МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **СИСТЕМА ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**

Студент групи СЗД-41 Юрченко Дмитро Дмитрович _____
(підпис)

Науковий керівник: к.т.н., доцент Шуклін Герман Вікторович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович
_____
(підпис)

КИЇВ – 2023

ЗМІСТ

ВСТУП

Актуальність теми. Дивлячись на стрімкий розвиток Internet – технологій, стає зрозуміло, що кожного дня з’являється все більше загроз безпеки інформації. Безперервний розвиток суспільства складно уявити без постійного застосування інформаційних технологій, ми стикаємось з цим кожного дня: комп’ютери обслуговують банківські системи, відслідковують розклад потягів та літаків, телекомунікаційні системи визначають надійність безпеки та оборони нашої держави. Комп’ютери зберігають інформацію,здійснюють її обробку і надання споживачам, реалізуючи в такий спосіб інформаційні технології. Інформаційна безпека підприємства - це стан захищеності інформації від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Питання безпеки інформаційних систем наразі стоїть дуже гостро і привертає велику увагу з боку аналітиків, інженерів та інших фахівців в області інформаційної безпеки.

Об’єктом дослідження є система прийняття рішень оцінки загроз інформаційної безпеки.

Предметом дослідження є теоретичні, методологічні та практичні засади впровадження систем прийняття рішень оцінки загроз інформаційної безпеки.

Метою даного дослідження є розробка моделі оцінювання ризиків інформаційної безпеки.

Для досягнення вказаної мети виконуються такі основні задачі:

1. Аналіз проблем інформаційної безпеки;
2. Формування вимог до моделі оцінювання ризиків інформаційної безпеки;
3. Апробація адекватності побудованої математичної моделі;
4. Інтерпретація отриманих результатів;

Наукова новизна даної роботи полягає у адаптації системи прийняття рішень оцінки загроз інформаційної безпеки. Отримані результати припускають більш успішну протидію сучасним кібер-зловмисникам, забезпечення інформаційної безпеки.

Галузь застосування. Результатами та коментарями отриманими в ході виконання даної роботи можна керуватися при впровадженні систем прийняття рішень оцінки загроз інформаційної безпеки.

РОЗДІЛ 1. ОЦІНКА РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Методи оцінки інформаційної безпеки

Призначення системи інформаційної безпеки полягає в організації безпечних і надійних: заходів з доступу до інформації, способів передачі та зберігання інформації, методів обробки інформації, правил управління доступом до інформації, способів відновлення інформації, методів резервування інформації тощо.

Завдання системи інформаційної безпеки обумовлюються її призначенням і полягають у: забезпеченні безпечного, надійного зберігання і передачі інформації в електронному вигляді, розташованої на різних носіях; організації надійного доступу до електронної інформації; обмеження і контроль доступу до інформації, з якою працюють співробітники; створенні правил безпечної роботи з інформацією; проведенні заходів щодо резервування інформації; забезпеченні відновлення інформації в аварійних ситуаціях; підтримці інформаційної безпеки на заданому рівні. Забезпечення інформаційної безпеки в епоху постіндустріальної економіки стає життєво важливим для успішного існуванні підприємства. З іншого боку, постає питання належного визначення стану інформаційної безпеки підприємства, показників, що його характеризують, а також значень цих показників, які б забезпечували належний рівень інформаційної безпеки підприємства.

Також важливим є питання оцінювання значень цих показників в умовах невизначеності, яка притаманна сфері безпеки. В нинішній час для забезпечення належного стану інформаційної безпеки потрібна не просто розробка окремих механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних

посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства. Унаслідок сукупної дії зовнішніх і внутрішніх дестабілізуючих факторів перед службами захисту інформації стоять завдання не тільки створення, а й постійного вдосконалення захисту інформації. Необхідність вдосконалення призводить до постійного проведення моніторингу і аналізу стану інформаційної безпеки. Розглянемо один з методів оцінки захищеності
інформації наведений у [1].

Удосконалення, поліпшення стану ІБ можливо за умови знання станів характеристик і параметрів використовуваних засобів захисту, процесів менеджменту, усвідомлення ІБ і розуміння ступеня їх відповідності необхідним результатам. Зрозуміти ці аспекти безпеки можна лише за результатами оцінки ІБ організації, отриманої за допомогою моделі оцінки ІБ на підставі свідчень оцінки, критеріїв оцінки та з урахуванням контексту оцінки. Критерії оцінки – це все те, що дозволяє встановити значення оцінки для об’єкта оцінки. В якості критеріїв оцінки ІБ можуть використовуватися вимоги ІБ, процедури ІБ, поєднання вимог і процедур ІБ, рівень інвестицій, витрат на ІБ.

До свідчень оцінки ІБ відносяться записи, виклад фактів або будь-яка інформація, яка має відношення до критеріїв оцінки ІБ і може бути перевірена. Такими посвідченнями оцінки ІБ можуть бути докази виконуваної й виконаної діяльності по забезпеченню ІБ у вигляді звітних, нормативних, розпорядчих документів, результатів опитувань, спостережень.
Контекст оцінки ІБ об’єднує цілі і призначення оцінки ІБ, вид оцінки (незалежна оцінка, самооцінка), об’єкт та області оцінки ІБ, обмеження оцінки та ролі.

Модель оцінки ІБ визначає сферу оцінки, що відображає контекст оцінки ІБ в рамках критерію оцінки ІБ, відображення і перетворення оцінки в параметри об’єкта оцінки, а також встановлює показники, що забезпечують

оцінку ІБ у сфері оцінки.

У загальному вигляді процес проведення оцінки ІБ (рис. 1.1.) представлений основними компонентами процесу: контекст, свідоцтва, критерії та модель оцінки – необхідними для реалізації процесу оцінки. Оцінка ІБ полягає у виробленні оціночного судження щодо придатності (зрілості) процесів забезпечення ІБ, адекватності використовуваних захисних заходів або доцільності (достатності) інвестицій (витрат) для забезпечення необхідного рівня ІБ на основі вимірювання та оцінювання критичних елементів (факторів) об’єкта оцінки.

Рисунок 1.1 – Загальний вид процесу оцінки ІБ підприємства

Поряд з найважливішим призначенням оцінки ІБ – створення інформаційної потреби для вдосконалення ІБ, можливі й інші цілі проведення оцінки ІБ, такі як:

— аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки у відношенні до ресурсів ІБ;

— оцінка поточного рівня захищеності ІБ;

— локалізація вузьких місць у системі захисту ІБ;

— оцінка відповідності ІБ існуючим стандартам в галузі інформаційної безпеки;

— вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІБ; [2]

Результати оцінки ІБ підприємства можуть також використовуватися зацікавленою стороною для порівняння рівня ІБ схожих організацій. В залежності від обраного для оцінки ІБ критерію можна розділити способи оцінки ІБ організації на:

1) оцінку за еталоном;
2) ризик-орієнтовану оцінку;
3) оцінку за економічними показниками.

Спосіб оцінки ІБ за еталоном зводиться до порівняння діяльності та заходів щодо забезпечення ІБ організації з вимогами, закріпленими в еталоні. По суті справи проводиться оцінка відповідності СЗІБ організаці встановленому еталону. Під оцінкою відповідності ІБ організації встановленим критеріям розуміється діяльність, пов’язана з прямим або непрямим визначенням виконання або невиконання відповідних вимог ІБ в організації. За допомогою оцінки відповідності ІБ вимірюється правильність реалізації процесів системи забезпечення ІБ організації та ідентифікуються недоліки такої реалізації.

У результаті проведення оцінки ІБ має бути сформована оцінка ступеня відповідності системи захисту інформації еталону, в якості якого можуть бути прийняті (у сукупності і окремо):

1) вимоги вітчизняного законодавства в області ІБ;
2) галузеві вимоги щодо забезпечення ІБ;
3) вимоги нормативних, методичних та організаційно-розпорядчих
4) документів щодо забезпечення ІБ;
5) вимоги національних і міжнародних стандартів в області ІБ.

Основні етапи оцінки інформаційної безпеки за еталоном включають вибір еталона і формування на його основі критеріїв оцінки ІБ, збір свідчень оцінки

і вимірювання критичних елементів (факторів) об’єкта оцінки, формування оцінки ІБ.

Ризик-орієнтована оцінка ІБ підриємства являє собою спосіб оцінки, при якому розглядаються ризики ІБ, що виникають в інформаційній сфері організації, і зіставляються існуючі ризики ІБ і вжиті заходи по їх обробці. В результаті має бути сформована оцінка здатності організації ефективно управляти ризиками ІБ для досягнення своїх цілей.

Основні етапи ризик-орієнтованої оцінки інформаційної безпеки включають ідентифікацію ризиків ІБ, визначення адекватних процесів менеджменту ризиків і ключових індикаторів ризиків ІБ, формування на їх основі критеріїв оцінки ІБ, збір свідчень оцінки і вимірювання ризик-факторів, формування оцінки ІБ. Спосіб оцінки ІБ на основі економічних показників оперує зрозумілими для бізнесу аргументами про необхідність забезпечення та вдосконалення ІБ. Для проведення оцінки в якості критеріїв ефективності засобів інформаційної

безпеки використовуються, наприклад, показники сукупної вартості володіння (Total Cost of Ownership - TCO). Під показником TCO розуміється сума прямих і непрямих витрат на впровадження, експлуатацію та супровід системи захисту інформації. Під прямими витратами розуміються всі матеріальні витрати, такі як купівля обладнання та програмного забезпечення, трудовитрати відповідних категорій співробітників. Непрямими є всі витрати на обслуговування системи захисту інформації, а також втрати від інцидентів, що відбулися. Збір та аналіз статистики по структурі прямих і непрямих витрат проводиться, як правило, протягом року. Отримані дані оцінюються по ряду критеріїв із показниками TCO аналогічних організацій галузі. Оцінка на основі показника TCO дозволяє оцінити витрати на інформаційну безпеку і порівняти ІБ організації з типовим профілем захисту, а також управляти витратами для досягнення необхідного рівня захищеності.

