НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра комп’ютеризованих систем захисту інформації

**ЗВІТ**

**З НАСКРІЗНОГО МІЖДИСЦИПЛІНАРНОГО**

**КУРСОВОГО ПРОЄКТУ**

Тема: «Аудит системи інформаційної безпеки – проблеми і рішення»

Роботу виконав:

студент:

Білецький Дмитро Олександрович

група БІ – 242

захищено з оцінкою \_\_\_\_\_\_

Керівник:

Телющенко В.А.

« » 2021р.

Київ 2021

Зміст

[СПИСОК УМОВНИХ СКОРОЧЕНЬ 4](#_Toc71326492)

[АНОТАЦІЯ 5](#_Toc71326493)

[ВСТУП 6](#_Toc71326494)

[РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ АУДИТУ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 7](#_Toc71326495)

[1.1. Поняття аудиту інформаційної безпеки 7](#_Toc71326496)

[1.2. Основні складові системи аудиту інформаційної безпеки 9](#_Toc71326497)

[1.3. Напрями аудиту інформаційних систем 12](#_Toc71326498)

[1.4. Оціночний аудит інформаційних систем 14](#_Toc71326499)

[РОЗДІЛ 2. ХАРАКТЕРИСТИКА ВНУТРІШНЬОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 15](#_Toc71326500)

[2.1. Внутрішній аудит 15](#_Toc71326501)

[2.2. Цілі та задачі внутрішніх аудитів інформаційної безпеки 16](#_Toc71326502)

[2.3. Організаційні принципи 17](#_Toc71326503)

[2.4. Принципи ефективності інформаційної безпеки 17](#_Toc71326504)

[РОЗДІЛ 3. ХАРАКТЕРИСТИКА ЗОВНІШНЬОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 18](#_Toc71326505)

[3.1. Зовнішній аудит 18](#_Toc71326506)

[3.2. Цілі зовнішнього аудиту ІБ 18](#_Toc71326507)

[3.3. Принципи проведення 19](#_Toc71326508)

[3.4. Управління програмою інформаційної безпеки 19](#_Toc71326509)

[РОЗДІЛ 4. ХАРАКТЕРИСТИКА  АУДИТУ ЗА ОБ’ЄКТАМИ ДОСЛІДЖЕННЯ 22](#_Toc71326510)

[4.1. Основні види аудиту ІБ. 22](#_Toc71326511)

[4.2. Аудит на відповідність стандартам ІБ. 22](#_Toc71326512)

[4.3. Активний аудит інформаційних систем. 23](#_Toc71326513)

[РОЗДІЛ 5. МЕТОДИ АУДИТУ СИСТЕМ ТА МЕРЕЖ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ІНФОРМАЦІЙНІ РИЗИКИ ТА ЇХ ВИРІШЕННЯ. 24](#_Toc71326514)

[5.1. Методи аналізу даних при аудиті ІБ. 24](#_Toc71326515)

[5.2. Аналіз інформаційних ризиків підприємства. 25](#_Toc71326516)

[5.3. Методи оцінювання інформаційних ризиків підприємства. 29](#_Toc71326517)

[5.4. Управління інформаційними ризиками. 30](#_Toc71326518)

[РОЗДІЛ 6. ПРИКЛАД АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ 32](#_Toc71326519)

[6.1.Загальні поняття про компанію. 32](#_Toc71326520)

[6.2. Обстеження середовищ функціонування АС 33](#_Toc71326521)

[6.3. Визначення потенційних загроз для інформації 34](#_Toc71326522)

[6.4. Джерела загроз безпеці інформації, їх класифікація 36](#_Toc71326523)

[6.5. Розробка політики безпеки інформації в АС 38](#_Toc71326524)

[6.6. Цілі політики безпеки 39](#_Toc71326525)

[6.7. Методи протистояння загрозам 40](#_Toc71326526)

[6.8. Обмеження співробітників організації 44](#_Toc71326528)

[6.9. Порядок видалення інформації в мережі 45](#_Toc71326529)

[6.10. Порядок зберігання інформації на підприємстві 45](#_Toc71326530)

[6.11. Ідентифікація користувачів відбувається в такій послідовності: 45](#_Toc71326531)

[ВИСНОВКИ 46](#_Toc71326532)

[СПИСОК ЛІТЕРАТУРИ 47](#_Toc71326533)

# СПИСОК УМОВНИХ СКОРОЧЕНЬ

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission;

TCP/IP – Transmission Control Protocol/ Internet Protocol;

АС – автоматизована система;

ІС – інформаційна система;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

ІТ – інформаційні технології;

СУБІ (СМІБ) – система управління інформаційною безпекою;

КСЗІ – комплексна система захисту інформації;

PDCA – планування-дія-перевірка-коригування;

КІСП – комп'ютерна інформаційна система підприємства;

ПЗ – програмне забезпечення;

ОС – операційна система;

ДСТУ - національні стандарти України;

ПІБ – політика інформаційної безпеки;

ІР – інформаційний ресурс;

ІзОД – інформація з обмеженими доступом;

СУБД – система управління базами даних;

# АНОТАЦІЯ

Тема роботи: Аудит системи інформаційної безпеки – проблеми і рішення.

У цій роботі буде розглянуто аудит інформаційної безпеки його складові та напрями, характеристика внутрішнього та зовнішнього аудитів, характеристика аудиту за об’єктами дослідження, методи аудиту систем та мереж інформаційної безпеки, інформаційні ризики та їх вирішення, приклад застосування аудиту інформаційної безпеки на підприємстві.

Основна частина:

1. Ознайомимся з поняттям аудиту інформаційної безпеки.
2. Розглянемо основні складові системи аудиту інформаційної безпеки, напрями аудиту інформаційних систем, оціночний аудит інформаційних систем.
3. Дослідимо внутрішній аудит, цілі та задачі внутрішніх аудитів інформаційної безпеки, організаційні принципи та принципи ефективності інформаційної безпеки внутрішнього аудиту.
4. Дослідимо зовнішній аудит, його цілі та принципи проведення.
5. Дізнаємось про інші види аудиту, методи аналізу даних при аудиті інформаційної безпеки, інформаційні ризики підприємства.
6. На прикладі розглянемо аудит системи інформаційної безпеки компанії «Медок», загрози інформаційній безпеці та методи для боротьби ними.

**English Translation:**

This work will consider the information security audit, its components and directions, the characteristics of internal and external audits, the characteristics of the audit of research objects, methods of auditing information security systems and networks, information risks and their solutions, an example of information security audit in the enterprise.

Plan:

1. To get acquainted with the concept of information security audit.
2. To consider the main components of the information security audit system, areas of information systems audit, evaluation audit of information systems.
3. To investigate internal audit, goals and objectives of internal information security audits, organizational principles and principles of effective information security of internal audit.
4. To investigate the external audit, its objectives and principles.
5. To learn about other types of audit, methods of data analysis in information security audit, information risks of the enterprise.
6. Using the example we will consider the audit of «Медок» information security system, information security threats and methods to combat them.

# ВСТУП

В даний час все більш затребуваною на ринку інформаційної безпеки стає послуга аудиту. Однак, як показує практика, і замовники, і постачальники часто розуміють суть цієї послуги по-різному. Проблеми розвитку аудиту є досить різні, всі вони пов'язані з розвитком аудиторської діяльності в Україні, і потребують нагального вирішення.

Сьогодні інформаційні системи (ІС) відіграють ключову роль в забезпеченні ефективності роботи комерційних і державних підприємств. Повсюдне використання ІС для зберігання, обробки і передачі інформації робить актуальними проблеми їх захисту, особливо з огляду на глобальну тенденцію до зростання числа інформаційних атак, що приводять до значних фінансових і матеріальних втрат. Для ефективного захисту від атак підприємствам необхідна об'єктивна оцінка рівня безпеки ІС - саме для цих цілей і застосовується аудит безпеки.

Взагалі аудит - форма незалежного, нейтрального контролю будь-якого напрямку діяльності комерційного підприємства, широко використовувана в практиці ринкової економіки, особливо в сфері бухгалтерського обліку. Не менш важливим з точки зору загального розвитку підприємства є його аудит безпеки, який включає аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки, особливо щодо інформаційних ресурсів, оцінку поточного рівня захищеності інформаційних систем (ІС), локалізацію вузьких місць в системі їх захисту, оцінку відповідності ІС існуючим стандартам в області інформаційної безпеки і вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.

Якщо говорити про головну мету аудиту інформаційної безпеки, то можна її визначити як проведення оцінки рівня безпеки інформаційної системи підприємства для управління ним в цілому з урахуванням перспектив його розвитку.

В сучасних умовах, коли інформаційні системи пронизують всі сфери діяльності підприємства, а з урахуванням необхідності їх зв'язку з Інтернет вони виявляються відкритими для реалізації внутрішніх і зовнішніх загроз, проблема інформаційної безпеки стає не менш важливою, ніж економічна або фізична безпека.

Незважаючи на важливість даної проблеми для підготовки фахівців із захисту інформації, вона до цього часу не була включена в вигляді окремого курсу в існуючі навчальні плани і не розглядалася в підручниках і навчальних посібниках. Це було пов'язано з відсутністю необхідної нормативної бази, непідготовленістю фахівців і недостатнім практичним досвідом в області проведення аудиту інформаційної безпеки.

Загальна структура роботи включає наступну послідовність питань, що розглядаються:

• описується модель побудови системи інформаційної безпеки (ІБ), що враховує загрози, вразливості, ризики та прийняті для їх зниження або запобігання контрзаходи;

• розглядаються методи аналізу та управління ризиками;

• викладаються базові поняття аудиту безпеки і дається характеристика цілей його проведення;

• даються практичні рекомендації з проведення аудиту ІБ на підприємстві.

Аудит дозволяє оцінити поточну безпеку функціонування інформаційної системи, оцінити і прогнозувати ризики, управляти їх впливом на бізнес-процеси фірми, коректно і обґрунтовано підійти до питання забезпечення безпеки її інформаційних активів, стратегічних планів розвитку, маркетингових програм, фінансових і бухгалтерських відомостей, вмісту корпоративних баз даних. В кінцевому рахунку, грамотно проведений аудит безпеки інформаційної системи дозволяє домогтися максимальної віддачі від коштів, інвестованих у створення і обслуговування системи безпеки.

# РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ АУДИТУ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 1.1. Поняття аудиту інформаційної безпеки

Аудит являє собою незалежну експертизу окремих областей функціонування організацій.

Цілями проведення аудиту безпеки є:

* аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів;
* оцінка поточного рівня захищеності ІС;
* локалізація вузьких місць в системі захисту ІС;
* оцінка відповідності ІС існуючим стандартам в області інформаційної безпеки;
* вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.

Аудит безпеки підприємства (фірми, організації) повинен розглядатися як конфіденційний інструмент управління, що виключає з метою конспірації можливість надання інформації про результати його діяльності стороннім особам і організаціям.

Для проведення аудиту безпеки підприємства може бути рекомендована наступна послідовність дій.

1. Підготовка до проведення аудиту безпеки:

* вибір об'єкта аудиту (фірма, окремі будівлі і приміщення, окремі системи або їх компоненти);
* складання команди аудиторів-експертів;
* визначення обсягу і масштабу аудиту та встановлення конкретних термінів роботи.

1. Проведення аудиту:

* загальний аналіз стану безпеки об'єкта аудиту;
* реєстрація, збір і перевірка статистичних даних і результатів інструментальних вимірювань небезпек і загроз;
* оцінка результатів перевірки;
* складання звіту про результати перевірки за окремими складовими.

1. Завершення аудиту:

* складання підсумкового звіту;
* розробка плану заходів щодо усунення вузьких місць і недоліків у забезпеченні безпеки фірми.

Для успішного проведення аудиту безпеки необхідно:

* активна участь керівництва фірми в його проведенні;
* об'єктивність і незалежність аудиторів (експертів), їх компетентність і висока професійність;
* чітко структурована процедура перевірки;
* активна реалізація запропонованих заходів забезпечення та посилення безпеки.

Аудит безпеки, в свою чергу, є дієвим інструментом оцінки безпеки та управління ризиками. Запобігання загроз безпеки означає в тому числі і захист економічних, соціальних та інформаційних інтересів підприємства.

Звідси можна зробити висновок, що аудит безпеки стає інструментом економічного менеджменту.

Залежно від обсягу аналізованих об'єктів підприємства визначаються масштаби аудиту:

* аудит безпеки всього підприємства в комплексі;
* аудит безпеки окремих будівель і приміщень (виділені приміщення);
* аудит устаткування і технічних засобів конкретних типів і видів;
* аудит окремих видів і напрямків діяльності: економічної, екологічної, інформаційної, фінансової і т.д.

Слід підкреслити, що аудит проводиться не з ініціативи аудитора, а з ініціативи керівництва підприємства, яке в даному питанні є основною зацікавленою стороною. Підтримка керівництва підприємства є необхідною умовою для проведення аудиту.

Аудит являє собою комплекс заходів, в яких крім самого аудитора, виявляються залученими представники більшості структурних підрозділів компанії. Дії всіх учасників цього процесу повинні бути скоординовані. Тому на етапі ініціювання процедури аудиту повинні бути вирішені наступні організаційні питання:

* права та обов'язки аудитора повинні бути чітко визначені і документально закріплені в його посадових інструкціях, а також в положенні про внутрішній (зовнішній) аудит;
* аудитором повинен бути підготовлений і узгоджений з керівництвом план проведення аудиту;
* в положенні про внутрішній аудит має бути закріплено, зокрема, що співробітники підприємства зобов'язані сприяти аудитору і надавати всю необхідну для проведення аудиту інформацію.

На етапі ініціювання процедури аудиту повинні бути визначені межі проведення обстеження. Якщо якісь інформаційні підсистеми підприємства не є достатньо критичними, їх можна виключити з меж проведення обстеження.

Інші підсистеми можуть виявитися недоступними для аудиту через міркувань конфіденційності.

Межі проведення обстеження визначаються в наступних категоріях:

1. Список обстежуваних фізичних, програмних і інформаційних ресурсів.
2. Майданчики (приміщення), що потрапляють в межі обстеження.
3. Основні види загроз безпеки, що розглядаються при проведенні аудиту.
4. Організаційні (законодавчі, адміністративні і процедурні), фізичні, програмно-технічні та інші аспекти забезпечення безпеки, які необхідно врахувати під час проведення обстеження, і їх пріоритети (в якому обсязі вони повинні бути враховані).

План і кордони проведення аудиту обговорюються на робочих зборах, в яких беруть участь аудитори, керівництво компанії і керівники структурних підрозділів.

Для розуміння аудиту ІБ як комплексної системи потрібно виділити такі основні складові процесу:

* об'єкт аудиту;
* мета аудиту;
* вимоги, що пред'являються;
* використовувані методи;
* масштаб;
* виконавці;
* порядок проведення.

З точки зору організації робіт при проведенні аудиту ІБ виділяють три принципових етапи:

1. збір інформації;

2. аналіз даних;

3. вироблення рекомендацій та підготовка звітних документів.

## 1.2. Основні складові системи аудиту інформаційної безпеки

У загальному вигляді під час проведення аудиту ІБ вирішуються такі завдання:

* збір та аналіз первинних даних про організаційну та функціональну структури ІТС організації, необхідних для оцінки стану ІБ;
* аналіз існуючої політики забезпечення ІБ на предмет повноти та ефективності;
* аналіз інформаційних і технологічних ризиків, пов'язаних із реалізацією загроз ІБ;
* тестові спроби несанкціонованого доступу до критично важливих вузлів ІТС та визначення уразливості в налаштуваннях захисту цих вузлів;
* формування рекомендацій з розробки (або доопрацювання) політики забезпечення інформаційної безпеки на підставі аналізу існуючого режиму інформаційної безпеки;
* формування пропозицій щодо використання існуючих та встановлення додаткових засобів захисту інформації для підвищення рівня надійності та безпеки ІТС організації.

