Фінанси, банківська справа та страхування

УДК [658:004.056]:005.934

Вергун Антоніна Миколаївна

кандидат економічних наук, доцент,

доцент кафедри фінансів та фінансово-економічної безпеки

Київський національний університет технологій та дизайну

Вергун Антонина Николаевна

кандидат экономических наук, доцент,

доцент кафедры финансов и финансово-экономической безопасности

Киевский национальный университет технологий и дизайна

Verhun Antonina

PhD in Economics, Associate Professor,

Associate Professor of Finance and Financial and Economic Security

Kyiv National University of Technologies and Design

ORCID: 0000-0002-2825-9511

Сорока Марія Анатоліївна

студентка

Київський національний університет технологій та дизайну

Сорока Мария Анатольевна

студентка

Киевский национальный университет технологий и дизайна

Soroka Maria

Student of the

Kiev National University of Technology and Design

МЕТОДИЧНІ ПІДХОДИ ДО РОЗРОБКИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

МЕТОДИЧЕСКИЕ ПОДХОДЫ К РАЗРАБОТКЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

METHODOLOGICAL APPROACHES TO THE SYSTEM DEVELOPMENT OF THE ENTERPRISE'S INFORMATION SECURITY MANAGEMENT

Анотація. *Інформація та інформаційні системи, мережі, в яких вона функціонує, є важливими ресурсами організації. Їх доступність, цілісність та конфіденційність можуть мати особливе значення для забезпечення конкурентоздатності організації, рентабельності, відповідності правовим нормам та іміджу організації. Сучасні організації сьогодні не убезпечені від порушення режиму безпеки, що зумовлено низкою факторів. Водночас, внаслідок посилення залежності організацій від інформаційних, комунікаційних систем та послуг вони можуть стати вразливішими до порушень режиму безпеки.*

В статті досліджено теоретичні основи та методичні підходи до управління інформаційною безпекою підприємства. А саме: визначено сутність політики захисту інформації та виокремлено основні характеристики управління інформаційною безпекою, досліджено основні принципи та процеси при управлінні інформаційною безпекою.

Ключові слова: *інформаційна безпека, система управління інформаційною безпекою, організація інформаційної безпеки на підприємстві.*

Аннотация. *Информация и информационные системы, сети, в которых она функционирует, являются важны ресурсами организации. Их доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения конкурентоспособности организации, рентабельности, соответствия правовым нормам и имиджа организации.*

Современные организации сейчас не защищены от нарушения режима безопасности, что обусловлено рядом факторов. В то же время, вследствие усиления зависимости организаций от информационных, коммуникационных систем и услуг они могут стать более уязвимыми к нарушениям режима безопасности.

В статье исследованы теоретические основы и методические подходы к управлению информационной безопасностью предприятия. А именно: определены сущность политики защиты информации и выделены основные характеристики управления информационной безопасностью, исследованы основные принципы и процессы при управлении информационной безопасностью.

Ключевые слова: *информационная безопасность, система управления информационной безопасностью, организация информационной безопасности на предприятии.*

Summary. *Information and informational systems, networks in which it operates, are important resources of the enterprise. Their availability, integrity and confidentiality can be of particular importance to ensure the competitiveness of the enterprise, profitability, compliance with legal norms and the enterprise's image. Today's enterprises are not safe from security breaches due to a number of factors. At the same time, due to the increasing dependence of enterprises on informational, communication systems and services, they may become more vulnerable to security breaches.*

The article studies the theoretical foundations and methodological approaches to information security management of the enterprise. Namely: the essence of the information protection policy has been determined and the main characteristics of information security management have been singled out, the basic principles and processes in information security management have been studied.

Key words: *information security, system of information security management, organization of the enterprise's information security.*

Постановка проблеми. В сучасних умовах ведення бізнесу успіх часто залежить не тільки від уміння виготовляти та продавати якісні, конкурентоспроможні товари та послуги, але й від здібностей підприємця та його співробітників захистити свій бізнес від негативного впливу факторів зовнішнього середовища. Забезпечення стійкого зростання підприємства, стабільності результатів його діяльності, досягнення поставлених цілей, що відповідають інтересам власників і суспільства в цілому, неможливо без розробки і проведення виваженої стратегії підприємства, яка в сучасній економіці визначається наявністю ефективної системи її захисту [1].

