцент_____ С.В.Легомінова
(підпис)
"___"_____ 2019 р.

ЗАВДАННЯ
на дипломну роботу

Студенту **Бондарчуку Олександру Сергійовичу**

1.**Тема роботи** "**Побудова системи управління інформаційної безпеки підприємства**", затверджена наказом по університету від "14" листопада 2019 р. № 518.
2. **Термін здачі** студентом закінченої дипломної роботи 28 грудня 2019р.
3. **Вихідні дані до роботи**:
- сформулювати основні вимоги щодо побудови системи управління інформаційної безпеки підприємства,
- проаналізувати методичні матеріали щодо розробки і провести дослідження досвіду щодо впровадження систем управління інформаційною безпекою,
- розробити рекомендації щодо вдосконалення процесів розробки та впровадження системи управління інформаційною безпекою (для вибраного прикладу).

4. **Склад розрахунково-пояснювальної записки** (перелік питань до розробки).
1. Аналіз вимог щодо розробки системи управління інформаційної безпеки підприємства.
2. Аналіз методичних матеріалів щодо розробки системи управління інформаційної безпеки підприємства.
3. Дослідження процесів управління інформаційною безпекою підприємства та розробка рекомендацій.

5. **Перелік обов'язкових демонстраційних креслень**:
1. Схема вимог щодо розробки системи управління інформаційної безпеки підприємства.
2. Схема управління інформаційною безпекою підприємства.
3. Структурно-логічна схема дій керівництва підприємства по розробці системи управління інформаційною безпекою.
4. Алгоритм оцінки ефективності процесів розробки та впровадження

системи управління інформаційною безпекою.
5. Рекомендації щодо вдосконалення процесів розробки та впровадження системи управління інформаційною безпекою (для вибраного прикладу).
6. Презентація доповіді, виконана в Microsoft PowerPoint.

6. **Термін виконання дипломної роботи**:
подання закінченої роботи керівнику 24 грудня 2019 року.
подання роботи на рецензію 28 грудня 2019 року.
7. **Дата видачі завдання** 15.11.2019 року.

Керівник _____ Якименко Юрій Михайлович
(підпис) (прізвище, ім'я, по-батькові)

Завдання прийняв для виконання _____ Бондарчук Олександр Сергійович
(підпис) (прізвище, ім'я, по-батькові)

Календарний план

№ з/п	Назва етапів магістерської атестаційної роботи	Термін виконання етапів	Відмітка про виконання
1.	Підбор науково-технічної літератури.	18.11.2019 р.	
2.	Аналіз та систематизація матеріалу. Вступ	22.11.2019 р.	
3.	Аналіз вимог щодо розробки системи управління інформаційної безпеки підприємства.	29.11.2019 р.	
4.	Аналіз методичних матеріалів щодо розробки системи управління інформаційної безпеки підприємства.	6.12.2019 р.	
5.	Дослідження процесів управління інформаційною безпекою підприємства та розробка рекомендацій.	13.12.2019 р.	
6.	Підготовка демонстраційного матеріалу	20.12.2019 р.	
7.	Оформлення та друк пояснювальної записки	28.12.2019 р.	
8.	Оформлення презентацій	3.01.2020 р.	
9.	Отримання відгука та рецензії на роботу	9.01.2020 р.	
10.	Попередній захист на кафедрі	9.01.2020 р.	
11.	Захист в ДЕК	14.01.2020 р.	

РЕФЕРАТ

Дипломна робота присвячена дослідженню проблем побудови системи управління інформаційної безпеки в організації. Робота складається зі переліку умовних позначень та скорочень, вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг роботи становить 82 аркуша.

Об'єктом дослідження є забезпечення інформаційної безпеки підприємства.

Мета роботи – розробити рекомендації щодо вдосконалення процесів розробки та впровадження системи управління інформаційною безпекою, провести дослідження досвіду щодо впровадження систем управління інформаційною безпекою та розробити рекомендації.

Як результат у роботі проведено аналіз основних методів побудови системи управління інформаційною безпекою; досліджено особливості систем управління інформаційною безпекою підприємства; дослідженні стандарти побудови СУІБ на підприємстві

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ – інформаційна безпека
УІБ - управління інформаційною безпекою
СУІБ – система управління інформаційною безпекою
АСУ – автоматизована система управління
ІСУ – інформаційна система управління
НБУ – Національний банк України

ВСТУП

Актуальність теми. Останнім часом все чіткіше стає помітний деякий перекіс: кажучи про інформаційну безпеку, все в першу чергу мають на увазі захист від вірусів і хакерів. Але якщо попросити фахівців з безпеки розповісти про те, що їх хвилює, то найбільшу заклопотаність викликають дії інсайдерів. Так, за даними досліджень, збиток від необережних і неправомірних дій співробітників в кілька разів перевищує за обсягом заподіяної шкоди збиток від дії вірусів і т.п. «Хакерських» атак. І незважаючи на те, що кількість інцидентів з вини зовнішніх і внутрішніх порушників спокою - можна порівняти.

У внутрішнього порушника, особливо якщо його дії свідомі, а не є помилкою, стимулів може бути більше: від банальної образи до матеріальної вигоди в разі підкупу з боку конкурентів. А можливостей у нього - не в приклад більше. Він уже є легальним користувачем мережі, має доступ в т.ч. і до конфіденційних ресурсів організації, може користуватися корпоративними додатками і робочою в них даними на законних підставах.

Саме тому досить актуальним є питання в побудові системи управління інформаційною безпекою, щоб уреголювати рух інформації в підприємстві та контролювати росповсюдження секретної інформації на підприємстві.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

- сформулювати основні вимоги щодо побудови системи управління інформаційної безпеки підприємства,
- проаналізувати методичні матеріали щодо розробки і провести дослідження досвіду щодо впровадження систем управління інформаційною безпекою,
- розробити рекомендації щодо вдосконалення процесів розробки та впровадження системи управління інформаційною безпекою

Об’єктом дослідження є система управління інформаційною безпекою підприємства.

Предметом дослідження є організація управління інформаційною безпекою підприємства в сучасних умовах України.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, інфраструктури та персоналу підприємства у відповідності до цілей бізнесу, можливостей та ресурсів підприємства.

1. Аналіз вимог щодо розробки системи управління інформаційної безпеки підприємства.

У цьому розділі буде розглянуто основні міжнародні та українські стандарти інформаційної безпеки та побудови системи управління інформаційною безпекою. Також проаналізовано розвиток міжнародних стандартів з плином часу та визначено важливість їх застосування в підприємстві.

1.1. Вимоги міжнародних стандартів щодо розробки системи управління інформаційною безпекою.

Найбільш поширеним і загальновизнаним у світі збіркою рекомендацій в сфері захисту інформації є стандарт ISO / IEC 27001 Information technology - Security techniques - Information security management systems - Requirements.

Стандарт ISO / IEC 27001 по праву вважається найбільш концептуальним і комплексним. Його історія почалася в 80-х роках минулого століття, коли Центр комп'ютерної безпеки Департаменту торгівлі і промисловості Великобританії опублікував рекомендації DTI CCSC User's Code of Practice. Документ був розроблений на основі політики інформаційної безпеки компанії Royal Dutch Shell (нині Shell). Він представляв собою перелік ключових заходів інформаційної безпеки, яким необхідно було дотримуватися при роботі з корпоративними мейнфреймами. У 1993 році документ був доопрацьований і опублікований Британським інститутом стандартів (British Standards Institute, BSI) під назвою Code of Practice for Information Security Management. Результатом подальшого доопрацювання документа BSI став виданий в 1995 році британський національний стандарт BS 7799: 1995, що містив актуалізований перелік рекомендованих для застосування в організаціях заходів захисту інформації. Однак вибір оптимальних для конкретної організації заходів захисту інформації залишався за рамками стандарту. Для вирішення цієї проблеми в 1998 році BSI розробив стандарт-додаток - BS 7799 Part 2: 1998. Саме його можна вважати прямим попередником стандарту ISO / IEC 27001.

Важливою подією в подальшій історії розвитку стандартів BS 7799 стало їх визнання з боку Міжнародної організації зі стандартизації (International Organization for Standardization, ISO) і Міжнародної електротехнічної комісії (International Electrotechnical Commission, IEC). У 2000 році технічним комітетом, створеним під егідою цих організацій, був прийнятий стандарт ISO / IEC 17799: 2000, що є розвитком стандарту BS7799-1. У 2005 році аналогічну процедуру пройшов стандарт BS 7799 Part 2: 1998, який отримав назву ISO / IEC 27001. З цього моменту всі міжнародні стандарти менеджменту інформаційної безпеки, що випускаються під патронажем ISO / IEC, входять в серію 270xx. Так, в 2007 році оновлена версія стандарту ISO / IEC 17799: 2000 отримала найменування ISO / IEC 27002. А що утворилася різниця в часі між випуском стандартів ISO / IEC 27001 та ISO / IEC 27002 була усунена в 2013 році, коли оновлені версії обох стандартів були видані одночасно (рис. 1.1.).

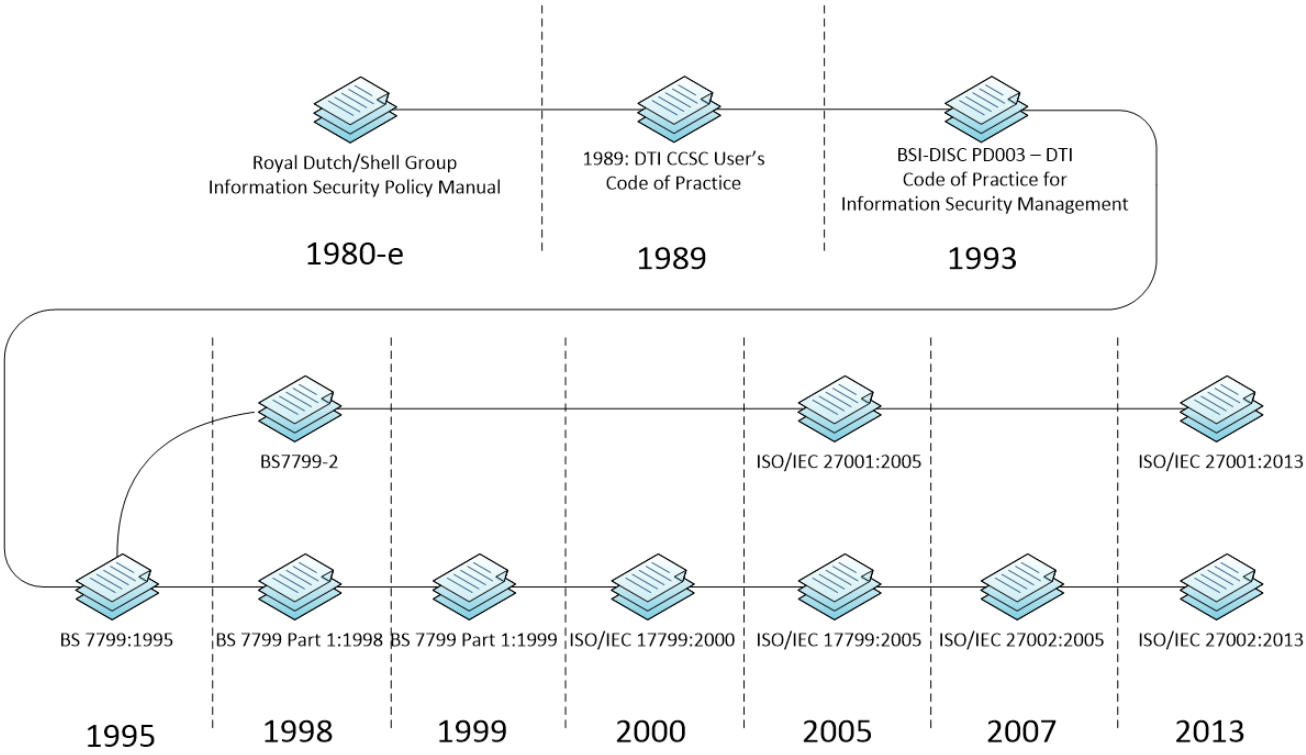

Рис. 1.1. Хронологія розвитку стандарту ISO/IEC 27001

В даний час серія 27xxx містить більше 30 стандартів з різних напрямків системи управління інформаційної безпеки (СУІБ), починаючи з рівня стратегічного управління і контролю СУІБ і закінчуючи технічними

рекомендаціями щодо застосування окремих програмно-технічних і організаційних заходів захисту інформації. Всі ці стандарти можна розділити на кілька груп (рис. 1.2).

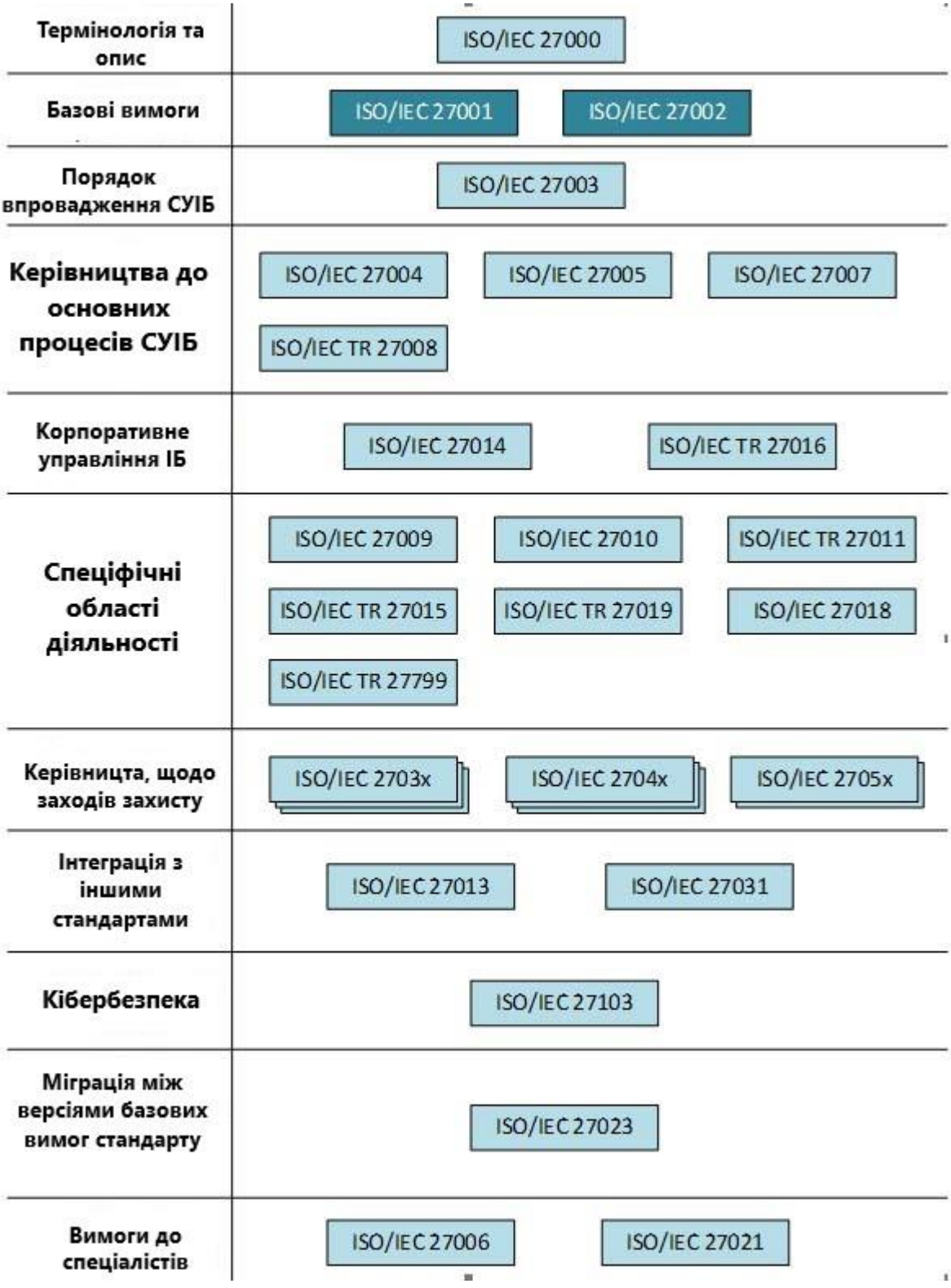

Рис. 1.2. Групування стандартів серії 27xxx

Базові стандарти ISO / IEC 27001 та ISO / IEC 27002 згодом були доповнені наступними документами:

- стандартом ISO / IEC 27000, що описує термінологію і загальний підхід всієї серії стандартів;
- стандартом ISO / IEC 27003 до вказівок по порядку впровадження СУІБ;
- стандартами по окремим процесам СУІБ: вимірювання ефективності, ризик-менеджменту, аудиту;
- стандартами за напрямками стратегічного управління ІБ і економіці СУІБ;
- стандартами за особливостями СУІБ в специфічних областях діяльності: телекомунікаційні послуги, фінансові операції, обробці персональних даних в хмарних сервісах, паливно-енергетичному комплексі, спільнотах інформаційного обміну, організаціях охорони здоров'я;
- детальними вимогами до заходів захисту інформації, в тому числі з управління інцидентами, мережевої безпеки;
- посібниками по інтеграції СУІБ з системами IT-менеджменту (ISO 20000) і системами забезпечення безперервності діяльності (в тому числі ISO 22301);
- керівництвом щодо забезпечення кібербезпеки відповідно до загальним підходом і практиками СУІБ;
- стандартами ISO / IEC 27006 та ISO / IEC 27021, що описує вимоги до експертів і аудиторів СМІБ.