Основна мета аудиту ІС – об'єктивно оцінити, наскільки поточний стан ІБ компанії відповідає висунутим вимогам і стандартам ІБ, а також завданням бізнесу щодо підвищення ефективності і рентабельності економічної діяльності компанії. Таким чином, завдання, які вирішуються при проведенні аудиту, можна розбити на дві групи:

1. Завдання, пов'язані з бізнес-процесами компанії.
2. Технічні завдання, пов'язані з особливостями функціонування мережі зв'язку, які зображаютьь самі бізнес-процеси. У першій групі завдань аудиту піддаються бізнес-процеси, а в другій – технологічні процеси обміну інформацією, які зображають бізнес-процеси компанії.

Деталізуючи завдання аудиту ІБ, можна виділити такі три важливі цілі, які реалізуються в процесі його проведення:

* оцінка поточної безпеки функціонування мережі зв'язку та корпоративної інформаційної системи;
* прогноз ризиків, а також створення системи управління їх впливом на бізнес-процеси компанії;
* технічно коректний і економічно обґрунтований підхід до питання забезпечення безпеки інформаційних активів компанії.

Процедура аудиту ІБ складається з:

* ініціювання та планування;
* обстеження, документування та збору інформації;
* аналізу отриманих даних і уразливостей;
* вироблення рекомендацій;
* підготовки звітних документів і здавання робіт.

В якості критеріїв аудиту ІБ використовуються:

* міжнародні, національні та галузеві стандарти;
* законодавча та нормативна база;
* внутрішні організаційно-розпорядчі документи організації;
* вимоги, сформульовані за результатами оцінки ризиків.

Методика проведення аудиту ІБ включає:

* методи аналізу захищеності, включаючи тестування на вторгнення (penetration testing), аналіз конфігурації засобів захисту інформації, аналіз сценаріїв здійснення атак і використання списків перевірки (checklists); -
* інтерв'ю зі співробітниками організації з використанням заздалегідь підготовлених і стандартизованих опитувальників;
* документування системи та аналізу ризиків з використанням спеціалізованого програмного забезпечення і шаблонів звітів;
* аналіз організаційно-розпорядчих документів з організації захисту інформації;
* оцінку процесів забезпечення інформаційної безпеки в організації, кваліфікації співробітників, знання ними своїх посадових обов'язків та ступеня їх обізнаності в питаннях інформаційної безпеки;
* оцінку достатності фізичних механізмів безпеки.

Аудит може бути внутрішнім і зовнішнім. Внутрішні аудити проводяться самою організацією або від її імені для різних внутрішніх цілей, наприклад для оцінки відповідності системи забезпечення ІБ встановленим вимогам. Зовнішні аудити проводяться сторонами, зацікавленими у діяльності організації, наприклад споживачами або іншими особами від їх імені, а також зовнішніми незалежними організаціями. Не зважаючи на важливість забезпечення ІБ, аудит ІБ далеко не у всіх організаціях визнається критично необхідним процесом менеджменту ІБ.

Усвідомлення необхідності аудиту ІБ формується в результаті аналізу проблем ІБ організації та подальшого визначення потреб організації в оцінці відповідності політик, процесів, процедур забезпечення відповідності рівня ІБ організації встановленим критеріям. Основні елементи процесу усвідомлення аудиту ІБ представлені на рис. 1.2.

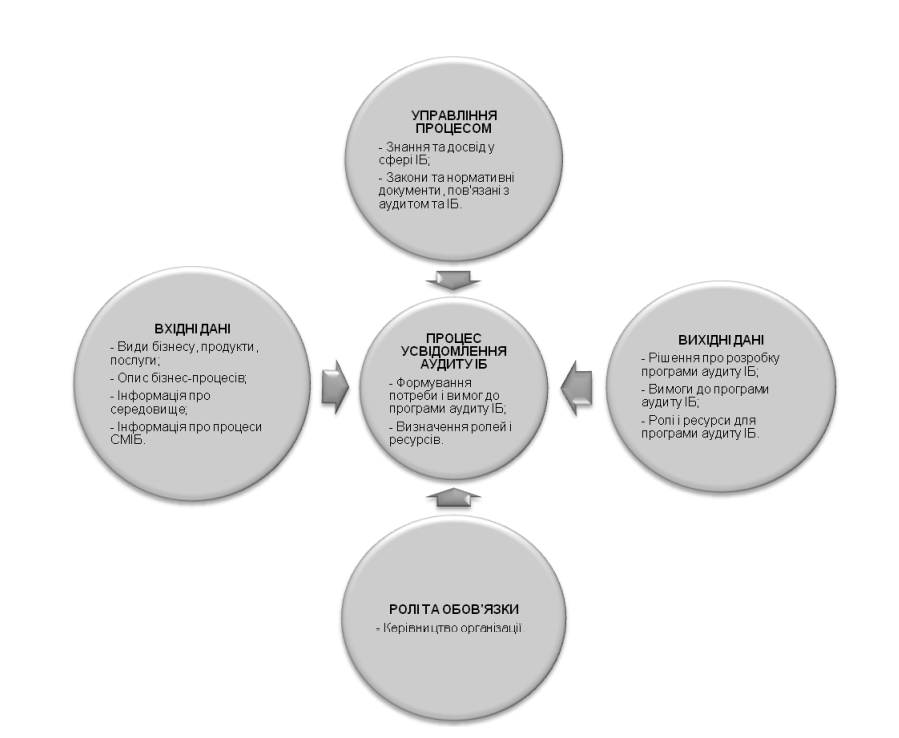


Рис. 1.1. Основні елементи процесу усвідомлення аудиту ІБ.

Для процесу усвідомлення аудиту ІБ вхідними даними є:

1. види бізнесу (діяльності), продукти та послуги організації;
2. опис бізнес-процесів;
3. інформація про внутрішнє і зовнішнє середовище організації;
4. інформація про поточний стан процесів СМІБ.

Опис видів бізнесу, продуктів і послуг організації та опис бізнес-процесів, завдяки яким реалізуються цілі бізнесу, має містити перелік критичних з точки зору ІБ продуктів, послуг і відповідних бізнес-процесів, визначати їх значення для досягнення цілей бізнесу. Інформація про внутрішнє і зовнішнє середовище організації повинна містити повний перелік загроз та ризиків цілям бізнесу, а також відомості про зміни в останніх, пов'язані з ІБ. Інформація про поточний стан процесів СМІБ повинна відображати відповідність процесів цілям ІБ організації, їх результативність. Учасниками процесу усвідомлення ІБ є керівники організації, які приймають рішення і впливають на рішення щодо підтримки і розвитку СМІБ організації. Основою для накопичення досвіду і знань є, насамперед власний унікальний досвід організації, а також відомі факти та інформація, отримана з таких джерел як Інтернет, книги, стандарти, довідники, публікації тощо. Джерелом власного досвіду є минула діяльність щодо забезпечення ІБ організації, а також аналіз загроз і уразливостей для організації.

До заходів процесу усвідомлення аудиту ІБ відносяться:

* формування потреби в розробці та менеджменті програми аудиту ІБ;
* формування вимог до програми аудиту ІБ;
* визначення ролей для розробки та менеджменту програми аудиту ІБ;
* визначення і виділення фінансових, кадрових та інфраструктурних ресурсів для розробки та менеджменту програми аудиту ІБ.

Під програмою аудиту ІБ розуміють сукупність кількох аудитів ІБ та інших перевірок ІБ (наприклад, самооцінок ІБ), запланованих на конкретний період часу і спрямованих на досягнення конкретної мети. Потреба в розробці та менеджменті програми аудиту ІБ організації формується залежно від цілей вимірювань ІБ, які стосуються аудиту ІБ. Цілі аудиту ІБ визначаються керівництвом організації на основі бізнес-цілей і результатів діяльності організації, а також на основі інформації про внутрішнє і зовнішнє середовище організації, яка враховує оцінку ризиків ІБ. Такими цілями можуть бути: ідентифікація уразливостей системи забезпечення ІБ організації, оцінка відповідності ІБ організації встановленим критеріям ІБ, підвищення довіри до організації. При формуванні рішень щодо програми аудиту ІБ аналізуються вартість програми аудиту ІБ і вигода від її реалізації. Потреба в розробці та менеджменті програми аудиту ІБ документується у вигляді рішення керівництва організації та затверджується ним. Вимоги до програми аудиту повинні містити: вимоги до обсягу програми аудиту ІБ, методології проведення аудиту, компетентності аудиторів, обізнаності співробітників організації щодо програми аудиту ІБ і вимоги до перегляду і коригування програми аудиту ІБ.

Принципи проведення аудиту є передумовою результативної і надійної підтримки політики керівництва та контролю. Вони забезпечують менеджмент організації інформацією, на основі якої реалізуються цілі, спрямовані на удосконалення характеристик бізнес-діяльності, а також є основою для об'єктивних висновків аудиту. До принципів проведення аудиту відносять:

1. етичність поведінки – основа професіоналізму. Істотними при аудиті є відповідальність, непідкупність, уміння зберігати таємницю і обережність;
2. неупередженість (fair presentation) – зобов'язання надавати правдиві і точні звіти. Висновки за результатами аудиту і записи мають правдиво і точно відображати діяльність з аудиту. Невирішені проблеми або розбіжності між аудиторською групою та організацією, що перевіряється, відображають у звітах (актах);
3. професійна обережність (due professional care) – старанність і вміння приймати правильні рішення при проведенні аудиту. Професійна обережність аудиторів має відповідати важливості виконуваних завдань і довірі з боку замовників та інших зацікавлених сторін. Важливим фактором є необхідна компетентність;
4. незалежність (independence) – основа неупередженості та об'єктивності висновків аудиту. Аудитори незалежні у своїй діяльності і вільні від упередженості і конфліктів інтересів. Аудитори зберігають об'єктивну думку під час усього процесу аудиту з метою забезпечення того, що в основі висновків знаходяться тільки свідчення (дані) аудиту;
5. підхід, заснований на свідченнях, фактах, даних (evidence-based approach) – розумна основа для досягнення надійних і відтворювальних висновків аудиту.

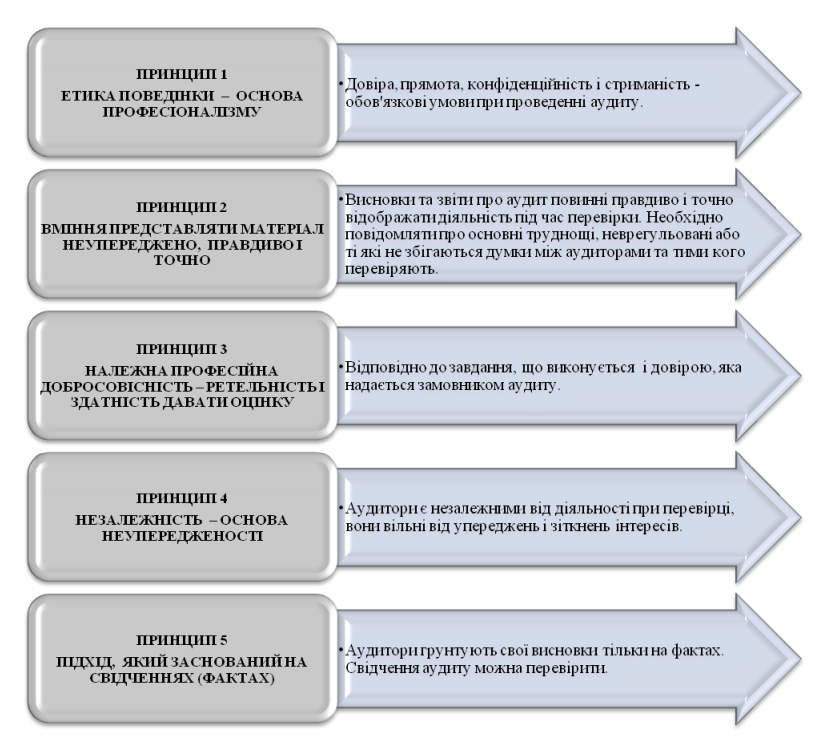


Рис. 1.2. Принципи проведення аудиту

Дані аудиту є вибірковими, оскільки аудит здійснюється в обмежений період часу і обмеженими ресурсами. Відповідно використання вибірок тісно пов'язане з довірою, з якою ставляться до висновків, отриманими за результатами аудиту. Під даними аудиту розуміють записи, виклад фактів або іншу інформацію, які стосуються критеріїв аудиту і можуть бути перевірені.

## 1.3. Напрями аудиту інформаційних систем

Для перевірок ефективності й безпечності інформаційної системи як такої здійснюють комп’ютерний аудит інформаційної системи. Під ним мається на увазі оцінка поточного стану комп’ютерної системи на відповідність певному стандарту або запропонованим вимогам. Цей термін використовується насамперед спеціалістами з загальної безпеки комп’ютерних інформаційних систем і у вузькому значенні не стосується аудиту фінансової звітності. Такий аудит не спрямований на пропонування конкретного рішення, він дає можливість поглянути на інформаційну систему комплексно, виявити проблемні місця, сформувати обґрунтовані рекомендації для ухвалення рішення про усунення недоліків та включає декілька напрямів.

Аудит технічного стану інформаційної системи спрямований на зменшення втрат, викликаних системними збоями. Збої можуть стати причиною відчутних втрат підприємств. Враховуючи, що в інформаційних системах, в яких не налагоджені належні процеси контролю і попередження можливих причин збоїв, вони виникають в найвідповідальніші, а отже, і найнапруженіші моменти, втрати можуть виливатися у величезні суми. Скорочення таких втрат можна досягти шляхом комплексного дослідження технічного стану всіх компонентів інформаційної системи. Аудит технічного стану інформаційної системи, перш за все, призначений для оцінки поточного стану інформаційної системи з метою реконструкції і модернізації, щоб підготуватися до розширення інформаційної системи і впровадження нових технологій. Його проведення дає змогу також організувати і налагодити підтримку інформаційної системи та розробити корпоративні стандарти підтримки інформаційної системи.

Аудит технічного стану інформаційної системи включає проведення таких заходів, як облік наявних на підприємстві апаратних засобів, програмного забезпечення, периферійних пристроїв і аналіз побудови структурованої кабельної системи, мереж передачі даних, функціонування ІТ-служби підприємства, технічних параметрів ефективності роботи інформаційної системи, її надійності та безпеки.

Аудит ефективності інформаційної системи дає можливість підприємству оцінити сукупну вартість володіння інформаційною системою і порівняти показники досліджуваної системи з лідером в цій галузі, а також оцінити строки повернення інвестицій при вкладенні коштів в інформаційну систему, розробити оптимальну схему вкладень, здійснити ефективне витрачання коштів на обслуговування й підтримку, понизити виробничі витрати. Цей вид аудиту включає такі частини інформаційної системи підприємства, як апаратні засоби, програмне забезпечення, периферійні пристрої, ІТ-персонал компанії, а також документи, бізнес-процеси, інформаційні потоки, користувачі.

У результаті проведення такого аудиту підприємству-клієнту надається перелік звітності, що включає підсумковий звіт з рекомендаціями щодо оптимізації інформаційної системи і звіт за наслідками розрахунку сукупної вартості володіння.

Результати аудиту інформаційної безпеки дають змогу побудувати оптимальну за ефективністю й витратами корпоративну систему захисту інформації, адекватну завданням і меті бізнесу. Аудит інформаційної безпеки не обмежується перевіркою тільки фізичної безпеки, наявні методики дають можливість проаналізувати бізнес-процеси і визначити основні інформаційні потоки компанії, які мають бути захищені.

При проведенні аудиту інформаційної безпеки виявляється поточний стан системи безпеки і визначаються найкритичніші ділянки системи, перевіряється відповідність наявної в компанії системи захисту інформації вимогам інформаційної безпеки, що висуваються до неї, оцінюється ефективність вкладень в корпоративну систему захисту інформації. Аудит включає такі етапи:

* + комплексна перевірка рівнів забезпечення інформаційної безпеки;
  + аналіз інформаційних ризиків;
  + аналіз системи захисту зовнішніх мереж;
  + аналіз системи контролю інформації, яка передається через телефонні з’єднання та електронною поштою;
  + визначення можливих каналів просочування конфіденційної інформації.