З кожним днем з'являються нові загрози, які здатні нанести збитків організації. Це зокрема хакерські дії, соціальна інженерія, втручання до системи, злом, несанкціонований доступ до системи, комп'ютерні злочини, продаж інформації, спуфінг, 4 руйнування інформаційної системи, атаки на систему (наприклад, розподілена відмова в обслуговуванні), перегляд інформації з обмеженим доступом, фальсифікація та підроблення даних, зловмисні коди (віруси, логічні бомби, "троянські коні" тощо), продаж персональної інформації, дефекти системи тощо. Можна стверджувати, що такі загрози з часом набуватимуть все більшого поширення.

Поширення інформаційних та комунікаційних систем надає все нові можливості для несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості спеціалістів централізовано контролювати інформаційні системи та мережі [3]. З огляду на зазначене, дослідження ключових складових забезпечення інформаційної безпеки підприємства є актуальним.

Аналіз останніх досліджень і публікацій. Теоретико-методичні аспекти інформаційної безпеки підприємства та особливості її управління знайшли відображення в працях таких вчених як: Ю.Р. Гарасим [2], П.І. Гаранюк [2], В.Б. Дудикевич [2], І.О. Козлюк [2], В.А. Ромака [2], Тарасенко І. О. [1] та ін.

Формулювання цілей статті. Мета статті полягає у дослідженні теоретичних основ та аналізі методичних підходів до управління інформаційною безпекою на основі системного підходу.

Реалізація поставленої мети потребує вирішення таких завдань: визначення сутності політики захисту інформації та виокремити основні характеристики управління інформаційною безпекою, дослідити основні принципи та процеси при управлінні інформаційною безпекою.

Виклад основного матеріалу. На сьогоднішній день інформація є одним із пріоритетних ресурсів, який забезпечує підприємству додану вартість, і внаслідок цього потребує захисту. Система управління інформаційною безпекою (СУІБ) – це частина загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси [3].

Найбільш вагомою метою більшості систем інформаційної безпеки (ІБ) є захист бізнесу та знань компанії від знищення або витоку. Також однією з основних цілей системи інформаційної безпеки є гарантія майнових прав та інтересів клієнтів. У той же час заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією в компанії, оскільки це може поставити під загрозу розвиток організації [3].

З точки зору цільового призначення, процеси ІБ в організації класифікуються на процеси забезпечення та процеси управління. Процеси

забезпечення ІБ призначені для реалізації безпосередніх організаційних і технічних функцій захисту активів компанії (технічних засобів, програмного забезпечення та інформаційних активів). Процеси управління ІБ призначені для реалізації керуючих дій щодо системи забезпечення ІБ.

Серед основних процесів управління інформаційною безпекою можна виділити наступні:

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

Процес забезпечення інформаційної безпеки підприємства – це безперервна діяльність з планування, реалізації, оцінювання та удосконалення процесів забезпечення і управління ІБ.

Необхідно відзначити, що найбільш ефективним способом управління інформаційною безпекою є впровадження системного підходу, що включає в себе введення керівництвом і власниками підприємств єдиних вимог до всіх елементів системи управління підприємством та організації контролю їх виконання, розподіл сфер відповідальності по всіх категоріях персоналу, встановлення нормативних значень показників інформаційної безпеки [1; 4].

Основний рушійним процесом системи управління ІБ є аналіз ризиків, оскільки він виконується не тільки при створенні СУІБ, але й при зміні бізнес-процесів організації і вимог з безпеки. Необхідно підібрати таку методику аналізу ризиків, яку можна було б використовувати з мінімальними змінами на постійній основі. Є два шляхи: використовувати

існуючі на ринку методики і інструментарій для оцінки ризиків або ж розробити свою власну методику, яка найкращим чином буде підходити до специфіки компанії і охоплена системою управління інформаційної безпеки області діяльності. Останній варіант найкращий, оскільки поки більшість існуючих на ринку продуктів, що реалізують ту чи іншу методику аналізу ризиків, не відповідають вимогам стандартів ISO / IEC 27001 та ISO / IEC 27002. Типовими недоліками таких методик є:

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

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

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

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

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

Процес впровадження спланованих методів обробки ризиків, що описує процедуру запуску нового процесу забезпечення інформаційної безпеки, або модернізації існуючого. Особливу увагу слід приділити опису ролей і обов'язків, а також планування впровадження.

Процес моніторингу функціонуючих процесів СЗІБ.

Процес вдосконалення заходів безпеки та безпеки відповідно до результатів моніторингу, що дає можливість здійснити коригувальні та профілактичні дії.

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

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

аудиту.

