УДК 004.056

АНАЛІЗ МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА БАЗІ ТЕХНОЛОГІЇ GRUNDSCHUTZ

М. О. Марісов[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Стаття присвячена проблемі розвитку інформаційної безпеки з урахуванням ризик-орієнтованого підходу для вирішення задач управління інформаційною безпекою підприємства. Сучасні тенденції розвитку підприємств ствоюють необхідність управління ризиками. Автором досліджено методи та засоби технології Grundschutz, що дають можливість реалізувати ризик-орієнтований підхід у контексті забезпечення інформаційної безпеки підприємства і провести аналіз та оцінювання інформаційних ризиків системи захисту інформації. В роботі розглянуто технологію Grundschutz, методи впровадження , моделі реалізації технології, а також проаналізовано методології, за допомогою яких здійснюється оцінювання ризиків, зокрема, методологія аналізу і управління ризиками.

Ключові слова: інформаційні технології, інформаційна безпека, загрози, вразливість, інформаційні ризики, оцінювання ризику.

Вступ

Протягом останніх років інформація стала відігравати важливу роль в усіх сферах людського життя, що пов'язано з поступовим становленням інформаційного суспільства. В умовах сьогодення для підвищення показників ефективності і працездатності складних систем застосовують сучасні інформаційні технології та системи, внаслідок чого інформація виступає універсальним товаром для взаємовідносин між різними структурами підприємства чи організації. Питання її захисту набувають великої актуальності. Особливе значення відводиться оптимальному проектуванню систем захисту, що дозволяє з найбільшою ймовірністю вибирати найкращі рішення на множині альтернатив. В наші часи це стає актуальним для більшості підприємств, оскільки правильно спроектована і впроваджена система захисту буде запорукою успішного функціонування і конкурентоспроможності всієї організації.

Зважаючи на ускладнення комп'ютерних систем і збільшення кількості загроз, виникає потреба в оцінюванні інформаційної безпеки таких систем. Оцінювання ризиків порушення інформаційної безпеки є однією з найважливіших складових процесу управління інформаційною безпекою. В результаті питання необхідності оцінювання ризиків інформаційної безпеки для побудови ефективних систем захисту інформації на підприємстві є актуальним.

Згідно зі стандартом ISO/IES 17799:2000 оцінювання ризиків інформаційної безпеки визначається як систематичний аналіз можливої шкоди, що завдається бізнесу в результаті порушень інформаційної безпеки, з урахуванням можливих наслідків від втрати конфіденційності, цілісності або доступності інформації та інших ресурсів і ймовірності настання такого порушення, враховуючи існуючі загрози, вразливості, а також впроваджені заходи захисту [1].

Метою роботи є дослідження та аналіз систем захисту інформаційних ресурсів підприємства на основі удосконалення моделей управління ризиками інформаційної безпеки на базі технології Grundschutz.

1. Потреба у створення систем захисту інформації

Інформаційні системи і технології являють собою комплекс програмно-технічних засобів і методів виробництва, передачі, обробки та споживання інформації. Метою їх впровадження є створення системи, в якій інформаційні потоки налагоджені таким чином, що користувачі з мінімальними витратами одержують доступ до необхідної інформації в той час, коли вона потрібна, і там, де вона потрібна, а базовими принципами є: релевантність, час та місце. Оскільки інформація перестала бути просто необхідним допоміжним ресурсом для виробництва, а набула відчутної вартісної ваги, яка чітко визначається реальним прибутком, що одержується при її використанні, або розмірами збитку, з різним ступенем ймовірності завданого власнику інформації в разі її спотворення або втрати, проблема забезпечення інформаційної безпеки набула в умовах сьогодення виняткового значення [2].

Якщо інформація підприємства становить державну таємницю, то процес створення систем захисту інформації (СЗІ) полягає в задоволенні нормативним

вимогам із застосуванням спеціального обладнання, програмного забезпечення та залученням спеціалізованих організацій. У комерційних організаціях, в яких наявна інформація, що становить комерційну та професійну таємниці, а також персональна інформація, процес побудови СЗІ повинен грунтуватися на аналізі ризиків.