У перелік матеріалів, що надаються за підсумками аудиту, входять також звіт про поточний стан системи інформаційної безпеки й ефективність вкладень в систему інформаційної безпеки, а також рекомендації щодо політики безпеки і плану інформаційного захисту.

Якщо підприємство починає великі проекти модернізації інформаційної системи підприємства, використовує послуги системних інтеграторів з метою визначення реальних строків і вартості проектів перед початком робіт або ставить перед собою мету контролю проектів впровадження в своїх філіях і дочірніх компаніях, застосовується аудит проектів впровадження і реінжинірингу. Він дає змогу оцінити ризики впровадження або реінжинірингу інформаційної системи, строки та плановані ресурси на розробку і впровадження рішень, правильність вибору методів і технологій, а також завчасно виявити можливі помилки й отримати рекомендації, спрямовані на підвищення ефективності проекту. У проведення аудиту проектів впровадження і реінжинірингу входить перевірка проекту і складного технічного завдання на відповідність реальним вимогам підприємства та стандартам, перевірка виконаних робіт на відповідність технічному завданню, а також здійснюється оцінка ефективності виконаних робіт.

Роботи, що підтримують практичну реалізацію плану інформаційної безпеки, зокрема, полягають у наступному:

* розробка технічного проекту модернізації засобів захисту ІС, установлених на фірмі за результатами проведеного комплексного аналітичного дослідження корпоративної мережі;
* підготовка компанії до атестації (до атестації об’єктів інформатизації замовника на відповідність вимогам керівних документів, а також на відповідність вимогам безпеки міжнародних стандартів ІSO 15408, ІSO 17799, стандарту ІSO 9001 при забезпеченні вимог інформаційної безпеки компанії);
* розробка розширеного переліку відомостей обмеженого поширення як частини політики безпеки;
* розробка пакета організаційно-розпорядницької документації відповідно до  рекомендацій корпоративної політики ІБ компанії на організаційно-управлінському й правовому рівні;
* поставка комплекту типової організаційно-розпорядницької документації відповідно до  рекомендацій корпоративної політики ІБ компанії на організаційно-управлінському й правовому рівнях.

Рівень інформаційної безпеки компанії багато в чому залежить від кваліфікації фахівців. З метою підвищення кваліфікації й перепідготовки кадрів рекомендується проводити тренінги по застосуванню засобів захисту інформації, технології захисту інформації, навчати співробітників основам економічної безпеки.

Немаловажну роль грає й щорічна переоцінка стану інформаційної безпеки компанії.

Проведення аудиту стану інформаційної безпеки корпоративної інформаційної системи замовника здійснюється в три етапи:

* проведення комплексного обстеження корпоративної інформаційної системи;
* проведення аналізу ризиків;
* розробка рекомендацій з удосконалювання системи захисту корпоративної інформаційної системи і плану впровадження рекомендацій.

## 1.4. Оціночний аудит інформаційних систем

Державні органи, а також зарубіжні партнери компанії можуть зажадати сертифікації інформаційної системи підприємства з метою відповідності послуг необхідному рівню якості. Для цього проводиться оціночний аудит інформаційних систем. У рамках оціночного аудиту інформаційної системи, як правило, виявляються відхилення від наявних стандартів і формуються рекомендації, які дають змогу усунути знайдені невідповідності.

Програмне забезпечення посідає важливе місце в інформаційній системі будь-якого підприємства. Оціночний аудит програмного забезпечення дозволяє визначити економічну ефективність від впровадження й експлуатації як певного виду програм, так і комплексу програмних продуктів. Результати, отримані після його проведення, допоможуть підвищити економічну ефективність використання програмного забезпечення, визначити функціональність його використання й оптимальну схему впровадження, здійснити вибір найдешевшого варіанта переходу до ліцензійного програмного забезпечення, отримати рекомендації з оптимізації програмної інфраструктури.

У перелік звітності, що надається, входять опис результатів аналізу програмної інфраструктури, рекомендації щодо сумісності й коректності настроювання програмного забезпечення та підвищення ефективності й функціональності його використання.

Поєднання різних за змістом видів діяльності (технічних і фінансових), якими доводиться займатися в сучасних умовах аудитору, можна легко сприйняти та пояснити, якщо погодитись з думкою відомого американського фахівця в галузі менеджменту П. Дракера стосовно того, що застосування комп’ютерних інформаційних технологій приносить в наше життя такі масштабні зміни, які можна порівняти зі змінами, що свого часу спричинили винайдення писемності та винайдення технології друкування книг. Саме тому в умовах застосування КІСП відбувається взаємне проникнення різних за своїм змістом та суб’єктами видів контрольної та організаційної діяльності. Наприклад, після виконання комп’ютерного аудиту інформаційної системи аудитор отримує змогу всебічного оцінити реальний стан комп’ютерної інформаційної системи підприємства. А це безпосередньо впливає на оцінку аудитором системи внутрішнього контролю на підприємстві.

Здебільшого комп’ютерний аудит інформаційних систем потрібний, якщо автоматизована система призначена для обробки конфіденційної чи секретної інформації. Але саме до таких належать комп’ютерні системи бухгалтерського обліку. Проведення комп’ютерного аудиту корисно також після побудови автоматизованої системи та її підсистеми безпеки на етапі приймання в експлуатацію для оцінки ступеня дотримання висунутих до неї вимог.

# РОЗДІЛ 2. ХАРАКТЕРИСТИКА ВНУТРІШНЬОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1. Внутрішній аудит

Внутрішні аудити, які іноді називають «аудити першої сторони», проводяться самою організацією або від її імені з метою аналізу з боку керівництва та для інших внутрішніх цілей (наприклад, для підтвердження результативності системи менеджменту або для отримання інформації про підвищення ефективності системи менеджменту).

Керівництво підприємства повинно проводити планові перевірки внутрішнього аудиту, як одну з найбільш головних форм контролю роботи системи управління інформаційною безпекою. Аудит в апаратно-програмній інформаційній безпеці систем інформаційних технологій (ІТ), що застосовані на підприємстві (як самостійний аудит або як частина аудиту інформаційної безпеки підприємства) – контроль стану захищеності інформації з обмеженим доступом на підприємстві від внутрішніх і зовнішніх загроз інформаційної безпеки, а також програмно-апаратне забезпечення, від якого залежить постійна та злагоджена робота системи інформаційних технологій. Цей спосіб має за мету документальний та технічний аудит стану захищеності інформації при її створенні, редагуванні, зберіганні з використанням різних систем інформаційних технологій.

Аудит технічного стану проводиться комплексом програмно-апаратних засобів контролю, для того щоб забезпечити максимально ефективну діяльність по реєстрації подій інформаційної безпеки, а також за для дослідження порушень інформаційної безпеки на основі інформаційних даних реєстрації. В момент проведення здійснюється загальна оцінка побудови обміну інформації на підприємстві. Дається оцінка наявність і поточного стану інформаційної безпеки. Не обов’язково але як правило аналізується повнота і цілісність організаційно та розпорядчої методичної документації, рівень супроводу системи виявлення вторгнень. Актуальність застосовуваних політико-технічних регламентів та вказівок. Досліджується, наскільки коректно налаштовані корпоративні і приватні політики інформаційної безпеки в програмно-апаратних, каналах зв'язку і процесах (наприклад, оцінюється поточний стан конфігурацій і правил фільтрації мережевого обладнання з точки зору забезпечення інформаційної безпеки мережевої інфраструктури, достовірність в використанні існуючої архітектури обробки даних). Описується внутрішній аудит інформаційної безпеки регламентуючись внутрішніми інформаційними даними підприємства з перевіркою роботи її системою управління інформаційною безпекою і різних критеріїв забезпечення інформаційної безпеки, що виконується кваліфікованими спеціалістами контролюючого органу - відділу підприємства маючи на меті допомогу в управлінні підприємством. Стандартами ISO / IEC 19011 та ДСТУ внутрішній аудит визначено як аудит першої сторони, що здійснюється безпосередньо працівниками підприємства. Основні переваги аудитів першої сторони інформаційної безпеки перед зовнішніми (рис.2.1).



Рис.2.1 Основні переваги внутрішнього аудиту

Програма внутрішнього аудиту інформаційної безпеки розробляється з важливостями статусу та урахуванням процесів і сфері зберігання та керування інформаційною безпекою, що необхідно перевірити, а також з урахуванням розроблених раніше аудитів. Слід врахувати всі критерії, сфера діяльності, частота і підходи до проведення внутрішнього аудиту інформаційної безпеки. Потрібно встановити відповідального в плануванні і проведенні аудитів та всі вимоги для їх планування і проведення, а також підтримка комп’ютерної системи підприємства в робочому стані а також для повідомлення результатів і підтримки записів в робочому стані, визначають створити в документовані процедури внутрішнього аудиту інформаційної безпеки. Назначити відповідальних за негайне усунення виявлених невідповідностей без необґрунтованих затримок. На наступному етапі йде перевірка виконаних дій та складання звіту за результатами проведеної роботи.

## 2.2. Цілі та задачі внутрішніх аудитів інформаційної безпеки

Поставленими цілями внутрішнього аудиту інформаційної безпеки на підприємстві відповідають:

1. наскільки гуманні документи, дії та результат в сфері управління інформаційною безпекою та застосовані до них стандартів ДСТУ та ISO / IEC 19011 ;
2. чи дієво впроваджуються результати с сфері управління інформаційною безпекою розробленням яких займалося саме підприємство;
3. наскільки якісно впровадили та використовують розроблені заходи керування інформаційною безпекою;
4. наскільки якісно виконуються поставлені задачі, засоби, процеси і процедури система управління інформаційною безпекою підприємства.

Для досягнення цілей вирішуються наступні завдання (Рис. 2.2):

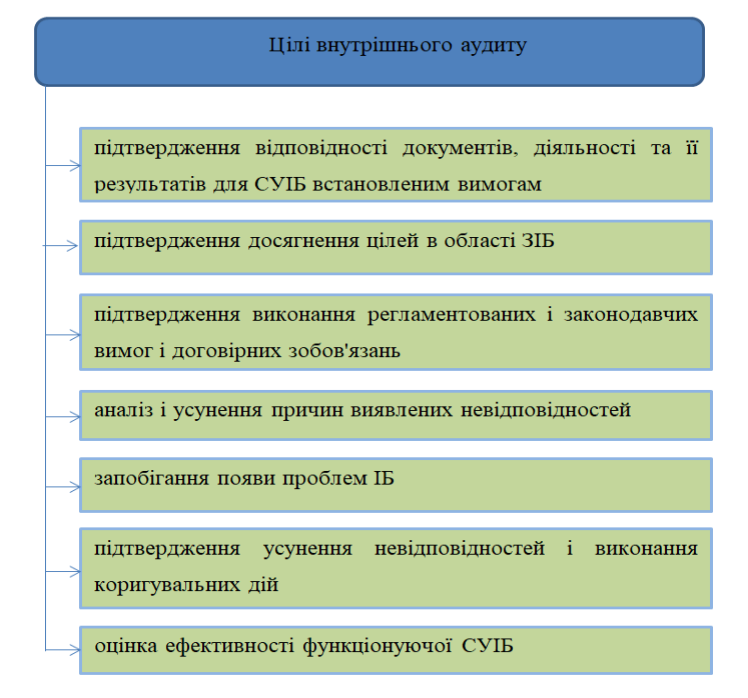


Рис.2.2. Цілі внутрішнього аудиту

## 2.3. Організаційні принципи

Можна виділити організаційні підходи до внутрішнього аудиту що використовуються в сфері інформаційної безпеки:

Індивідуальність – перевірку проводять незалежні експерти які не мають прямих зв’язків із керівництвом підприємства, що унеможливлює тиск на аудитора.

Підкорегованість – всі перевірки здійснюються заздалегідь розробленою схемою та порядком дій.

Систематичність – аудит проводиться з розрахунків структури взаємозв’язків системи управління інформаційною безпекою.

Архівованість – всі перевірки задукоментовані та зберігаються надійним методом.

Ввічливість - про перевірки персонал попереджується заздалегідь, і доноситься до їх відому з якою метою здійснюється перевірка, що є об'єктом перевірки, та час проведення аудиту.

Періодичність - аудит проводяться з певною регулярність з тим, щоб всі процеси системи і всі відділи організації були об'єктом постійного аналізу та оцінювання з боку керівництва підприємства.

Публічність - результати аудиторської перевірки є публічними у всіх випадках, крім тих що передбачені законом як інформація з обмеженим доступом.

## 2.4. Принципи ефективності інформаційної безпеки

Загально прийнятим фактором успіху здійсненням внутрішнього аудиту інформаційної безпеки на підприємстві - це дотримання загальних вказівок забезпечення його ефективності:

Дисциплінарність – всі працівники підприємства внутрішні аудитори як суб'єкт бездоганного контролю несуть повну відповідальність за неправильне (за незнання чи навмисно) виконання певної із затверджених пунктів, які ясно визначені і формально закріплені за кожним працівником.

Логічність – працівнику відповідають лише ті функції – які він в змозі повністю виконувати і забезпечувати безпеку інформаційних систем підприємства. Термінове сповіщення про відхилення від затверджених стандартів - данні про відхилення надаються працівникам, що приймати рішення з підконтрольних відхилень. При запізненні сповіщення, виникають небажані наслідки відхилень поглиблюються. Об'єкт переходить в інший стан (діяльність), що передбачає проведення контролю. Відповідність системи контролю та контролючих програм повинен відповідати ступеню аудиту інформаційної підконтрольної системи.

Цілісність – всі об’єкти аудиту повинні бути грамотно скомпоновані внутрішнім аудитом інформаційної безпеки.

Адміністрування – обов’язки кожного члена аудиту повинні бути розподілені таким чином, щоб йому не доводилося одночасно виконувати несумісні дії.

Рішення - має бути відповідно обговорене всіма операційними аудиторами в межах їх повноважень.

# РОЗДІЛ 3. ХАРАКТЕРИСТИКА ЗОВНІШНЬОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 3.1. Зовнішній аудит

Зовнішні аудити – це аудити, які проводяться другою і третьою сторонами. Аудити другої сторони проводяться сторонами, що мають інтерес до організації (наприклад, споживачами), або іншими особами від їх імені. Аудити третьої сторони проводяться незалежними аудиторськими організаціями (наглядовими органами або організаціями, що здійснюють сертифікацію). Якщо дві системи менеджменту якості різного типу або більше (наприклад, система менеджменту якості, система екологічного менеджменту, СМІБ і забезпечення безпеки праці) піддаються аудиту спільно, це називається комбінованим аудитом. Якщо дві аудиторські організації або більше об’єднуються, щоб провести аудит однієї аудиторської організації, це називається спільним аудитом. Організація повинна проводити внутрішній аудит СМІБ в заплановані інтервали для визначення, чи відповідають мета, засоби управління, процеси та процедури СМІБ наступним положенням:

* відповідність вимогам Міжнародного стандарту і відповідним нормативним та установчим актам;
* відповідність ідентифікованим вимогам ІБ;
* ефективне забезпечення і підтримка СМІБ.

## 3.2. Цілі зовнішнього аудиту ІБ

Визначає клієнт аудиту - організація або ж особистість, яка його замовила. Як правило потрібно свідоцтво 1-го або ж негайно 2-ух положень:

1. об'єкт аудиту тримається особистих політичних діячів, цілей і процедур в області ОІБ;
2. співвідношення СУІБ аудиту всім вимогам стереотипів ISO / IEC, ДСТУ ISO / IEC 27001 та цілям політичних діячів організації.

У базі зовнішнього аудиту ІБ лежить потяг управління організації з підтримкою проведення незалежної і компетентної оцінки кваліфікувати ступінь організації справ в області заперечення і рівня співвідношення ІБ організації встановленими критеріями аудиту ІБ - сукупності домагань та конкретних в загальновизнаних організаціях документах, що характеризує певний ступінь ІБ. Оцінка співвідношення ІБ організації аспектам аудиту ІБ виконується на базі документів і прецедентів, які свідчать про виконання, вибіркове виконання або ж невиконання поставлених домагань.