Підхід ISO 27001 до забезпечення інформаційної безпеки

Підхід до управління інформаційною безпекою в даний час визначається двома взаємопов'язаними стандартами: ISO / IEC 27001 та ISO / IEC 27002 (рис. 1.3). Основну роль тут відіграє стандарт 27001, який містить рекомендації щодо менеджменту ІБ в організації на основі широко використовуваного в корпоративному середовищі циклу управління якістю PDCA (Plan, Do, Check, Act). Стандарт ISO / IEC 27002 носить скоріше довідковий характер, описуючи

набір можливих заходів захисту інформації, з яких організація може вибрати необхідні саме їй.

Рис. 1.3. Управління інформаційною безпекою

Стандарт ISO / IEC 27001 дає рекомендації щодо функціонування СУІБ як комплексної системи, спрямованої на захист інформаційних активів організації від загроз і, отже, мінімізацію ризиків. З точки зору бізнесу СУІБ являє собою одну з безлічі систем організації, до якої висуваються певні вимоги і яка повинна виправдати очікування і повернути вкладені в неї кошти (рис. 1.4).

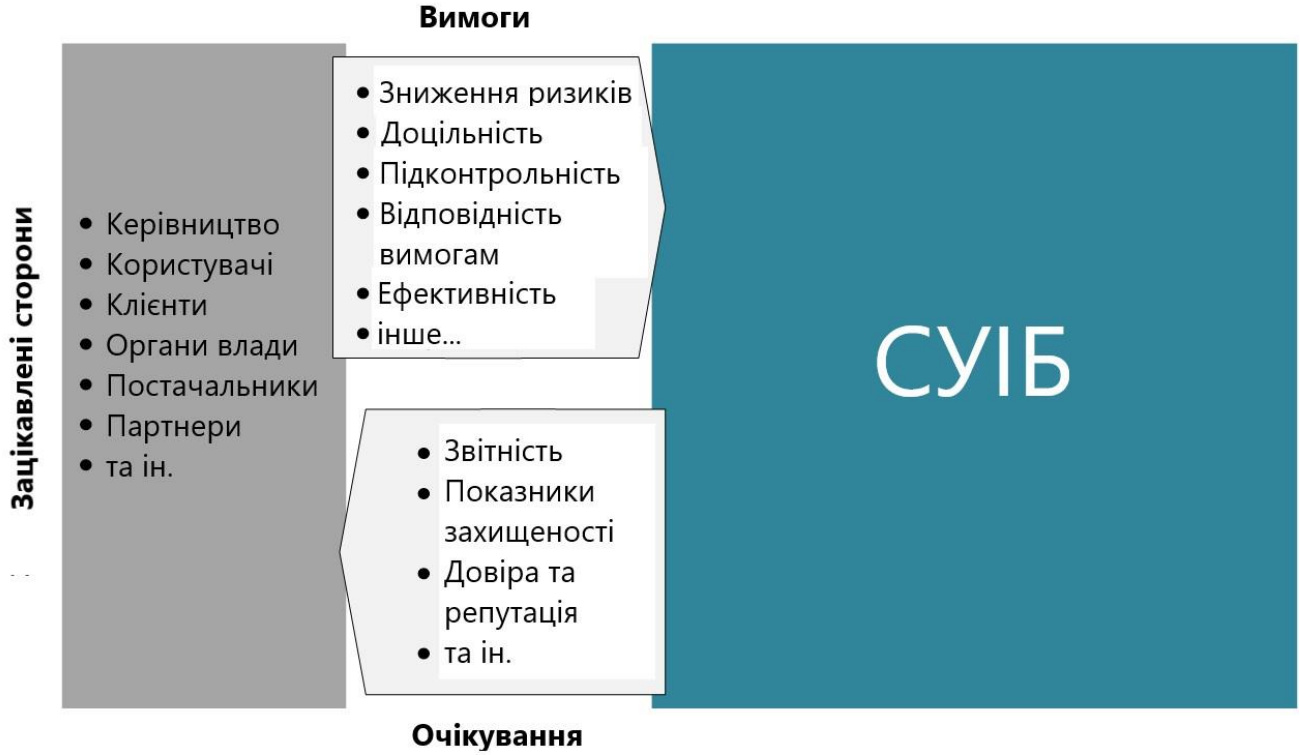

Рис. 1.4. Місце СУІБ в бізнесі організації

Відповідно до рекомендацій стандарту, СУІБ включає в себе повний комплекс дій по забезпеченню інформаційної безпеки, в тому числі організацію діяльності та управління ризиками, а також безпосереднє застосування заходів захисту інформації. Робити вибір тих чи інших способів захисту інформації слід на основі оцінки ризиків ІБ, тобто розміру можливих збитків від реалізації загроз конфіденційності, цілісності та доступності інформації. І, звичайно, виходячи з необхідності виконання нормативних зобов'язань перед державою, партнерами та іншими зацікавленими сторонами.

Таким чином, пропонований підхід дозволяє застосовувати стандарт для реалізації СУІБ в організаціях будь-якого масштабу і рівня нормативної зарегульованості.

Відзначимо також, що ISO / IEC 27001 сумісний з іншими стандартами систем менеджменту якості, такими як ISO 9001, ISO 14000, ISO 31000, ISO / IEC 38500, ISO / IEC 20000, ISO / IEC 22301 та ін. Це дозволяє використовувати єдиний підхід і принципи, загальну термінологію, реалізувати інтегровані процеси за напрямками контролю якості продукції, що випускається, охорони

навколишнього середовища, стратегічного управління та управління IT-сервісами, забезпечення безперервності діяльності організації, і, нарешті, інформаційної безпеки. Що, в свою чергу, дає можливість побудувати структуровану і прозору систему менеджменту організації і підвищити загальну ефективність відповідних процесів.

1.2. Нормативна база управління інформаційною безпекою в Україні

Стандарти є однією з форм накопичення знань на процедурному та програмно-технічному рівнях інформаційної безпеки. Вони також включають тестування, якісні рішення та методології, розроблені кваліфікованими фахівцями.

З практичної точки зору кількість стандартів та специфікацій (міжнародних, національних, галузевих, тощо) у сфері інформаційної безпеки нескінченна. Відповідність систем управління організацією законодавчим актам, вимогам міжнародних та національних стандартів підтверджується сертифікатами. Міжнародні стандарти для систем управління пропонують модель для використання при побудові та експлуатації системи управління. Ця модель включає елементи, визнані експертами в цій галузі шляхом консенсусу найкращих міжнародних практик.

Своєчасний облік змін, викладених у стандартах, є запорукою успішності впровадження інноваційних рішень у навчальний процес фахівців. Особливу увагу слід приділити стандартам, що стосуються безпеки інформаційних технологій та методів їх захисту.

Технічний комітет ITC ISO / IEC 1 «Інформаційні технології» (підкомітет SC 27) виконує роль експертного комітету та здійснює розробку міжнародних стандартів для систем управління в галузі інформаційної безпеки.

Серія стандартів управління інформаційною безпекою ISO / IEC 27000, активно розробляється та оновлюється щорічно, містить кращі практики та рекомендації в галузі інформаційної безпеки для створення, розвитку та підтримки систем управління інформаційною безпекою.

Положення Закону «Про стандартизацію» встановлюють добровільне застосування національних стандартів, скасовують необхідність узгодження проектів національних стандартів з державними органами та скасовують галузеву стандартизацію.

За наказом від 16 жовтня 2019 року державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» були введені такі національні стандарти, гармонізовані з європейськими та міжнародними стандартами, методом підтвердження з наданням чинності з 01 листопада 2019 року:

1.	ДСТУ ISO/IEC 8825-1:2019 (ISO/IEC 8825-1:2015, IDT)	Інформаційні технології. Правила кодування ASN.1. Частина 1. Специфікація правил базового кодування (BER), правил канонічного кодування (CER) і правил витонченого кодування (DER) - На заміну ДСТУ ISO/IEC 8825-1:2012
2.	ДСТУ ISO/IEC 8825-2:2019 (ISO/IEC 8825-2:2015, IDT)	Інформаційні технології. Правила кодування ASN.1. Частина 2. Специфікація правил упакованого кодування (PER) - На заміну ДСТУ ISO/IEC 8825-2:2012
3.	ДСТУ ISO/IEC 8825-3:2019 (ISO/IEC 8825-3:2015, IDT)	Інформаційні технології. Правила кодування ASN.1. Частина 3. Специфікація керівної нотації кодування (ECN) - На заміну ДСТУ ISO/IEC 8825-3:2012
4.	ДСТУ ISO/IEC 25022:2019 (ISO/IEC 25022:2016, IDT)	Інженерія систем і програмних засобів. Вимоги до якості систем програмних засобів та їхнього оцінювання (SQuaRE). Вимірювання якості під час застосування - На заміну ДСТУ ISO/IEC TR 9126-4:2012
5.	ДСТУ ISO/IEC 25023:2019 (ISO/IEC 25023:2016, IDT)	Інженерія систем і програмних засобів. Вимоги до якості систем програмних засобів та їхнього оцінювання (SQuaRE). Вимірювання якості систем та програмних продуктів - На заміну ДСТУ ISO/IEC TR 9126-3:2012; ДСТУ ISO/IEC TR 9126-2:2008
6.	ДСТУ ISO/IEC 27000:2019	Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів

	(ISO/IEC 27000:2018, IDT)	- На заміну ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)
7.	ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT)	Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки - На заміну ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT)
8.	ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT)	Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки - На заміну ДСТУ ISO/IEC TR 27008:2018 (ISO/IEC TR 27008:2011, IDT)
9.	ДСТУ ISO/IEC 27018:2019 (ISO/IEC 27018:2019, IDT)	Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII - На заміну ДСТУ ISO/IEC 27018:2016 (ISO/IEC 27018:2014, IDT)
10.	ДСТУ ISO/IEC TS 27034-5-1:2019 (ISO/IEC TS 27034-5-1:2018, IDT)	Інформаційні технології. Захист застосунків. Частина 5-1. Структура даних керування протоколами та захистом застосунків. Схеми XML - Вперше

Були прийняті зміни до національних стандартів, гармонізованих з міжнародними стандартами, з наданням чинності 1 листопада 2019 року:

1.	ДСТУ ISO/IEC 8825-2:2019 (ISO/IEC 8825-2:2015, IDT) / Поправка N 1:2019 (ISO/IEC 8825-2:2015/Cor 1:2017, IDT)	Інформаційні технології. Правила кодування ASN.1. Частина 2. Специфікація правил упакованого кодування (PER)
2.	ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) / Поправка N 2:2019 (ISO/IEC 27001:2013/Cor 2:2015, IDT)	Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги

3.	ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Поправка N 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT)	Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки
4.	ДСТУ ISO/IEC 27011:2018 (ISO/IEC 27011:2016, IDT) / Поправка N 1:2019 (ISO/IEC 27011:2016/Cor 1:2018, IDT)	Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування інформаційною безпекою на основі ISO/IEC 27002

Та скасовані такі національні стандарти з 01 травня 2020 року:

1.	ДСТУ ISO/IEC 8825-1:2012	Інформаційні технології. Правила кодування ASN.1. Частина 1. Специфікація правил базового кодування (BER), правил канонічного кодування (CER) і правил витонченого кодування (DER) (ISO/IEC 8825-1:2008, IDT)
2.	ДСТУ ISO/IEC 8825-2:2012	Інформаційні технології. Правила кодування ASN.1. Частина 2. Специфікація правил упакованого кодування (PER) (ISO/IEC 8825-2:2008, IDT)
3.	ДСТУ ISO/IEC 8825-3:2012	Інформаційні технології. Правила кодування ASN.1. Частина 3. Специфікація керівної нотації кодування (ECN) (ISO/IEC 8825-3:2008, IDT)
4.	ДСТУ ISO/IEC TR 9126-2:2008	Програмна інженерія. Якість продукту. Частина 2. Зовнішні метрики (ISO/IEC TR 9126-02:2003, IDT)
5.	ДСТУ ISO/IEC TR 9126-3:2012	Програмна інженерія. Якість продукту. Частина 3. Внутрішні метрики (ISO/IEC TR 9126-3:2003, IDT)
6.	ДСТУ ISO/IEC TR 9126-4:2012	Програмна інженерія. Якість продукту. Частина 4. Метрики якості під час використовування (ISO/IEC TR 9126-4:2004, IDT)

7.	ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT)	Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів
8.	ДСТУ ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT)	Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки
9.	ДСТУ ISO/IEC TR 27008:2018 (ISO/IEC TR 27008:2011, IDT)	Інформаційні технології. Методи захисту. Настанова для аудиторів щодо елементів контролювання за інформаційною безпекою
10.	ДСТУ ISO/IEC 27018:2016 (ISO/IEC 27018:2014, IDT)	Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (РП) у загальнодоступних хмарах, що діють як процесори РП

Скасований стандарт може використовуватися виключно як довідковий матеріал без посилання на них у технічній, юридичній тощо документації, підготовленій виробником (підприємством). Такі стандарти не застосовуються і не визнаються національними органами зі стандартизації.

Виробник може розробити та запропонувати власний ДСТУ або затвердити технічні умови на свою продукцію.

Під час застосування стандарту, який є обов'язковим, слід також враховувати, що стандарти зазвичай містять посилання на інші стандарти, положення яких разом складають суть цього стандарту, а також повинні дотримуватися вимоги таких стандартів.

Національний банк України вніс дуже важливий внесок у розвиток СУІБ в країні, прийнявши Постанову «Про вступ в силу стандартів управління інформаційною безпекою в банківській системі України». Таким чином, НБУ запровадив стандарти по банківській системі ISO 27001, ISO 27002 та підвищив рівень інформаційної безпеки банківської системи в Україні.

Деякий час по тому НБУ розробив керівні принципи для впровадження СУІБ і методів оцінки ризиків відповідно до введених стандартами. У цих методах згадується необхідність впровадження стандартів управління інформаційною безпекою в банках в Україні, що продиктовано вимогами Базельського комітету Базель II з управління та зниження операційних ризиків банків.

Впровадження стандартів управління інформаційною безпекою в банках України дозволить:

- оптимізувати витрати на побудову і підтримку системи інформаційної безпеки;
- постійно відстежувати і оцінювати ризики в світлі бізнес-цілей;
- ефективно виявляти найбільш критичні ризики та знижувати ймовірність їх реалізації;
- розробити ефективну політику інформаційної безпеки і забезпечити її якісну реалізацію;
- ефективно розробляти, впроваджувати і тестувати плани
- відновлення бізнесу;
- забезпечити розуміння питань інформаційної безпеки
- керівництво і всі співробітники банку;
- підвищити репутацію і привабливість ринку
- банки;
- знизити ризики рейдерства та інших шкідливих для банку
- атаки;

Слід зазначити, що вищевказані переваги не будуть досягнуті за рахунок «формального» підходу до розробки, впровадження, експлуатації системи управління інформаційною безпекою та відсутності зацікавленості керівництва і співробітників банку в підвищенні рівня інформаційної безпеки.

Аудит СУІБ може бути ініційований керівництвом банку (компанії) - внутрішнього аудиту СУІБ, контрагентів (наприклад, аудит СУІБ може бути

запитом клієнта або обговорено в умовах Угоди), а також третіми особами. - контролюючі органи (НБУ) - перевірки, що проводяться незалежними компаніями.