Основні етапи оцінки ефективності СЗІБ на основі моделі TCO

включають збір даних про поточний рівень ТСО, аналіз областей забезпечення ІБ, вибір порівнянної моделі ТСО в якості критерію оцінки, порівняння показників з критерієм оцінки, формування оцінки ІБ. Однак цей спосіб оцінки вимагає створення загальної інформаційної бази даних про ефективність СЗІБ організацій схожого бізнесу та постійної підтримки бази даних в актуальному стані. Така інформаційна взаємодія організацій, як правило, не відповідає цілям бізнесу. Тому оцінка ІБ на основі
показника ТСО практично не застосовується.

1.2 Процес оцінки інформаційної безпеки

Процес оцінки ІБ включає такі елементи проведення оцінки:

- контекст оцінки, який визначає вхідні дані: цілі й призначення оцінки
- ІБ, вид оцінки (незалежна оцінка, самооцінка), об’єкт та області оцінки ІБ,
- обмеження оцінки і ролі;
- критерії оцінки;
- модель оцінки;
- заходи процесу оцінки: збір свідчень оцінки та перевірка їх
- достовірності, вимірювання та оцінювання атрибутів об’єкта оцінки;
- вихідні дані оцінки.

Основні елементи процесу оцінки ІБ представлені на рисунку 1.2.

Рисунок 1.2 – Основні елементи процесу оцінювання ІБ

1.3 Заходи та вихідні дані процесу оцінки

Призначення заходу: збір свідчень оцінки з дотриманням умов забезпечення достовірної оцінки ІБ. Незалежна оцінка ІБ може бути здійснена за допомогою внутрішнього і зовнішнього аудиту ІБ. Аудит безпеки інформаційної безпеки – це системний процес одержання об'єктивних якісних і кількісних оцінок поточного стану безпеки інформаційної системи, комплексна оцінка рівня інформаційної безпеки клієнта з урахуванням трьох основних факторів: персоналу, процесів і технологій. Порівняльний аналіз поточного стану інформаційної системи, що визначається за підсумками анкетування, з тестовою моделлю вимог стандарту ISO 27001 [3].

Аудит ІБ визначається як систематичний, незалежний і документований процес отримання доказів діяльності організації по забезпеченню ІБ, визначення ступеня виконання в організації критеріїв ІБ, а також допускає можливість формування професійного аудиторського судження про інформаційну безпеку організації [4]. Необхідними умовами забезпечення достовірної оцінки ІБ при проведенні аудиту є:

– використання довіреної процесу аудиту та дотримання основних принципів аудиту;

– менеджмент програми аудиту ІБ;

– використання найбільш достовірних джерел свідоцтв оцінки;

– визначення обсягу вибірки з урахуванням заданої достовірності свідчень оцінки;

– облік факторів, що впливають на аудиторський ризик, з метою зниження аудиторського ризику.

Довірений процес аудиту ІБ повинен відповідати вимогам прийнятого в організації нормативного документа, що описує процес аудиту ІБ, або вимогам визнаного співтовариством міжнародного (національного) нормативного документа (стандарту, рекомендації). До основних принципів проведення аудиту ІБ відносяться:

1) незалежність аудиту ІБ. Аудитори (група оцінки) незалежні у своїй діяльності і невідповідальні за діяльність, яка піддається аудиту ІБ. Незалежність є підставою для неупередженості при проведенні аудиту ІБ і об’єктивності при формуванні висновку за результатами аудиту ІБ.

2) повнота аудиту ІБ. Аудит ІБ повинен охоплювати всі області аудиту ІБ, відповідні цілі оцінки. Крім того, повнота аудиту ІБ визначається достатністю затребуваних і наданих матеріалів, документів та рівнем їх відповідності поставленим завданням. Повнота аудиту ІБ є необхідною умовою для формування об’єктивних висновків за результатами оцінки ІБ.

3) оцінка на основі доказів аудиту ІБ. При періодичному проведенні аудиту ІБ оцінка на основі доказів аудиту ІБ є єдиним способом, що дозволяє отримати повторюваний висновок за результатами аудиту ІБ, що підвищує довіру до такого висновку. Для повторюваності укладення свідоцтва аудиту ІБ повинні бути перевіреними.

4) достовірність доказів аудиту ІБ. Оцінювачі повинні бути впевнені в достовірності свідчень оцінки ІБ. Довіра до документальних свідчень оцінки ІБ підвищується при підтвердженні їх достовірності третьою стороною або

керівництвом організації. Довіра до фактів, отриманих при опитуванні співробітників об’єкта оцінки, підвищується при підтвердженні даних фактів з різних джерел. Довіра до фактів, отриманим при спостереженні за діяльністю в області ІБ об’єкта оцінки, підвищується, якщо вони отримані безпосередньо при функціонуванні процедур або процесів, які перевіряються.

5) компетентність і етичність поведінки. Довіра до процесу і результатів оцінки ІБ залежить від компетентності тих, хто проводить аудит ІБ, і від етичності їх поведінки. Компетентність базується на здатності аудитора застосовувати знання та навички. Етичність поведінки передбачає відповідальність, непідкупність, уміння зберігати таємницю, неупередженість.

Дотримання принципів проведення аудиту ІБ є передумовою для об’єктивних висновків за результатами оцінки. Основними методами одержання свідчень оцінки повинні бути:

– перевірка та аналіз документів, що відносяться до об’єкта оцінки; – спостереження за процесами об’єкта оцінки;

– опитування співробітників об’єкта оцінки і незалежної (третьої) сторони.

Поряд з ручними способами збору інформації формування доказів аудиту може бути автоматичним або напівавтоматичним в результаті застосування якогось інструментального засобу чи застосування декількох інструментальних засобів. При зборі даних оцінювачі повинні виходити з того, що діяльність по забезпеченню ІБ в області оцінки здійснюється відповідно до критеріїв оцінки ІБ, якщо цьому є докази. Оцінювачі повинні проявляти достатню ступінь професійного скептицизму у відношенні збираних свідоцтв оцінки, беручи до уваги можливість наявності порушень ІБ. Перевірка та аналіз документів дозволяють оцінювачу отримати свідоцтва оцінки, що володіють найбільшою повнотою і зручністю сприйняття і використання в порівнянні з іншими методами отримання доказів аудиту. Однак ці свідчення аудиту мають різну ступінь достовірності залежно від їх характеру і джерела,

а також від ефективності контролю за процесом підготовки та обробки поданих документів.

Свідоцтвами оцінки ІБ, отриманими в результаті перевірки та аналізу документів, можуть бути, наприклад:

– наявність документа (документів) з релевантним вмістом;

– витяги з документа (документів), що підтверджують реалізацію діяльності по забезпеченню ІБ, покладання відповідальності та обов'язків на співробітника (співробітників) за реалізацію діяльності по забезпеченню ІБ;

– витяги з документа (документів), що містять описи реалізованих захисних методів, процесів забезпечення ІБ.

Спостереження являє собою відстеження оцінювачем процедур або процесів забезпечення ІБ, виконуються іншими особами (в т.ч. персоналом організації). Інформація вважається достовірною тільки в тому випадку, якщо вона отримана безпосередньо в момент функціонування процедур або процесів, які перевіряються. Свідоцтвами аудиту, отриманими за допомогою спостереження за діяльністю, можуть бути, наприклад, записи, факти або інша інформація, які мають відношення до результатів автоматичного контролю технічними засобами, зафіксовані оцінювачами в ході спостереження. Усне опитування проводять оцінювачі серед співробітників (власників активів), затверджених представником об'єкта оцінки для надання джерел свідоцтв і свідоцтв оцінки. Результати усних опитувань повинні оформлятися у вигляді протоколу чи короткого конспекту, в якому обов'язково має бути зазначено прізвище, ім'я, по батькові оцінювача, який проводив опитування, прізвище, ім'я, по батькові опитуваної особи, а також їх підписи. Для проведення типових опитувань можуть бути підготовлені бланки з переліками питань, що цікавлять. Результати усного опитування слід перевіряти, так як опитуваний може виражати свою суб'єктивну думку. Свідоцтвами аудиту, отриманими при проведенні опитування, можуть бути, наприклад, описи та роз'яснення опитуваних осіб по реалізації процесів, процедур по забезпеченню ІБ. Для впевненості в достовірності оцінки оцінювачі повинні бути впевнені в

достовірності виявлених доказів аудиту. Зібрані свідчення оцінки, використовувані для оцінювання показників, повинні бути точним представленням оцінюваного об’єкта оцінки. Для цього слід враховувати достовірність джерел доказів аудиту.

За ступенем достовірності (від найбільшої до найменшої) джерела свідоцтв оцінки діляться на:

– документальні джерела свідоцтв, отримані з різних джерел третьої сторони (відомості про використання ліцензійних заходів і засобів забезпечення ІБ, договору із супроводу заходів і засобів забезпечення ІБ і т.д.);

– документальні джерела свідоцтв, отримані на (від) об’єкті (та) оцінки та підтверджені третьою стороною (план заходів за результатами зовнішнього аудиту ІБ, матеріали відомчих перевірок ІБ і т.д.);

– джерела свідоцтв, отримані в ході проведення аудиторських процедур, які не передбачають періодичну документальну звітність (результати спостереження за діяльністю, аналізу даних системи моніторингу ІБ і т.д.);

– джерела свідоцтв, отримані у вигляді нормативних та розпорядчих документів (політики, регламенти, звіти про діяльність, накази, розпорядження і т.д.), що вказують на належне застосування процесів і заходів забезпечення ІБ на практиці (наявність дозвільних записів уповноважених осіб, даних контролю ризиків і т.д.);

– свідоцтва, отримані в результаті усних і письмових опитувань про об’єкт оцінки, і спостереження за застосуванням заходів і засобів забезпечення ІБ, які не залишають документальних свідчень (виявлення ролей процесів, послідовності застосування захисних методів і т.д.). Поряд з достовірністю джерел свідоцтв слід враховувати часовий період отримання свідоцтв та поєднання джерел свідоцтв оцінки. Наприклад, довіра до фактів, отриманим при спостереженні за діяльністю, підвищується, якщо вони отримані безпосередньо при функціонуванні процедур або процесів; довіру до фактів,

отриманим при опитуванні співробітників, підвищується при підтвердженні даних фактів з різних джерел.