Нарешті, зовнішній аудит ІБ зобов'язаний сконцентруватися в першу чергу на належному:

* дотриманні вимог по документації, сформульованих в ISO / IEC і ISO / IEC 27001;
* відповідальності управління за ПІБ;
* виконану організацією оцінці ризиків ІБ і на те, виділяють ці оцінки зіставні і відтворювані результати;
* отримання свідоцтв, тест небезпек ІБ вважається вагомим і відповідним в роботі організації;
* встановлення, чи узгодження процедури з ідентифікації, вивчення і оцінці загроз ІБ, активів, уразливості і впливів та результатами їх застосування з політикою, цілями і планами організації;
* процесі обробки ризиків ІБ в організації;
* оцінці вибору цілей і засобів управління ІБ в рамках СУІБ, що базуються на процесах обробки ризиків ІБ;
* аналізі і вимірах продуктивності і результативності СУІБ і засобів управління ІБ по досягненню цілей ПІБ;
* виявленні функціонування процедур повторюваної оцінки і перевірки відповідності правовим і нормативним вимогам;
* підсумки внутрішніх аудитів СУІБ і їх аналізі з боку керівництва;
* заходи, прийняті по невідповідності, виявлених під час останнього аудиту ІБ;
* встановлення співвідношення між обраними і впровадженими способами управління ІБ;
* визначенні вступу в дію і результативності засобів управління ІБ і встановлення їх продуктивності для досягнення встановлених цілей;
* програмах, процесах, процедурах, записах, внутрішніх аудитів ІБ і аналізах продуктивності СУІБ з метою забезпечення їх простежуваності до висновків управління, політичні діячі та цілей СУІБ.

Провідними документами зовнішнього аудиту ІБ вважають:

1. програму зовнішнього аудиту ІБ, охоплюючи опис роботи, важливою для планування, проведення, контролю, аналізу і поліпшення зовнішніх аудитів ІБ;
2. проект зовнішнього аудиту ІБ;

Висновок за підсумками аудиту ІБ - високоякісна і (чи) кількісна оцінка співвідношення встановленим критеріям аудиту ІБ, виставлені аудиторською групою згодом перегляду всіх висновків аудиту ІБ відповідно до цілей аудиту ІБ.

## 3.3. Принципи проведення

Проведення зовнішнього аудиту ІБ базується на ряді основ, дотримання яких вважається посилом для забезпечення неупереджених висновків за підсумками зовнішнього аудиту ІБ. Ці основи проробляють зовнішній аудит ІБ дієвим і достовірним способом підтримки політичних діячів управління і контролю, забезпечуючи інформацією, на базі якої організація має можливість удосконалювати власні властивості. Основи зобов'язані бути визнані і дотримані всіма сторонами, які беруть участь у зовнішньому аудиті ІБ. Основам зовнішнього аудиту ІБ відносять:

* незалежність;
* повнота;
* оцінка на базі доказів аудиту ІБ;
* достовірність доказів аудиту ІБ;
* потреба усвідомлення аудитором роботи організації, яку перевіряють;
* професіоналізм, етичність і неупередженість;
* відповідальність;
* відкритість;
* конфіденційність;
* реагування на претензії.

## 3.4. Управління програмою інформаційної безпеки

Програма зовнішнього аудиту ІБ базується на виявлених ризиках ІБ для організації, як зазначається в ідеалі ISO / IEC 27007: 2011. Вона розробляється самою організацією, яка проводить перевірку. Залежно від обсягу, вигляду роботи і труднощів організації дана програма має можливість підключати раз і більше аудитів, які мають всі шанси володіти різними цілями. Може бути створено більше однієї програми аудиту ІБ. Програма зовнішнього аудиту ІБ підключає всі свої заходи, потрібні для планування, організації і проведення зовнішніх аудитів ІБ, а ще для забезпечення ресурсами, важливими для дієвого та здорового проведення аудитів в конкретні короткочасні рамки. У програмі зовнішнього аудиту ІБ орієнтуються на її завдання. Для цього береться наступне:

* поставлені запити;
* небезпеки ІБ для організації;
* наведені цифри щодо заперечення;
* робота за прогнозом і аналізу СУІБ;
* жорсткість узгодженні організацією власним політичним діячам і завданням, виконання поставлених процедур;

Зміст програми зовнішнього аудиту ІБ залежить в першу чергу від обсягу і труднощів СУІБ, кількості персоналу та тимчасових її співробітників, числа застосовуваних ІС та ІТ, ризиків ІБ для самої СУІБ, критичності активів в області впливу СУІБ. Програма зовнішнього аудиту ІБ вимагає постійного контролю, аналізу і поліпшення. Процедури програми зовнішнього аудиту ІБ містять наступне:

* планування і формування планів-графіків їх проведення;
* підбір належних аудиторських груп і розподіл ролей і відповідальності;
* виконання вчинків за підсумками аудиту, у разі якщо це необхідно;
* прогноз характеристик результативності програми;

Управління програмою зовнішнього аудиту ІБ слід проводити в рамках циклу PDCA. На рубежі планування розробляється програма зовнішнього аудиту ІБ. При цьому орієнтуються мета і розмір зовнішнього аудиту ІБ, серйозність його проведення, ресурсів і способу. Для визначення цілей необхідно розглянути належне:

* цінності керівництва;
* запити стереотипів (зовнішніх і внутрішніх);
* необхідності зацікавлених сторін;
* небезпеки організації. Послідовність процесів управління програмою зовнішнього аудиту (Рис. 3.1):

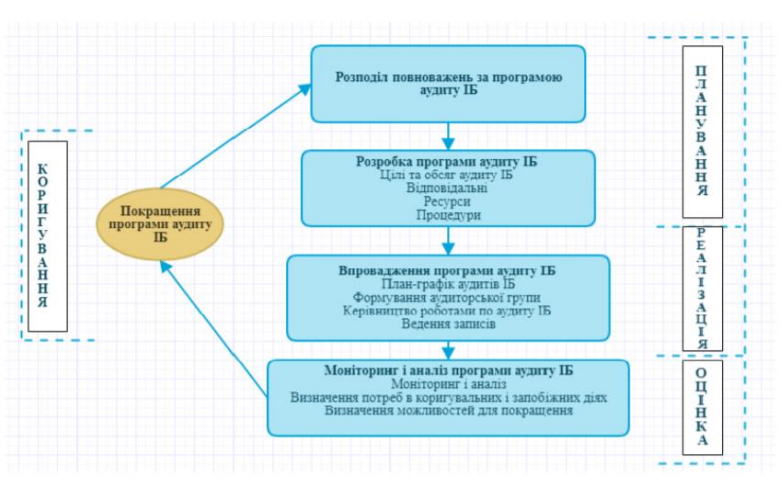


Рис.3.1. Послідовність процесів управління програмою зовнішнього аудиту ІБ

Розміром програми зовнішнього аудиту ІБ знаходиться в залежності від обсягу, вигляду роботи, труднощів структури об'єкта аудиту, а ще:

* області, мети і тривалості всякого здійснюваного аудиту;
* частоти виконаних аудитів;
* числа, значущості, комплексності, одноманітності, місцеперебування загонів, які підлягають аудиту;
* стереотипів, законодавчих, нормативних та контрактних домагань та інших критеріїв аудиту;
* необхідностей організації в оцінці повноту і якість виконання домагань, що пред'являються до організації або ж її систем ІТ, при появі потреби їх акредитації або ж реєстрації / сертифікації;
* рішень за підсумками минулих аудитів або ж аналізу підсумків минулих програм аудитів;
* кожних завдань, пов'язаних з мовою, культурою;
* значних змін в організації або ж її роботі.

Найвища інструкція організації дає можливості по управлінню програмою зовнішнього аудиту ІБ. Обов'язок за управління даної програми покладають на одного або ж кілька осіб, які мають уявлення про принципи аудиту ІБ, компетентності аудитора по ІБ і використанні способів аудиту ІБ. Ці особи ще зобов'язані володіти здібностями управління, технічними і фінансовими знаннями в області ІБ. Вони зобов'язані:

* визначати цілі і розмір програми зовнішнього аудиту ІБ;
* визначати обов'язок і процедури, а ще забезпечувати важливими ресурсами;
* розробляти і запроваджувати програму;
* робити записи за програмою;
* втілити в життя прогноз, тест і вдосконалення програми;
* визначати потребу програмки в ресурсах;
* сприяти прийняттю висновків про забезпечення програми важливими ресурсами.

При визначенні ресурсів для програми призначають належне:

* грошові ресурси для становлення, впровадження, управління та вдосконалення роботи по зовнішньому аудиту ІБ;
* способи проведення аудитів ІБ;
* процеси по досягненню і підтримці компетентності та вдосконалення роботи аудиторів по ІБ;
* присутність аудиторів по ІБ і технічних фахівців, професіоналізм яких потрібно для досягнення певних цілей програми аудиту ІБ;
* розмір програми;
* час у дорозі аудиторів по ІБ, облагороджування і інші потреби для проведення аудиту ІБ.
* визначати потребу програми в ресурсах;
* сприяти прийняттю висновків про забезпечення програми важливими ресурсами.

Характеристики роботи по зовнішньому аудиту ІБ як правило застосовувалися для прогнозу належних даних:

* здатності аудиторської групи втілити в життя проект зовнішнього аудиту ІБ;
* співвідношення програмами аудитів ІБ (зокрема досягнення цілей аудиту) та планів-графіків;
* доповіді та висновки аудиту ІБ;
* зворотний зв'язок від клієнтів аудиту ІБ, що перевіряються організацій та аудиторів.

Тест програми зовнішнього аудиту ІБ зазвичай охоплює належні питання:

* підсумки прогнозу і поставлені тенденції;
* співвідношення процедурам програми;
* виявлення потреб і очікувань зацікавлених сторін;
* записи за програмою;
* узгодженість вчинків аудиторських груп в аналогічних ситуаціях. На рубежі коригування ведеться (при необхідності) вдосконалення програми зовнішнього аудиту ІБ. Це стосується, наприклад, перегляду і коригування термінів проведення аудитів ІБ і важливих ресурсів, вдосконалення способів підготовки доказів аудиту ІБ та ін.

Підсумовуючи наявні запити стереотипів і найкращі практики в цій галузі, виділю належні рубежі втілення справ з проведення зовнішнього аудиту ІБ:

* організація проведення аудиту;
* тест документації;
* підготовка до проведення аудиту на просторі його проведення; - проведення аудиту на місці;
* підготовка, заяву і розсилка звіту по аудиту;
* закінчення аудиту;
* виконання вчинків за підсумками аудиту.

# РОЗДІЛ 4. ХАРАКТЕРИСТИКА  АУДИТУ ЗА ОБ’ЄКТАМИ ДОСЛІДЖЕННЯ

## 4.1. Основні види аудиту ІБ.

* Експертний аудит ІБ, під час якого виявляються недоліки у системі заходів ЗІ на основі досвіду експертів, що беруть участь у процедурі аудиту;
* Аудит ІБ на відповідність міжнародним стандартам, наприклад, стандарту ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги», розробленому Міжнародною організацією зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC) на основі британського стандарту BS 7799-2:2002 «Системи управління інформаційною безпекою. Специфікація і керівництво по застосуванню»;
* активний аудит, головним завданням якого є оперативне виявлення підозрілої активності і надання засобів для автоматичного реагування на неї. Під підозрілою активністю розуміють поведінку користувача або компоненти інформаційної системи, яка є зловмисною (відповідно до заздалегідь визначеної політики безпеки) або нетиповою (згідно з прийнятими критеріями);
* комплексний аудит, що містить всі перераховані вище форми проведення обстеження. В якості об'єкта аудиту може виступати як інформаційно-телекомунікаційна система (ІТС) організації в цілому, так і її окремі складові, що забезпечують обробку інформації, яка підлягає захисту.

Варіанти аудиту СМІБ:

* плановий внутрішній аудит;
* позаплановий внутрішній аудит;
* пошук загроз;
* моделювання загроз.

## 4.2. Аудит на відповідність стандартам ІБ.

При проведенні цього виду аудиту реальний стан ІБ компанії порівнюється з вимогами щодо безпеки, описаними в обраному стандарті. Звіт, складений за результатами проведення даного виду аудиту, має містити таку інформацію:

* ступінь відповідності ІТС, що перевіряється, обраному стандарту;
* ступінь відповідності внутрішнім вимогам компанії з питань ІБ;
* кількість і категорії отриманих невідповідностей і зауважень;
* рекомендації з побудови або модифікації системи забезпечення ІБ, які дозволяють привести її у відповідність до даного стандарту;
* детальне посилання на основні документи підприємства, включаючи політику безпеки, опис процедур забезпечення ІБ, додаткові обов'язкові і необов'язкові стандарти і норми, які застосовуються у даній компанії;
* перелік політик, інструкцій, посібників, положень, необхідність яких визначена в стандартах та рекомендації щодо їх розробки.

## 4.3. Активний аудит інформаційних систем.

Одним з найпоширеніших видів аудиту є активний аудит. Він полягає у дослідженні стану захищеності ІС з точки зору зловмисника (або зловмисника, що володіє високою кваліфікацією в галузі ІТ). Найчастіше компанії-постачальники послуг активного аудиту іменують його інструментальним аналізом захищеності, щоб відокремити даний вид аудиту від інших. Сутність активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів, здійснюється збір інформації про стан системи мережевого захисту. Під станом системи мережевого захисту розуміють лише ті параметри і налаштування, використання яких допомагає зловмисникові проникнути в мережі і завдати збитків компанії. При здійсненні даного виду аудиту система мережевого захисту піддається якомога більшій кількості мережевих атак, які може виконати зловмисник. При цьому аудитор штучно ставиться саме в ті умови, в яких працює зловмисник. Йому надається мінімум інформації, тільки та, яку можна здобути у відкритих джерелах. Атаки тільки моделюються і не завдають будь-якого деструктивного впливу ІС. Їх різноманітність залежить від використовуваних систем аналізу захищеності і кваліфікації аудитора. Активний аудит умовно можна розділити на два види – зовнішній і внутрішній. При зовнішньому активному аудиті фахівці моделюють дії зовнішнього зловмисника. У даному випадку проводяться наступні процедури:

* визначення доступних із зовнішніх мереж IP-адрес підприємства;
* сканування даних адрес з метою визначення працюючих сервісів і служб, а також призначення відсканованих хостів;
* визначення версій сервісів і служб хостів, що скануються;
* вивчення маршрутів проходження трафіку до хостів замовника;
* збір інформації про ІС замовника з відкритих джерел;
* аналіз отриманих даних з метою виявлення уразливостей. Внутрішній активний аудит за складом робіт аналогічний зовнішньому, однак при його проведенні за допомогою спеціальних програмних засобів моделюються дії «внутрішнього» зловмисника.

Даний розподіл активного аудиту на «зовнішній» і «внутрішній» актуальний для підприємства в таких випадках:

* існують фінансові обмеження на придбання послуг і продуктів ЗІ;
* модель зловмисника, яка існує, не містить «внутрішніх» зловмисників;
* розслідується факт обходу системи мережевого захисту. Найчастіше організація у своїй ІС використовує спеціалізоване програмне забезпечення (ПЗ) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерські системи або системи документообігу).

Подібні ПЗ унікальні, тому яких-небудь готових засобів і технологій для аналізу їх захищеності та відмовостійкості не існує. У даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ. Також під час активного аудиту здійснюється дослідження виробленості і стабільності системи, або стрес-тестування. Воно спрямоване на визначення критичних точок навантаження, при якій система внаслідок атаки на відмову в обслуговуванні або підвищеної завантаженості перестає адекватно реагувати на легітимні (визначені політикою безпеки) запити користувачів. Стрес-тест дозволить виявити «вузькі» місця у процесі формування та передачі інформації і визначити ті умови, за яких нормальна робота системи неможлива. Таке тестування передбачає моделювання атак на відмову в обслуговуванні запитів користувача до системи і загальний аналіз її продуктивності. Результатом активного аудиту є інформація про всі уразливості, ступені їх критичності і методи усунення, відомості про загальнодоступну інформацію (інформацію, доступну будь-якому потенційному порушнику) мережі замовника. За результатами активного аудиту надаються рекомендації з модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливості, і таким чином підвищити рівень захищеності ІС від дій «зовнішнього» зловмисника при мінімальних витратах на ІБ. Однак без проведення інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення «ідеальної» системи мережевого захисту. Наприклад, за результатами даного виду аудиту неможливо зробити висновок про коректність, з точки зору безпеки, проекту ІС. Експертний аудит ІС Експертний аудит можна умовно представити як порівняння стану ІБ з «ідеальним» описом, що передбачає:

* вимоги, які були висунуті керівництвом у процесі проведення аудиту;
* опис «ідеальної» системи безпеки, заснованої на акумульованому у компанії-аудитора загальновідомому та власному досвіді.