Зовнішній аудит СУІБ забезпечує розуміння існування, створення, впровадження, контролю та функціонування СУІБ в банку або компанії, яка відповідає вимогам не тільки стандартів ІСО, а й нормативних документів Національного банку України, інших організацій. регулюючі органи. Зовнішній аудит СМІБ дасть можливість оцінити якість СУІБ з наступних питань:

- ступінь, в якій інструменти управління активами СУІБ визначені і впроваджені, правильність оцінки ризику,
- чи виконуються робота, моніторинг та аналіз СУІБ,
- якість підтримки та поліпшення.

Крім того, зовнішній аудит СУІБ укладатиме, як керівництво продемонструвало підтримку процесів і зусиль, пов'язаних з плануванням, впровадженням, експлуатацією, контролем, обслуговуванням і модернізацією СУІБ відповідно до вимог стандартів і правил.

2. Аналіз методичних матеріалів щодо розробки системи управління інформаційної безпеки підприємства.

2.1. Організація розробки системи управління інформаційною безпекою.

Рішення про створення та подальшої сертифікації СУІБ повинно прийматися вищим керівництвом організації. Таким чином керівництво висловлює свою підтримку початку даного процесу, що є ключовим фактором для успішного впровадження СУІБ в організації. При цьому керівництво повинно усвідомлювати кінцеву мету даного заходу і цінність сертифікації для бізнесу компанії.

2.1.1. Основні процеси управління інформаційною безпекою.

З точки зору цільового призначення процеси ІБ в організації класифікуються на процеси забезпечення та процеси управління. Процеси забезпечення ІБ призначені для реалізації безпосередніх організаційних і технічних функцій захисту активів компанії (технічних засобів, програмного забезпечення та інформаційних активів). Процеси управління ІБ призначені для реалізації керуючих дій щодо системи забезпечення ІБ (СЗІБ).

Серед основних процесів управління інформаційною безпекою можна виділити наступні:

- підтримка в актуальному стані документаційного забезпечення ІБ;
- ідентифікація та класифікація активів компанії (об'єктів захисту);
- оцінка ризиків ІБ;
- робота з персоналом з питань ІБ;
- управління інцидентами ІБ;
- оцінка відповідності вимогам власних політик ІБ і вимогам регуляторів в області ІБ і ін.

Необхідно акцентувати увагу на тому, що забезпечення інформаційної безпеки компанії - це не разова акція, а безперервна діяльність з планування, реалізації, вимірюванню та вдосконалення процесів забезпечення і управління ІБ. Впровадження процесного підходу до управління інформаційною безпекою в

умовах обмеженого штату підрозділів ІБ ускладнює створення, впровадження і підтримку СУІБ, особливо для великих компаній.

Зокрема, представляються скрутними здійснення і підтримка в актуальному стані результатів класифікації об'єктів захисту та оцінки ризиків ІБ без засобів автоматизації, враховуючи складність інформаційної інфраструктури, велика кількість прикладних систем, де обробляється інформація обмеженого доступу, великий перелік критичних активів, які підлягають захисту. Або ж, наприклад, впровадження і функціонування СУІБ з урахуванням процесного підходу вимагає звернення всередині системи значного обсягу документів. Зазначені особливості обумовлюють необхідність використання засобів автоматизації для підтримки процесів управління ІБ.

Аналіз ризиків - це основний рушійний процес СУІБ. Він виконується не тільки при створенні СУІБ, але і періодично при зміні бізнес-процесів організації і вимог з безпеки. Необхідно підібрати таку методику аналізу ризиків, яку можна було б використовувати з мінімальними змінами на постійній основі. Є два шляхи: використовувати існуючі на ринку методики і інструментарій для оцінки ризиків або ж розробити свою власну методику, яка найкращим чином буде підходити до специфіки компанії і охоплена системою управління інформаційної безпеки області діяльності. Останній варіант найкращий, оскільки поки більшість існуючих на ринку продуктів, що реалізують ту чи іншу методику аналізу ризиків, не відповідають вимогам стандарту. Типовими недоліками таких методик є:

- стандартний набір загроз і вразливостей, який часто неможливо змінити;
- прийняття в якості активів тільки програмно-технічних і інформаційних ресурсів - без розгляду людських ресурсів, сервісів і інших важливих ресурсів;
- загальна складність методики з точки зору її стійкого і повторюваного використання.

У процесі аналізу ризиків для кожного з активів або групи активів проводиться ідентифікація можливих загроз і вразливостей, оцінюється

ймовірність реалізації кожної із загроз і, з урахуванням величини можливих збитків для активу, визначається величина ризику, що відображає критичність тієї чи іншої загрози. Необхідно відзначити, що відповідно до вимог Стандарту в процедурі аналізу ризиків повинні бути ідентифіковані критерії прийняття ризиків та прийнятні рівні ризику. Ці критерії повинні базуватися на досягненні стратегічних, організаційних і управлінських цілей організації. Вище керівництво компанії використовує дані критерії, приймаючи рішення щодо прийняття контрзаходів для протидії виявленим ризикам. Якщо виявлений ризик не перевищує встановленого рівня, він є прийнятним, і подальші заходи щодо його обробці не проводяться. У разі ж, коли виявлений ризик перевищує прийнятний рівень критичності загрози, вище керівництво повинне прийняти одне з таких можливих рішень:

- зниження ризику до прийнятного рівня за допомогою застосування відповідних контрзаходів;
- прийняття ризику;
- уникнення ризику;
- переклад ризику в іншу область, наприклад, за допомогою його страхування.

Як відомо, в основі СУІБ лежить модель безперервного поліпшення якості, також відома як цикл Демінга або цикл PDCA. Звідси стають очевидні чотири процесу СУІБ:

- Процес планування, метою якого є виявлення, аналіз та проектування способів управління ризиками інформаційної безпеки. При створенні цього процесу слід розробити методику категоріювання інформаційних активів і формальної оцінки ризиків на основі даних про актуальні для нашої інформаційної інфраструктури загрози і вразливості. Стосовно до аудиту PCI DSS можна виділити два типи цінних інформаційних активів, що володіють різним рівнем критичності - дані про власників карт і критичні аутентифікаційні дані.

- Процес впровадження спланованих методів обробки ризиків, що описує процедуру запуску нового процесу забезпечення інформаційної безпеки, або модернізації існуючого. Особливу увагу слід приділити опису ролей і обов'язків, а також планування впровадження.
- Процес моніторингу функціонуючих процесів СЗІБ.
- Процес вдосконалення заходів безпеки та безпеки відповідно до результатів моніторингу, що дає можливість здійснити коригувальні та профілактичні дії.

На практиці ці процеси описуються політикою управління інформаційною безпекою, яка є або частиною політики захисту інформації, або незалежним документом, представленим на найвищому рівні трирівневої структури бази даних регуляторних документів..

Для невеликих компаній, а також окремих підрозділів буде досить розробити методику формального аналізу інформаційних ризиків і передбачити процедуру перегляду процесів за результатами регулярного аудиту.

Таким чином основними характеристиками управління інформаційною безпекою на сучасному етапі є комплексний підхід, оперативне прийняття управлінських рішень, персональна відповідальність.

Основними процесами управління інформаційною безпекою на підприємстві визначені: підтримка в актуальному стані документації ІБ, ідентифікація та класифікація активів, оцінка ризиків ІБ, робота з персоналом з питань ІБ, управління інцидентами ІБ, оцінка відповідності вимогам власних політик ІБ.

Не менш важливим фактором успішного впровадження СУІБ є створення робочої групи, відповідальної за впровадження СУІБ. До її складу мають увійти:

- представники вищого керівництва організації;
- представники бізнес-підрозділів, охоплених СУІБ;
- фахівці підрозділів, що забезпечують інформаційну безпеку в компанії, які мають відповідну освіту або підготовку, знають основні принципи і кращі практики в області інформаційної безпеки.

Перераховані співробітники повинні розуміти універсальні механізми систем управління, знати вимоги стандартів і пройти навчання з питань створення та експлуатації СУІБ. До складу робочої групи, окрім співробітників компанії, можуть входити також залучені консультанти, що спеціалізуються в питаннях побудови СУІБ. Доброю практикою є створення в організації комітету з інформаційної безпеки, який, крім питань, пов'язаних з впровадженням СУІБ, повинен на постійній основі забезпечити вирішення завдань, що визначаються експлуатацією даної СУІБ і її безперервним вдосконаленням.

2.1.2. Структурно-логічна схема дій керівництва підприємства по розробці системи управління інформаційною безпекою.

Організація інформаційної безпеки - складова частина системи захисту інформації, яка визначає і виробляє порядок і правила функціонування об'єктів захисту і діяльності посадових осіб з метою забезпечення захисту інформації.

Організація інформаційної безпеки на підприємстві - регламентація виробничої діяльності та взаємовідносин суб'єктів (працівників підприємства) на нормативно-правовій основі, що виключає або послаблює нанесення збитку даному підприємству.

Перше з наведених визначень більшою мірою показує сутність організаційної захисту інформації. Друге - розкриває її структуру на рівні підприємства. Разом з тим обидва визначення підкреслюють важливість нормативно-правового регулювання питань захисту інформації поряд з комплексним підходом до використання в цих цілях наявних сил і засобів. Основні напрямки організаційної захисту інформації наведені нижче.

Організація інформаційної безпеки:

- Організація роботи з персоналом;
- Організація внутрішньо об’єктного і пропускного режимів і охорони;

- Організація роботи з носіями відомостей;
- Комплексне планування заходів щодо захисту інформації;
- Організація аналітичної роботи і контролю.

Основна ціль організації інформаційної безпеки, це збереження головних для організації характеристик інформаційної безпеки: доступність, конфіденційність, цілісність

Доступність - це можливість у прийнятний час отримати необхідну інформаційну послугу.

Конфіденційність - це захист від несанкціонованого доступу до інформації.

Інформаційні системи створюються (набуваються) для отримання певних інформаційних послуг. Якщо з будь-якої причини неможливо надати ці послуги користувачам, це завдає шкоди всім суб'єктам інформаційних відносин. Тому він визначений як найважливіший елемент інформаційної безпеки

Особливо зрозуміло, що провідна роль доступності проявляється у всіх типах систем управління - виробництві, транспорті тощо. Зовнішньо менш драматичні, але й дуже неприємні наслідки - як матеріальні, так і моральні - можуть мати довгострокову недоступність використовуваних інформаційних послуг великою кількістю людей (квитки на поїзди та авіаквитки, банківські послуги тощо).

Цілісність можна розділити на статичну (розуміється як незмінність інформаційних об'єктів) та динамічну (що стосується правильного виконання складних дій (транзакцій)). Динамічний контроль цілісності використовується, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжок, упорядкування чи дублювання окремих повідомлень.

Цілісність є найважливішим аспектом інформаційної безпеки у випадках, коли інформація слугує "керівництвом до дії". Ліки, що відпускаються за рецептом, призначені медичні процедури, підбір та характеристики компонентів, перебіг процесу - все це приклади інформації, порушення цілісності яких може бути буквально смертельним. Спотворення офіційної інформації, тексту закону чи сторінки веб-сервера будь-якої урядової організації також неприємне.

Конфіденційність - це найбільш розвинений аспект інформаційної безпеки в нашій країні. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем стикається з серйозними труднощами. По-перше, інформація про технічні канали витоку інформації закрита, тому більшість користувачів позбавлені можливості отримати уявлення про потенційні ризики. По-друге, численні юридичні бар'єри та технічні проблеми стоять на шляху користувальницької криптографії як основного засобу забезпечення конфіденційності.

Якщо повернутися до аналізу інтересів різних категорій суб’єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, доступність є на першому місці. Цілісність практично не поступається їй за важливістю - який сенс у інформаційній службі, якщо вона містить спотворені дані?

Конфіденційні моменти існують також у багатьох організаціях (навіть у згаданих вище навчальних закладах намагаються не розголошувати інформацію про зарплату працівників) та окремих користувачів (наприклад, паролі).

Система інформаційної безпеки підприємства побудована на ряді принципів:

Комплексність / системність.

Цей принцип передбачає створення такої системи безпеки, яка б забезпечувала захист підприємства, його майна, персоналу, інформації, різних сфер діяльності від усіх можливих небезпек та загроз, форс-мажору, тобто системи безпеки (її складових , сили, засоби) повинні бути достатніми для забезпечення економічної, екологічної, наукової, технічної, кадрової, пожежної та інших видів безпеки. У забезпеченні безпеки підприємства повинні брати участь не тільки штатні працівники та спеціальні служби, але майже кожен, хто працює на підприємстві. Організаційною формою комплексного використання сил і засобів повинна бути програма забезпечення безпеки підприємства.

Пріоритет профілактичних заходів (своєчасність).

Система безпеки повинна бути побудована таким чином, щоб вона могла виявити різні руйнівні фактори на ранній стадії, вжити заходів щодо запобігання їх

шкідливого впливу та заподіяти шкоду підприємству. Реалізація цього принципу економічно набагато вигідніше, ніж усунення шкоди.

Неперервність.

Система безпеки повинна бути побудована таким чином, щоб вона працювала, постійно захищаючи інтереси підприємства в умовах ризику та опору зловмисникам.

Законність.

Усі дії щодо забезпечення безпеки підприємства повинні здійснюватися на основі чинного законодавства і не суперечити йому. Ті заходи безпеки, які розробляються на самому підприємстві, також повинні базуватися та здійснюватися в рамках діючих правових актів.

Плановість.

Цей принцип передбачає використання надійності у функціонуванні системи безпеки. Це дозволяє учаснику процесу логічно та послідовно виконувати дії для досягнення загального результату. На основі одного задуму організовується вся діяльність із забезпечення безпеки. Цей задум викладений в комплексній програмі та в конкретних планах по окремих видів та напрямках безпеки.

Економність.

Система безпеки повинна бути спроектована таким чином, щоб витрати на її забезпечення були економічно виправдані, а витрати були оптимальними і не перевищували рівень, при якому втрачається економічний сенс їх застосування..

Взаємодія.

Для того щоб забезпечити безпеку підприємства, необхідно, щоб зусилля всіх його співробітників, підрозділів, служб були скоординовані. Тобто всі учасники цього процесу повинні взаємодіяти один з одним, чітко знаючи, хто за що відповідає, а хто що робить. Принцип взаємодії також передбачає встановлення тісних ділових контактів і координацію дій з зовнішніми організаціями (правоохоронними органами, місцевими або районними службами безпеки, органами влади і т. д.), Здібними надати потрібну допомогу у забезпеченні безпеки

підприємства. Це завдання може виконати комітет (група, рада і т. д.) безпеки підприємства.

Поєднання гласності та конфіденційності.

Система основних заходів безпеки повинна бути відома всім працівникам підприємства; її вимоги повинні бути виконані. Це дозволить своєчасно виявляти і запобігати потенційні і реальні небезпеки та загрози. У той же час ряд способів, сил, коштів, методів безпеки повинен бути помітний і відомий дуже вузькому колу фахівців, що дозволить більш ефективно протистояти як внутрішнім, так і зовнішнім загрозам, своєчасно запобігати збиток підприємству..

Компетентність.

Питання забезпечення безпеки підприємства є актуальним. В результаті навмисних дій зловмисників, недобросовісної конкуренції, прийняття катастрофічно ризикованих рішень і т. Д Бізнесу може бути завдано непоправної шкоди. Тому питання безпеки підприємства повинні вирішувати не аматори, а професіонали, які глибоко знають суть проблеми, здатні своєчасно оцінити ситуацію і прийняти правильне рішення. Система безпеки підприємства повинна бути побудована відповідно до політики і стратегії безпеки.

Сама організація УІБ підприємства закладається у створенні служб, що відповідають за забезпечення конфіденційної інформації. Структура і склад таких служб залежить від фінансового стану фірми (організації). Утримання подібних служб вимагає чималих фінансових витрат. Однак в даний час є фірми (організації), які в змозі утримувати такі структури, забезпечуючи тим самим безпеку конфіденційної інформації, а значить, і її економічне благополуччя. І в подальшому кількість таких фірм, ми сподіваємося, буде постійно зростати.

Очолювати цю роботу повинен начальник служби безпеки інформації. Для більш дрібних фірм (організацій) - помічник начальника служби безпеки фірми з інформаційної безпеки. Ця посада може бути штатною, або її можна займати за сумісництвом (залежить від статусу фірми і її фінансового стану).

У службі безпеки повинні бути посадові особи, які відповідають спочатку за окремі напрямки захисту. Ними можуть бути:

- головний спеціаліст по забезпеченню безпеки інформації в виділених приміщеннях фірми;
- головний спеціаліст по забезпеченню безпеки інформації на об'єктах обчислювальної техніки фірми;
- головний спеціаліст по забезпеченню безпеки зв'язку.