2. Стандарти BSI

Федеральним відомством Німеччини з інформаційної безпеки (BSI) було розроблено методологію визначення та реалізації заходів комп'ютерної безпеки в організації - Базовий IT-захист (нім. IT-Grundschutz). Метою впровадження технології IT-Grundschutz є досягнення належного рівня безпеки IT-систем. Для досягнення цієї мети BSI рекомендує технічні, організаційні, кадрові та інфраструктурні заходи безпеки. Організації і федеральні агентства демонструють свій систематичний підхід до захисту своїх IT-систем (наприклад, системи управління інформаційною безпекою), отримуючи сертифікат ISO / IEC 27001 на основі IT-Grundschutz [3].

Щоб допомогти організаціям визначити і впровадити заходи для захисту IT-систем, Федеральне управління з інформаційної безпеки (BSI) створило базовий набір стандартів щодо захисту інформаційних технологій. Ці стандарти BSI включають наступне:

• BSI standart 200-1: Вимоги до систем менеджменту інформаційної безпеки. Стандарт визначає загальні вимоги до СМІБ. Він повністю сумісний з ISO 27001, а також бере до уваги рекомендації ISO 27002;

• BSI standart 200-2: Методологія IT-Grundschutz, що описує настройку і використання СМІБ. Дії і підхід до основних (базових) заходів захисту, практична реалізація стандарту 200-1. Стандарт надає практичну допомогу у вигляді численних порад, рекомендацій та прикладів;

• BSI standart 200-3: Метод аналізу ризиків на базі IT-Grundschutz.

2.1. BSI 200-1: Опис методів розробки СМІБ

Безпека повинна бути невід'ємною частиною планування, проектування та функціонування бізнес-процесів та обробки інформації. Як наслідок, повинні бути вжиті комплексні організаційні та кадрові заходи. Управління інформаційною безпекою на основі IT-Grundschutz, крім технічних аспектів, включає інфраструктурний, організаційний та кадровий аспекти. Тільки цілісний підхід щодо підвищення інформаційної безпеки може впливати на всі рівні стійким чином. Відповідний рівень безпеки в першу чергу залежить від системного підходу і лише вдруге від окремих технічних заходів. BSI standart 200-1 описує, як може бути розроблена система менеджмента інформаційною безпекою (СМІБ). Система менеджмента охоплює всі положення, що забезпечують нагляд і управління, щоб організація могла досягти своїх цілей. Отже, система менеджмента інформаційною безпекою визначає інструменти та методи управління, які організація повинна використовувати для зрозумілого управління діяльністю, спрямованою на досягнення інформаційної безпеки.

Цей стандарт визначає загальні вимоги до СМІБ. У ньому описано, які методи можуть бути використані для загального ініціювання та контролю інформаційної безпеки в організації. Стандарт BSI 200-1 повністю сумісний зі стандартом ISO / IEC 27001 і, крім того, враховує терміни, визначені стандартом ISO / IEC 27000, а також рекомендації стандарту ISO / IEC 27002. BSI надає зміст стандартів ISO, згаданих вище, у своєму власному стандарті BSI, щоб мати можливість детальніше описати деякі теми і, таким чином, забезпечити покращене представлення змісту[4].