При виконанні експертного аудиту проводяться наступні види робіт:

* збір первинних даних про систему ІБ, про її функції й особливості, використовувані технології автоматизованої обробки та передачі даних (з урахуванням найближчих перспектив розвитку);
* збір інформації про наявні організаційно-розпорядчі документи щодо забезпечення ІБ і їх аналіз;
* визначення точок відповідальності систем, пристроїв і серверів ІС;
* формування переліку підсистем кожного підрозділу компанії з категоруванням критичної інформації та схемами інформаційних потоків.

Одним із найбільших за обсягом видом робіт серед тих, які проводяться при експертному аудиті, є збір даних про ІС шляхом інтерв'ювання представників замовника і заповнення ними спеціальних анкет. Основна мета інтерв'ювання технічних фахівців – збір інформації про функціонування мережі, а керівного складу компанії – з’ясування вимог, які висуваються до системи ІБ.

# РОЗДІЛ 5. МЕТОДИ АУДИТУ СИСТЕМ ТА МЕРЕЖ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ІНФОРМАЦІЙНІ РИЗИКИ ТА ЇХ ВИРІШЕННЯ.

## 5.1. Методи аналізу даних при аудиті ІБ.

Зараз використовуються три основні методи (підходи) до проведення аудиту, які істотно різняться між собою.

Перший метод, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог безпеки, та найбільшою мірою враховує особливості даної ІС, середовища її функціонування і існуючі в даному середовищі загрози безпеки. Даний підхід є найбільш трудомістким і вимагає найвищої кваліфікації аудитора. На якість результатів аудиту, в цьому випадку, сильно впливає використовувана методологія аналізу та управління ризиками і її придатність до даного типу ІС.

Другий метод, самий практичний, спирається на використання стандартів інформаційної безпеки. Стандарти визначають базовий набір вимог безпеки для широкого класу ІС, який формується в результаті узагальнення світової практики. Стандарти можуть визначати різні набори вимог безпеки, в залежності від рівня захищеності ІС, який потрібно забезпечити, її приналежності (комерційна організація, або державна установа), а також призначення (фінанси, промисловості, зв'язок і т.п.). Від аудитора в даному випадку потрібно правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити для даної ІС. Необхідна також методика, що дозволяє оцінити цю відповідність. Через свою простоту (стандартний набір вимог для проведення аудиту вже заздалегідь визначений стандартом) і надійності (стандарт - є стандарт і його вимоги ніхто не спробує оскаржити), описаний підхід найбільш поширений на практиці (особливо при проведенні зовнішнього аудиту). Він дозволяє при мінімальних витратах ресурсів робити обґрунтовані висновки про стан ІС.

Третій метод, найбільш ефективний, передбачає комбінування перших двох.

Якщо для проведення аудиту безпеки обраний підхід, який базується на аналізі ризиків, то на етапі аналізу даних аудиту зазвичай виконуються наступні групи завдань:

* 1. Аналіз ресурсів ІС, включаючи інформаційні ресурси, програмні та технічні засоби, а також людські ресурси.
  2. Аналіз груп завдань, що вирішуються системою, і бізнес-процесів.
  3. Побудова (неформальній) моделі ресурсів ІС, що визначає взаємозв'язку між інформаційними, програмними, технічними та людськими ресурсами, їх взаємне розташування і способи взаємодії.
  4. Оцінка критичності інформаційних ресурсів, а також програмних і технічних засобів.
  5. Визначення критичності ресурсів з урахуванням їх взаємозалежностей.
  6. Визначення найбільш ймовірних загроз безпеки щодо ресурсів ІС і вразливостей захисту, які роблять можливим здійснення цих загроз.
  7. Оцінка ймовірності здійснення загроз, величини вразливостей і шкоди, що завдається організації в разі успішного здійснення загроз.
  8. Визначення величини ризиків для кожної трійки: загроза, група ресурсів, вразливість.

Перерахований набір завдань є досить загальним. Для їх вирішення можуть використовуватися різні формальні і неформальні, кількісні і якісні, ручні і автоматизовані методики аналізу ризиків. Суть підходу від цього не змінюється.

Оцінка ризиків може даватися з використанням різних як якісних, так і кількісних шкал. Головне, щоб існуючі ризики були правильно ідентифіковані і про ранжовані відповідно до ступеня їх критичності для організації. На основі такого аналізу може бути розроблена система першочергових заходів щодо зменшення величини ризиків до прийнятного рівня.

При проведенні аудиту безпеки на відповідність вимогам стандарту, аудитор, покладаючись на свій досвід, оцінює придатність вимог стандарту до обстежуваної ІС і її відповідність цим вимогам. Дані про відповідність різних областей функціонування ІС вимогам стандарту зазвичай представляються в табличній формі. З таблиці видно, які вимоги безпеки в системі не реалізовані. Виходячи з цього, робляться висновки про відповідність досліджуваної ІС вимогам стандарту і даються рекомендації щодо реалізації в системі механізмів безпеки, що дозволяють забезпечити таку відповідність.

## 5.2. Аналіз інформаційних ризиків підприємства.

Аналіз ризиків - це те, з чого має починатися побудова будь-якої системи інформаційної безпеки і те, що необхідно для проведення аудиту ІБ. Він містить заходи з обстеження безпеки підприємства з метою визначення того, які ресурси і від яких загроз треба захищати, а також в якій мірі ті чи інші ресурси потребують захисту. Визначення набору адекватних контрзаходів здійснюється в ході управління ризиками. Ризик визначається ймовірністю заподіяння шкоди і величиною збитку, що наноситься ресурсів інформаційних систем (ІС), в разі створення іншої загрози безпеці.

Аналіз ризиків полягає в тому, щоб виявити існуючі ризики і оцінити їх величину (дати їм якісну, або кількісну оцінку). Процес аналізу ризиків передбачає вирішення наступних завдань:

1. Ідентифікація ключових ресурсів ІС.
2. Визначення важливості тих чи інших ресурсів для організації.
3. Ідентифікація існуючих загроз безпеці та вразливостей, які роблять можливим здійснення загроз.
4. Обчислення ризиків, пов'язаних із здійсненням погроз безпеки.

Ресурси ІС можна розділити на наступні категорії:

* інформаційні ресурси;
* програмне забезпечення;
* технічні засоби (сервери, робочі станції, активне мережеве обладнання та т. П.);
* людські ресурси.

У кожній категорії ресурси діляться на класи і підкласи. Необхідно ідентифікувати тільки ті ресурси, які визначають функціональність ІС і істотні з точки зору забезпечення безпеки.

Важливість (або вартість) ресурсу визначається величиною збитку, що наноситься в разі порушення конфіденційності, цілісності або доступності цього ресурсу. Зазвичай розглядаються наступні види збитку:

* дані були розкриті, змінені, видалені або стали недоступні;
* апаратура була пошкоджена або зруйнована;
* порушена цілісність програмного забезпечення.

Збиток може бути завдано організації в результаті успішного здійснення наступних видів загроз безпеки:

* локальні і віддалені атаки на ресурси ІС;
* стихійні лиха;
* помилки, або навмисні дії персоналу ІС;
* збої в роботі ІС, викликані помилками в програмному забезпеченні або несправностями апаратури.

Величина ризику може бути визначена на основі вартості ресурсу, ймовірності здійснення загрози і величини уразливості за такою формулою:

**вартість ресурсу \* ймовірність загрози Ризик = величина вразливості**

Завдання управління ризиками полягає у виборі обґрунтованого набору контрзаходів, що дозволяють знизити рівні ризиків до прийнятної величини. Вартість реалізації контрзаходів повинна бути менше величини можливого збитку. Різниця між вартістю реалізації контрзаходів і величиною можливого збитку повинна бути обернено пропорційна ймовірності заподіяння шкоди.

Підхід на основі аналізу інформаційних ризиків підприємства є найбільш значущим для практики забезпечення інформаційної безпеки. Це пояснюється тим, що аналіз ризику дозволяє ефективно управляти ІБ підприємства. Для цього на початку робіт з аналізу ризику необхідно визначити, що саме підлягає захисту на підприємстві, впливу яких загроз це схильне, і по практиці захисту. Аналіз ризику проводиться виходячи з безпосередніх цілей і завдань щодо захисту конкретного виду інформації конфіденційного характеру. Однією з найважливіших завдань в рамках захисту інформації є забезпечення її цілісності і доступності. При цьому слід мати на увазі, що порушення цілісності може відбутися не тільки внаслідок навмисних дій, а й по ряду інших причин:

* збоїв обладнання, що ведуть до втрати або перекручування інформації;
* фізичних впливів, в тому числі в результаті стихійних лих;
* помилок в програмному забезпеченні (в тому числі недокументованих можливостей).

Тому під терміном «атака» більш перспективно розуміти не тільки людські дії на інформаційні ресурси, але і впливу навколишнього середовища, в якому функціонує система обробки інформації підприємства.

При проведенні аналізу ризику розробляються:

* загальна стратегія і тактика проведення потенційним порушником «наступальних операцій і бойових дій»;
* можливі способи проведення атак на систему обробки і захисту інформації;
* сценарій здійснення протиправних дій;
* характеристики каналів витоку інформації і несанкціонованого доступу;
* ймовірності встановлення інформаційного контакту (реалізації загроз);
* перелік можливих інформаційних інфекцій;
* модель порушника;
* методика оцінки інформаційної безпеки.

Крім того, для побудови надійної системи захисту інформації підприємства необхідно:

* виявити всі можливі загрози безпеки інформації;
* оцінити наслідки їх прояву;
* визначити необхідні заходи і засоби захисту з урахуванням вимог нормативних документів, економічної
* доцільності, сумісності і безконфліктності з використовуваним програмним забезпеченням;
* оцінити ефективність обраних заходів і засобів захисту.

Аналіз ризику рекомендується проводити згідно з наступною методикою за сценарієм, зображеному на рис.5.1

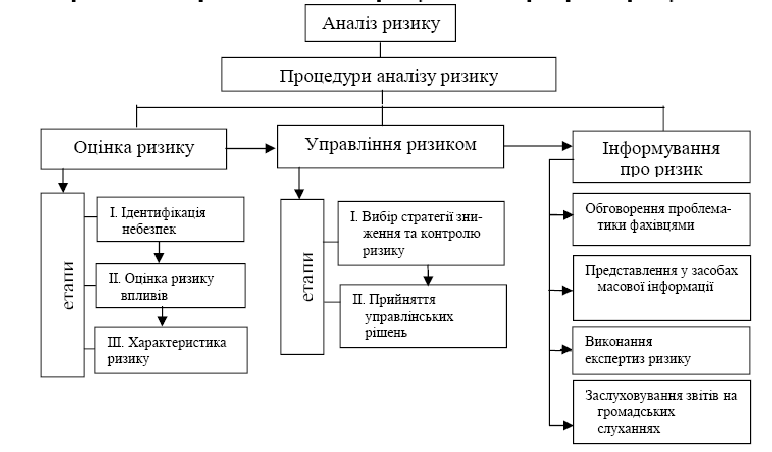


Рис.5.1 Сценарій аналізу інформаційних ризиків

Всього існує 6 етапів аналізу ризику. На першому і другому етапах визначаються відомості, які становлять для підприємства комерційну таємницю і які належить захищати. Зрозуміло, що такі відомості зберігаються в певних місцях і на конкретних носіях, передаються по каналах зв'язку. При цьому визначальним фактором в технології поводження з інформацією є архітектура ІС, яка багато в чому визначає захищеність інформаційних ресурсів підприємства. Третій етап аналізу ризику - побудова каналів доступу, витоку або впливу на інформаційні ресурси основних вузлів ІС. Кожен канал доступу характеризується великою кількістю точок, з яких можна «зняти» інформацію. Саме вони і являють уразливості і вимагають застосування засобів недопущення небажаних впливів на інформацію.

Четвертий етап аналізу способів захисту всіх можливих точок так відповідає цілям захисту та його результатом має бути характеристика можливих прогалин в обороні, в тому числі за рахунок несприятливого збігу обставин.

На п'ятому етапі виходячи з відомих на даний момент способів і засобів подолання оборонних рубежів визначаються ймовірності реалізації загроз по кожній з можливих точок атак.

На кінцевому, шостому, етапі оцінюється збиток організації в разі реалізації кожної з атак, який разом з оцінками уразливості дозволяє отримати ранжирований список загроз інформаційних ресурсів. Результати роботи подаються у вигляді, зручному для сприйняття і вироблення рішень щодо корекції існуючої системи захисту інформації. При цьому кожен інформаційний ресурс може бути підданий впливу кількох потенційних загроз. Принципова ж значення має сумарна ймовірність доступу до інформаційних ресурсів, яка складається з елементарних ймовірностей доступу до окремих точок проходження інформації.

Величина інформаційного ризику по кожному ресурсу визначається як добуток імовірності нападу на ресурс, ймовірності реалізації і загрози і шкоди від інформаційного вторгнення. У цьому творі можуть використовуватися різні способи зважування складових.

Додавання ризиків по всіх ресурсів дає величину сумарного ризику при прийнятій архітектурі ІС і впровадженої в неї системи захисту інформації.

Таким чином, варіюючи варіанти побудови системи захисту інформації та архітектури ІС, стає можливим уявити і розглянути різні значення сумарного ризику за рахунок зміни ймовірності реалізації загроз. Тут дуже важливим кроком є ​​вибір одного з варіантів відповідно до відібраних критеріїв прийняття рішення. Таким критерієм може бути допустима величина ризику або відношення витрат на забезпечення інформаційної безпеки/небезпеки до залишкового ризику.

При побудові систем забезпечення інформаційної безпеки також потрібно визначити стратегію управління ризиками на підприємстві.

На сьогодні відомо кілька підходів до управління ризиками. Один з найбільш поширених - зменшення ризику шляхом використання відповідних способів і засобів захисту. Близьким по суті є підхід, пов'язаний з ухиленням від ризику. Відомо, що від деяких класів ризиків можна ухилитися: наприклад, винесення Web-сервера організації за межі локальної мережі дозволяє уникнути ризику несанкціонованого доступу в локальну мережу з боку Web-клієнтів.

Нарешті, в деяких випадках допустиме прийняття ризику. Тут важливо визначитися з наступною дилемою: що для підприємства вигідніше - боротися з ризиками або ж з їх наслідками. У цьому випадку доводиться вирішувати оптимізаційну задачу.

Після того як визначена стратегія управління ризиками, проводиться остаточна оцінка заходів щодо забезпечення інформаційної безпеки з підготовкою експертного висновку про захищеність інформаційних ресурсів. В експертний висновок включаються всі матеріали аналізу ризиків та рекомендації щодо їх зниження.



Рис.7 Основні загрози інформаційної безпеки підприємства

## 5.3. Методи оцінювання інформаційних ризиків підприємства.

На практиці використовуються різні методи оцінки і управління інформаційними ризиками на підприємствах. При цьому оцінка інформаційних ризиків передбачає виконання наступних етапів:

* ідентифікація та кількісна оцінка інформаційних ресурсів підприємств, які є значущими для бізнесу;
* оцінювання можливих загроз;
* оцінювання існуючих вразливостей;
* оцінювання ефективності засобів забезпечення інформаційної безпеки.