Ці посади можуть виконуватися за сумісництвом, але, безумовно, підготовленими співробітниками в питаннях забезпечення інформаційної безпеки. Крім того, в кожному виділеному приміщенні повинні бути призначені відповідальні за забезпечення безпеки інформації. Такі ж відповідальні призначаються і на кожен об'єкт обчислювальної техніки. Що стосується безпеки зв'язку, то тут повинні бути відповідальні за забезпечення безпеки кожного виду зв'язку (телефонного, телеграфного, факсимільного, при передачі даних). Ці посади також займаються за сумісництвом.

Таким чином, у начальника служби безпеки інформації з'являється структура, яку можна навчити і організувати її ефективне функціонування щодо забезпечення безпеки інформації в цілому на фірмі.

2.2. Методичні матеріали щодо оцінки ефективності процесів розробки та впровадження системи управління інформаційною безпекою.

Основна мета будь-якої системи захисту інформації - забезпечити стабільну роботу об'єкта: запобігти загрозам його безпеці, захистити законні інтереси власника інформації від протиправних атак, у тому числі кримінальних злочинів у цій галузі відносин, за Кримінальним кодексом , для забезпечення нормальної виробничої діяльності всіх підрозділів об'єкта. Ще одна мета - покращити якість наданих послуг та гарантувати безпеку прав власності та інтересів клієнтів.

2.2.1. Моделі з управління інформаційною безпекою.

Модель системи інформаційної безпеки підприємства являє собою сукупність зовнішніх і внутрішніх факторів, їх вплив на стан інформаційної безпеки підприємства і забезпечення безпеки ресурсів. На рис. 2.1. уявити модель системи інформаційної безпеки підприємства, в якій представлені напрямки впливу наступних факторів:

- загроза інформаційній безпеці, що характеризується ймовірністю виникнення і реалізації;
- вразливість системи інформаційної безпеки, яка впливає на ймовірність виникнення загрози;
- ризики, які відображають передбачуваність шкоди в результаті реалізації загрози інформаційній безпеці.

Інформація та матеріальні ресурси, що підлягають захисту, контролюються об'єктами захисту. Це включає:

- мовну інформацію;
- інформацію, що зберігається і обробляється засобами зв'язку у вигляді різних носіїв;
- документи на паперових носіях;
- технічні засоби зв'язку та інформатизації;
- приміщення, призначені для обговорення, обробки та зберігання інформації;

• інформаційні системи в цілому, включаючи системи зв'язку;

• документація на технічні та програмні засоби зв'язку та інформатизації;

• програмні засоби.

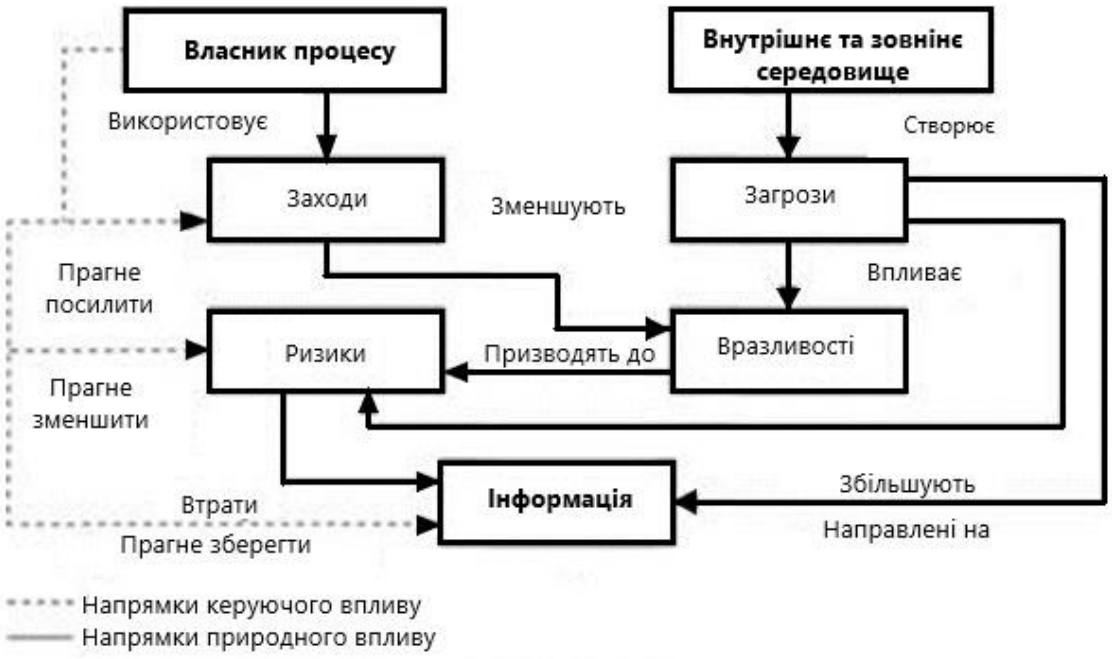

Рис. 2.1. Модель системи інформаційної безпеки підприємства

Представлена модель захисту інформації - це сукупність об'єктивних зовнішніх та внутрішніх факторів та їх впливу на стан інформаційної безпеки на об'єкті та на безпеку матеріальних чи інформаційних ресурсів.

Розглядаються наступні об'єктивні фактори:

- загрози інформаційній безпеці, що характеризуються ймовірністю виникнення та ймовірністю реалізації;
- вразливості інформаційної системи або системи контрзаходів (систем захисту інформації), які впливають на ймовірність реалізації загрози;
- ризик - фактор, що відображає потенційну шкоду організації внаслідок загрози інформаційній безпеці: витік інформації та її неправильне використання (ризик врешті-решт відображає ймовірні фінансові втрати - прямі чи непрямі).

Для побудови збалансованої системи інформаційної безпеки спочатку планується провести аналіз ризиків у галузі інформаційної безпеки. Потім визначається оптимальний рівень ризику для організації на основі заданого критерію. Система захисту інформації (контрзаходи) буде побудована таким чином, щоб досягти заданого рівня ризику

Загрози, з якими може зіткнутися підприємство, класифікуються за характером їх виникнення, тобто загрозам випадкового або навмисного характеру, і по тому, як вони пов'язані з захищеними, тобто зовнішніми і внутрішніми загрозами.

Джерела зовнішніх загроз:

- дії конкурентів по перехопленню важливої інформації;
- навмисні дії по знищенню, знищення чи зміни інформації;
- ненавмисні дії співробітників сторонніх організацій, які привели до виходу з ладу елементів системи;
- стихійні лиха і катастрофи, аварії, екстремальні ситуації.

Джерела внутрішніх загроз включають в себе:

- неузгодженість діяльності підрозділів підприємства в області захисту інформації;
- навмисні дії персоналу по знищенню або зміні інформації;
- ненавмисні помилки персоналу, збої устаткування і збої інформаційних систем;
- порушення встановлених правил збору, накопичення, зберігання, обробки, перетворення, відображення і передачі інформації.

Порушення можуть бути декількох типів.

Організаційні та правові порушення - порушення, пов'язані з відсутністю єдиної послідовної політики компанії в області захисту інформації, недотримання вимог нормативних документів, доступу, зберігання та знищення інформації.

Організаційні типи порушень включають несанкціонований доступ до баз даних і наборів даних, несанкціонований доступ до активного мережевого

обладнання, серверів, неправильне вбудовування засобів безпеки і помилки в їх управлінні, порушення в цільовому розповсюдженні інформації при проведенні обміну інформацією.

Фізичні види порушень включають в себе пошкодження обладнання автоматизованих систем, ліній зв'язку та комунікаційного обладнання, крадіжку або несанкціоноване ознайомлення зі змістом носія, їх крадіжку.

Радіоелектронні типи порушень включають введення електронних пристроїв для перехоплення інформації, отримання інформації шляхом перехоплення і дешифрування інформаційних потоків, фотографування моніторів, накладення неправдивої інформації в локальні мережі, передачі даних і лінії зв'язку.

Для протидії загрозам і запобігання порушень на підприємствах організований процес управління ризиками, який є основою системи інформаційної безпеки підприємства.

Створення ефективної системи інформаційної безпеки - це комплексний процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз при обмеженні ресурсів і часу.

З точки зору процесного підходу, система інформаційної безпеки підприємства може бути представлена як процес управління ризиками (рис. 2.2.), Який включає в себе наступні компоненти.

1. Опис бізнес-процесів. Бізнес-процеси коригуються і аналізуються. Відповідно до критеріїв, які визначені в процесі формування політики ризику, виявлення бізнес-процесів.

2. Збір ризиків. Проводиться для виявлення ступеня схильності підприємства загрозам, які можуть завдати значної шкоди. Для цього проводиться аналіз його бізнес-процесів і анкетування експертів домену. Результатом цього процесу є класифікаційний список всіх потенційних ризиків.

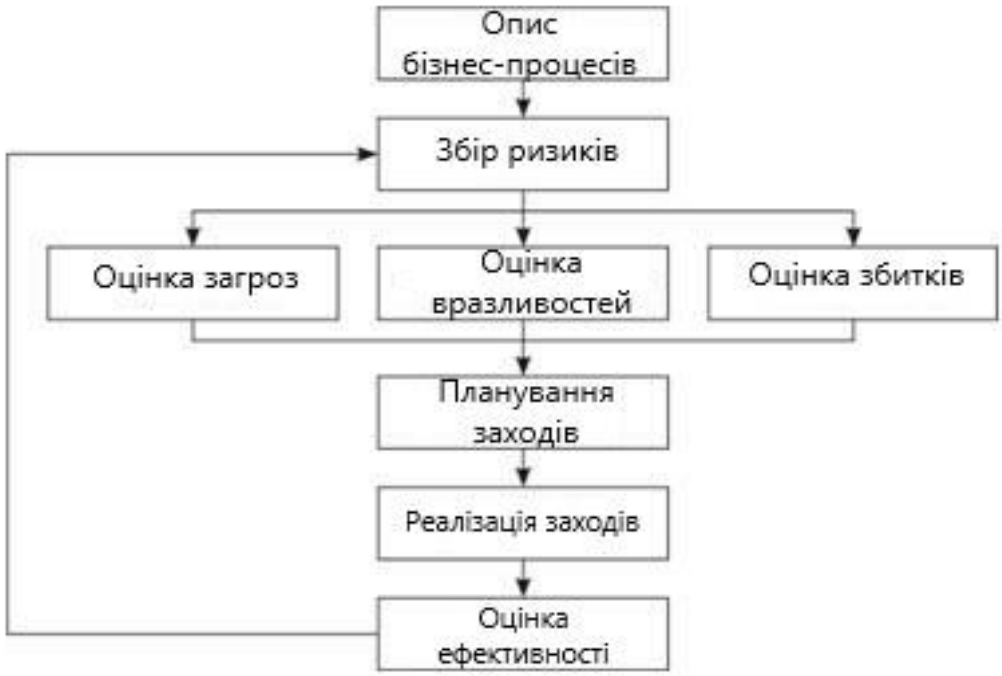

Рис.2.2. Модель процесу управління ризиками для СУІБ

Стандартні ризики інформаційної безпеки включають в себе:

- видалення конфіденційної інформації з локальних місць розташування;
- умисна зміна інформації з метою знищення;
- копіювання важливих документів і передача конкуренту;
- незаконне вторгнення в корпоративну мережу;
- знищення через технічні причини.

3. Оцінка ризику. Визначення характеристики ризику та ресурси інформаційної системи. Основним результатом цього процесу є список всіх потенційних ризиків з їх кількісної та якісної оцінкою втрат і можливостей для реалізації, а додатковий - список ризиків, які не будуть відслідковуватися на підприємстві.

Процес оцінки ризику складається з наступних етапів:

1) опис об'єкту та заходів захисту;
2) виявлення ресурсу і визначення його кількісних показників;
3) аналіз загроз ІБ;
4) оцінка вразливості;

5) оцінка існуючих і прогнозованих засобів забезпечення ІБ.

Планування події. Метою планування зниження ризику є визначення термінів і списку робіт по усуненню або мінімізації збитку завдяки зниженню ризику.

Розрізняють такі види заходів інформаційної безпеки:

- організаційний;
- законний;
- організаційно-технічні;
- програмне забезпечення;
- інженерно-технічні.

5. Реалізація заходів. Реалізація заходів щодо мінімізації ризиків має на увазі виконання запланованих робіт, контроль якості результатів і термінів. Результатом цього процесу є робота по мінімізації ризиків і часу їх реалізації.

6. Оцінка ефективності. Оцінка ефективності системи управління інформаційною безпекою являє собою систематичний процес отримання та оцінки об'єктивних даних про поточний стан системи, дії і події, які в ній відбуваються, встановлює рівень їх відповідності певним критеріям.

Цілі процесу:

- оцінка поточного рівня ефективності системи;
- зосередження в конкретному місці «вузьких місць» в системі;
- оцінка відповідності системи підприємства чинним стандартам в області інформаційної безпеки;
- розробка рекомендацій і правил з безпеки об'єктів безпеки.

2.2.2. Метрики управління інформаційною безпекою.

Для проведення дослідження управління інформаційною безпекою та захисту інформації підприємства в Україні треба розглянути: методичні інструменти для проведення досліджень управлінських процесів, вибір підходів до дослідження та використання системного підходу при проведенні в системі управління інформаційною безпекою підприємства, проведення досліджень на прикладі. При проведенні досліджень на підприємствах перед дослідниками ставляться цілі, що вимагають не тільки аналізу і виявлення проблем, а й обґрунтування рекомендацій, запропонованих для їх вирішення. Оцінка стану, діагностика, профілактика негативних тенденцій, пошук «вузьких місць» в системі управління, визначення нових напрямків діяльності вимагають від менеджера системного бачення, володіння науково-категоріальним апаратом дослідження. Для досягнення мети дослідження необхідно чітко визначити основні поняття: об'єкт, предмет, новизну, практичну значущість, методи дослідження; знати технології управління, вміти визначати проблему в дослідженні процесів і систем управління, здійснювати системний аналіз чинників прямого і непрямого впливу, розуміти ефективність, обмеження і умови використання різних методів.

Загальні і окремо-наукові методи дослідження систем управління

Вивчення систем управління в залежності від рівня проблеми, цілей, завдань дослідження може бути глобальним або локальним. Глобальні проблеми, як правило, носять системний, міждисциплінарний характер, досліджуються загальноприйнятими науковими методами. Проблеми, обмежені за обсягом, мають яскраво виражену специфіку дослідження в основному з використанням окремих наукових методів.

В цілому, методи застосовні до досліджень в предметних областях ряду наукових областей: економіка, менеджмент, соціологія, психологія і т. д. Дослідження вузької або конкретної проблеми в одній обраній області проводиться з використанням окремих наукових методів, застосовується в основному в обраному науковому напрямку. Наприклад, методи вивчення попиту продукцію

використовуються в маркетингових дослідженнях, а метод функціонально-вартісного аналізу знаходить застосування в економіці підприємств.

Загально методи дослідження в ІСУ включають в себе: управління та діагностику проблем, системний аналіз, експертні методи дослідження, моделювання і статистичні дослідження, морфологічний аналіз і функціонально-декомпозіціонние уявлення в формі одиниці, аналіз і синтез понять.

Окремі наукові методи включають в себе: методи вибіркового та соціологічного дослідження, Delphi, методи середньозважених критеріїв в оцінці постачальників, метод Монте-Карло, тестування, параметричний метод, факторний аналіз, функціональний і вартісний аналіз, фінансовий аналіз, бюджетування, розрахунок, хронометраж, фотографування робочого часу, метод Парето, який використовується для визначення найвищих витрат, пов'язаних з дефектами, і багато інших методів, що використовуються в підсистемах функціонального управління. Основою сучасних досліджень в галузі управління є системний підхід, який аналізує фактори зовнішнього і внутрішнього середовища організації, в той час як сама вона розглядається як відкрита, динамічна система.

Моделювання - це метод прогнозування можливих станів об'єкта в майбутньому, способів досягнення заданих параметрів з використанням моделей: предметних, знакових, математичних, імітаційних, аналітичних. Модель при дослідженні систем управління являє собою спрощене уявлення об'єкта, який повинен відповідати вимогам повноти адаптивності, щоб забезпечити можливість включення досить широких змін. Модель повинна бути досить абстрактною, щоб можна було варіювати велика кількість змінних, і бути орієнтованою на реалізацію існуючими технічними засобами, тобто вона повинна бути фізично здійсненною на цьому рівні розвитку науки і техніки з урахуванням конкретного підприємства який виконує прогнозування.