Система управління охоплює всю політику, що стосується нагляду та управління з метою досягнення цілей організації. СМІБ визначає інструменти та методи, який рівень управління повинен використовувати для чіткого управління (планування, прийняття, впровадження, нагляду та вдосконалення) завдань та заходів, спрямованих на досягнення інформаційної безпеки. СМІБ включає такі основні компоненти: - принципи управління - ресурси - службовці - процес безпеки - політика інформаційної безпеки, в якій задокументовані цілі безпеки та стратегії їх реалізації - концепція безпеки - організація безпеки

2.2. BSI 200-2: Методи впровадження технології IT-Grundschutz

Стандарт BSI 200-2 описує, як можна створити ефективну систему управління інформаційною безпекою та як для цього завдання можна використовувати Компендіум IT-Grundschutz. Компендіум IT-Grundschutz – це збірник, что містить рекомендації щодо безпеки з найрізноманітніших тем. Детальні поради в керівних принципах впровадження модулів IT-Grundschutz, что полегшують працівникам інформаційної безпеки застосовування інформаційної безпеки у повсякденній роботі. Підходи відповідно до IT-Grundschutz в поєднанні з модулями Компендіуму IT-Grundschutz забезпечують систематичну методологію для розробки концепцій безпеки та випробуваних гарантій безпеки, які успішно використовуються в численних державних установах та компаніях.

Впровадження ефективної системи управління інформаційною безпекою складається з наступних етапів:.

1. Ініціювання процесу безпеки.

Рівень управління повинен ініціювати і контролювати процес безпеки. Для цього необхідні стратегічні керівні заяви щодо інформаційної безпеки, з одного боку, та загальні організаційні умови, з іншого. Співробітник з питань інформаційної безпеки відіграє центральну роль у цьому процесі. Основою для проектування процесу безпеки є Політика щодо інформаційної безпеки. Вона описує цілі безпеки та

який рівень безпеки організація передбачає, яка мотивація для цього та за допомогою яких гарантій та яких структур це має бути досягнуто.

2. Організація процесу безпеки.

Для управління інформаційною безпекою повинна бути створена організаційна структура, яка відповідає розміру та типу організації. Для цього необхідно визначити інтерфейси, канали зв'язку та процеси співпраці. У випадку дуже маленьких компаній це повинно бути якомога простішим.

3. Впровадження процесу безпеки.

Після того, як ініційовано процес інформаційної безпеки та визначено політику безпеки та спосіб організації захисту інформації, впровадження концепції безпеки для організації є наступним кроком. В якості основи модулі Компендіуму IT-Grundschutz містять відповідні вимоги до безпеки відповідно до рівня техніки для типових компонентів бізнес-процесів, додатків, IT-систем та інших об'єктів.

2.3. BSI 200-3: Аналіз ризиків на базі Grundschutz

Стандарт BSI 200-3 BSI забезпечує просту у застосуванні та визнану процедуру, яка дозволяє організаціям адекватно та цілеспрямовано контролювати свої ризики інформаційної безпеки. Процедура базується на елементарних загрозах, описаних у Компедіумі IT-Grundschutz, на основі яких також були розроблені модулі IT-Grundschutz.

Коли використовується методологія згідно з IT-Grundschutz, при складанні модулів IT-Grundschutz BSI неявно проводиться оцінка ризику для сфер із нормальними вимогами захисту від BSI. Враховуються лише ті загрози, які мають таку високу частоту виникнення або такі суттєві наслідки, що для них повинні застосовуватися гарантії безпеки. Типові загрози, включають, наприклад, пошкодження внаслідок пожежі, води, крадіжки, зловмисного програмного забезпечення чи дефектів обладнання. Такий підхід має ту перевагу, що користувачам IT-Grundschutz не потрібно проводити індивідуальний аналіз загрози та вразливості для більшої частини інформаційної системи, оскільки ця оцінка вже була заздалегідь проведена BSI.

Цей документ описує, як можна визначити для конкретних цільових об'єктів, чи є і в якому відношенні необхідність вживати заходів, з метою зменшення ризиків для обробки інформації. Для цього ризики, що походять від елементарних загроз оцінюються за допомогою матриці. Оцінка проводиться з використанням частоти виникнення та масштабів збитків, спричинених, коли шкода сталася. Відповідний ризик походить від цих двох параметрів.