1.4.Методи моделювання та оцінювання рівня інформаційної безпеки

Основними способами знаходження уразливостей в системі є такі способи: статичний аналіз кожного елементу, перевірка шляхом створення фіктивних атак, отримання інформації про вразливості від розробника ПО або моделювання ризиків.

Саме моделювання ризиків дозволяє продумати методи захисту системи ще в процесі її проектування. Моделювання ризиків – це неперервний процес, який допомагає знаходити та зменшувати кількість загроз в вашій системі шляхом прийняття певних дій.

Перевага моделювання інформаційних ризиків полягає в тому, що ми отримуємо розуміння реальних атак, чітко визначаємо зв’язок компонентів системи, отримуємо сценарії та ймовірності використання вразливостей та отримуємо розуміння впливу на систему проведення атаки. На сьогоднішній день існує багато різних методологій для моделювання інформаційних ризиків інформаційної безпеки. Основними є:

1. STRIDE
2. PASTA
3. Trike
4. VAST
5. OCTAVE

Методологія STRIDE була розроблена та введена корпорацією Microsoft в 1999 році та використовується для опису та узагальнення ризиків по їх спільним характерним признакам, наприклад: ціль атаки, спосіб проведення атаки, вразливості, що використовуються для проведення атаки тощо, на продукти компанії Micrsoft. Слово STRIDE – це абревіатура слів

Spoofing, Tampering, Repudation, Information disclosure, DoS, Elevation of Privilege.

Процес моделювання атаки і аналізу загроз (PASTA) є відносно новою методологією моделювання загроз і являє собою семирівневу, орієнтовану на ризик методологію. Він забезпечує семи-етапний процес узгодження бізнесцілей і технічних вимог з урахуванням аналізу впливу бізнесу і вимог. Мета 17 методу - забезпечити динамічну ідентифікацію загрози, підрахунок і процес підрахунку очок. Як тільки модель загрози буде завершена, експерти з питань безпеки розроблять детальний аналіз виявлених загроз. Ця методологія призначена для забезпечення орієнтованого погляду, з боку зловмисника, на систему і її інфраструктуру, з яких експерти з безпеки можуть розробити певну стратегію дії.

Ідея методології Trike у використанні моделі загроз як інструменту управління ризиками. Тут моделі загроз використовуються для забезпечення аудиту безпеки. Моделі загроз засновані на «моделі вимог». Модель вимог встановлює визначений зацікавленими сторонами «прийнятний» рівень ризику, присвоєний кожному класу активів. Аналіз моделі вимог дає модель загрози, з якою перераховуються загрози, і присвоюються значення ризику. Завершена модель загрози використовується для побудови моделі ризику, заснованої на активах, ролях, діях і розрахованої схильності до ризику.

VAST – це абревіатура від слів Visual, Agile і Simple Threat modeling. Основним принципом цієї методології є необхідність масштабування процесу моделювання загроз по всій інфраструктурі і її інтеграція в методологію розробки Agile. Методологія спрямована на забезпечення дієвих результатів для особливих потреб різних зацікавлених сторін: архітекторів застосунків і розробників, співробітників сфери захисту інформації і керівників вищої ланки. Методологія забезпечує схему візуалізації додатків та інфраструктури, так що створення і використання моделей загроз не вимагають спеціальних знань по предмету безпеки.

OCTAVE – це також абревіатура від слів The Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology була однією з перших, створених спеціально для моделювання загроз кібербезпеки. Розроблена в Інституті програмного забезпечення Університету Карнегі-Меллона (SEI) у співпраці з CERT, методологія моделювання загроз OCTAVE зосереджена на оцінці організаційних (нетехнічних) ризиків, які можуть виникнути в результаті порушення даних. Використовуючи цю методологію моделювання загроз, ідентифікуються інформаційні активи організації, а на наборах даних вони містять атрибути прийому, засновані на типі даних, що зберігаються. Мета полягає в тому, щоб усунути плутанину щодо масштабів моделі загрози і зменшити надмірну документацію для активів, які або погано визначені, або знаходяться поза сферою дії системи. Хоча OCTAVE-моделювання загроз забезпечує надійне, орієнтоване на активи уявлення і організаційну обізнаність про ризики, документація може стати об'ємною. Цей метод найбільш корисний при створенні корпоративної системи захисту, орієнтованої на ризик. Цей метод дуже добре налаштовується для конкретних цілей безпеки і середовища ризику для організації.

1.4. 1 Джерела загроз інформаційної безпеки

Джерела загроз інформаційній безпеці розуміються як вихідні причини небезпечного впливу на життєво важливі інтереси підприємства.

За типом джерела загрози підрозділяються на

1. що мають соціальний характер;
2. що мають природний характер;

Загрози соціального характеру проявляються в процесі взаємодії між соціальними спільнотами (групами), а природні загрози - взаємодії соціальних груп з навколишнім природним середовищем.

Залежно від характеру прояву небезпечного впливу на об'єкти інформаційної безпеки джерела загроз можуть носити зовнішній або внутрішній характер.

До зовнішніх джерел загроз інформаційної безпеки відносяться діяльність розвідувальних і спеціальних служб; діяльність політичних, військових, фінансових та інших економічних структур, спрямована проти інтересів держави та підприємств, злочинні дії окремих груп, формувань та фізичних осіб.

До внутрішніх джерел загроз інформаційної безпеки відносяться загрози всередині підприємства (недостатня компетентність персоналу, недоброчесність, тощо).

1.4.2 Загрози інформаційній безпеці

Загроза інформаційної безпеки — сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки. Під загрозою (в загальному) розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам.

Загрози інформаційній безпеці можна умовно розділити на 4 групи:

- Підрив конфіденційності та розкриття комерційної таємниці- перехоплення пересланих даних, стороннє вторгнення в систему зі скачуванням конфіденційних файлів;
- Хакерство-це зміна маршруту або створення “лівих” транзакцій, стирання або переадресація масивів даних, злом захисту інформації підприємства з метою дестабілізації роботи або нанесення фінансового збитку;
- Обмеження або блокування санкціонованого доступу в ході якого користувачі не можуть увійти в систему, використовувати окремі

ресурси або сервіси, створювати й пересилати документи і т. д. тобто паралізуються всі робочі процеси;

- Внутрішнє шкідництво- передача персоналом секретних відомостей стороннім особам за допомогою електронних мереж, зараження вірусами, організація “витоків” і надання доступу третім особам.

РОЗДІЛ 2. СИСТЕМА ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1 Поняття та аналіз основних систем прийняття рішень

Очевидно, що розвиток та постійне розширення сфери впливу інформаційних технологій покращує та полегшує ведення бізнесу. Однак, чим більше джерел даних з'являється в корпоративних IT-системах, тим складніше стають завдання адміністраторів інформаційної безпеки, які не встигають «вручну» відстежувати і блокувати загрози. Без своєчасного моніторингу та запобігання несанкціонованих дій втрачається сенс системи захисту інформації. І тут на допомогу фахівцям з інформаційної безпеки приходять рішення класу SIEM - Security Information and Event Management.

Сучасні кіберзлочинці не атакують безпосередньо IT-інфрастуктуру. Вони діють завуальовано, використовуючи вразливості захисних ресурсів. Такі інциденти залишаються поза увагою, так як без «контексту» не вказують на загрозу. Відстежити протиправні дії допомагає постійний моніторинг і аналіз всіх подій, що відбуваються в IT-інфраструктурі компанії. Таку здатність аналізувати і виявляти інциденти по окремим подіям мають SIEM-рішення.

Керування захистом інформації (SIEM) – це тип рішення, що допомагає організаціям виявляти, аналізувати й усувати кіберзагрози, перш ніж вони зможуть нашкодити бізнес-процесам.

SIEM поєднує інструменти для керування інформаційною безпекою, а також засоби для керування подіями безпеки в одне рішення. Воно допомагає краще керувати системою безпеки. Технологія SIEM збирає дані журналу подій із низки джерел, визначає нетипові дії за допомогою аналізу в реальному часі й уживає відповідних заходів.Якщо коротко: SIEM покращує видимість подій у всій корпоративній мережі, що дає організаціям змогу швидко реагувати на потенційні кібератаки й дотримуватися вимог.

За останнє десятиліття технологія SIEM розвивалася, щоб забезпечувати швидше й ефективніше виявлення загроз і реагування на них за допомогою штучного інтелекту.

Системи SIEM відрізняються за своїми можливостями, але зазвичай усі вони пропонують наведені нижче основні функції.

• Керування журналами. Системи SIEM збирають великий обсяг даних в одному місці, упорядковують їх, а потім визначають, чи є ознаки загрози, атаки або порушення безпеки.

• Кореляція подій. Потім дані сортуються для визначення зв'язків і закономірностей між ними, що дає змогу швидко виявляти потенційні загрози й реагувати на них.

• Моніторинг інцидентів і реагування на них. Технологія SIEM відстежує інциденти безпеки в корпоративній мережі, а також створює оповіщення й перевіряє всі дії, пов'язані з інцидентом. Процес роботи SIEM-системи наведено на схемі 2.1.