Приклади моделей, що використовуються при вивченні систем управління: уявлення функціональної декомпозиції - агрегат, моделювання за методом Монте-Карло, блокова модель, представлена у вигляді логічної блок-схеми, модель

функціональних витрат, модель консультативної групи в Бостоні, матриця факторів, модель прогнозування витрат і прибуток.

Імітаційні моделі в ІСУ будуються за аналогією з об'єктом дослідження з використанням статистичних методів. Для випадкового моделювання був розроблений метод статистичних тестів (метод Монте-Карло), основна ідея якого полягає в моделюванні випадкових явищ за допомогою реалізації «розіграшів». Результати такого моделювання обробляються з використанням обчислень. Визначено тип і параметри розподілу випадкових величин. Припустимо, що ми називаємо один елементарний елемент будь-яким досвідом, який вирішує одне із запитань:

• Чи відбулося подія А чи ні?

• яка з можливих подій А, В, С сталася?

• яке значення прийняла випадкова величина Х?

Реалізація випадкового явища заснована на математичному законі великих чисел. Найбільш важливим є принцип випадковості появи частини значень параметрів і, отже, реалізація моделі в цілому. Імітаційне моделювання може використовуватися для прогнозування можливих станів системи, динаміки продажів, змін в конкурентному середовищі організації та т. д.

Функціональні - декомпозіціонние уявлення системи у вигляді сукупності доповнюють методи математичного моделювання, що використовуються в MIS. Загальне уявлення системи найбільш зручно використовувати у вигляді математичної моделі, наприклад, у вигляді сервісних ланцюгів або агрегатів (рис.2.3). Розглянуто абстрактна схема функціонування складної системи, центральною ланкою якої є одиниця. У кожен момент часу t блок знаходиться в одному з можливих станів Z (t). Стан пристрою в фіксований час визначається керуючим дією g (t) відповідно до оператором переходу H з використанням залежності:

$$Z(t) = H\{Z(t^{\circ}), g(t)\} \quad (2.1)$$

Пристрій має вхідні контакти. Вони отримують вхідні сигнали X (t), які відповідно до оператора G перетворюються у вихідні сигнали Y (t). Ця схема дозволяє варіювати велику кількість параметрів, використовуваних для характеристики стану системи, в той же час вимагає спрощення набору цих параметрів до сильно абстрактної моделі, найбільш повно відображає основні з них і дозволяє прогнозувати майбутнє тенденції. Видимість і абстрактність є перевагою даної векторної моделі.

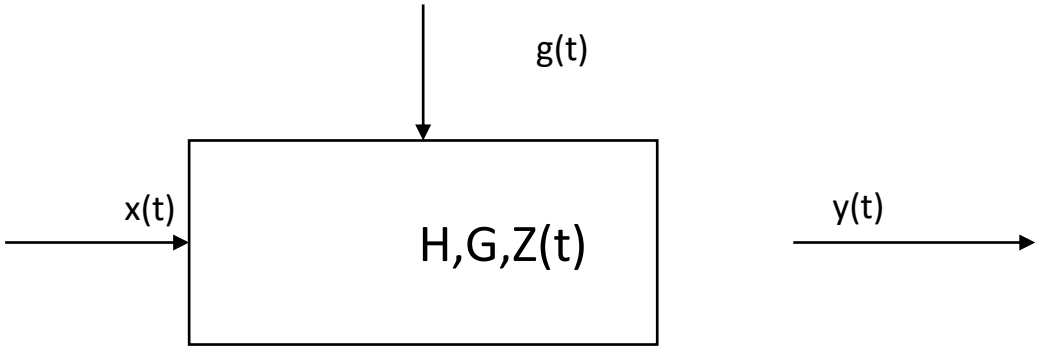

Рис.2.3 Уявлення системи у вигляді агрегату

Експертні методи вивчення систем управління - методи, засновані на аналізі та усередненні по-різному мислення, думки експертів з цих питань. Часто супроводжується створенням спеціальних робочих груп експертів, експертної комісії, мережі експертів.

Відбір експертів заснований на аналізі їх компетентності, який визначається об'єктивною оцінкою і самооцінкою експертів, а також методом стабілізації експертної мережі.

Спосіб стабілізації експертної мережі полягає у відборі ряду компетентних експертів, наприклад, 10 чоловік для обраної завдання, які вибирають однакову кількість експертів і т.д.. Ця процедура повторюється до тих пір, поки не буде сформована достатня мережу експертів. В даному випадку мова йде про загальну чисельність фахівців, компетентних в області прогнозованої проблеми. Наступним етапом є формування репрезентативної вибірки із загальної сукупності та створення необхідної експертної комісії.

Методи експертної оцінки: Delphi, круглий стіл, інтерв'ю, експертне опитування, мозковий штурм, метод сценаріїв, метод зваженого середнього рейтингу, ділова гра, метод японських «рингів».

Delphi - це один з методів експертного прогнозування, заснований на послідовній оцінці експертами будь-яких запропонованих альтернатив. Це може бути застосоване в процесі групового прийняття рішення, вибираючи кращу альтернативу.

Мозковий штурм - це метод активізації творчої активності учасників, заснований на спонтанному вираженні ідей, які формуються і виражаються учасниками в короткій і зрозумілій формі. Критика ідей в даний час є неприпустимою. Це можливо тільки після закінчення «мозкового штурму». Головне правило - кількість висловлених ідей важливіше, ніж їх якість. Основоположником методу є американський психолог А. Осборн. При мозковому штурмі вважається, що людина може видавати геніальні ідеї, якщо він висловлює свої думки «негайно», не думаючи заздалегідь, покладаючись тільки на свою підсвідомість. Метод заснований на вільних асоціаціях ідей.

Метод номінальної групи заснований на принципі обмеження міжособистісного спілкування. Члени групи представляють свої пропозиції в письмовій формі незалежно і незалежно від інших. На наступному етапі кожен учасник повідомляє про суть свого проекту, і представлені варіанти розглядаються членами групи без обговорення і критики. Потім кожен член групи знову, незалежно від інших, в письмовому вигляді представляє рейтингові оцінки розглянутих ідей. Проект з найвищою оцінкою приймається за основу рішення. Метод дозволяє організувати групову роботу, не обмежуючи індивідуальне мислення кожного учасника. Подібним методом номінальної групової техніки є японський метод прийняття групового рішення «ринги».

Методологія, запропонована в цьому розділі, заснована на дослідженнях ІБ, українських і міжнародних стандартах управління інформаційною безпекою та методах оцінки ІБ. Для практичної реалізації запропонованої методології була використана система управління інформаційною безпекою «Матриця».

Область застосування пропонованої методології - аудит ІБ і оцінка безпеки комп'ютерних систем.

Метою пропонованої методології є оцінка загального рівня безпеки комп'ютерної системи, виявлення найбільш вразливих активів і найбільш небезпечних загроз для конкретної організації, визначення пріоритетів в усуненні вразливостей ІБ.

Процедура для пропонованої методології заснована на оцінці ризику ІБ і полягає в наступному:

- початкове опитування клієнтів;
- визначення активів;
- визначення важливості активів по словесній шкалі;
- пошук вразливостей конкретних активів;
- виявлення загроз, що виникають з виявлених вразливостей;
- визначення ступеня небезпеки загроз, виявлених в словесному масштабі;
- переклад значущості активів і ступеня загрози загроз в кількісні оцінки;
- розрахунок оцінки ризиків;
- ранжування по оцінці загального ризику. Виявлення найбільш вразливих активів і найбільш небезпечних загроз;
- ранжування вразливостей кожного активу;
- вироблення рекомендацій щодо усунення вразливостей і складання звітів.

Кожен з цих кроків описаний нижче.

Початкове опитування клієнтів

На цьому етапі необхідно з'ясувати і визначити наступне:

- структура мережі: фізична і логічна, розміщення обладнання, в т.ч. характеристики приміщень;
- набір перевірок безпеки: бажані і рекомендовані;
- активи: список і їх значення для клієнта;
- загрози: список і рівень небезпеки для клієнта;

- облікові записи (потрібно для виконання вибраних перевірок): логіни користувачів, паролі, точки входу.

Визначення активів

Щоб ідентифікувати список активів цільової організації, необхідно перерахувати всі невеликі об'єкти клієнта, які схильні до загрозам інформаційної безпеки (і, отже, викликають ризики). Список активів повністю залежить від структури і характеристик цільової організації.

Активами можуть бути не тільки фізичні об'єкти (сервери, термінали, камери, друковані документи і т.д.), але і інформація (файли, згенеровані ключі і т.д.).

Експерти рецензуються сторони складають остаточний список активів на основі первинного опитування.

Визначення важливості активів по словесній шкалі

Початкові дані опитування клієнта перевіряються на основі думок експертів перевіряє боку і офіційних документів (таких як стандарти ІВ або інформаційні бюлетені Microsoft).

В кінці цього етапу кожен актив повинен мати усну оцінку його важливості. Рекомендовані рівні важливості: Критичний, Важливий, Звичайний, Маловажливий, Неважливий.

Приклад результату цього кроку наведено в табл. 3.

Пошук вразливостей конкретних активів

Пошук вразливостей певних активів виконується відповідно до діапазону доступних перевірок:

- тест на проникнення;
- виявлення зловмисників серед співробітників організації;
- аналіз конфігурації;
- аналіз фізичного доступу до об'єктів мережі організації;
- інші аудити ІБ.

Виявлення загроз, що виникають з виявлених вразливостей

Одна вразливість може бути джерелом кількох погроз (наприклад, фізичний доступ до сервера може викликати як руйнування, так і захоплення обладнання). Отже, загрози повинні бути ідентифіковані для кожної знайденої уразливості на основі думок експертів перевіряє боку і офіційних документів (наприклад, стандартів ІБ або інформаційних бюлетенів Microsoft).

Список загроз повинен бути складений в кінці цього етапу.

Визначення ступеня небезпеки загроз, виявлених в словесному масштабі

Визначення рівня небезпеки загроз відбувається в словесному масштабі.

Початкові дані опитування клієнта перевіряються на основі думок експертів перевіряє боку і офіційних документів (таких як стандарти ІВ або інформаційні бюлетені Microsoft).

В кінці цього етапу кожна загроза повинна мати усну оцінку рівня небезпеки. Рекомендовані критерії важливості: Критичний, Важливий, Середній, Низький, Малоймовірний

Приклад результату даного етапу наведений в табл. 4.

Переклад значущості активів і ступеня загрози загроз в кількісні оцінки

Для автоматизованої оцінки ризиків слід перевести попередньо отримані словесні оцінки активів і загроз в кількісні. Рекомендовані шкали оцінок, що приведені в табл. 2.1 та 2.2. Приклад результату даного етапу наведений в табл. 2.3 та 2.4.

Таблиця 2.1.

Рекомендована шкала оцінок важливості активів

Важливість активу	**Збиток при реалізації загроз (умовна оцінка)**
Критичний	5
Важливий	4
Рядовий	3
Маловажливий	2
Неважливий	1

Таблиця 2.2.

Рекомендована шкала оцінок ступеня небезпеки загроз

Рівень небезпеки загрози	**Вірогідність реалізації (умовна оцінка)**
Критичний	5
Важливий	4
Середній	3
Низький	2
Малоймовірний	1

Таблиця 2.3.

Приклад оцінок важливості активів

Актив	**Важливість**	**Збиток**
Сервер доступу до Інтернет	Критичний	5
Сервер 1С:Підприємство, термінал.сервер	Критичний	5
Головний контролер домену	Критичний	5
Поштовий сервер	Важливий	4
Запасний контролер домену, сервер БД	Важливий	4

Таблиця 2.4.

Приклад оцінок рівня небезпеки загроз

Загроза	**Рівень небезпеки**	**Частота**
Переповнення буфера	Критичний	5
Несанкціоноване отримання прав	Важливий	4
Виток інформації	Важливий	4
Віддалене виконання коду	Середній	3
Відмова в обслуговуванні	Низький	2

Розрахунок оцінок ризиків

Щоб автоматизувати розрахунок оцінки ризиків в СУІБ «Матриця», треба виконати такі дії в головному меню «Списки елементів»:

1. Введення активів, що заявлені в СУІБ, у вигляді списку назв активів і вартості втрат відповідно до обраної шкалою оцінок;
2. Введення ідентифікованих загроз в СУІБ у вигляді списку, що містить назви загроз і їх частоту (ймовірність реалізації), відповідно до обраної шкалою оцінок;
3. Створення список ризиків, призначивши загрозу активам.

Автоматичне перехресне об'єднання активів-загроз недоступно, якщо можуть виникнути неіснуючі, незначні або навіть неможливі ризики (наприклад, фізичний збиток цифрових підписів).

Оцінки ризику розраховуються автоматично шляхом множення величини втрат активу на частоту загрози:

$R = W \times n$

де R - ризик, W - збиток, n - частота.

У головному меню пункту «Оцінка ризиків» у зведеній діаграмі представлений огляд ризиків, а в зведеній таблиці - розподіл загроз за активами і навпаки, із загальними оцінками для кожного активу і кожної загрози.

Зведена оцінка ризиків (в зведеній таблиці ризиків) необхідна для періодичної оцінки. Це дає вам можливість відстежувати зміни загального рівня ризику на протязі деякого часу. Приклад зведеної таблиці та зведеної діаграми ризику показані на рис. 2.3 і рис. 2.4.

Оцінка ризиків

Відображення: Таблиця / Діаграма

	Актив					
	Головний контрол	Запасний контрол	Поштовий сервер	Сервер 1С:Підпри	Сервер доступу до	Общие итоги
Загроза	Оцінка ризику	Оцінка ризику	Оцінка ризику	Оцінка ризику	Оцінка ризику	Оцінка ризику
Виток інформації	20	16	16	20	20	92
Віддалене виконання коду	15	12	12	15	15	69
Відмова в обслуговуванні	10	8	8	10	10	46
Несанкціоноване отримання прав	20	16	16	20	20	92
Переповнення буфера	25	20	20	25		90
Общие итоги	90	72	72	90	65	389

Рис. 2.3. Приклад сформованої таблиці ризиків

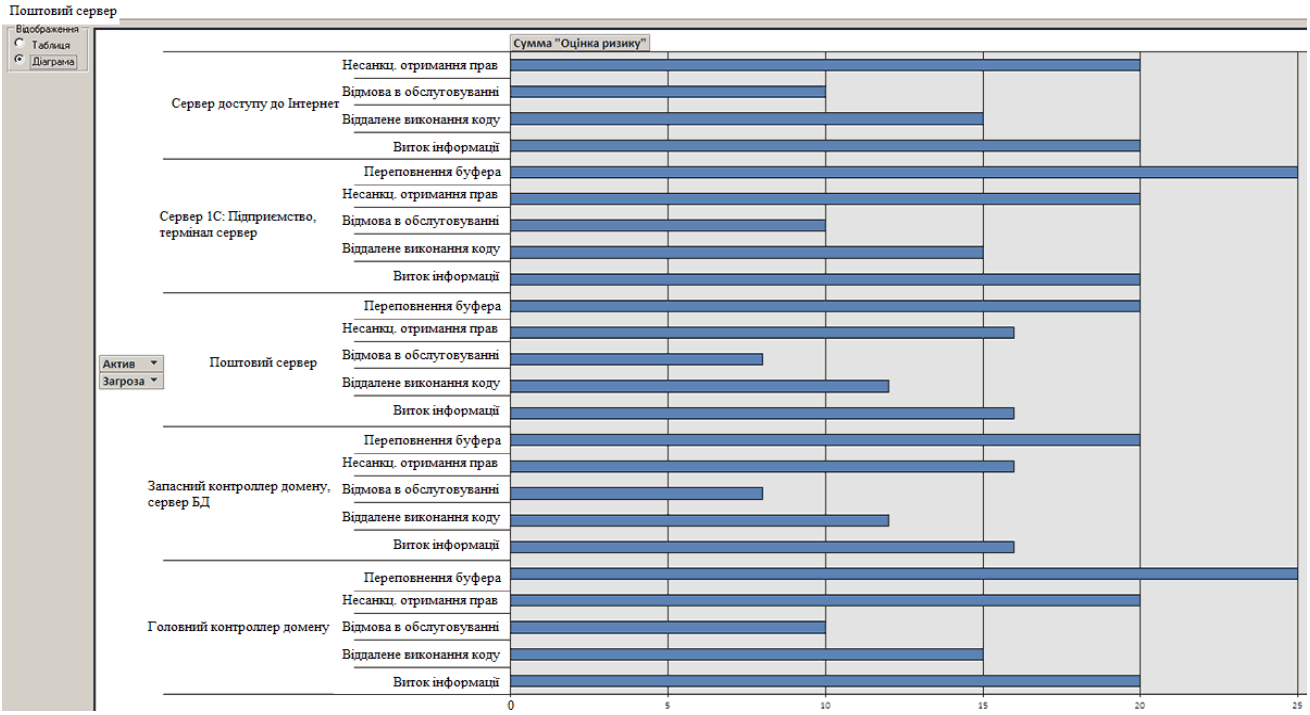

Рис. 2.4. Приклад сформованої діаграми ризиків

Виявлення найбільш вразливих активів і найбільш небезпечних загроз

У зведеній діаграмі оцінки ризиків, видаляючи поля з області даних одне за іншим, спочатку отримаєте діаграму загальних активів, а потім загроз. Приклади сумарних оцінок активів і загроз показані на рис. 2.5 і рис. 2.6.