Передбачається, що значущі для бізнесу вразливі інформаційні ресурси компанії підприємства піддаються ризику, якщо стосовно них існують які-небудь погрози. Іншими словами, ризики характеризують небезпеку, якій можуть піддаватися компоненти корпоративної системи Internet / Intranet. При цьому інформаційні ризики компанії залежать:

* від показників цінності інформаційних ресурсів;
* ймовірності реалізації загроз для ресурсів;
* ефективності існуючих або планованих коштів забезпечення ІБ.

Мета оцінювання ризиків полягає у визначенні характеристик ризиків корпоративної інформаційної системи і її ресурсів. В результаті оцінки ризиків стає можливим вибрати засоби, що забезпечують бажаний рівень ІБ підприємства. При оцінюванні ризиків враховуються цінність ресурсів, важливість загроз і вразливостей, ефективність існуючих і планованих засобів захисту. Самі показники ресурсів, значущості загроз і вразливостей, ефективність засобів захисту можуть бути визначені як кількісними методами, наприклад при визначенні вартісних характеристик, так і, якісними, наприклад враховують штатні або надзвичайно небезпечні нештатні впливу зовнішнього середовища.

Можливість реалізації загрози оцінюється ймовірністю її реалізації протягом заданого відрізка часу для деякого ресурсу підприємства. При цьому ймовірність того, що загроза реалізується, визначається такими основними показниками:

* привабливістю ресурсу використовується при розгляді загрози від навмисного впливу з боку людини;
* можливістю використання ресурсу для отримання доходу при розгляді загрози від навмисного впливу з боку людини;
* технічними можливостями реалізації загрози застосовується при навмисному впливі з боку людини;
* ступенем легкості, з якою вразливість може бути використана.

Нині відомо безліч табличних методів оцінки інформаційних ризиків компанії. Важливо, щоб працівники служби безпеки вибрали для себе відповідний метод, який забезпечував би коректні і достовірні відтворювані результати.

Кількісні показники інформаційних ресурсів рекомендується оцінювати за результатами опитувань співробітників підприємства-власників інформації, тобто посадових осіб, які можуть визначити цінність інформації, її характеристики і ступінь критичності, виходячи з фактичного стану справ. На основі результатів опитування проводиться оцінювання показників і ступеня критичності інформаційних ресурсів для найгіршого варіанту розвитку подій аж до розгляду потенційних впливів на бізнес-діяльність підприємства при можливому несанкціонованому ознайомленні з конфіденційною інформацією, порушення її цілісності, недоступності на різні терміни, викликаних відмовами в обслуговуванні систем обробки даних і навіть фізичне знищення. При цьому процес отримання кількісних показників може доповнюватися відповідними методиками оцінювання інших критично важливих ресурсів підприємства, які враховують:

* безпеку персоналу;
* розголошення приватної інформації;
* вимоги щодо дотримання законодавчих і нормативних положень;
* обмеження, що випливають із законодавства;
* комерційні та економічні інтереси;
* фінансові втрати і порушення у виробничій діяльності;
* громадські відносини;
* комерційну політику і комерційні операції;
* втрату репутації компанії.

Далі кількісні показники використовуються там, де це допустимо і виправдано, а якісні - де кількісні оцінки по ряду причин утруднені. При цьому найбільшого поширення набуло оцінювання якісних показників за допомогою спеціально розроблених для цих цілей бальних шкал, наприклад, з чотирьох бальною шкалою.

Наступною операцією є заповнення пар опитувальних листів, в яких по кожному з типів загроз і пов'язаної з ним групі ресурсів оцінюються рівні загроз як ймовірність реалізації загроз і рівні вразливостей як ступінь легкості, з якою реалізована загроза здатна привести до негативного впливу. Оцінювання проводиться в якісних шкалах. Наприклад, рівень загроз і вразливостей оцінюється за шкалою «високий-низький». Необхідну інформацію збирають, опитуючи ТОР-менеджерів компанії, співробітників комерційних, технічних, кадрових та сервісних служб, виїжджаючи на місця і аналізуючи документацію компанії.

Поряд з табличними методами оцінки інформаційних ризиків, можуть бути використані сучасні математичні методи, наприклад метод типу дельті, а також спеціальні автоматизовані системи, окремі з яких будуть розглянуті нижче.

Загальний алгоритм процесу оцінювання інформаційних ризиків (рис.5.2). В цих системах включає наступні етапи.

* опис об'єкта і заходів захисту;
* ідентифікація ресурсу і оцінювання його кількісних показників (визначення потенційного негативного впливу на бізнес);
* аналіз загроз інформаційної безпеки;
* оцінювання вразливостей;
* оцінювання існуючих і передбачуваних засобів забезпечення інформаційної безпеки;
* оцінювання ризиків.

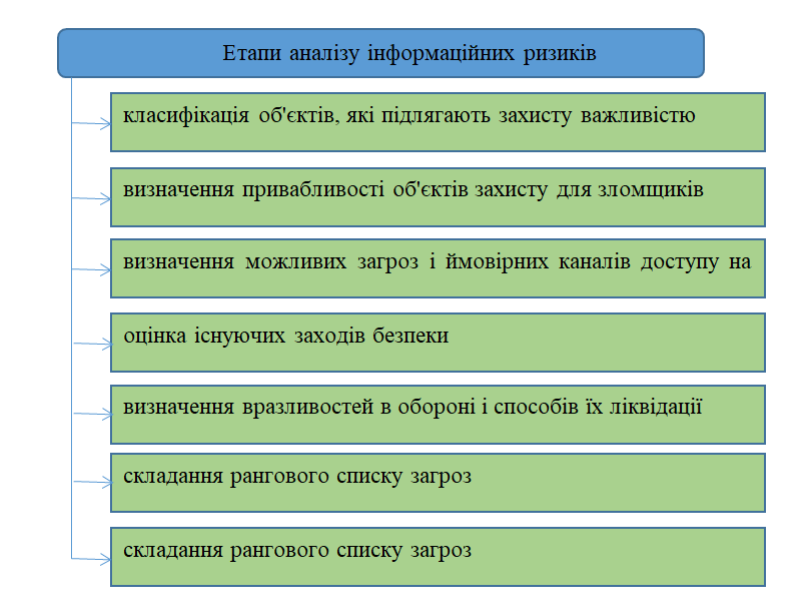


Рис.5.2. Етапи аналізу інформаційних ризиків

## 5.4. Управління інформаційними ризиками.

В даний час управління інформаційними ризиками є одним з найбільш актуальних і динамічно розвиваються напрямків стратегічного і оперативного менеджменту в області захисту інформації. Його основне завдання об'єктивно ідентифікувати і оцінити найбільш значущі для бізнесу інформаційні ризики компанії, а також адекватність використовуваних засобів контролю ризиків для збільшення ефективності і рентабельності економічної діяльності підприємства. Тому під терміном «управління інформаційними ризиками» зазвичай розуміється системний процес ідентифікації, контролю та зменшення інформаційних ризиків компаній відповідно до певних обмежень російської нормативно-правової бази в галузі захисту інформації і власної корпоративної політики безпеки.

Використання інформаційних систем пов'язане з певною сукупністю ризиків. Коли можливий збиток неприйнятно великий, необхідно економічно виправдані заходи захисту. Періодична (пере) оцінка ризиків необхідна для контролю ефективності діяльності в області безпеки і для врахування змін обстановки.

Суть заходів з управління ризиками полягає в тому, щоб оцінити їх розмір, виробити ефективні і економічні заходи зниження ризиків, а потім переконатися, що ризики укладені в прийнятні рамки (і залишаються такими). Отже, управління ризиками включає в себе два види діяльності, які чергуються циклічно:

1. (пере) оцінка (вимірювання) ризиків;
2. вибір ефективних і економічних захисних засобів (нейтралізація ризиків).

Стосовно виявлених ризиків можливі наступні дії:

* ліквідація ризику (наприклад, за рахунок усунення причини);
* зменшення ризику (наприклад, за рахунок використання додаткових захисних засобів);
* прийняття ризику (шляхом вироблення плану дії у відповідних умовах):
* переадресація ризику (наприклад, шляхом укладення страхової угоди).

Процес управління ризиками можна розділити на наступні етапи:

1. Вибір аналізованих об'єктів і рівня деталізації їх розгляду.
2. Вибір методології оцінки ризиків.
3. Ідентифікація активів.
4. Аналіз загроз і їх наслідків, виявлення вразливих місць в захисті.
5. Оцінка ризиків.
6. Вибір захисних заходів.
7. Реалізація та перевірка вибраних заходів.
8. Оцінка залишкового ризику.

Етап 6 відноситься до вибору захисних засобів (нейтралізація ризиків), решта - до оцінки ризиків.

Вже перерахування етапів показує, що управління ризиками процес циклічний. По суті, останній етап це оператор кінця циклу, який наказував би повернутися до початку. Ризики потрібно контролювати постійно, періодично проводячи їх переоцінку. Слід зазначити, що виконана і ретельно документована оцінка може істотно спростити подальшу діяльність.

Управління ризиками, як і будь-яку іншу діяльність в області інформаційної безпеки, необхідно інтегрувати в життєвий цикл ІС. Тоді ефект виявляється найбільшим, а витрати мінімальними.

Управління ризиками необхідно проводити на всіх етапах життєвого циклу інформаційної системи: ініціація, розробка, установка, експлуатація, утилізація (виведення з експлуатації). На етапі ініціації відомі ризики слід врахувати при виробленні вимог до системи взагалі і засобів безпеки зокрема. На етапі розробки знання ризиків допомагає вибирати відповідні архітектурні рішення, які грають ключову роль в забезпеченні безпеки. На етапі установки виявлені ризики слід враховувати при конфігуруванні, тестуванні і перевірці раніше сформульованих вимог, а повний цикл управління ризиками повинен передувати впровадженню системи в експлуатацію. На етапі експлуатації управління ризиками повинно супроводжувати всі істотні зміни в системі. При виведенні системи з експлуатації управління ризиками допомагає переконатися в тому, що міграція даних відбувається безпечним чином.

# РОЗДІЛ 6. ПРИКЛАД АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

## 6.1.Загальні поняття про компанію.

Фармацевтична компанія «Медок» - працює на ринку України з 2000 року і займається широко профільною медичною продукцією:

* медичні препарати (повне виробництво та переупакування готової продукції);
* медичне обладнання для українського та зарубіжного ринку;
* повна підтримка медичного обладнання та забезпечення відповідним програмним забезпеченням.

Компанія вивчає потреби споживачів продукції, проводить регулярні дослідження економічної та соціально-демографічної ситуації регіонів для надання доступних медичних продуктів за вигідною ціною жителям кожного регіону, аналізує ринки фармацевтичної продукції для виготовлення товарів, що мають попит.

Стратегічною ціллю компанії «Медок» є забезпечення клієнтів якісними медичними препаратами та обладнанням, досягнення нових стандартів якості та позицій на ринку збуту власної медичної продукції, високої рентабельності ведення бізнесу та подальший розвиток компанії.

Діяльність фармацевтичної компанії «Медок» регулюється відповідно до норм чинного законодавства дозволяє розділити законодавче (правове) забезпечення охорони здоров’я в Україні на наступні види:

1. конституційні приписи, тобто ті, що закріплені в Конституції України (право на збереження життя, особисту недоторканність, вимоги від держави здійснення заходів, спрямованих на підтримку життя, на охорону здоров’я і медичну допомогу тощо);
2. міжнародно-правові приписи, тобто ті, які містяться у міжнародних договорах та інших правових документах, що ратифіковані Верховною Радою України й знаходяться у відповідності з конституційними нормами (рівність усіх людей, право на життя, свободу, особисте щастя);
3. загальні правові приписи, тобто ті, дія яких поширюється на всі галузі права, в тому числі в на фармацевтичне право (утвердження та забезпечення державою прав і свобод людини і громадянина, рівності громадян та держави перед законом, законності, відповідальності держави перед людиною;
4. фармацевтичні приписи, тобто ті, що мають відношення виключно до фармацевтичного права (встановлення медичних стандартів, визначення режиму контролю лікарських засобів, ліцензування фармацевтичної діяльності, закріплення умов обігу лікарських засобів та встановлення відповідальності за порушення норм чинного законодавства та ін.).

Загальна організаційна структура фармацевтичної компанії «Медок», представлена на рисунку 6.1.

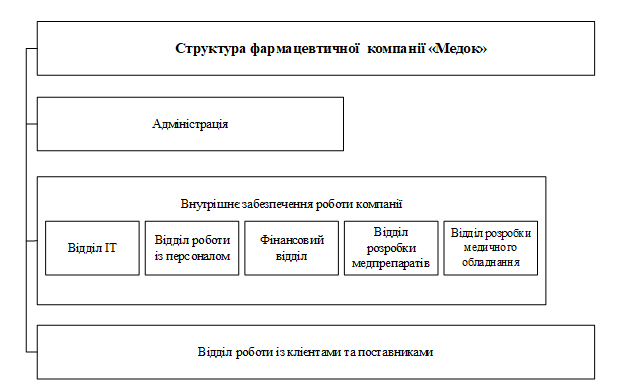


Рис. 6.1 Організаційна структура фармацевтичної компанії «Медок»

Основними складовими в системі інформаційного забезпечення діяльності ФК є: інформаційні ресурси; інформаційне програмне забезпечення; інформаційно-аналітична робота.

І**нформаційні ресурси** – це упорядкована сукупність інформації в будь-якій формі та вигляді, яка забезпечує систему управління відповідною кількістю даних, відомостей, знань для прийняття управлінських рішень.

**Інформаційне програмне забезпечення** − це технічні засоби обробки, зберігання та поширення інформації; програмні, технічні, організаційні засоби комп’ютерної мережі, призначені для розв’язання завдань користувачів.

**Інформаційно-аналітична робота**  – це діяльність фахівців фармацевтичної компанії «Медок», що спрямована на дослідження, розробку, впровадження, вивчення, створення медичних препаратів та обладнання.

Основними об’єктами захисту в фармацевтичній компанії є:

* фінансові ресурси;
* персонал компанії;
* матеріальні засоби;

інформації ресурси з обмеженим доступом (службова інформація різного роду про медичні препарати або розробки).

## 6.2. Обстеження середовищ функціонування АС

Метою обстеження є підготовка даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах розслідування.

При обстеженні обчислювальної системи ІТС повинні бути проаналізовані й описані:

* загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);
* види і характеристики каналів зв'язку;
* особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;
* можливі обмеження щодо використання засобів та ін.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1.

Аналізу підлягають такі характеристики фізичного середовища:

* територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);
* наявність охорони території та перепускний режим;
* наявність приміщень, в яких мають розміщуватися компоненти ІТС;
* режим доступу до компонентів фізичного середовища ІТС;
* вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;
* наявність елементів комунікацій, систем життєзабезпечення і зв’язку, що мають вихід за межі контрольованої зони;
* наявність та технічні характеристики систем заземлення;
* умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;
* наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

## 6.3. Визначення потенційних загроз для інформації

Модель загроз інформації - опис методів та засобів здійснення загроз для інформації, в конкретних умовах функціонування автоматизованої інформаційної системи чи засобу електронної обчислювальної техніки.

Модель загроз для секретної інформації - формалізований опис методів та засобів здійснення загроз для секретної інформації.

При складанні моделі загроз треба врахувати всі джерела загроз безпеці інформації, циркулюючої в автоматизованій системі, і розділити їх на три основні групи:

* загрози витоку за рахунок несанкціонованого доступу;
* загрози витоку інформації за допомогою технічних каналів;
* загрози, обумовлені стихійними джерелами.

Модель порушника - модель, у якій відбиваються його практичні і теоретичні можливості, апріорні знання, технічна оснащеність, час і місце дії тощо.

Порушник – це особа, яка помилково чи усвідомлено почала спробу виконання заборонених операцій і використовує для цього різні можливості та засоби. Будь-який порушник для реалізації своїх задумів керується певною мотивацією і намірами, володіє сукупністю знань, умінь і навичок здійснення протиправних дій із застосуванням технічних засобів, що володіють відповідним потенціалом.

Ціль порушника: можливість отримання доступу до ІзОД, яка циркулює в АС, з метою її отримання, корегування, знищення; можливість доступу до матеріальних носіїв ІзОД з метою їх отримання і знищення.