Схема 2.1.- Процес роботи SIEM-системи

Системи SIEM допомагають зменшувати ризики для кібербезпеки за допомогою низки сценаріїв використання, які активуються під час виявлення підозрілих дій користувачів, моніторингу поведінки користувачів, обмеження спроб доступу й створення звітів про відповідність.

Інструменти SIEM мають багато переваг, які можуть допомогти посилити захищеність організації, зокрема:

• централізоване подання потенційних загроз;

• виявлення загроз у реальному часі й реагування на них;

• розширений аналіз кіберзагроз;

• моніторинг відповідності вимогам і створення звітів;

• ефективніше відстеження дій користувачів, програм і пристроїв.

SIEM став основним компонентом безпеки сучасних організацій. Основна причина полягає в тому, що кожен користувач або трекер залишає за собою віртуальний слід у даних журналу мережі. Системи SIEM розроблені для використання цих даних журналу, щоб генерувати уявлення про минулі атаки та події. Система SIEM не тільки визначає, що стався напад, але дозволяє вам побачити, як і чому це сталося. По мірі того, як організації оновлюють і покращують масштабність все складніших IT-інфраструктур, SIEM набуває ще більшого значення в останні роки. Всупереч поширеній думці антивірусних пакетів недостатньо для захисту мережі в цілому. Нульові атаки все ще можуть проникнути в захисні сили системи навіть при застосуванні цих заходів безпеки. SIEM вирішує цю проблему, виявляючи активність атаки та оцінюючи її щодо попередньої поведінки в мережі. Система SIEM має можливість розрізняти законне використання та зловмисну атаку. Це допомагає підвищити захист від аварій у системі та уникнути пошкоджень систем та віртуальної власності. Використання SIEM також допомагає компаніям дотримуватися різноманітних галузевих правил управління кібер. Управління журналом – це стандартний галузевий метод аудиторської діяльності в IT-мережі. Системи SIEM забезпечують найкращий спосіб задоволення цієї нормативної вимоги та забезпечують прозорість журналів, щоб генерувати чітку інформацію та вдосконалення.

2.2.Аналіз інструментальних методів визначення ризиків інформаційної безпеки

Як показує огляд інформаційних джерел, у галузі оцінки та управління інформаційними ризиками в ІТС на даний момент переважають інструментальні засоби їх оцінки такі, як CRAMM, Risk Watch, NIST.

Метод CRAMM був розроблений службою безпеки Великої Британії та взятий на озброєння як державний стандарт. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, який поєднує кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій для отримання відповідних результатів економічного обґрунтування витрат організації на забезпечення інформаційної безпеки.

Метод CRAMM має базу знань по ризикам і видам їх мінімізації, засоби збору інформації, формування звітів, а також реалізує алгоритм для визначення величини ризику. Метод CRAMM пропонує всі процедури методу поділити на три послідовних етапи, які розглянуто на рис. 2.1. .У метод CRAMM закладено широкий набір типових рекомендацій щодо проведення контрзаходів для зменшення ризиків , але її ефективне використання можливе тільки фахівцями вищої кваліфікації.

Перевагами методу CRAMM:

− даний метод є універсальним і підходить,

як для державного, так і комерційного використання;

− має властивість кількісної та якісної оцінки

ризиків;

− оптимальні затрати на засоби контролю та

захисту інформації;

− оперативність в прийнятті рішення з питань управління безпекою;

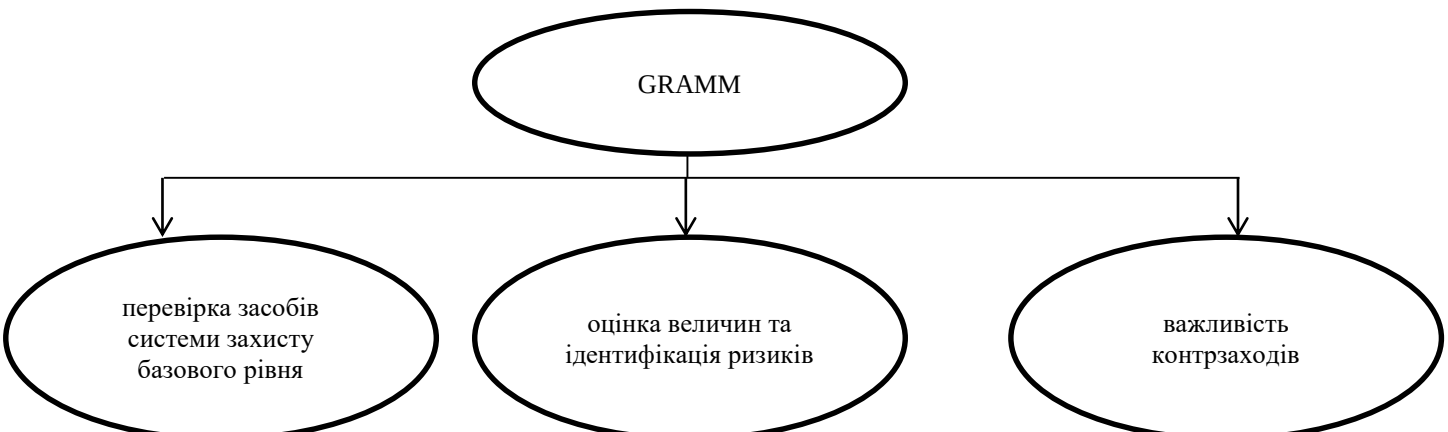


Рис. 2.1. Етапи проведення аналізу ризиків ІБ методом CRAMM

До недоліків CRAMM можна віднести:

− використання даного методу вимагає спеціальної підготовки користувача;

− потребує велику кількість годин безперервної роботи з аналізу інформації;

− відсутня можливість внесення додатків у базу даних та знань;

− програмне забезпечення CRAMM існує тільки на англійській мові ;

− дане програмне забезпечення є платним —вартість від $ 2000 до $ 5000.

Наступним програмним забезпеченням є експертна система Risk Watch яка презентує себе як потужний засіб аналізу та управління ризиками. RiskWatch являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів. Система Risk Watch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту ІБ в ІТС. Даний метод забезпечує проведення аналізу ризиків ІБ та включає чотири етапи роботи, які представлено на рис. 2.2.

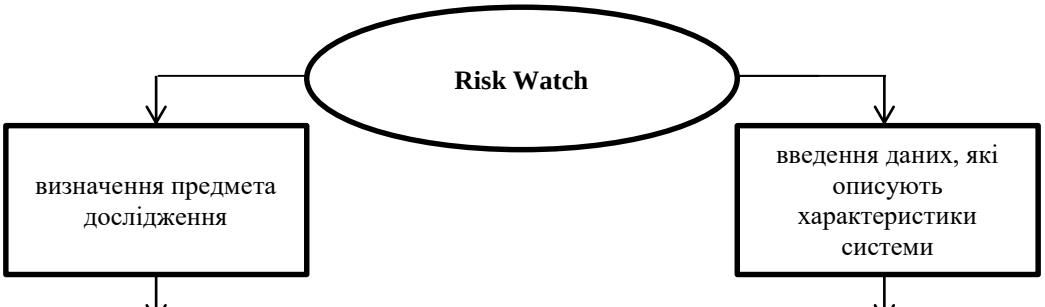


Рис. 2.2. Етапи проведення аналізу ризиків ІБ методом Risk Watch

У результаті аналізу експертної системи Risk Watch можна дійти висновку, що трудомісткість робіт з аналізу ризиків цим методом порівняно невелика. З точки зору вітчизняного споживача порівняльною характеристикою Risk Watch є його простота, мала трудомісткість перекладу інтерфейсу і велика гнучкість, що забезпечує можливість створення своїх нових профілів захищеності та є основною перевагою даного методу.

До недоліків Risk Watch можна віднести:

− метод ефективний лише при проведенні
аналізу ризиків на програмно-технічному рівні
захисту без урахування організаційних і адміністративних чинників;

− дане програмне забезпечення англомовне;

− висока вартість ліцензії — $ 15000;

Метод NIST (National Institute of Standards and Technology) є методом оцінки ризиків Національного інституту стандартів і технологій США. Цей метод передбачає попереднє оцінювання двох параметрів: потенційного збитку і ймовірності можливого інциденту. Такий механізм отримання оцінки ризику значно обмежує точність результатів, забезпечуючи при цьому оперативність та відтворюваність. Запропонований процес управління ризиками ІБ представлено на рис. 2.3.

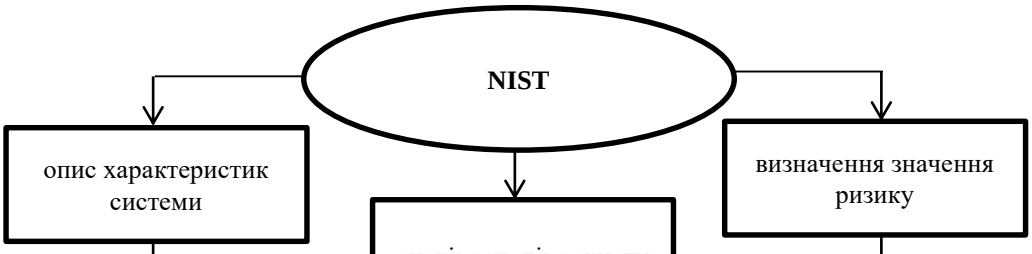


Рис. 8. Поетапний порядок роботи методу NIST

2.3 Огляд існуючих підходів до моделювання оцінювання ризиків інформаційної безпеки

Строгої класифікації для методів аналізу ризиків не існує, однак існують відмінності в підходах до аналізу ризиків, способах подання елементів ризику, функціональних можливостях та ін. На основі таких відмінностей можна виділити три основні групи – графічні, математичні та лінгвістичні методи.