Зробіть висновки про найбільш вразливих активах і найбільш небезпечних загроз (вони матимуть найвищі оцінки загального ризику).

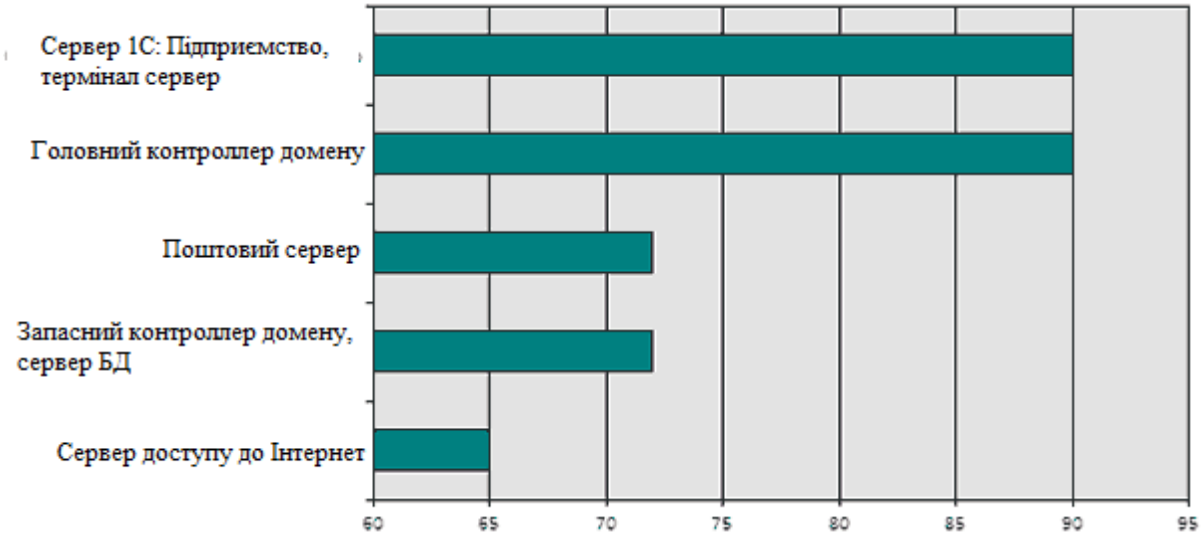

Рис. 2.5. Приклад графіку загальних оцінок за активами

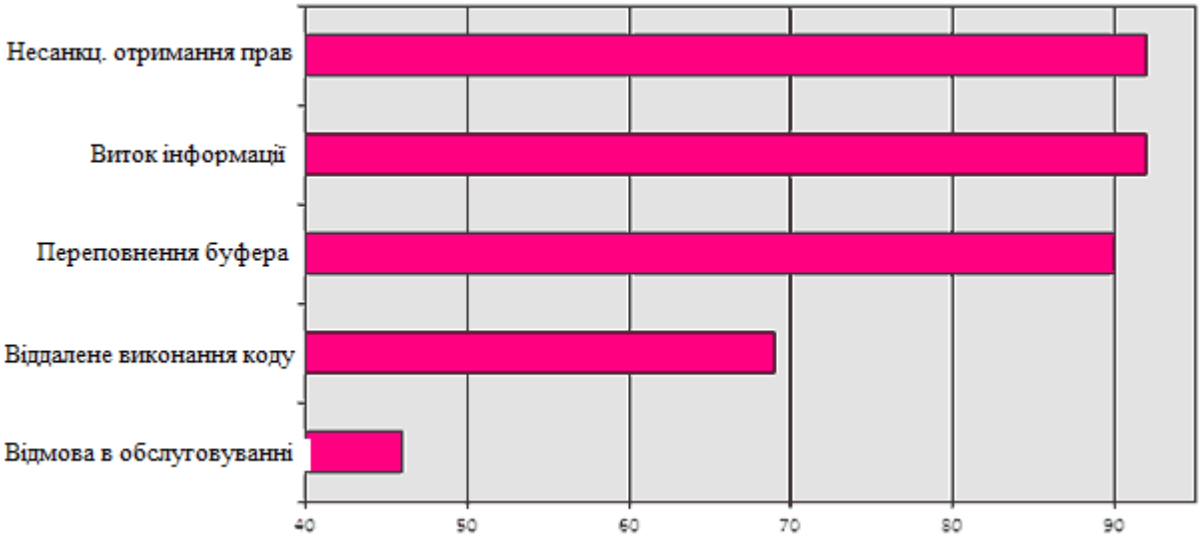

Рис. 2.6. Приклад графіку загальних оцінок за загрозами

Ранжування вразливостей кожного активу

Вразливості активів слід згрупувати і розрахувати оцінки загального ризику для кожної уразливості кожного активу. Слід мати на увазі, що кожна вразливість може бути джерелом однієї або декількох загроз.

Оцінка загального ризику для уразливості розраховується для кожного активу, оскільки активи мають різні значення для одних і тих же погроз.

Числова сукупна оцінка ризику для уразливості конкретного активу розраховується як сума оцінок ризику для кожної загрози, якої схильна ця активність:

$$V_a = \sum R_a = W_a \times \sum n_a$$

де V_a - вразливість активу, R_a - ризик активу, W_a - збиток активу, n_a - частота загрози.

Приклад розрахунку чисельної оцінки сукупного ризику для однієї уразливості наведено в табл. 2.5. Після отримання кількісних підсумкових оцінок ризику для всіх вразливостей відсортуйте їх за ступенем зниження і потім переведіть їх в словесні оцінки, використовуючи рекомендовану шкалу оцінок, представлену в таблиці. 2.6.

Таблиця 2.5.

Приклад розрахунку чисельної оцінки сукупного ризику для однієї уразливості

Вразливість	**Загроза для даного активу**	**Оцінка ризику загрози для даного активу**	**Числова сумарна оцінка ризику вразливості**
Не встановлені критичні оновлення Windows: MS04-012, MS08-061, MS08-063, MS08-064.	Несанкціоноване отримання прав	20	70
	Віддалене виконання коду	15	
	Відмова в обслуговуванні	10	
	Переповнення буфера	25	

Таблиця 2.6.

Рекомендована шкала сумарних оцінок ризику вразливості

Числова сумарна оцінка ризику вразливості	**Словесна оцінка**	**Опис для клієнта**
>100	Критична	Несе найбільшу кількість загроз для даного активу; найбільший збиток у разі використання зловмисниками.
51-100	Важлива	Несе серйозні загрози і, ймовірно, буде використана зловмисниками.
25-50	Середня	Представляє небезпеку, проте її використання зловмисниками малоймовірно.
<25	Низька	Малоймовірні загрози, або мінімальний збиток.

Вироблення рекомендацій щодо усунення вразливостей і складання звітів.

Дати типові рекомендації щодо усунення вразливостей на основі офіційних документів (таких як стандарти ІБ або інформаційні бюлетені Microsoft). Потім подальші рекомендації, основані на думках і досвіді експертів перевіряючої сторони.

Скомпілювати таблиці вразливостей для активу скінів зі стовпцями: Уразливість, Загрози, Релевантность (словесна оцінка загального ризику уразливості), Рекомендації.

Звіт з наступних розділів, в якому будуть викладені основні етапи оцінки ризиків інформаційної безпеки за цією методологією:

1. Терміни, визначення та скорочення, використовувані в звіті;
2. Цілі та обсяг досліджень;
3. Дослідження вразливості: виявлення уразливості і короткий виклад оцінок ризику;
4. Рекомендації щодо усунення вразливостей;
5. Додаткові розділи (для споживання),
6. Загальні висновки.

Запропоновано метод оцінки IP-безпеки за допомогою СУІБ "Матриця". У свою чергу, Кількісна оцінка забезпечує точний вибір пріоритетів в усуненні вразливостей ІБ.

Пропонована методологія є універсальною з точки зору розміру і профілю організації.

3. Дослідження процесів управління інформаційною безпекою підприємства та розробка рекомендацій.

3.1. Досвід впровадження системи управління інформаційною безпекою

Сьогодні багато українських компаній вирішують завдання створення системи інформаційної безпеки (системи ІБ), яка відповідала б «найкращим практикам» і стандартам в області ІБ і відповідала сучасним вимогам захисту інформації за параметрами конфіденційності, цілісності та доступності. Причому, це питання є важливим не тільки для «молодих» компаній, що розвивають свій бізнес з використанням сучасних інформаційних технологій управління. Не менш, а швидше і більш важливою ця проблема є для підприємств і організацій, які давно працюють на ринку, які приходять до необхідності модернізувати існуючу у них систему ІБ.

З одного боку, необхідність підвищення ефективності системи ІБ пов'язана із загостренням проблем захисту інформації. Тут можна згадати, по-перше, зростаючу потребу забезпечення конфіденційності даних. Українські компанії, слідом за своїми західними колегами, приходять до необхідності враховувати так звані репутаційні ризики, відповідальність за забезпечення конфіденційності даних своїх клієнтів, субпідрядників, партнерів. Однак в більшості українських компаній організаційна складова системи ІБ розвинена слабо. Наприклад, дані як такі часто вже не класифікуються, тобто компанія не має чіткого уявлення про те, які типи даних вона має, з точки зору їх конфіденційності, критичності для бізнесу. І це тягне за собою ряд проблем, починаючи від складності обґрунтування адекватності заходів інформаційної безпеки і закінчуючи неможливістю використовувати законні методи їх розслідування в разі інциденту.

Ще одна актуальна проблема в області захисту даних - це безперервність функціонування інформаційних систем. Для багатьох сучасних компаній, в першу чергу, фінансові інститути, виробничі холдинги, великі дистриб'ютори, безперебійна робота інформаційних систем, що підтримують основний бізнес, і доступність даних стають критичною проблемою. Збої в роботі систем призводять до переривання бізнес-процесів і, як наслідок, до незадоволеності клієнтів, штрафів

та інших збитків. А в забезпеченні доступності даних важливу роль відіграють системи захисту, що запобігають зловмисні атаки на інформаційну систему (атаки типу «відмова в обслуговуванні» і ін.).

З іншого боку, в більшості великих компаній має місце успадкована «клаптева» автоматизація. Розвиток корпоративної інформаційної системи (ІС) здійснюється досить хаотично; небагато компаній спираються на продуману ІТ-стратегію або плани розвитку ІС. Зазвичай використовується політика «латання дірок», нові ІТ-сервіси додаються без прив'язки до вже існуючих і без урахування їх взаємозв'язку. І точно так само відсутня продумана архітектура системи ІБ, мало хто до теперішнього часу визначав, наскільки система ІБ повна, наскільки вона покриває ризики, надлишкова вона або, навпаки, є недостатньою і т.д. І що важливо - система ІБ рідко буває обґрунтована економічно.

Досвід роботи деяких компаній свідчить, що побудова ефективної системи ІБ має спиратися на аналіз ризиків (в тому числі аналіз можливого збитку), який є основою при виборі технічних підсистем, їх економічному обґрунтуванні. Плюс комплекс організаційних заходів і створення системи управління ІБ (системи управління інформаційними ризиками). І, нарешті, дотримання вивірених на практиці принципів побудови системи ІБ, наприклад, принципу «багаторівневого» захисту.

Таким чином, при побудові (модернізації) системи ІБ доцільно реалізовувати цикл робіт (рис. 3.1), що включає обов'язковий етап діагностичного обстеження з оцінкою вразливостей інформаційної системи і загроз, на основі якого проводиться проектування системи і її впровадження.

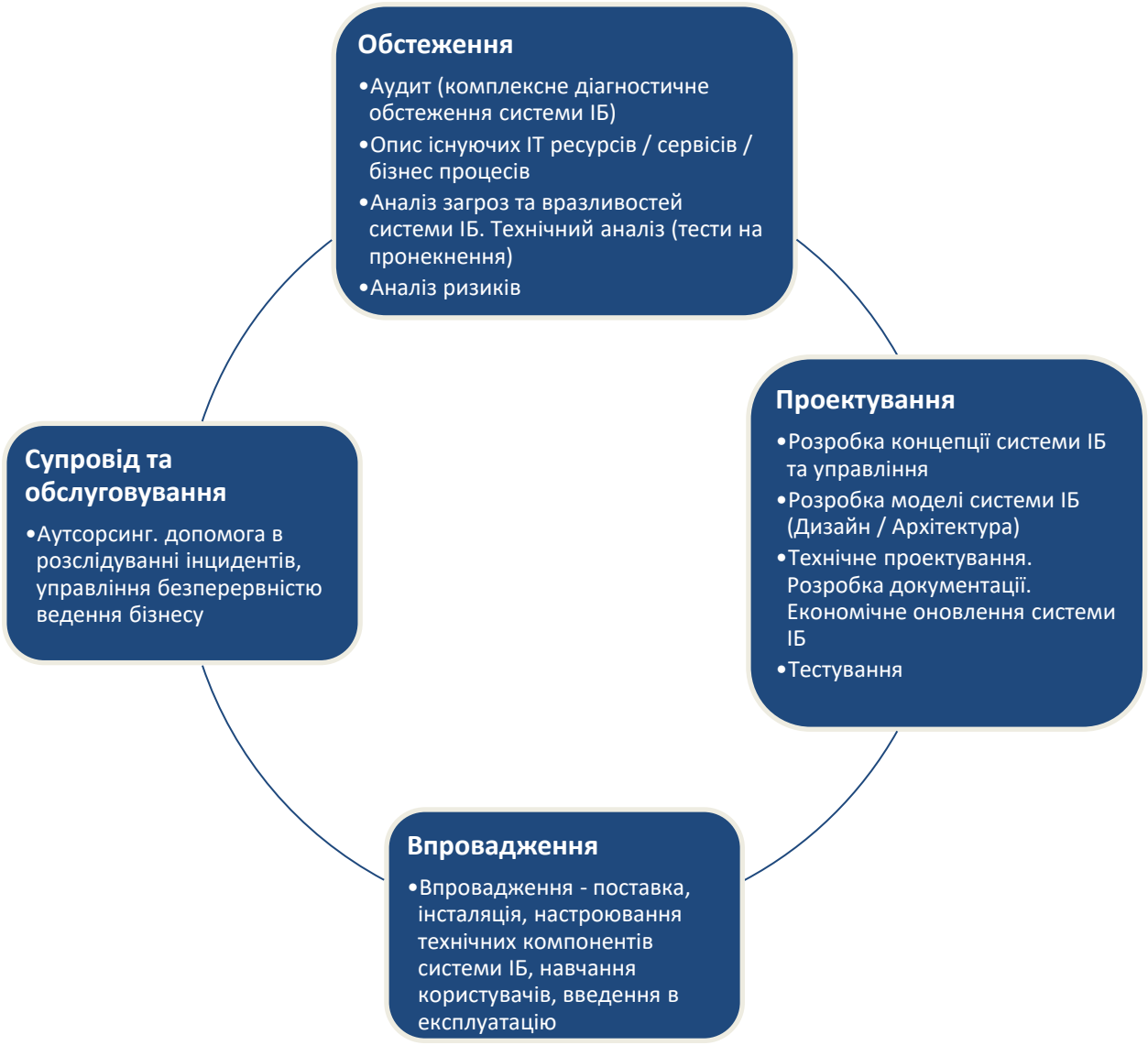

Рис.3.1. Повний цикл робіт для забезпечення інформаційної безпеки

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

Стосовно до забезпечення безпеки інформаційної системи (ІС) це можна представити таким чином.