Кожна категорія ймовірних порушників повинна бути проаналізована окремо за наступними параметрами:

* технічна оснащеність і використовувані для здійснення порушення методи і засоби;
* передбачувані місця і час здійснення незаконних дій порушника;
* обмеження і припущення щодо кваліфікації порушника.

**Потенційні загрози інформації наведені в Табл. 8**

Таблиця 8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Потенційні загрози інформації** | **Наслідки (порушення властивостей)** | | |
| **К** | **Ц** | **Д** |
| **1** | **Загрози об’єктивної природи** |  |  |  |
| 1.1. | Стихійні явища (пожежа, землетрус, затоплення, метеоритний чи кислотний дощ тощо) |  | + | + |
| 1.2. | Збої та відмови системи електроживлення |  | + | + |
| 1.3. | Збої та відмови обчислювальної техніки |  | + | + |
| 1.4. | Збої, відмови та пошкодження носіїв інформації |  | + | + |
| 1.5. | Збої та відмови програмного забезпечення |  | + | + |
| **2.** | **Загрози суб’єктивної природи** |  |  |  |
| 2.1 | Помилки |  |  |  |
| 2.1.1 | Дії, що призводять до відмови АС (окремих компонентів) |  |  | + |
| 2.1.2 | Ненавмисне пошкодження носіїв інформації |  | + | + |
| 2.1.3 | Втрата засобів розмежування доступу | + | + | + |
| 2.1.4 | Неправомірна зміна режимів роботи АС | + | + | + |
| 2.1.5 | Невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів | + |  | + |
| 2.1.6 | Помилки під час введення даних в систему, виведення даних за невірними адресами | + |  |  |
| 2.1.7 | Помилки адміністраторів (неправильна настройка та адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту). | + | + | + |
|
| 2.1.8 | Недбале зберігання та облік: документів, носіїв інформації, даних | + | + | + |
| 2.2 | Несанкціоноване перехоплення інформації |  |  |  |
| 2.2.1 | Несанкціоноване підключення до технічних засобів | + |  |  |
| 2.2.2 | Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду документів | + |  |  |
| 2.3 | Порушення нормальних режимів роботи |  |  |  |
| 2.3.1 | Ураження програмного забезпечення комп’ютерними вірусами | + | + | + |
| 2.3.2 | Втрата (розголошення) засобів розмежування доступу (паролів), магнітних носіїв інформації та резервних копій | + | + | + |
| 2.3.3 | Несанкціоноване внесення змін до технічних засобів, в програмне забезпечення, в компоненти інформаційного забезпечення, тощо |  | + | + |
| 2.3.4 | Використання недозволеного ПЗ або модифікація компонент програмного та інформаційного забезпечення |  | + | + |
| 2.3.5 | Пошкодження носіїв інформації |  | + | + |
| 2.4 | Зовнішні загрози |  |  |  |
| 2.4.1 | Несанкціоноване перехоплення інформації за рахунок витоку інформації за рахунок побічного електромагнітного випромінювання та наводок | + |  |  |
| 2.4.2 | Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу | + |  |  |

К – конфіденційність; Ц – цілісність; Д – доступність.

## 6.4.Джерела загроз безпеці інформації, їх класифікація

Загрози власними силами не виявляються. Усі загрози можна реалізувати лише за наявності якихось слабких місць – вразливостей, властивих об'єкту інформатизації. Уразливість – якась слабкість, що може використовувати порушення інформаційної автоматизованої системи чи інформації яка міститься у ній. (ГОСТ РИСО 7498-2-99 «Інформаційна технологія. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Архітектура захисту»). Особливу увагу під час розгляду ВБ має приділятися джерелам загроз, які можуть виступати як суб'єкти (особистість), і об'єктивні прояви. Причому самі джерела загроз можуть бути і в середині об'єкта інформатизації – внутрішні, і поза нею – зовнішні.

Джерела загроз можуть бути: дії суб'єкта (антропогенні джерела загроз); технічні засоби (техногенні джерела загрози); стихійні джерела.

До антропогенних джерел загроз відносяться суб'єкти, дії яких можуть бути кваліфіковані як навмисні чи випадкові злочину. До техногенних джерел загроз відносять джерела, зумовлені технократичною діяльністю людей й розвитком цивілізації. До стихійних джерел загроз відносять стихійні лиха чи інші обставини, які неможливо чи можливо передбачити, але неможливо запобігти при рівні людського знання і набутих можливостей. Проте найбільшої шкоди інформації та інформаційним системам завдають неправомірні дії працівників і комп'ютерні віруси. Американські спеціалісти стверджують, щодо 85% випадків промислового шпигунства ведеться силами компанії, у якій це відбувається. У 2005 р. більш як третина фінансових втрат в організаціях відбулося за вини своїх власних співробітників. Рішення всіх цих проблем належить до компетенції адміністрації, і служби безпеки організації. У цьому випадку рекомендується шифрувати листування навіть в середині фірми.

Віруси представляють широко поширене явище, у більшості користувачів комп'ютерів, особливо у тих, що працюють у мережах з неліцензійним програмним забезпеченням. Віруси з'явилися у результаті створення самозапускних програм. Зовнішня схожість цих програм з біологією і медициною характером на програмно-технічні кошти сприяла появі таких термінів, як: вірус, зараження, лікування, профілактика, щеплення, лікар та інших. Процес впровадження вірусом своєї копії до іншої програми (системну область диска тощо.) називається зараженням, а програма чи інший об'єкт –зараженими. Віруси – це клас програм, незаконно проникаючих в комп'ютери користувачів і які завдають шкоди їх програмному забезпеченню, інформаційним файлам і навіть технічним пристроям, наприклад, жорсткому магнітному диску. З розвитком мережевих інформаційних технологій віруси стали представляти реальну загрозу для користувачів мережевих і локальних комп'ютерних систем.

Віруси проникають й у кишенькові персональні комп'ютери (КПК) Перша троянська програма для КПК (Backdoor.WinCE.Brador.a – утиліта прихованого дистанційного доступу) виявлена у серпні 2004 року. Вона може додавати, видаляти файли на КПК, і навіть пересилати їх автору вірусу. Програма-вірус зазвичай складається з унікальної послідовності команд – сигнатур (знаків) і поводжень, що дозволяє створювати виявляючі програми-антивіруси. Деякі віруси немають унікальних сигнатур та правильної поведінки і можуть видозмінювати себе (поліморфні). Всі великі ролі у сфері несанкціонованих впливів на інформацію, будинку, приміщення, безпеку користувача грають помилкові (зокрема. випадкові) і навмисні дії людей.

Типовими причинами порушення безпеки на об'єкті є: помилки індивідів чи неточні їхні діяння; несправність і (чи) відмова використовуваного устаткування; непередбачені та неприпустимі зовнішні прояви; несправність і (чи) відсутність необхідних засобів захисту;.

Встановлено, що помилкові дії людей становлять 50–80%, а технічних засобів – 15–25% порушень безпеки об'єктів та об'єктивності даних. Помилкові і несанкціоновані дії людей пояснюються недостатньою їх дисциплінованістю і підготовленістю на роботу, небезпечної технологією та недосконалістю використовуваної ними техніки. Негативні інформаційні соціально-психологічні впливи, зокрема дискомфорт, людина має і під час роботи із величезними масивами даних. Крім стресу, він працює жертвою інформаційних перевантажень, інформаційного шуму й т.д.

Аналіз загроз ВБ показує, що їх також можна розділити на два види: внутрішні і зовнішні. Внутрішні загрози національній безпеці об'єкта захисту: некваліфікована корпоративна політика з організації інформаційних технологій й управління безпекою корпорації; відсутність належної кваліфікації персоналу з забезпечення роботи і управлінням об'єктами захисту; навмисні і ненавмисні дії персоналу з порушення безпеки; техногенні аварії та руйнування, пожежі.

Зовнішні загрози національній безпеці об'єкта захисту: навмисні і ненавмисні дії зацікавлених структур (збирати інформацію, шантаж, спотворення іміджу, загрози фізичної сили та інших.); витік конфіденційної комп'ютерної інформації з носіїв інформації та обумовлених каналів зв'язку; несанкціоноване проникнення на об'єкт захисту; несанкціонованого доступу до носіїв інформації та обумовленою каналами зв'язку з єдиною метою розкрадання, спотворення, знищення, блокування інформації; стихійні лиха і інші форс-мажорні обставини; навмисні і ненавмисні дії системних інтеграторів і постачальників послуг із забезпечення безпеки, постачальників технічних і програмних продуктів, кадрів.

При комплексному підході до аналізу загроз ВБ об'єкта інформатизації необхідно провести: опис об'єкта; класифікацію джерел загроз; класифікацію вразливостей; класифікацію методів реалізації загроз; ранжування актуальних атак; класифікацію методів парирування загроз.

Структурований опис об'єкта інформатизації, представляє типові структурні компоненти інформаційної системи та перетини поміж ними, характеризуючих напрямів циркуляції і параметрів потоків інформацією поєднанні з текстовими поясненнями, дає змогу виявити точки можливого застосування загроз чи розкрити існуючі вразливості.

Аналіз і оцінка можливостей реалізації загроз повинні бути засновані на побудові моделі загроз, класифікації, аналізі та оцінки джерел загроз, вразливостей і методів реалізації. Моделювання процесів порушення інформаційної безпеки може здійснюватися з урахуванням розгляду логічного ланцюжка: загроза – джерело загрози – метод реалізації – вразливість – наслідки. Кожен компонент аналізованого логічного ланцюжка доцільно описується із необхідною подробицею.

## 6.5. Розробка політики безпеки інформації в АС

Під політикою безпеки інформації слід розуміти набір вимог, правил, обмежень, рекомендацій та ін., які регламентують порядок обробки інформації що спрямовані на захист інформації від певних загроз.

Політика стосується всіх осіб, що мають відношення до вирішення питань щодо забезпечення надійного та безпечного функціонування АС, службовців сторонніх організацій, постачальників та розробників апаратних та програмних компонентів КСЗІ.

Політика безпеки визначає ресурси, що потребують захисту, враховує основні загрози для інформації і моделі порушників, впроваджені технології обробки інформації і вимоги до захисту інформації від загроз.

На етапі розробки політики безпеки здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в АС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001. Політику безпеки рекомендується оформляти у вигляді окремого документу.

На етапі оформлення політики безпеки здійснюється:

* вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.д., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;
* документальне оформлення політики безпеки інформації.

Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

Під час розробки політики безпеки повинні бути враховані технології обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В АС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в АС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів АС), взаємодії об’єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів АС політика безпеки стосується, а яких - ні).

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в АС кожного з цих видів.

Роботи цього етапу включають в себе вибір способів протидії найбільш значущим погрозам, формування загальних вимог, правил, обмежень по використанню захищеної технологією обробки інформації, окремих заходів і засобів захисту інформації, а також документальне оформлення політики інформаційної безпеки.

Політика інформаційної безпеки або політика безпеки являє собою документально оформлений набір вимог, правил, обмежень і рекомендацій, при дотриманні яких може бути забезпечений заданий рівень захисту інформації. Політика безпеки може бути представлена ​​як у вигляді одного документа, так і у вигляді декількох документів, із складанням їх переліку.

## Цілі політики безпеки

Основною метою, на досягнення якої спрямовані усі положення справжньої Політики, являється захист суб'єктів інформаційних стосунків підприємства від можливого нанесення їм матеріального, фізичного, морального або іншого збитку, за допомогою випадкової або умисної дії на інформацію, її носії, процеси обробки і передачі, а також мінімізація рівня операційного і інших ризиків (ризик нанесення ущербу діловій репутації підприємства, правовий ризик і так далі).

Вказана мета досягається за допомогою забезпечення і постійної підтримки наступних властивостей інформації:

* доступності інформації для легальних користувачів (стійкого функціонування інформаційної системи підприємства, при якому користувачі мають можливість отримання необхідної інформації і результатів рішення завдань за прийнятний для них час);
* цілісності і автентичності (підтвердження авторства) інформації, що зберігається і обробляється в інформаційній системі підприємства та передається по каналах зв'язку;
* конфіденційності - збереження в таємниці певної частини інформації, зв'язку, що зберігається, обробляється і передається по каналах;

Необхідний рівень доступності, цілісності і конфіденційності інформації забезпечується такими, що відповідають безлічі значимих загроз методами і засобами.

## 6.7. Методи протистояння загрозам

Кошти та фізичні методи захисту зазвичай розділяють на великі групи: організаційні і технічні. Під організаційними маються на увазі законодавчі, адміністративні і обов'язкові фізичні, а під технічними – апаратні, програмні і писав криптографічні заходи, створені задля забезпечення захисту об'єктів, покупців, безліч інформації. З метою організації захисту об'єктів використовують системи охорони та безпеки об'єктів – це сукупність взаємодіючих радіоелектронних приладів, пристроїв й електрообладнання, коштів технічною відсталістю та інженерного захисту, спеціально підготовлений персонал, і навіть транспорту, виконують названу функцію. У цьому використовуються різні методи, щоб забезпечити санкціонованим особам доступом до об'єктах та ІР. До них відносять автентифікацію й ідентифікації користувачів.

Автентифікація – це метод незалежного джерела інформації встановлення дійсності інформації з урахуванням перевірки справжності її внутрішньої структури (“що це, ким назвався?”).

Авторизація – в основі інформаційних технологій це надання певних повноважень тій особі чи групі осіб виконання деяких дій у системі обробки даних. (“чи є право виконувати цю діяльність?”). З допомогою авторизації встановлюють і реалізуються права доступу до ресурсів.

Ідентифікація – це метод порівняння предметів чи осіб із їх характеристикам, шляхом впізнання з предметів чи документам, визначення повноважень, що з доступом осіб, у приміщення, до документів тощо. (“що це, ким назвався і проти неї виконувати цю діяльність?”).

Ефективність захисту значною мірою залежить від своєчасності виявлення й винятку впливів на неї, а, за необхідності, відновлення програм, файлів, інформації, працездатності комп'ютерних пристроїв і систем. Важливою складовою виконання таких дії є програмні і технічні засоби захисту.

Програмні засоби захисту – це найбільш поширений метод захисту в комп'ютерах та інформаційних мережах. Зазвичай їх застосовують при тупику використання деяких інших методів і коштів. Перевірка дійсності користувача зазвичай здійснюється операційній системою. Користувач ідентифікується своїм добрим ім'ям, а засобом автентифікації служить пароль.

Програмні засоби захисту представляють комплекс алгоритмів і програм спеціального призначення і спільного забезпечення роботи комп'ютерів, і інформаційних мереж. Вони націлені для контролювання і розмежування доступу до інформації, несанкціонованих дій управління охоронними пристроями тощо. Програмні засоби захисту мають універсальність, простоту реалізації, гнучкість, адаптивність, можливість настройки системи та ін.

Широко застосовуються програмні кошти на захист від комп'ютерних вірусів. Для захисту машин від комп'ютерних вірусів, профілактики та “лікування” використовуються програми-антивіруси, і навіть кошти діагностики і профілактики, дозволяють недопущення влучення вірусу в комп'ютерну систему, лікувати зараженні файли і диски, виявляти і запобігати підозрілі дії. Антивірусні програми оцінюються точностю виявлення й ефективному усунення вірусів, просте використання, вартість, можливості працювати у мережі.

Найбільшу популярність користуються програми, призначені для профілактики зараження, виявлення й знищення вірусів. У тому числі вітчизняні антивірусні програми DrWeb (Doctor Web) І. Данилова і AVP (Antiviral Toolkit Pro) Є.Касперського. Вони мають зручним інтерфейсом, засобами сканування програм, перевірки системи за мінімального завантаження тощо. У Росії її використовують і зарубіжні антивірусні програми.

Абсолютно надійних програм, які гарантують виявлення і знищення будь-якого вірусу, немає. Тільки багаторівнева оборона здатна забезпечити найповнішу захисту від вірусів. Важливим елементом захисту від комп'ютерних вірусів є профілактика. Антивірусні програми застосовують разом з регулярним резервуванням даних, і профілактичними заходами. Разом цього заходу дозволяють значно знизити ймовірність зараження вірусом.