Графічні методи – методи, які передбачають візуалізацію об'єктів аналізу і процесів взаємодії між ними. При цьому будуються графи, дерева або діаграми, що дозволяють різним способом відображати інформацію про досліджувані об'єкти. У більшості випадків ці методи дозволяють здійснити лише ідентифікацію елементів ризику і способи взаємодії між ними.

Математичні методи – методи, які передбачають визначення властивостей об'єктів і їх взаємодії за допомогою деяких формальних мов опису, що визначають закони функціонування, зміни властивостей і ін.

Дані методи дозволяють не тільки ідентифікувати елементи, але і аналізувати їх поведінку, зміну їх властивостей і вплив на інші елементи.

Лінгвістичні методи є найбільш популярними і простими у використанні, проте не завжди здатні привести до адекватної оцінки ситуації. Дані методи не передбачають будь-яких інструментальних засобів і програм, і вимагають лише наявності команди осіб, відповідальних за аналіз ризику. При цьому всі етапи оцінки ризику, на скільки це можливо, припускають тільки усне спілкування між групою осіб, в ході якого ідентифікуються елементи ризику, будуються припущення про їх поведінку і здійснюється приблизна оцінка можливостей і збитків.

2.4 Програмне забезпечення для моделювання інформаційних ризиків

Часто для виконання моделювання інформаційних ризиків використовують програмне забезпечення спрямоване на створення моделі системи та визначення вразливих місць. Найрозповсюдженішими такими програмами є:

• Microsoft threat modeling tool – безкоштовна програма що була створена корпорацією Microsoft для методології STRIDE, дозволяє створити діаграму потоків в системі та генерує детальний звіт в форматі html про всі можливі вразливості вашої системи.

• Mozilla threat modeling tool – безкоштовний онлайн застосунок від компанії Mozilla для моделювання інформаційних ризиків

• OWASP Threat Dragon - вільне, відкрите програмне забезпечення для онлайн-моделювання загроз, що включає системні діаграми та механізм автоматичного генерування загроз.

• MyAppSecurity - пропонує перший комерційно доступний засіб для моделювання загроз - ThreatModeler . Він використовує методологію

VAST, на основі PFD і ідентифікує загрози на основі настоюваної всебічної бібліотеки загроз. Він призначений для спільного використання для всіх зацікавлених сторін організації.

• IriusRisk - пропонує як домашню, так і комерційну версію застосунку. Цей застосунок зосереджується на створенні та підтримці живої моделі загроз. Він керує процесом, використовуючи повністю настроювані анкети та бібліотеки шаблонів ризиків і з'єднує інші різні інструменти (OWASP ZAP, BDD-Security, Threadfix) для розширення можливостей автоматизації процесу моделювання ризиків.

• securiCAD - є інструментом моделювання загроз і управління ризиками скандинавської компанії foreseeti. Призначений для управління кібербезпекою компанії, від CISO, для інженерів з безпеки та технічного персоналу. securiCAD проводить автоматизовані симуляції атаки для поточних і майбутніх інформаційних архітектур, визначає та кількісно оцінює ризики, які цілісно включають структурні уразливості, і надає підтримку прийняття рішень на основі отриманих результатів. securiCAD пропонується в комерційних і домашніх виданнях.

• SD Elements by Security Compass - це платформа управління вимогами безпеки програмного забезпечення, яка включає автоматизовані можливості моделювання загроз. Набір загроз створюється шляхом заповнення короткої анкети про технічні деталі та драйвери програми. Контрзаходи зображені у вигляді завдань для розробників, які потрібно виконати для побудови захисту.

РОЗДІЛ 3. РОЗРОБКА І ПЕРЕВІРКА АДЕКВАТНОСТІ МАТЕМАТИЧНОЇ МОДЕЛІ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1.Основні вимоги до моделі

В основу оцінки ризику було покладено метод факторного аналізу, який є найбільш адекватним в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників, та дозволяє поєднати якісну і кількісну складові аналізу.

Для забезпечення правдоподібності побудованої моделі і використанні її в подальшому вона повинна відповідати ряду вимог. Запропонована модель оцінювання ризику інформаційної безпеки має
відповідати таким вимогам:

– модель має бути адекватною стосовно досліджуваного процесу та давати результати, схожі з реальними;

– давати характеристику сучасного стану інформаційної безпеки підприємства;

– повинна надавати кількісну і якісну оцінку ризиків інформаційної безпеки;

– має дозволяти виділити найбільш небезпечні фактори ризику і їх ймовірність настання.

– давати можливість використання даної моделі для прийняття управлінських рішеннь щодо інформаційної безпеки.

Вхідні дані моделі, а саме експертні оцінки вимагають достатньої підготовки експертів, а саме:

– чітке визначення мети і завдань опитування;

– набір достатньо компетентних незалежних експертів в
досліджуваній області;

– вибір оптимально підходящих методів обробки оцінок експертів.

Для більш ефективного аналізу загроз інформаційній безпеці підприємства і їх обробки необхідно встановити існуючі зв'язки між

факторами уразливостей, які впливають на підсумковий рівень ризиків інформаційної безпеки.

Після розробки моделі оцінки ризиків інформаційної безпеки у працівників відділу інформаційної безпеки і керівників структурних підрозділів буде можливість з легкістю проводити моніторинг, оцінювати ризик інформаційної безпеки, як окремого підрозділу, так і всього підприємства в цілому.

Успішна розробка даної моделі дасть змогу спростити роботу усім вищевказаним працівникам, щоб надалі здійснювати свою діяльність більш точніше, приділяти більше уваги тим ризикам, які більше сприяють виникненню ризикових ситуацій та швидше попереджати, реагувати на їх виникнення.

3.2.Розробка моделі оцінювання ризиків інформаційної безпеки

Існують ситуації, коли із різних причин, значною мірою в зв'язку з відсутністю достовірної інформації, використання статистичних чи розрахунково-аналітичних методів не надається можливим. У таких випадках широко застосовуються методи, що використовують результати досвіду й інтуїцію, тобто евристичні чи методи експертних оцінок. Особливістю даного методу є відсутність строгих математичних доказів оптимальності рішень. Загальною спрямованістю цього методу є використання людини як "вимірювального" приладу для одержання кількісних оцінок процесів і суджень, що через неповноту і невірогідність наявної інформації не піддаються безпосередньому виміру.

Загальна схема експертних опитувань включає наступні основні етапи:

1) підбір експертів і формування експертних груп;

2) формування питань і складання анкет;

3) робота з експертами;

4) формування правил визначення сумарних оцінок на основі оцінок окремих експертів;

6) аналіз і обробка експертних оцінок.

У практичній діяльності застосовуються як індивідуальні, так і групові (колективні) експертні оцінки.

Цілі індивідуальних експертних оцінок:

1) прогнозування ходу розвитку подій і явищ у майбутньому, а також оцінка їх у сьогоденні;
2) аналіз і узагальнення результатів, представлених іншими експертами;
3) складання сценаріїв дій;
4) видача висновків іншим фахівцям і організаціям (рецензії, відзиви, експертизи тощо).

Позитивною особливістю індивідуальної експертизи є оперативність одержання інформації для ухвалення рішення і відносно невеликі витрати. Як недолік варто виділити високий рівень суб'єктивності і, як наслідок, відсутність впевненості у ймовірності отриманих оцінок. Зазначений недолік покликаний усунути чи послабити групові експертні оцінки.

Для проведення анкетного опитування був складений анонімний оцінювальний лист та шкала оцінки. При цьому обов'язково окрім самого ризику або ймовірності появи ризикової ситуації, передбачається оцінка ваги впливу кожного фактору на показники ризику.

При дослідженні складних систем часто немає можливості безпосередньо вимірювати величини, що визначають їх властивості (фактори). Більше того, нерідко є невідомими кількість та зміст цих факторів. Але можуть вимірюватися інші величини, що залежать від них. Якщо невідомий фактор впливає на декілька вимірюваних ознак, останні виявляють певний зв’язок між собою. Тому загальна кількість факторів може бути значно меншою, ніж кількість вимірюваних ознак. Для виявлення таких факторів використовують факторний аналіз. Зменшення кількості факторів може бути необхідним також для забезпечення збіжності алгоритмів подальшого аналізу даних, скорочення ресурсів пам’яті ЕОМ та часу, потрібних для їх обробки, бажанням візуалізувати отримані результати тощо.

В основу оцінки ризику було покладено метод факторного аналізу, який є найбільш адекватним в умовах невизначеності, конфліктності та нечіткої оцінки впливу окремих чинників, та дозволяє поєднати якісну і кількісну складові аналізу.

Запропонований факторний підхід є універсальним і може бути використаний для оцінювання ризику на різних стадіях розвитку підприємства та етапах вибору й обґрунтування напрямів мінімізації ризиків інформаційної безпеки.

Обов’язковими умовами факторного аналізу є такі:

– всі досліджувані ознаки мають бути кількісними;

– кількість ознак має бути принаймні вдвічі більшою, ніж кількість змінних;

– вибірка має бути однорідною.

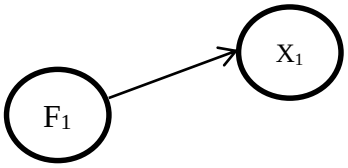
Нехай на підприємстві, для оцінки інформаційної безпеки виділено *N* експертів. Кожен з яких проставляє значення *K* ризикам, і на виході отримуємо значення випадкових багатовимірних нормально розподілених величин:

$$X_t = (X_{1t} , X_{2t}, ..., X_{kt}),$$

де $t = 1,2,\ldots,N$.

Значення випадкових багатовимірних величин обумовлені якимись об'єктивними причинами, які будемо називати факторами. Передбачається, що число цих факторів завжди менше, ніж число K вимірюваних ризиків інформаційної безпеки. Ці чинники є прихованими, їх не можна безпосередньо виміряти і тому вони представляються гіпотетичними.