У стандарті BSI 200-3 аналіз ризиків складається з двох етапів. На першому етапі список загроз систематично опрацьовується. Для кожного цільового об'єкта та кожної загрози проводиться оцінка, припускаючи, що гарантії безпеки вже впроваджені або заплановані. Це, як правило, гарантії безпеки, які були виведені з основних та стандартних вимог Компедіума IT-Grundschutz. За першою оцінкою слідує інша оцінка, в якій розглядаються гарантії безпеки для зменшення ризиків. Шляхом порівняння до і після цього можна перевірити ефективність захисних засобів, які використовувались для зменшення ризиків.

Можливості та ризики - це прогнози, які часто базуються на розрахунках можливої вигоди в позитивному випадку або збитку в негативному випадку. Цей стандарт зосереджений на розгляді негативних наслідків ризиків, маючи на меті показати адекватні запобіжні заходи для мінімізації ризиків. На практиці лише негативні наслідки розглядаються як частина управління в більшості випадків. Крім того, організації, тим не менше, повинні також розглядати позитивні ефекти.

2.3.1. Аналіз ризику

У цьому стандарті термін "аналіз ризику"означає повний процес визначення (виявлення, визначення та оцінки) та зменшення ризиків. Однак, відповідно до відповідних стандартів ISO 31000 та ISO 27005, "аналіз ризику"стосується лише одного етапу як частини визначення ризику, який складається з наступних етапів:

• Визначення ризику
• Аналіз ризиків
• Оцінка ризику

Тим часом, однак, термін «аналіз ризику» був встановлений для всього процесу визначення ризику та зменшення ризику. Тому термін "аналіз ризику"все ще використовується в IT-Grundschutz, а також у цьому документі для позначення всебічного процесу. Аналіз ризиків відповідно до стандарту BSI 200-3 передбачає наступні кроки:

• Крок 1: Складання огляду загроз
- Складання переліку потенційних елементарних загроз
- Визначення додаткових загроз, які виходять за рамки елементарних загроз і виникають із конкретних оперативних сценаріїв
• Крок 2: Класифікація ризиків
- Оцінка ризику (визначення частоти виникнення та масштабу шкоди)
- Оцінка ризику (визначення категорії ризику)
• Крок 3: Зменшення ризику
- уникнення ризику
- зниження ризику (визначення гарантій безпеки)
- передача ризику
- прийняття ризику
• Крок 4: Закріплення концепції безпеки
- Інтеграція додаткових запобіжних заходів, визначених на основі аналізу ризиків, у концепцію безпеки

Висновки

За допомогою BSI Standard, BSI забезпечує просту та зрозумілу процедуру, що дозволяє організаціям цілеспрямовано контролювати свої інформаційні ризики. Процедура заснована на елементарних загрозах,

описаних у методиці IT-Grundschutz. IT-Grundschutz забезпечує організацію методом створення системи менеджменту інформаційною безпекою (СМІБ). Він містить як загальні рекомендації щодо IT-безпеки для встановлення застосованого процесу IT-безпеки, так і докладні технічні рекомендації для досягнення необхідного рівня IT-безпеки для конкретного домену.

Перелік використаних джерел

1. ISO/IEC 17799:2000 Міжнародний стандарт Інформаційні технології -Практичні правила управління інформаційною безпекою — 2000. — С. 89 с.
2. Замула А. А., Северинов А. В., Корниенко М. А. Аналіз моделей оцінки ризиків інформаційної безпеки для побудови системи захисту інформації. Наука і техніка Повітряних Сил Збройних Сил України — 2014. — С. 133-138 с.
3. Гарасим Ю. Р., Ромака В. А., Рибій М. М. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. Вісник Національного університету "Львівська політехніка". Сер.: Автоматика, вимірювання та керування. — 2013. — С. 90-99 с.
4. Мельник Г. Модель оцінювання рівня інформаційних ризиків в корпоративних системах. Вісник Київського національного університету імені Тараса Шевченка. Сер.: Економіка. — 2015. — С. 48-54 с.