Основними заходами профілактики вірусів є:

1. застосування ліцензійного програмного забезпечення;
2. регулярне використання кількох постійно обновлюваних антивірусних програм для перевірки як власних носіїв інформації при перенесення ними сторонніх файлів, а й будь-яких “чужих” дискет і дисків з кожного інформацією них, зокрема. І переформатованих;
3. застосування різних захисних коштів під час роботи за комп'ютером у будь-якій інформаційної середовищі (наприклад, з Інтернету). Перевірка на наявність вірусів файлів, отриманих через мережу;
4. періодичне резервне копіювання найцінніших даних, і програм.

Однією з найвідоміших засобів захисту інформації є її кодування (шифрування, криптографія). Воно не від фізичних впливів, але у інших випадках служить надійною засобом. Код характеризується: довжиною – числом знаків, використовуваних при кодування і структурою – порядком розташування символів, що використовуються позначення класифікаційного ознаки. Засобом кодування служить таблиця відповідності (наприклад кодова таблиця ASCII).

Загальні методи криптографії існують давно. Вона вважається потужним засобом забезпечення конфіденційності і місцевого контролю цілісності інформації. Поки альтернативи методам криптографії немає. Стійкість криптоалгоритма залежить від складності методів перетворення. Питаннями розробки, продаж і використання коштів шифрування даних, і сертифікації засобів захисту даних займається Гостехкомісія РФ. Якщо 256 і більше розрядні ключі, то рівень надійності захисту даних становитиме десятки і сотні років суперкомп'ютера. Для комерційного застосування досить 40-,44-разрядних ключів.

Однією із поважних проблем інформаційної безпеки є організація захисту електронних даних, і електронних документів. Для їх кодування, з задоволення вимогам забезпечення безпеки даних від несанкціонованих впливів ними, використовується електронний цифровий підпис (ЕЦП).

Цифровий підпис представляє послідовність символів. Він залежить від самого повідомлення й від секретного ключа, відомого лише підпису це повідомлення.

Технічні засоби захисту використовують у різних ситуаціях, входять до складу фізичних засобів і програмно-технічних систем, комплексів і пристроїв доступу, відео-нагляду, сигналізації та інших видів захисту. У найпростіших ситуаціях за захистом персональних комп'ютерів від несанкціонованого запуску і його використання наявних ними даних пропонується встановлювати устрою, обмежують доступу до них, і навіть працювати знімними жорсткими магнітними і магнітооптичними дисками, самозавантажуючими компакт дисками, флеш-пам’яттю та інших.

Як технічні засоби захисту використовують різноманітні електронні ключі, наприклад, HASP (Hardware Against Software Piracy), які мають апаратно-програмну система захисту програм, тож даних від нелегального використання коштів і піратського тиражування. Електронні ключі Hardlock йдуть на захист програм, файлів даних. До складу системи входить власне Hardlock, крипто-карта для програмування ключів і забезпечення до створення захисту додатків і що з ними файлів даних.

До основних програмно-технічних заходів, застосування яких дозволяє розв'язувати проблеми забезпечення безпеки ІР, є:

- автентифікація користувача встановлення його ідентичності;

- управління доступом до БД;

- підтримку цілісності даних;

- захист комунікацій між клієнтом і сервером;

- відбиток загроз, специфічних для СУБД та інших.

Підтримка цілісності даних передбачає наявність програмно-апаратних коштів підтримки й заходи щодо захисту і архівуванню ІР, дублювання їх тощо. Найбільшу небезпеку обману інформаційних ресурсів, особливо організацій, представляє несанкціонований вплив на структуровані дані – БД. З метою захисту в БД найважливішими є такі аспекти інформаційної безпеки (європейські критерії):

- умови доступу (нагоду отримати деяку необхідну інформаційну послугу);

- цілісність (несуперечність інформації, її захищеності від руйнації та несанкціонованого зміни);

- конфіденційність (захист від несанкціонованого прочитання).

Ці аспекти є основними для будь-якого програмно-технічного забезпечення, покликаного забезпечити створення умов безпечного функціонування даних в комп'ютерах і комп'ютерних інформаційних мережах. Контроль доступу – це процес захисту даних, і програм від використання об'єктами, які мають на це право.

Управління доступом служить контролю входу/виходу працівників і відвідувачів організації через автоматичні прохідні (турнікети, аркові металошукачі). Контроль їх переміщення здійснюється з допомогою систем відео-нагляду. У управлінні доступом входять пристрої і (чи) системи огорожі обмеження входу завезеними на територію. Використовуються також методи візуалізації (представлення вахтеру відповідних документів) і автоматичної ідентифікації вхідних/вихідних працівників і відвідувачів.

До заходів, які забезпечують традиційні і нетрадиційні типи носіїв інформації та, як наслідок, самої інформації відносять технології штрихового кодування. Ця відома технологія широко використовується при маркуванні різних товарів, зокрема документів, книжок та часописів.

Для захисту в інформаційних комп'ютерних мережах використовують спеціальні програмні, технічні і програмно-технічні кошти. З метою захисту мереж, і контролю доступу у яких використовують: фільтри пакетів, які забороняють встановлення сполук, котрі перетинають кордону захищеної мережі; фільтруючі маршрутизатори, реалізують алгоритми аналізу адрес відправлення та призначення пакетів у мережі; шлюзи прикладних програм, перевіряльники права доступу до програм.

Як устрою, який перешкоджає отриманню зловмисником доступу до інформації, використовують Firewalls (анг. “вогненна стіна” чи “захисний бар'єр” – брандмауер). Такий пристрій мають між внутрішньою локальною мережею організації та Інтернетом. Він обмежує трафік, кладе край спробам несанкціонованого доступу до внутрішніх ресурсів організації. Це зовнішній захист. Сучасні брандмауери можуть “відсікати” від користувачів корпоративних мереж незаконну і небажану їм кореспонденцію, передану електронною поштою. У цьому обмежується можливість отримання надлишкової інформації так званого “сміття” (спаму).

Іншим технічним пристроєм захисту в комп'ютерних мережах є маршрутизатор. Він здійснює фільтрацію пакетів переданих даних. У результаті виникає можливість заборонити доступ деяким користувачам до визначеного “хосту”, програмно здійснювати детальний контроль адрес відправників і одержувачів. Також можна обмежити доступ всім чи певним категоріям користувачів до різних серверів, наприклад, провідним поширення протиправній чи антисоціальній інформації.

Захист може здійснюватися у глобальній сіті або локальній мережі організації, окремих комп'ютерів. З цією метою створюються спеціальні програмно-апаратні комплекси.

Отже, методів парирування загроз досить багато. Найважливішими є такі:

* економічні: запровадження системи коефіцієнтів і надбавок; страхування устаткування й інформації; відшкодування збитків та компенсацію шкоди.
* організаційні: фізичний захист і організація охорони; добір і з персоналом; організація інструктажу персоналу; вибір, і роботу з партнерами; контроль виконання вимог щодо захисту; протипожежна охорона; організація взаємодії з компетентними органам.

Для комплексного захисту, об'єктів в різних підприємствах рекомендується розробляти та активніше впроваджувати відповідні заходи. Комплексні заходи щодо забезпечення збереження і захисту, об'єктів включають організаційні, фізичні, соціально-психологічні заходи й інженерно-технічні засоби захисту. Організаційні заходи припускають об'єднання складових безпеки. В усьому світі основну загрозу інформації організації представляють її працівники, що виявляються психічно неврівноваженими, скривдженими чи незадоволеними характером його роботи, зарплатою, взаємовідносинами з і керівниками.

## 6.8. Обмеження співробітників організації

Співробітникам організації категорично забороняється:

- використовувати компоненти програмного і апаратного забезпечення АС організації в неслужбових цілях;

- самовільно вносити які-небудь зміни до конфігурації апаратно-програмних засобів робочих станцій або встановлювати додатково будь-які програмні і апаратні засоби, не передбачені формулярами робочих станцій;

- здійснювати обробку конфіденційної інформації у присутності сторонніх (не допущених до даної інформації) осіб;

- записувати і зберігати конфіденційну інформацію (що містить відомості обмеженого розповсюдження) на неврахованих носіях інформації (гнучких магнітних дисках і т.д.);

- залишати включеною без нагляду свою робочу станцію, не активізувавши засобу захисту від НСД (тимчасове блокування екрану і клавіатури);

- передавати кому-небудь свою персональну ключову дискету (окрім відповідального за інформаційну безпеку або керівника свого підрозділу встановленим порядком), робити невраховані копії ключової дискети (на будь-який інший носій),

-використовувати свою ключову дискету (диск, flew носій) для формування цифрового підпису будь-яких електронних документів, окрім регламентованих технологічним процесом на його робочому місці;

- залишати без особистого нагляду на робочому місці або де б то не було свою персональну ключову дискету, персональний пристрій ідентифікації, машинні носії і роздруковані матеріали, що містять інформацію, що захищається (відомості обмеженого розповсюдження);

- умисне використовувати недокументовані властивості і помилки в програмному забезпеченні або в настройках засобів захисту, які можуть привести до виникнення кризової ситуації. Про виявленні такого роду помилок – повідомляти відповідального за безпеку інформації і керівника свого підрозділу.

## 6.9. Порядок видалення інформації в мережі

Визначити наступні типи інформації по відношенню до проблеми зберігання/видалення:

* програми і програмні комплекси. До вказаного типу віднести всі розробки підприємства, всі комерційні або оцінні програми, всі тестові і антивірусні засоби;
* інформація, БД, комп'ютерні архіви. До вказаного типу віднести всю інформацію, що знаходиться в локальних і мережевих базах даних будь-яких типів (виключаючи персональні робочі набори даних), в комп'ютерних архівах, на будь-яких типах комп'ютерних носіїв.
* Робочі матеріали. До вказаного типу віднести всю інформацію, що знаходиться на локальних або мережевих носіях, яка є результатом проектування, в т.ч. проміжним або варіантним.
* аварійні/архівні копії. До вказаного типу віднести всі екземпляри документів (файлів), створені методами копіювання з метою запобігти втрати або руйнуванню інформації.
* персональні набори даних. До вказаного типу віднести всю інформацію, що знаходиться на локальних або мережевих носіях, яка з'являється в результаті технологічних процесів застосування комп'ютерної техніки або є елементами організації персонального робочого процесу і не входить у вище перелічені типи інформації.
* інформація не знищується спеціальними засобам, так як після отримання її замовником вона вже не має вартості.

## 6.10. Порядок зберігання інформації на підприємстві

Відповідно до типів інформації визначити наступний порядок видалення інформації в мережі підприємства:

* готові роботи і копії. Підлягають видаленню з комп'ютерних носіїв відповідно до угод з замовником.
* данні, БД, комп'ютерні архіви. Інформація цього типу видаленню не підлягає. Відповідальність за виконання заходів по організації збереження вказаного типу інформації несе адміністратор.
* робочі матеріали. По закінченню роботи над проектом (завданням) керівник досліду (або призначений робітник) проводить аудит з метою розділення всієї проектної комп'ютерної інформації на робочі матеріали і персональні набори даних.
* аварійні/архівні копії підлягають зберіганню відповідно до встановлених правил. По закінченню часу зберігання інформації носій використовується повторно, попередня інформація затирається. Відповідальність за збереження носіїв і за виконання правил зберігання і перезапису несе адміністратор.

## 6.11. Ідентифікація користувачів відбувається в такій послідовності:

* на КПП проходячи через охорону;
* за допомогою спеціальної картки;
* паролем, який встановлено на комп’ютері кожного користувача.

# ВИСНОВКИ

Аудит інформаційної безпеки стає необхідною умовою для ефективного функціонування підприємств. При цьому особлива увага надається процесу знаходження слабких місць та виробітку рекомендацій завдяки яким потім удосконалюється система захисту інформації підприємств, оскільки саме результати проведення аудиту є необхідним підґрунтям для побудови надійної системи інформаційної безпеки. Проведення аудиту безпеки підприємства дають можливість забезпечити формування єдиної політики і концепції безпеки підприємства; розрахувати, узгодити і обґрунтувати необхідні витрати на захист підприємства; об'єктивно і незалежно оцінити поточний рівень інформаційної безпеки підприємства; забезпечити необхідний рівень безпеки і в цілому підвищити економічну ефективність підприємства; ефективно створювати і використовувати профілі захисту конкретного підприємства на основі неодноразово апробованих і адаптованих якісних і кількісних методів оцінки інформаційної безпеки підприємств замовника.

У роботі було проаналізовано:

* загальні відомості про аудит в інформаційній сфері та його види;
* проблеми інформаційної безпеки;
* методики проведення аудиту інформаційної безпеки;

Постанова задачі:

* розглянути особливості проведення аудиту інформаційної безпеки;
* розробити рекомендації щодо проведення аудиту інформаційної безпеки на підприємстві;
* визначити ефективність проведення аудиту;
* дослідити проблеми в інформаційній безпеці;
* знайти способи вирішення загроз в системі інформаційної безпеки.

В ході виконання курсової роботи було створено, досліджено і введено в дію комплексну систему захисту інформації на фармацевтичній компанії «Медок» , яка дозволяє виконувати захист інформації та інших активів фірми від викрадення, пошкодження та інших несанкціонованих дій.

КСЗІ являє собою діючі в єдиній сукупності законодавчі, організаційні, технічні та інші заходи, що спрямовані на виявлення та блокування різноманітних каналів витоку мовної інформації. Сполучною ланкою в цій системі є керуючий орган (наприклад, відділ по ЗІ), який може бути представлений як підрозділом, який здійснює керівництво, так і одним працівником, відповідальним за цю діяльність.

Результати проведення аудиту інформаційної безпеки дозволяють:

* виявити значущі загрози для інформації, що циркулює в межах підприємства;
* оцінити ймовірність кожної події, що представляє загрозу для безпеки, і збиток від нього;
* скласти неформальну модель порушника; визначити основні вимоги до системи захисту;
* оцінити з точки зору цих вимог ефективність застосовуваних організаційних заходів і інженерно-технічних засобів захисту;
* розробити пропозиції і рекомендації щодо вдосконалення комплексної системи забезпечення безпеки.

# СПИСОК ЛІТЕРАТУРИ

1. Інформаційна технологія. Методи і засоби забезпечення безпеки. Частина 1. Концепція та моделі менеджменту безпеки інформаційних і телекомунікаційних технологій : ГОСТ Р ІСО / МЕК 13335-1-2006. – Введ. 2007.05.31. – М.: ІПК «Видавництво стандартів», 2007. – 23 с.
2. Дмитрієв А.А. Внутрішній аудит системи менеджменту інформаційної безпеки за вимогами ISO/IEC 27001. Один з варіантів реалізації процесу / Das Management. – 2011. – № 2. – С. 58-64.
3. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017 [Електронний ресурс] .- Режим доступу: [УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017 — Офіційне інтернет-представництво Президента України (president.gov.ua)](https://www.president.gov.ua/documents/472017-21374)
4. Аверченков В.И. Организационная защита информации: учеб.пособие/В.И.Аверченков, М.Ю. Рытов – Брянск: БГТУ, 2005 – 184с.
5. Аверченков В.И., Служба защиты информации: организация и управление: учеб.пособие / В.И. Аверченков, М.Ю. Рытов – Брянск: БГТУ, 2005 – 186с.
6. Астахов А. Аудит безопасности информационных систем / А.Астахов.
7. Галатенко В.А. Основы информационной безопасности: учеб. пособие/В.А. Галатенко– М: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2004. – 264с.
8. Мак-Мак В.П. Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности/В.П. Мак-Мак – М.: ИД МБ, 1999. –160 с.
9. Петренко С.А. Аудит безопасности Iuranrt / С.А. Петренко, А.А. Петренко – М: Академии АиТи: ДМК Пресс, 2002. – 438с.
10. Петренко С.А. Возможная методика построения системы информационной безопасности предприятия.
11. Симонов С. Анализ рисков, управление рисками.
12. Гузик С. Зачем проводить аудит информационных систем? /С. Гузик // Jet Info on line. – 2000. – 10 (89). articlel. 10.2000.