Однак є методи їх виявлення, які і складають сутність факторного аналізу. Нехай в інформаційній безпеці ми виділили чотири ризики, які обумовлені дією двох чинників (факторів) F_1 і F_2. Фактор F_1 пояснює вплив всіх ризиків на інформаційну безпеку, в свою чергу F_2 описує вплив лише X_2 і X_3.



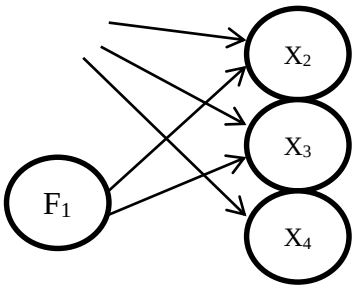


Рисунок 3.1.-Взаэмозв'язок факторів і ризиків інформаційної безпеки

Отже, значення ризиків X_1 і X_4 визначаються тільки фактором F_1, а ризики X_2 і X_3 визначаються сукупною дією факторів F_1 і F_2. Але все це, поки що нам не відомо, і перед нами стоїть завдання оцінити інтенсивність впливу факторів F_1 і F_2 на ризики X_i і виділити в X_i ті частини, які обумовлені дією кожного з факторів F_1 і F_2 окремо.
Для вирішення цього завдання припускають, що X_i лінійно залежить від F_m, (m=1,2). Для нашого випадку маємо:

$$X_i = a_{i1} \cdot F_1 + a_{i2} \cdot F_2$$

де $i = 1,2,3,4,5$;

a_{i1}, a_{i2} – факторні навантаження

З даної гіпотези, можемо отримати дві моделі факторного аналізу:
1) метод головних компонент (МГК), в якому значення оцінки кожного з ризиків представляються у вигляді лінійних комбінацій факторних навантажень a_{ij} і факторів Z_j, де $j = 1,2,\ldots,m$.

$$R_F = \sum_{j=1}^{m} a_{ij} Z_j ,$$

де m – число факторів.
2) модель власне факторного аналізу (ФА), коли спостережувані ризики визначаються не тільки факторами, але і дією локальних випадкових причин.

$$R_F = \sum_{j=1}^{m} a_{ij} Z_j + e_1$$

У факторному аналізі вихідні значення ознак вибіркової сукупності

центруються і нормуються за допомогою перетворення:

$$Z_i = \frac{X_1 - \overline{X}_i}{\sigma_i}$$

де $\overline{X_1}$ – середнє значення і-ї змінної;

σ_i – середньоквадратичне відхилення і-ї змінної.

На основі обчислених головних компонент можна побудувати більш просту і разом з тим найбільш інформативну систему опису ризиків, оцінити силу причинно-наслідкового зв'язку між факторами і виділеними головними компонентами, досліджувати можливості зміни аналізованих чинників під впливом головних компонент.

Крім того, результати групування по головних компонентах можна використовувати для проведення порівняльного аналізу факторів, за рахунок яких підприємство домоглося найкращих результатів у збільшенні безпеки. Це дозволяє виявити прогресивні тенденції підвищення ефективності використання виробничих ресурсів.

Метод головних компонент виявляє k-компоненти - фактори, що пояснюють всю дисперсію і кореляції вихідних k випадкових величин; при цьому компоненти будуються в порядку спадання частки сумарної дисперсії вихідних величин, які пояснюються ними, що дозволяє часто обмежитися декількома першими компонентами.

Перша головна компонента F_1 визначає такий напрямок в просторі вихідних ознак, за яким сукупність об'єктів (точок) має найбільший розкид (дисперсію).

Друга головна компонента F_2 будується з таким розрахунком, щоб її напрямок був ортогональний напрямку F_1 і вона пояснювала якомога більшу частину залишкової дисперсії і так до k-ї головної компоненти F_k. Так як виділення головних компонент відбувається в порядку спадання з точки зору частки, дисперсії, що пояснюється ними, то ознаки, що входять в першу

головну компоненту з великими коефіцієнтами, надають максимальний вплив на диференціацію досліджуваних об'єктів.

Таке перетворення дозволяє знижувати інформацію шляхом відкидання координат, відповідних напрямках з мінімальною дисперсією. У факторному аналізі використовують також інші міри інформативності, що дають змогу визначити кількість істотних факторів. Критерій Кайзера, або критерій власних чисел, запропонований американським психологом Генрі Феліксом Кайзером, передбачає, що до моделі включають тільки фактори, для яких власні числа є не меншими, ніж одиниця. За змістом це означає, що таким факторам відповідає дисперсія, еквівалента принаймні дисперсії одної змінної. У протилежному випадку виокремлення фактору не має сенсу. Цей критерій іноді залишає в моделі занадто багато факторів.

Критерій кам’янистого осипу (критерій відсіювання) передбачає побудову графіка, де по осі абсцис відкладають порядковий номер власного числа, а по осі ординат – його значення.

Згідно з Р. Кеттелом необхідно знайти точку найбільшого уповільнення спадання власних значень і враховувати лише фактори, яким відповідають власні числа, розташовані лівіше цієї точки.

На відміну від попереднього цей критерій статистично необґрунтований і часто залишає в моделі не всі істотні фактори. Втім у випадках, коли істотних факторів небагато, а кількість змінних є великою, обидва критерії є придатними для практичного застосування. На практиці часто здійснюють розрахунки, використовуючи різні критерії, а потім обирають модель, що містить найбільшу кількість факторів, яким можна надати змістову інтерпретацію.

Усі загальні фактори, кількість яких дорівнює кількості параметрів, пояснюють 100% дисперсії. Якщо сума відсотків за факторами перевищує 100%, це свідчить про отримання від’ємних власних значень і, відповідно, комплексних власних векторів, що може бути наслідком некоректної редукції вихідної кореляційної матриці. Доцільно здійснювати двоетапну процедуру

аналізу. На першому етапі максимальну кількість факторів не задають. Після його проведення аналізують дисперсії, оцінюють приблизну кількість факторів і проводять повторний аналіз.

Схема опису моделі методу головних компонент визначальних факторів оцінки ризиків інформаційної безпеки представлена на рис. 2.4:

Рисунок 3.2 – Схема опису моделі методу головних компонент визначальних факторів

Оцінка ризику є досить спрощеним відображенням реальності. Показник свідчить про те, що, незважаючи на вжиття всіх попереджувальних заходів, рівень небезпеки для підприємств залишається суттєвим. Проте його розрахунки дають можливість побудувати єдину шкалу, де в ранжируваному порядку розміщуються всі ризики. Конкретне значення R_a в цьому випадку не є визначальним, а важливим є лише місце, що займає кожний ризик.

3.3.Програмна реалізація розробленої математичної моделі

Сутність факторного аналізу полягає в переході від опису деякої множини досліджуваних об’єктів заданої великим набором вимірюваних ознак до їх опису меншим число, що відображає найбільш істотні властивості явища. Для реалізації використано пакет аналізу даних
STATISTICA.

Пакет STATISTICA розроблений фірмою StatSoft (США) як самостійний продукт у 1991 р. Пакет може працювати у сполученні з іншими Windows-додатками. В останні версії включена також мова програмування Statistica-BASIC, що дозволяє розширювати можливості пакета відповідно до потреб користувача. STATISTICA дозволяє проводити вичерпний, всебічний аналіз даних, представляти результати аналізу у вигляді таблиць і графіків,
автоматично створювати звіти. За допомогою зручної системи підказок можна навчатися не тільки роботі з пакетом, але й сучасним методам статистичного аналізу. Дані в системі STATISTICA організовані у вигляді електронних таблиць, як у програмі Excel. У пакеті STATISTICA всі операції,
включаючи копіювання, перетягування й автоматичне заповнення комірок, виконуються так само, як і в електронних таблицях. Загальне число змінних у стандартному файлі STATISTICA може бути до 4092, кількість спостережень обмежена лише обсягом диску.

Програма STATISTICA містить вичерпний набір аналітичних процедур в галузі вивчення бізнесу, здобуття даних, науки і промислового виробництва. Вона дозволяє будувати різні графіки, ефективно керувати даними і розробляти власні програми. STATISTICA не тільки включає в себе

універсальні статистичні, графічні процедури та засоби керування даними, але також реалізує спеціалізовані методи аналізу даних. Всі аналітичні інструменти STATISTICA доступні як окремі компоненти єдиного інтегрованого пакета. Для проведення факторного аналізу початкових заданих даних, скористаємося пунктом меню Аналіз / Багаторівневий розвідувальний аналіз/ Факторний аналіз.

На вкладці швидких опцій потрібно вказати змінні. Натискуємо на кнопку «Змінні» і вибираємо за умовою всі 9 факторних ознак для дослідження. Головною метою аналізу чинників є редукція даних та класифікація змінних. А також – виявлення загальних для факторних ознак латентних (прихованих) чинників, впливом яких обумовлені варіації та коваріації ознак ризиків. Діалогове вікно початкового задання змінних буде мати вигляд (рис. 3.1).