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

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

Мати інструменти контролю правильності налаштувань ІС.

Розробками такого роду останнім часом займається кілька великих корпорацій. Свої рішення пропонують Oracle і IBM.

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

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

Для опису інформаційної системи зазвичай необхідно знати наступне.

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

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

Відповідальний за адміністрування цих ресурсів.

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

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

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

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

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

Виявляти невідповідність моделі ІС і її поточного стану системи управління безпекою дозволяють агенти-сенсори. Такі агенти регулярно стежать за всіма пов'язаними з безпекою ІС настройками операційних систем, додатків, засобів захисту, мережевого обладнання.

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

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

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

Використання описаного підходу до управління інформаційною безпекою - це серйозна зміна звичного ритму роботи інформаційної системи.

Але витрачені зусилля більш ніж окупаються. Переваги впровадження систем управління безпекою зрозумілі. І, перш за все, це підвищення безпеки IP-адреси, оскільки відтепер усі зміни, внесені до налаштувань, будуть відслідковуватися та здійснюватися в суворій відповідності з політикою організації інформаційної безпеки. Додатковим бонусом стане зменшення витрат, пов'язаних з управлінням документообігом.

Крім того, після впровадження такої системи управління забезпечення безпеки інформації перестає бути спадщиною, відповідальністю та обов'язком лише вузьких спеціалістів. В управлінні інформаційною системою керівництво організації починає реально активно брати участь: зрештою, саме вони формулюють вимоги до налаштувань через механізм додатків.

Як приклад однією з головною задач діючої СУІБ є захист від витоку інформації на підприємстві.

Витік інформації є серйозною проблемою та реальною загрозою для більшості підприємств, що представляють різні галузі. Дані можуть бути втрачені через зловмисні наміри третіх осіб, через халатність працівників. При цілеспрямованій організації наносяться серйозні збитки. У конкурентному середовищі ця методика використовується багатьма сторонніми організаціями для отримання переваги над конкурентами, хоча і в такий незаконний спосіб.

Щоб усунути несприятливі наслідки втрати даних, потрібно використовувати системи захисту інформаційних активів. Їх створення повинно бути на високому професійному рівні, використовуючи сучасне обладнання та програмне забезпечення. Найкращим рішенням для боротьби з витоком інформації та відстеження робочого часу буде програма контролю NeoSpy. Це професійна програма-шпигунське програмне забезпечення, розроблена спеціально для відстеження вашого комп'ютера. Якщо говорити про законність спостереження за працівниками, то варто зазначити, що метою використання представленого програмного продукту є захист даних компанії (внутрішня програма обслуговування). Програма не використовується для вторгнення в конфіденційність, хакерські атаки. Цей продукт підходить для:

- підприємств;
- державних компаній;
- комерційних структур.

Чи законно використовувати програму стеження за співробітниками?

На будь-якому етапі розвитку бізнесу може знадобитися програмний продукт для захисту інформаційних активів. Як же зробити використання законним і ефективним? Перед встановленням програми потрібно провести збори серед співробітників. Керівник доносить до їхнього відома, що він володіє відповідними засобами для проведення моніторингу роботи. Він виступає в якості наглядача, але не шпигуна. Щоб при вирішенні конфліктних ситуацій з персоналом не виникло труднощів, потрібно грамотно скласти трудовий договір. У ньому потрібно прописати наступні пункти:

- за розголошення інформації підприємства, яка є комерційною таємницею, передбачено покарання. Це кваліфікується як посадовий злочин;
- заборона на застосування в робочий час сторонніх засобів зв'язку в особистих цілях: електронної пошти, телефону, факсиміле;
- майбутній співробітник підприємства дає згоду виконувати вищевикладені вимоги.

Які переваги дає використання спеціальної програми контролю за співробітниками?

Представлений інструмент сьогодні використовують багато підприємств і організації. Від збереження відомостей, що становлять комерційну або іншу таємницю, залежить майбутнє будь-якої організації. Щоб воно було безхмарним, потрібно використовувати ефективні інструменти захисту. Програми моніторингу комп'ютерів в локальних мережах дозволяють виключити найменшу ймовірність втрати інформації. Витік даних призводить до серйозних проблем у вигляді призупинення проекту і додаткових витрат. У разі звільнення працівника з вини якого були втрачені відомості, доведеться витратити час на пошук нового майстра. Якщо ж спроби злому були виявлені і припинені своєчасно, то можна виключити негативні наслідки.

Ще одна важлива перевага безперервного моніторингу - раціональне використання комп'ютерних засобів і оргтехніки. Практика багатьох організацій показує, що це дозволяє істотно скоротити витрати. Недобросовісні співробітники

можуть використовувати в своїх цілях інтернет, наприклад, для спілкування з друзями в соціальних мережах. Моніторинг дозволить ефективно контролювати робочий час, що позитивно позначиться на продуктивності і ефективності праці.

3.2. Проведення досліджень та обробка їх результатів (для вибраного прикладу).

Діагностичне обстеження / аудит системи ІБ

Для побудови ефективної системи інформаційної безпеки, вибір і впровадження адекватних технічних засобів захисту повинен передувати аналізом загроз, вразливостей інформаційної системи і на їх основі - аналізом ризиків інформаційної безпеки. Вибір програмно-апаратного забезпечення захисту та проектування систем ІБ грунтується на результатах такого аналізу з урахуванням економічної оцінки співвідношення «вартість контрзаходів щодо зниження ризиків / можливі втрати компанії від інцидентів інформаційної безпеки».

Таким чином, побудова системи ІБ компанії доцільно починати з комплексного діагностичного обстеження основних бізнес-процесів і інформаційної системи компанії, а також існуючих засобів контролю ІБ. Обстеження (аудит) існуючої системи інформаційної безпеки дозволить встановити, чи відповідає рівень безпеки інформаційно-технологічних ресурсів компанії висунутим вимогам, тобто забезпечуються необхідні параметри конфіденційності, цілісності і доступності ресурсів інформаційної системи. Аналіз ризику проводиться під час діагностичного обстеження. Щоб перевірити здатність інформаційної системи протистояти спробам отримати доступ і впливати на інформацію, іноді доцільно проводити тести на проникнення.

Існує кілька видів експертизи:

- Передпроектна діагностичне обстеження, яке проводиться під час модернізації або будівництва системи ІБ.;
- аудит системи ІБ (або системи управління ІБ) на відповідність вимогам внутрішньокорпоративних стандартів або міжнародним / національним

стандартам. Прикладом може служити сертифікаційний аудит системи управління ІБ по ISO 27001;

- спеціальні види обстеження, наприклад, при розслідуванні комп'ютерних інцидентів.

В процесі обстеження і аналізу системи інформаційної безпеки також ідентифікуються «власники» IT-ресурсів (включаючи автоматизовані системи і корпоративні дані) і особи, відповідальні за цілісність цих ресурсів. Встановлюються вимоги до системи поділу прав доступу (паролі, дозволу), включаючи всі правила доступу до інформаційної системи компанії. IT-ресурси класифікуються за ступенем важливості / критичності.

Перевіряються всі процедури безпеки, в тому числі підтримка системи ІБ, процес розслідування порушень ІБ, організація системи резервного копіювання, розмежування прав користувачів, процедури віддаленого доступу, захисту облікових записів і ін. Визначаються особи, відповідальні за розвиток і підтримку системи ІБ.

В ході аналізу і моделювання можливих сценаріїв атак на систему ІБ виявляються ситуації, які можуть призвести до порушення нормального «течії» бізнес-процесів. Визначаються можливі наслідки невідповідності системи ІБ політиці безпеки компанії.

Якщо обстеження виконується сторонньою організацією, то на всіх стадіях проекту необхідне залучення до робіт персоналу компанії-замовника. Це гарантує облік основних вимог, специфіки та інтересів компанії, що обстежується.

Істотною перевагою залучення до аудиту зовнішнього виконавця (компанії-інтегратора) є можливість використання накопиченого консультантом досвіду при аналізі кожного компонента системи ІБ на відповідність вимогам щодо забезпечення інформаційної безпеки, в тому числі і з позиції «кращої практики» для конкретної індустрії.

Методи аналітичної роботи

Пропонований методі дозволяє:

- повністю проаналізувати і задокументувати вимоги забезпечення інформаційної безпеки послуг, що надаються і гарантії захисту майнових прав та інтересів клієнтів.
- уникати зайвих заходів безпеки, які можливі в разі суб'єктивної оцінки ризику;
- допомога в плануванні і реалізації захисту на всіх етапах життєвого циклу інформаційних систем;
- забезпечити виконання робіт в короткі терміни;
- надати обґрунтування вибору заходів протидії;
- оцінити ефективність контрзаходів, порівняти різні варіанти.

Досягти поставлених цілей можна при вирішенні таких основних завдань:

• класифікація інформації в категорії обмеженого доступу (професійна таємниця);

• прогнозування і своєчасне виявлення загроз причин і умов безпеки інформаційних ресурсів, які сприяють фінансовій, матеріального і морального збитку, порушення нормального функціонування і розвитку об'єкта;

• створення умов функціонування з найменшою вірогідністю реалізації загроз безпеки інформаційних ресурсів і стану різних видів шкоди;

• створення механізму і умов для оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні, ефективного припинення посягань на ресурси на основі правових, організаційних і технічних заходів, засобів забезпечення безпеки;

• створення умов для максимально можливої компенсації та локалізації шкоди, завданої незаконними діями фізичних і юридичних осіб, пом'якшення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічних цілей.

Визначення меж дослідження

Межі дослідження повинні бути встановлені в ході роботи. Для цього необхідно виділити ресурси інформаційної системи, для яких в майбутньому будуть проводитися оцінки ризиків. При цьому необхідно розділити ці ресурси і зовнішні елементи, з якими вони взаємодіють. Ресурсами можуть бути комп'ютерне обладнання, програмне забезпечення, інформаційні дані. Прикладами зовнішніх елементів є мережі зв'язку та інші засоби.

Побудова моделі інформаційної технології

При побудові моделі слід враховувати взаємозв'язок між ресурсами. Наприклад, вихід з ладу деякого обладнання може призвести до втрати даних або виходу з ладу іншого критичного елемента системи. Такі відносини визначають основу для побудови організаційної моделі інформаційної безпеки.

Дана модель, відповідно до запропонованої методології, будується наступним чином: для виділених ресурсів визначають їх вартісну оцінку, так як пов'язані з ними можливі фінансові втрати, а також для зниження репутації організації, дезорганізації її діяльності, нематеріальних збитків від розкриття конфіденційної інформації. інформація і т. д. Потім опишіть взаємозв'язок ресурсів, визначте загрози безпеки та оцініть ймовірність їх реалізації..

Вибір контрзаходів

Грунтуючись на побудованої моделі, ви можете розумно вибрати систему контрзаходів, які знижують ризики до прийнятних рівнів і мають найвищу рентабельність. До складу системи контрзаходів входять рекомендації з проведення регулярних перевірок ефективності системи безпеки..

Управління ризиками

Підвищені вимоги до інформаційної безпеки припускають відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Вони планують ці дії після завершення фази аналізу ризиків та протидії. Обов'язковою частиною цих планів є періодична перевірка відповідності існуючого режиму інформаційної безпеки політиці безпеки, сертифікація інформаційної системи на відповідність вимогам певного стандарту безпеки.

Оцінка досягнутої безпеки

На закінчення слід визначити ступінь безпеки оцінки інформаційного середовища замовника, на підставі якої можна довіряти інформаційному середовищі об'єкта. Цей підхід передбачає, що таке положення пов'язане з великими зусиллями при оцінці безпеки. Адекватність оцінки можлива при:

- Залучення до процесу оцінки якомога більшої кількості елементів інформаційного середовища об'єкта замовника
- Досягнення певного рівня безпеки за рахунок використання більшої кількості проектів і опису деталей реалізації при проектуванні системи безпеки;
- Строгість роботи, яка полягає в застосуванні більшої кількості пошукових інструментів і методів для виявлення менш очевидних недоліків або зменшення ймовірності їх присутності.

Методологія аналізу ризиків

Метою процесу оцінки ризиків є визначення їх характеристик в інформаційній системі і її ресурсах. На підставі таких даних вибираються необхідні засоби управління інформаційною безпекою.

Процес оцінки ризику складається з декількох етапів:

- опис об'єкта і заходи захисту;
- виявлення ресурсу і оцінка його кількісних показників (виявлення потенційного негативного впливу на бізнес);
- аналіз загроз інформаційної безпеки;
- оцінка слабких сторін;
- оцінка існуючих і перспективних засобів забезпечення інформаційної безпеки;
- оцінка ризику.

Ризик - це небезпека можливих втрат, якій піддається система система і організація, яка її використовує. Ризик залежить від:

- показників вартості ресурсів;
- ймовірність того, що буде завданий збиток ресурсам;
- ступінь легкості використання систем захисту від вразливостей в разі загроз;
- існуючі або плановані засоби захисту інформації.

Ці показники розраховуються математичними методами, що мають такі характеристики, як параметри обґрунтування і точності.

Створення профілю безпеки

На цьому етапі вони розробляють план проектування системи захисту інформаційного середовища клієнта; оцінити наявні кошти, провести аналіз і спланувати розробку і впровадження засобів захисту (рис. 3.2.). Необхідною елементом роботи є наявність допустимого ризику для об'єкта захисту.

Робота над створенням плану безпеки об'єкта починається зі створення профілю безпеки для цього об'єкта. Частина цієї роботи вже виконана в аналізі ризиків.

Рис. 3.2. Алгоритм оцінки інформаційних ризиків

3.3.Рекомендації щодо вдосконалення процесів розробки та впровадженням системи управління інформаційною безпекою (для вибраного прикладу).

Перш ніж пропонувати будь-які технічні рішення для системи інформаційної безпеки об'єкта, необхідно розробити політику безпеки для нього.

Саме політика безпеки організації описує процедуру надання та використання прав доступу користувачів, а також вимоги до звітності користувачів про їхні дії безпеки.

Система інформаційної безпеки (СІБ) об'єкта ефективна, коли вона надійно підтримує реалізацію правил політики безпеки, і навпаки. Кроки для побудови політики безпеки організації:

- впровадження автоматизації структури вартості та аналізу ризиків в опис об'єкта;

- визначення правил будь-якого процесу використання цього типу доступу до ресурсів об'єкта автоматизації, які мають таку ступінь цінності.

Організаційна політика безпеки формуються у вигляді документа, який узгоджується з замовником, затверджується.

Формулювання цілей безпеки об'єкта

Детальний опис загальної мети побудови системи безпеки для об'єкта клієнта виражається набором факторів або критерії, які визначають мету. Сукупність факторів є основою для визначення системних вимог (вибору альтернатив). Фактори безпеки можна розділити на технологічні, технічні та організаційні.

Визначення вимог функціональної безпеки

Функціональні вимоги профілю безпеки визначаються добре відомими, усталеними і узгодженими функціональними вимогами безпеки. Всі вимоги до функцій безпеки можна розділити на два типи: управління доступом до інформації та управління інформаційним потоком.

На цьому етапі необхідно правильно визначити компоненти функцій безпеки для об'єкта. Компонент функції безпеки описує певний набір вимог безпеки - найменший обраний набір вимог безпеки для входу в профіль безпеки. Можуть бути залежності між компонентами.

Вимоги гарантії досягнутої безпеки

Структура гарантійних вимог аналогічна структурі функціональних вимог і охоплює класи, групи, компоненти і елементи гарантій, а також рівні гарантії. Класи і групи гарантії відображають такі питання, як розробка, управління конфігурацією, робоча документація, підтримка життєвого циклу, тестування, оцінка вразливостей і багато іншого.

Вимоги захисту безпеки виражаються шляхом оцінки можливостей інформаційної безпеки об'єкта. Така оцінка проводиться на рівні окремого механізму безпеки, який дозволяє визначити здатність відповідної функції безпеки

протистояти ідентифікованим загрозам. Залежно від відомого потенціалу атаки сила захисної функції визначається, наприклад, категоріями «базовий», «середній», «високий».

Потенціал атаки визначається досвідом, ресурсами і мотивами зловмисника. Пропонується використовувати зведення рівнів захисту безпеки. Рівні гарантій мають ієрархічну структуру, де кожний наступний рівень забезпечує гарантії і включає в себе всі вимоги попереднього.

Формування списку вимог

Список вимог до системи інформаційної безпеки, ескізний проект, план безпеки (далі - технічна документація, ТД) - це вимоги до середовища безпеки об'єкта замовника, які можуть містити посилання на відповідний профіль безпеки, а також як чітко заявлені вимоги.

Загалом, ТД забезпечує:

- уточнення функцій захисту;
- вибір архітектурних принципів побудови системи інформаційної безпеки;
- розробка логічної структури системи інформаційної безпеки (чіткий опис інтерфейсів);
- з'ясування вимог функцій забезпечення безпеки системи інформаційної безпеки;
- розробка методології та програми випробувань на відповідність сформульованим вимогам.

Оцінка досягнутої безпеки

На цьому етапі оцінюють рівень безпеки інформаційного середовища об'єкта автоматизації на основі оцінки, при якій після реалізації рекомендованих заходів можна довіряти інформаційному середовищі об'єкта.

Основи цієї методології припускають, що ступінь впевненості залежить від ефективності зусиль, зроблених до оцінки безпеки. Збільшення цього зусилля означає:

- значна кількість елементів інформаційного середовища об'єкта, залучених до процесу оцінки;
- розширення типів проектів і опису деталей виконання при проектуванні системи забезпечення безпеки;
- строгість роботи, яка включає використання більшої кількості пошукових інструментів і методів для виявлення менш очевидних слабких місць або зменшення їх ймовірності.

В цілому, методологія, розглянута вище, дозволяє оцінити або переоцінити поточний стан інформаційної безпеки підприємства, дати рекомендації по її забезпеченню (підвищенню), знизити можливі втрати підприємства (організації) за рахунок підвищення стабільності функціонування системи. корпоративна мережа, для розробки концепції та політики безпеки підприємства, а також для пропозиції планів щодо її захисту. конфіденційна інформація, передана по відкритих каналах зв'язку, захист корпоративної інформації від навмисного спотворення (знищення), несанкціонованого доступу, копіювання або використання.

Проектування системи ІБ

Наступним кроком в побудові системи ІБ є її проектування, включаючи систему управління ІБ.

Завдання проектування системи ІБ тісно пов'язана з концепцією архітектури системи ІБ. Побудова архітектури системи ІБ як інтегрованого рішення, підтримання балансу між безпекою та інвестиціями в систему ІБ забезпечує кілька переваг: інтеграція підсистем може знизити загальну вартість володіння, збільшити повернення інвестицій при впровадженні та поліпшити керованість системи, пов'язані з ІБ.

Інтегрована архітектура системи ІБ

До ідеології і створення комплексної архітектури системи ІБ компанія TopS BI прийшла після багатьох років роботи з великими компаніями за проектами забезпечення ІБ. Висока ефективність системи ІБ може бути досягнута, якщо все її компоненти представлені якісними рішеннями, функціонують як єдиний комплекс

і мають централізоване управління. Система безпеки повинна ґрунтуватися на аналізі ризиків, а витрати на його впровадження і підтримка повинні бути адекватні існуючим загрозам, тобто економічно обґрунтовані.

Інтегрована архітектура системи ІВ включає в себе набір наступних підсистем:

- підсистема захисту периметра мережі і міжмережеві екрани (брандмауери і т. Д.);
- підсистема безпеки мережевого сервера;
- захист робочих станцій;
- підсистема моніторингу та аудиту безпеки;
- засоби виявлення атак і автоматичного реагування;
- комплексна підсистема антивірусного захисту;
- інструменти аналізу безпеки і управління політикою безпеки;
- інструменти моніторингу цілісності даних;
- засоби криптографічного захисту інформації;
- інфраструктура відкритих ключів;
- підсистема резервного копіювання та відновлення;
- автоматизована система установки оновлень програмного забезпечення;
- інструменти управління безпекою;
- підсистема автентифікації і ідентифікації.

Необхідно ще раз підкреслити, що архітектура системи ІБ включає в себе систему управління (процеси і процедури щодо забезпечення ІБ) інформаційною безпекою (СУІБ). Завданнями СУІБ є систематизація процесів забезпечення ІБ, розстановка пріоритетів компанії в області ІБ, досягнення адекватності системи ІБ існуючим ризикам, досягнення її «прозорості». Останнє особливо важливо, тому що дозволяє чітко визначити, як взаємопов'язані процеси і підсистеми ІБ, хто за них відповідає, які фінансові та людські ресурси необхідні для їх забезпечення і т.д. Створення СУІБ дозволяє також забезпечити відстеження змін, що вносяться до

системи інформаційної безпеки, відстежувати процеси виконання політики безпеки, ефективно управляти системою в критичних ситуаціях.

В цілому, процес управління безпекою (Security Management) відповідає за планування, виконання, контроль і технічне обслуговування всієї інфраструктури безпеки. Організація цього процесу ускладняється тією обставиною, що забезпечення інформаційної безпеки компанії пов'язано не тільки із захистом інформаційних систем і бізнес-процесами, які підтримуються цими інформаційними системами. У компанії часто існують бізнес-процеси, не пов'язані з IT, але потрапляють в сферу забезпечення ІБ, наприклад, процеси кадрової служби по найму персоналу.

Етапи розробки системи ІБ

1. Розробка концепції інформаційної безпеки. Визначено основні цілі, завдання та вимоги, а також загальна стратегія побудови системи ІВ. Критичні інформаційні ресурси визначені. Розроблено вимоги до системи ІБ і визначені основні підходи до їх реалізації.

2. Створення / розвиток політики ІБ.

3. Побудова моделі системи управління ІБ (на основі процесно-рольової моделі).

4. Підготовка технічного завдання на створення системи інформаційної безпеки.

5. Створення моделі системи ІБ.

6. Розробка технічно-робочого проекту (ТРП) створення системи ІБ і архітектури системи ІБ. ТРП зі створення системи ІБ включає наступні документи.

- Пояснювальну записку, яка містить опис основних технічних рішень по створенню системи ІБ і організаційних заходів з підготовки системи ІБ до експлуатації.
- Обґрунтування вибраних компонентів системи ІБ і визначення місць їх розміщення. Опис розроблених профілів захисту.
- Специфікацію на комплекс технічних засобів системи ІБ.

- Специфікацію на комплекс програмних засобів системи ІБ.
- Визначення установок і режиму функціонування компонентів системи ІБ.

7. Тестування на стенді спроектованої системи ІБ.

8. Розробка організаційно-розпорядчих документів системи управління ІБ (політик щодо забезпечення інформаційної безпеки, процедур, регламентів і ін.).

9. Розробка робочого проекту (включаючи документацію на використовувані засоби захисту і порядок адміністрування, план введення системи ІБ в експлуатацію та ін.), Планування навчання користувачів і обслуговуючого персоналу інформаційної системи.

Впровадження системи ІБ

Після проведення повного тестування спроектованої системи ІБ, можна приступати до її впровадження. Роботи по впровадженню системи включають виконання наступних завдань:

- поставку програмних і технічних засобів захисту інформації;
- інсталяцію програмних компонентів;
- настройку всіх компонентів і підсистем;
- проведення приймально-здавальних випробувань;
- впровадження системи управління ІБ;
- навчання користувачів;
- введення системи ІБ в промислову експлуатацію.

Для ефективної подальшої експлуатації системи необхідно забезпечити її підтримку і супровід (власними силами компанії або силами залучених фахівців).

Як вибрати виконавця?

При проведенні робіт зі створення або модернізації системи інформаційної безпеки компанія часто звертається за допомогою до зовнішніх консультантів. Як вибрати надійного партнера, з яким можна було б довірити одну з найбільш критичних областей бізнесу?

В першу чергу, компанія-консультант має мати хорошу репутацію на ринку. По-друге, необхідно переконатися в великому досвіді роботи в сфері ІБ як самої компанії-консультанта, так і конкретних співробітників, задіяних в проекті. По-третє, необхідна наявність у виконавця програмно-апаратних засобів для побудови тестових стендів, проведення робіт з проектування та моделювання системи ІБ. Крім того, додаткові вигоди принесе наявність у виконавця високих партнерських статусів з постачальниками програмно-апаратних комплексів (це також є певною гарантією досвіду компанії-консультанта). І, головне, - необхідна наявність у виконавця центру підтримки, що працює в цілодобовому режимі. Послуги служби технічної підтримки виконавця можуть включати і аутсорсинг, і віддалений моніторинг стану засобів захисту інформації, і обслуговування підтримуваних засобів. Виконавці можуть виконувати роботи по супроводу продуктів - плановій заміні їх версій, консультування користувачів і ін. Тобто забезпечується технологічна основа для того, щоб система ІБ «жила» і розвивалася.

ВИСНОВКИ

За результатами роботи:

1. Досліджено міжнародні стандарти побудови системи управління інформаційної безпеки, які постійно вдосконалюються та розроблюються нові. Основою усіх цих стандартів є ISO / IEC 27001.

2. Встановлено, що проведення комплексу заходів із побудови СУІБ підприємства відповідно до вимог стандарту ISO 27001 дозволить вирішити такі завдання, як: підвищення рівня безпеки; покращення управління організацією; оптимізація витрат; зменшення ризиків; збільшення привабливості та довіри у клієнтів; підвищення репутації в умовах конкуренції.

3. Проаналізовано вимоги і методичні матеріали щодо розробки СУІБ підприємства. Були розглянуті проблеми побудови СУІБ та досліджені процеси УІБ підприємства, які показали, що стандарти побудови СУІБ постійно розвиваються з року в рік і проблема побудови більше не в застарілості нормативної бази, не в актуальності стандартів, а в халатному відношенні керівництва підприємства до організації забезпечення ІБ або надмірною економією на її складових. Доказами цьому являються недавні «спалахи» масових кібернетичних атак на середні та малі підприємства, які в основному надають інформаційні послуги. Проаналізувавши ці атаки, виявилось що більшість організацій працювало на неліцензованих («піратських») версіях програмного забезпечення «Windows», що зв’язано з надмірною економією на покупці оригінальної та захищеної версії для підприємств.

4. Розроблено рекомендації щодо покращення побудови системи управління інформаційною безпекою. Особливу увагу треба виділити знаходженню та оцінки ризиків, загроз та можливих матеріальних та репутаційних втрат організації, щоб правильно оцінити економічну доцільність побудови СУІБ. Для управління будь-якої складної системою необхідно створити жорсткий, але простий регламент обслуговування цієї системи і забезпечити контроль за тим, щоб настройки системи змінювалися відповідно до цього регламенту.

У застосовності до забезпечення безпеки інформаційної системи це можна уявити так:

1) Мати в наявності політику безпеки, в якій повинно бути чітко описано, хто і на якій підставі повинен мати доступ до ресурсів інформаційної системи.
2) Мати єдину точку взаємодії співробітників організації з інформаційною системою, через яку вони зможуть формулювати свої побажання на надання доступу до тих чи інших ресурсів інформаційної системи.
3) Мати інструменти контролю основних показників функціонування інформаційної системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Стаття: «Как избежать двойных стандартов в информационной безопасности» Станислав ПРИЩЕП. – Електронний ресурс – Режим доступу: http://www.iksmedia.ru/articles/5558688-Kak-izbezhat-dvojnyx-standartov-v.html

2. Про прийняття та скасування національних стандартів, прийняття поправок до національних стандартів Наказ № 312 від 16.10.2019. – Електронний ресурс – Режим доступу: http://uas.org.ua/ua/services/standartizatsiya/nakazi-dp-ukrndnts/2019-2/zhovten/

3. Стаття: «Изменения в нормативных документах Украины по вопросам защиты информации» – Електронний ресурс – Режим доступу: http://www.dut.edu.ua/ru/news-1-0-5143-

4. Стаття «Інформаційна безпека і її складові». – Електронний ресурс – Режим доступу: https://egrivna.com/informacijna-bezpeka-i-ii-skladovi-2/

5. Стаття «Система економічної безпеки підприємства та її методологічні засади» – Електронний ресурс – Режим доступу: https://studopedia.su/8_58207_sistema-ekonomichnoi-bezpeki-pidpriiemstva-ta-ii-metodologichni-zasadi.html

6. Про захист інформації в автоматизованих системах: Закон України // Відомості Верховної Ради. 1994.-№31.-286 с.

7. МЕЖДУНАРОДНЫЙ СТАНДАРТ ISO/IEC 27001 [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/ISO/IEC_27001

8. ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ СОВРЕМЕННОЙ ОРГАНИЗАЦИИ Шахалов Ігор Юр’євич, Дорофеев Олександр Володимирович [Електронний ресурс] Режим доступу: https://cyberleninka.ru/article/n/osnovy-upravleniya-informatsionnoy-bezopasnostyu-sovremennoy-organizatsii

9. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ «Матриця». [Електронний ресурс] Режим доступу: http://www.epos.ua/view.php/about_pubs_archive

10. Про інформацію:,Закон України від 2 жовтня 1992 року №2657-XII.

11. Батюк А.Є. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Двуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2004. – С. 343–384.

12. Власова Л.А. Защита информации / Л.А. Власова. – Хабаровск: РИЦ ХГАЭП, 2007. – 84 с.

13. Замкова Т.В. Проблемы защиты информации в современных информационных системах / Т.В. Замкова. – [Електронний ресурс]. – Режим доступу: http://www.rae.ru/snt/?section=content&op=show_article&article_id=3893

14. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування // А.А. Литвинюк. – [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf

15. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Джабраил Матиев. – Електронний ресурс. – Режим доступу: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/

16. Про концепцію національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28.

17. Про національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28

18. Стаття «Методика построения корпоративной системы защиты информации» Сергей ПЕТРЕНКО. – Електронний ресурс. – Режим доступу: http://citforum.ru/security/articles/metodika_zashity/

19. Стаття «Система управления безопасностью: простые рецепты» – Електронний ресурс. – Режим доступу: http://citforum.ru/security/articles/sec_simple/

20. Стаття «Информационная безопасность и интересы бизнеса» А. Березин Електронний ресурс. – Режим доступу: http://citforum.ru/security/articles/business_interests/

21. Агафонов Г. Г., Буришев С. А., Прохоров С. Л. Концепции безопасности. / - К.: А-ДЕПТ, 2005.-Кн. 2.

22. Браіловський М. М., Дорошко В. О., Чирков Д. В., Шелест М. Е. Захист економічної інформації: Навч. посібник / За ред. проф. В. О. Хорошка: - К.: НАУ, 2002

23. Бруксбенк Д., Уилсон Дж. Руководство по безопасности: Пер. с англ. - М.: ЮНИТИ-ДАНА, 2003.

24. Стаття «Управління безпекою підприємств в умовах ринкової економіки» . – Електронний ресурс. – Режим доступу: https://gospodarstva.com/upravlinnya-bezpekoyu-pidpriyemstv/

25. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: Автореф. дис. ... канд. юрид. наук: 12.00.08 / НАН України; Іа-т держави і права ім. В.М. Корецького. — К., 2003.

26. Брижко В.М., Гальченко О.М., Цимбалюк В.С. і ін. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. — К.: Інтеграл, 2002.

27. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. —- М.: Академический Проект; Фонд "Мир", 2003.

28. Василъченко 3. М. Структурні диспропорції у розвитку банківської системи України // Фінанси України. - 2005.

29. Віхорсв С. В., Кобцев Р. Ю. Як дізнатися - звідки напасти або звідки виходить загроза безпеці інформації // Захист інформації. Конфідент. – 2002

30. Вольоводз А. Г. Проект Європейської конвенції про кіберзлочини // Захист інформації. Конфідент -2001

31. Живко М. О. Захист інформації в системі економічної безпеки та підприємства /' Регіональне і місцеве самоврядування в нових умовах: партійна публічна адміністрація і безпосередня демократія: Мат-ли НІ укр.-польськ. наук.-практ. конф. (Львів, 2-4 березня 2006р.). - Л., 2006

32. Зегжда Д. П., Івашко А. М. Основы безопасности информационных систем.- М.: Гаряча лінія - Телеком, 2000.

33. Зубок М., Ніколаєва Л. Організаційно-правові основи безпеки банківської діяльності в Україні. - К.: Істина, 2000.

34. Логінов О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: Авторсф. канд. юр. наук: 12.00.07/Нац. акад. внутр. справ України.

35. Організаційно-правові основи захисту інформації з обмеженим доступом: Навч. посібник / А. Б.Стоцький, А. М. Гуз, А. І. Марущак та ін.; За заг. ред. В. С. Сідака - К.: Вид-во Європ. ун-ту, 2006

36. Пархоменко П. И., Яковлев С. А., Пархоменко Н. Г. Правовые аспекты проблем обеспечения информационной безопасности: - Мат-ли V Междунар. науч.-практ. конф. "Інформационная безопасность".-Таганрог: ТРТУ, 2003.