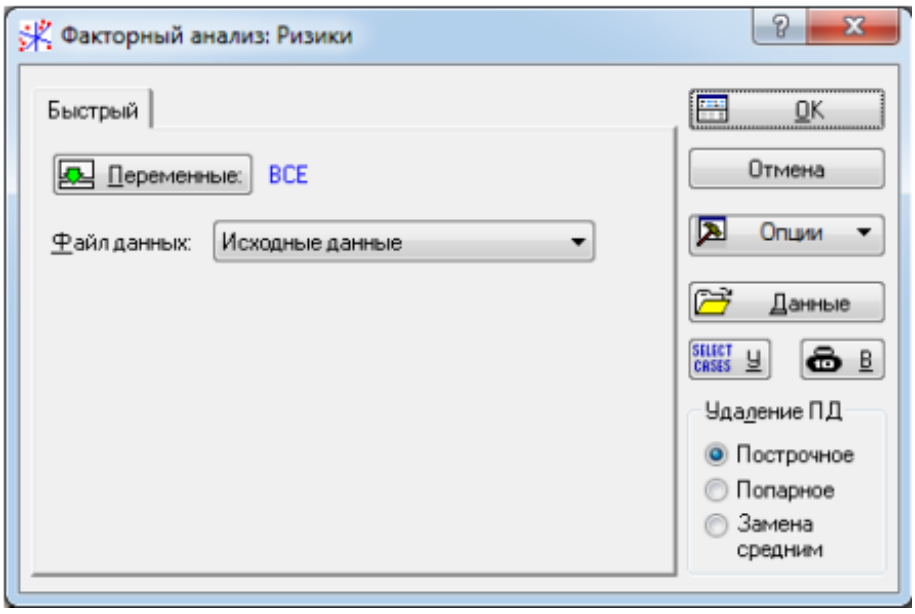


Рисунок 3.1 – Діалогове вікно вибору змінних для проведення факторного аналізу

Після натиснення на кнопку «ОК» програма переходить до вікна визначення методу виділення факторів. Вкладка «Додатково» дозволяє встановити максимальну кількість нових чинників у моделі та метод обчислення таких чинників. Вкладка описових статистик дозволяє переглянути кореляції, дисперсію та стандартне відхилення для ризиків, а

також побудувати регресійну модель між даними ознаками. Можна натиснути на кнопку перегляду основних статистик і перейти до діалогового вікна, де обираємо кнопку «Кореляції».

3.4.Досвід впровадження системи управління інформаційною безпекою

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

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

Ще одна актуальна проблема в області захисту даних - це безперервність функціонування інформаційних систем. Для багатьох сучасних компаній, в першу чергу, фінансові інститути, виробничі холдинги, великі

дистриб'ютори, безперебійна робота інформаційних систем, що підтримують основний бізнес, і доступність даних стають критичною проблемою. Збої в роботі систем призводять до переривання бізнес-процесів і, як наслідок, до незадоволеності клієнтів, штрафів та інших збитків. А в забезпеченні доступності даних важливу роль відіграють системи захисту, що запобігають зловмисні атаки на інформаційну систему (атаки типу «відмова в обслуговуванні» і ін.).

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

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

Таким чином, при побудові (модернізації) системи ІБ доцільно реалізовувати цикл робіт (рис. 3.2), що включає обов'язковий етап діагностичного обстеження з оцінкою вразливостей інформаційної системи і загроз, на основі якого проводиться проектування системи і її впровадження. За великим рахунком, для управління будь-якої складної системою необхідно створити жорсткий, але простий регламент обслуговування системи і

забезпечити контроль за тим, щоб настройки системи змінювалися відповідно до цього регламенту.

Рис.3.2. Повний цикл робіт для забезпечення інформаційної безпеки

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

Стосовно до забезпечення безпеки інформаційної системи (ІС) це можна представити таким чином. Мати в наявності документ, в якому повинно бути чітко описано, хто і на якій підставі повинен мати доступ до ресурсів інформаційної системи.Обстеження

•Аудит (комплексне діагностичне обстеження системи ІБ) •Опис існуючих ІТ ресурсів / сервісів / бізнес процесів •Аналіз загроз та вразливостей системи ІБ. Технічний аналіз (тести напронекнення) •Аналіз ризиків Проектування •Розробка концепції системи ІБ та управління •Розробка моделі системи ІБ (Дизайн / Архітектура) •Технічне проектування. Розробка документації. Економічне оновлення системи ІБ •Тестування Впровадження •Впровадження - поставка, інсталяція, настроювання технічних компонентів системи ІБ, навчання користувачів, введення в експлуатацію •Допомога в підготовці до сертифікації Супровід та обслуговування •Аутсорсинг. допомога в розслідуванні інцидентів, управління безперервністю ведення бізнесу.

Мати єдину точку взаємодії співробітників організації з інформаційною системою, через яку вони зможуть формулювати свої побажання на надання доступу до тих чи інших ресурсів ІС. Мати інструменти контролю правильності налаштувань ІС. Розробками такого роду останнім часом займається кілька великих корпорацій. Свої рішення пропонують Oracle і IBM. Особливість пропонованих рішень в тому, що в них з'єднуються не працюють окремо технічний і організаційний підходи до управління безпекою. При впровадженні таких систем передбачається, що організація вже має сформульовану політику безпеки. Ця політика разом з інформацією про ІС служить надалі фундаментом системи управління. Для опису інформаційної системи зазвичай необхідно знати наступне. Перелік інформаційних ресурсів. Під ресурсом можуть розумітися конкретні сервери і папки на них, експлуатовані додатки, обладнання та навіть сегменти мережі. Відповідальний за безпеку цих ресурсів. Це можуть бути власники ресурсів, голови підрозділів, куратори з боку служби безпеки та інші. Відповідальний за адміністрування цих ресурсів. Як ресурси інформаційної системи взаємопов'язані між собою. Часом для нормальної роботи програми необхідний комплекс налаштувань - від налаштувань

самого додатка до комутаційного обладнання. Адже навіть якщо ми виконаємо всі настройки, але забудемось прописати дозволяє правило на внутрішньому міжмережевому екрані, рішення всієї задачі буде зірвано.

Штатна структура компанії. Який доступ і до яких ресурсів має співробітник, що займає на певну посаду. На базі отриманої інформації система управління вибудовує ідеальну модель ІС. Цей момент можна вважати стартовим в роботі системи управління безпекою. Відтепер усі спілкування з питань змін у налаштуваннях інформаційної системи починає відбуватися через спеціалізовану систему документообігу, що входить до складу системи управління безпекою.

Заявка на зміну доступу, складена в системі управління безпекою, буде перевірена на несуперечливість вимогам політики безпеки, узгоджена з власниками ресурсів і спрямована на виконання адміністраторам. Виявляти невідповідність моделі ІС і її поточного стану системи управління безпекою дозволяють агенти-сенсори. Такі агенти регулярно стежать за всіма пов'язаними з безпекою ІС настройками операційних систем, додатків, засобів захисту, мережевого обладнання. Під невідповідністю системи управління безпекою ІС підприємства слід розуміти або невиконані адміністратором необхідних дій по адмініструванню інформаційної системи, які дії, вчинені ним в обхід прийнятого і затвердженого в організації порядку.

Наприклад, надання зайвих повноважень якого-небудь користувачеві або неправомірне обмеження користувача в правах. Інформація про невідповідності тут же надходить в служби безпеки і в службу ІТ. Адже кожне з них пов'язане з тим, що хтось із співробітників або набуває права на доступ до ресурсів ІС, або втрачає їх. Це означає, що він може отримати зайву інформацію або позбутися доступу до необхідних йому відомостей. А це, як ми вже відзначали, рівнозначно неприпустимо, оскільки таїть загрозу безпеці або ж призводить до зриву виконання бізнес-завдань. Наявність в системі документообігу механізму архівування заявок на зміни доступу до

інформаційної системи дозволить в будь-який момент зрозуміти, хто має доступ до ресурсів інформаційної системи і хто запитував надання цього доступу.

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

Крім того, після впровадження такої системи управління забезпечення безпеки інформації перестає бути спадщиною, відповідальністю та обов'язком лише вузьких спеціалістів. В управлінні інформаційною системою керівництво організації починає реально активно брати участь: зрештою, саме вони формулюють вимоги до налаштувань через механізм додатків. Як приклад однією з головною задач діючої СУІБ є захист від витоку інформації на підприємстві. Витік інформації є серйозною проблемою та реальною загрозою для більшості підприємств, що представляють різні галузі. Дані можуть бути втрачені через зловмисні наміри третіх осіб, через халатність працівників. При цілеспрямованій організації наносяться серйозні збитки. У конкурентному середовищі ця методика використовується багатьма сторонніми організаціями для отримання переваги над конкурентами, хоча і в такий незаконний спосіб.

Щоб усунути несприятливі наслідки втрати даних, потрібно використовувати системи захисту інформаційних активів. Їх створення повинно бути на високому професійному рівні, використовуючи сучасне обладнання та програмне забезпечення. Найкращим рішенням для боротьби з витоком інформації та відстеження робочого часу буде програма контролю NeoSpy. Це професійна програма-шпигунське програмне забезпечення,

розроблена спеціально для відстеження вашого комп'ютера. Якщо говорити про законність спостереження за працівниками, то варто зазначити, що метою використання представленого програмного продукту є захист даних компанії (внутрішня програма обслуговування). Програма не використовується для вторгнення в конфіденційність, хакерські атаки. Цей продукт підходить для:

• підприємств;

• державних компаній;

• комерційних структур.

Чи законно використовувати програму стеження за співробітниками?

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

• за розголошення інформації підприємства, яка є комерційною таємницею, передбачено покарання. Це кваліфікується як посадовий злочин;

• заборона на застосування в робочий час сторонніх засобів зв'язку в особистих цілях: електронної пошти, телефону, факсиміле;

• майбутній співробітник підприємства дає згоду виконувати вищевикладені вимоги.

Які переваги дає використання спеціальної програми контролю за співробітниками?

Представлений інструмент сьогодні використовують багато підприємств і організації. Від збереження відомостей, що становлять комерційну або іншу таємницю, залежить майбутнє будь-якої організації. Щоб воно було безхмарним, потрібно використовувати ефективні інструменти захисту. Програми моніторингу комп'ютерів в локальних мережах дозволяють

виключити найменшу ймовірність втрати інформації. Витік даних призводить до серйозних проблем у вигляді призупинення проекту і додаткових витрат. У разі звільнення працівника з вини якого були втрачені відомості, доведеться витратити час на пошук нового майстра. Якщо ж спроби злому були виявлені і припинені своєчасно, то можна виключити негативні наслідки.

Ще одна важлива перевага безперервного моніторингу – раціональне використання комп'ютерних засобів і оргтехніки. Практика багатьох організацій показує, що це дозволяє істотно скоротити витрати. Недобросовісні співробітники можуть використовувати в своїх цілях інтернет, наприклад, для спілкування з друзями в соціальних мережах. Моніторинг дозволить ефективно контролювати робочий час, що позитивно позначиться на продуктивності і ефективності праці.

3.5.Рекомендації щодо вдосконалення процесів розробки та впровадженням системи управління інформаційною безпекою

Перш ніж пропонувати будь-які технічні рішення для системи інформаційної безпеки об'єкта, необхідно розробити політику безпеки для нього. Саме політика безпеки організації описує процедуру надання та використання прав доступу користувачів, а також вимоги до звітності користувачів про їхні дії безпеки.

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

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

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

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

*Формулювання цілей безпеки об'єкта.*Детальний опис загальної мети побудови системи безпеки для об'єкта клієнта виражається набором факторів

або критерії, які визначають мету. Сукупність факторів є основою для визначення системних вимог (вибору альтернатив). Фактори безпеки можна розділити на технологічні, технічні та організаційні. Визначення вимог функціональної безпеки. Функціональні вимоги профілю безпеки визначаються добре відомими, усталеними і узгодженими функціональними вимогами безпеки. Всі вимоги до функцій безпеки можна розділити на два типи: управління доступом до інформації та управління інформаційним потоком. На цьому етапі необхідно правильно визначити компоненти функцій безпеки для об'єкта. Компонент функції безпеки описує певний набір вимог безпеки - найменший обраний набір вимог безпеки для входу в профіль безпеки. Можуть бути залежності між компонентами.

Вимоги гарантії досягнутої безпеки. Структура гарантійних вимог аналогічна структурі функціональних вимог і охоплює класи, групи, компоненти і елементи гарантій, а також рівні гарантії. Класи і групи гарантії відображають такі питання, як розробка, управління конфігурацією, робоча документація, підтримка життєвого циклу, тестування, оцінка вразливостей і багато іншого. Вимоги захисту безпеки виражаються шляхом оцінки можливостей інформаційної безпеки об'єкта. Така оцінка проводиться на рівні окремого механізму безпеки, який дозволяє визначити здатність відповідної функції безпеки протистояти ідентифікованим загрозам. Залежно від відомого потенціалу атаки сила захисної функції визначається, наприклад, категоріями «базовий», «середній»,«високий».

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

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

Загалом, ТД забезпечує:

• уточнення функцій захисту;

• вибір архітектурних принципів побудови системи інформаційної безпеки;

• розробка логічної структури системи інформаційної безпеки (чіткий опис інтерфейсів);

• з'ясування вимог функцій забезпечення безпеки системи інформаційної безпеки;

• розробка методології та програми випробувань на відповідність сформульованим вимогам.

*Оцінка досягнутої безпеки.*На цьому етапі оцінюють рівень безпеки інформаційного середовища об'єкта автоматизації на основі оцінки, при якій після реалізації рекомендованих заходів можна довіряти інформаційному середовищі об'єкта. Основи цієї методології припускають, що ступінь впевненості залежить від ефективності зусиль, зроблених до оцінки безпеки.

Збільшення цього зусилля означає:

• значна кількість елементів інформаційного середовища об'єкта, залучених до процесу оцінки;

• розширення типів проектів і опису деталей виконання при проектуванні системи забезпечення безпеки;

• строгість роботи, яка включає використання більшої кількості пошукових інструментів і методів для виявлення менш очевидних слабких місць або зменшення їх ймовірності.

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

інформації від навмисного спотворення (знищення), несанкціонованого доступу, копіювання або використання.

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

Інтегрована архітектура системи ІБ. До ідеології і створення комплексної архітектури системи ІБ компанія TopSBI прийшла після багатьох років роботи з великими компаніями за проектами забезпечення ІБ. Висока ефективність системи ІБ може бути досягнута, якщо все її компоненти представлені якісними рішеннями, функціонують як єдиний комплекс і мають централізоване управління. Система безпеки повинна ґрунтуватися на аналізі ризиків, а витрати на його впровадження і підтримка повинні бути адекватні існуючим загрозам, тобто економічно обґрунтовані.

Інтегрована архітектура системи ІВ включає в себе набір наступних підсистем:

• підсистема захисту периметра мережі і міжмережеві екрани (брандмауери і т. Д.);

• підсистема безпеки мережевого сервера;

• захист робочих станцій;

• підсистема моніторингу та аудиту безпеки;

• засоби виявлення атак і автоматичного реагування;

• комплексна підсистема антивірусного захисту;

• інструменти аналізу безпеки і управління політикою безпеки;

• інструменти моніторингу цілісності даних;

• засоби криптографічного захисту інформації;

• інфраструктура відкритих ключів;

• підсистема резервного копіювання та відновлення;

• автоматизована система установки оновлень програмного забезпечення;

• інструменти управління безпекою;

• підсистема автентифікації і ідентифікації.

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

Створення СУІБ дозволяє також забезпечити відстеження змін, що вносяться до системи інформаційної безпеки, відстежувати процеси виконання політики безпеки, ефективно управляти системою в критичних ситуаціях. В цілому, процес управління безпекою (Security Management) відповідає за планування, виконання, контроль і технічне обслуговування всієї інфраструктури безпеки. Організація цього процесу ускладняється тією обставиною, що забезпечення інформаційної безпеки компанії пов'язано не тільки із захистом інформаційних систем і бізнес-процесами, які підтримуються цими інформаційними системами. У компанії часто існують бізнес-процеси, не пов'язані з IT, але потрапляють в сферу забезпечення ІБ, наприклад, процеси кадрової служби по найму персоналу.

ВИСНОВКИ

У дипломній роботі було розкрито сутність оцінювання ризиків інформаційної безпеки, в результаті реалізації яких, телекомунікаційні підприємства можуть понести, як фінансовий, так і іміджевий збиток. Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає

суттєво важливі характеристики для власного існування, які завжди пов’язана з певним ризиком. Ґрунтовний аналіз наукових праць з проблем ризику дав можливість узагальнити основні положення, що визначають сутність його оцінки й окреслюють основні підходи до управління ним. У процесі дослідження виявлено неоднозначність тлумачення поняття «ризик», що зумовило необхідність формування власного бачення сутності «ризик» та його місця у системі економічних категорій. Розглянувши існуючі методи оцінювання ризиків можна побачити, що основними проблемами в їх застосуванні є:

– високі фінансові витрати на здійснення аналізу ризиків;

– необхідність залучення великої кількості експертів;

– відсутність у багатьох методів можливості проведення швидкого повторного циклу оцінки ризиків;

Недосконаліть та обмеженість методик оцінки ризику інформаційної безпеки, врахування їх переваг і недоліків обумовили доцільність використання експертних оцінок для виявлення ризиків, що мають місце на телекомунікаційних підприємствах. Для подальшої оцінки був обрний факторний аналіз, для побудови моделі методу головних компонент визначального фактору. Сформульовані ризики, які формують інформаційні ризики, які характерні для різних структурних підрозділів в телекомунікаційних підприємствах. Основою для побудови моделі було обрано дев’ять вхідних змінних, які на сьогодні є визначеними ризиками для діючого підприємства в сфері телекомунікацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Оцінка інформаційної безпеки бізнесу (Електрон. ресурс) /Спосіб доступу: URL: http://www.cfin.ru/appraisal/business/special/ infosec. shtml?printversion
2. Стаття «Інформаційна безпека і її складові». – Електронний ресурс – Режим доступу: https://egrivna.com/informacijna-bezpeka-i-ii-skladovi-2/

3. Богуш В. Інформаційна безпека держави/ В. Богуш, О. Юдін; [Гол. ред. Ю.О. Шпак]. – К.: «МК-Прес», 2005. – 432 с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.
5. Інформаційна безпека (соціально-правові аспекти) / [В. Остроухов, В. Петрик, М. Присяжнюк та ін.] ; за ред. Є.Д. Скулиша. – К. : КНТ, 2010. – 776 с.,
6. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть [Текст] / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. - 1999. - № 14 : Міжнародні відносини. - С. 46-48.
7. Маракова, І. Захист інформації [Текст] : підручник / Маракова І., Рибак А., Ямпольский Ю. - Одеса : ОдНПУ, 2001. - 164 с.
8. Стаття «Система економічної безпеки підприємства та її методологічні засади» – Електронний ресурс – Режим доступу: https://studopedia.su/8_58207_sistema-ekonomichnoi-bezpek pidpriiemstva-ta-iimetodologichni-zasadi.html
9. Про захист інформації в автоматизованих системах: Закон України // Відомості Верховної Ради. 1994.-№31.-286 с.
10. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція "Інформаційна безпека в сучасному суспільстві" (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24
11. Про Концепцію Національної програми інформатизації: [закон України: офіц. текст: за станом на 9 січня 2007р., із змінами, внесеними Законом України від 7 серпня 2011р.] // Відомості Верховної Ради України (ВВР). – 2012. – № 7. – ст. 53
12. Світлична В.Ю., Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення

http://economy.kname.edu.ua/images/files/publishing/360369_%D0%A1%D0%B2%D1%96%D1%82%D0%BB%D0%B8%D1%87%D0%BD%D0%B0_2.pdf

13. Офіційний сайт кафедри комп'ютерних систем та мереж, Чернівецький національний університет [Електронний ресурс] - Режим доступу: csn.chnu.edu.ua
14. Типи Сайтів. Landing Page [Електронний ресурс] / Режим доступу:http://znet.ru/raskrutka/vidyi-saytov-i-ih-klassifikatsiya-s primerami/#Landing_Page
15. Щербина В.М. Інформаційне забезпечення економічної безпеки підприємств та установ / В.М. Щербина // Актуальні проблеми економіки.– 2008. – № 10. – С. 220-225.
16. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»
17. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук: [Електронний ресурс].– Режим доступу: http:// journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.