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

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

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

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

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

Організація інформаційної безпеки – складова частина системи захисту інформації, яка визначає і виробляє порядок і правила

функціонування об'єктів захисту і діяльності посадових осіб з метою забезпечення захисту інформації.

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

Перше з наведених визначень більшою мірою показує сутність організаційної захисту інформації. Друге – розкриває її структуру на рівні підприємства. Разом з тим обидва визначення підкреслюють важливість нормативно-правового регулювання питань захисту інформації поряд з комплексним підходом до використання в цих цілях наявних сил і засобів. Основними напрямками організації захисту інформації є: організація роботи з персоналом, організація внутрішньо об'єктного і пропускного режимів і охорони, організація роботи з носіями відомостей, комплексне планування заходів щодо захисту інформації, організація аналітичної роботи і контролю.

Основна мета організації інформаційної безпеки – це збереження головних для організації характеристик інформаційної безпеки: доступність, конфіденційність, цілісність.

Система інформаційної безпеки підприємства побудована на ряді принципів:

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

працює на підприємстві. Організаційною формою комплексного використання сил і засобів повинна бути програма забезпечення безпеки підприємства.

Пріоритет профілактичних заходів (своєчасність). Система безпеки повинна бути побудована таким чином, щоб вона могла виявити різні руйнівні фактори на ранній стадії, вжити заходів щодо запобігання їх шкідливого впливу та заподіяти шкоду підприємству. Реалізація цього принципу економічно набагато вигідніше, ніж усунення шкоди.

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

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

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

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

Взаємодія. Для того щоб забезпечити безпеку підприємства, необхідно, щоб зусилля всіх його співробітників, підрозділів, служб були скоординовані. Тобто всі учасники цього процесу повинні взаємодіяти один з одним, чітко знаючи, хто за що відповідає, а хто що робить.

Принцип взаємодії також передбачає встановлення тісних ділових контактів і координацію дій з зовнішніми організаціями (правоохоронними органами, місцевими або районними службами безпеки, органами влади і т. д.), Здібними надати потрібну допомогу у забезпеченні безпеки підприємства. Це завдання може виконати комітет (група, рада і т. д.) безпеки підприємства.

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

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

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

Очолювати цю роботу повинен начальник служби безпеки інформації. Для більш дрібних фірм (організацій) – помічник начальника служби безпеки фірми з інформаційної безпеки. Ця посада може бути штатною, або її можна займати за сумісництвом (залежить від статусу фірми і її фінансового стану). Крім того, за кожною зоною відповідальності повинні бути призначені відповідальні за забезпечення безпеки інформації. Такі ж відповідальні призначаються і на кожен об'єкт обчислювальної техніки. Що стосується безпеки зв'язку, то тут повинні бути відповідальні за забезпечення безпеки кожного виду зв'язку (електронного, телефонного, телеграфного, факсимільного, при передачі даних). Ці посади також займаються за сумісництвом.

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

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

Література

1. Тарасенко І. О. Використання системного підходу до управління фінансовою безпекою підприємства / І. О. Тарасенко, А. М. Вергун // Науковий вісник: фінанси, банки, інвестиції. 2014. № 1 (26). С. 6-10.
2. Навчальний посібник / В.А. Ромака, В.Б. Дудикевич, Ю.Р. Гарасим, П.І. Гаранюк, І.О. Козлюк. Львів: Видавництво Львівської політехніки, 2012. 232 с.

3. Система управління інформаційною безпекою як ключовий чинник успішності організації // Інститут Навчання Менеджерів Якості. URL: https://ua.ikmj.com/isms/
4. Вергун А. М. Інформаційно-аналітичне забезпечення моніторингу рівня фінансової безпеки промислових підприємств / А. М. Вергун // Формування ринкових відносин в Україні. 2016. № 11. С. 28-32.

References

1. Tarasenko I. O. Vykorystannja systemnogho pidkhodu do upravlinnja finansovoju bezpekoju pidpryjemstva / I. O. Tarasenko, A. M. Verhun // Naukovyj visnyk: finansy, banky, investyciji. 2014. # 1 (26). S. 6-10.
2. Navchaljnyj posibnyk / V.A. Romaka, V.B. Dudykevych, Ju.R. Gharasym, P.I. Gharanjuk, I.O. Kozljuk. Ljviv: Vydavnyctvo Ljvivsjkoji politekhniky, 2012. 232 s.
3. Systema upravlinnja informacijnoju bezpekoju jak kljuchovyj chynnyk uspishnosti orghanizaciji // Instytut Navchannja Menedzheriv Jakosti. Rezhym dostupu: https://ua.ikmj.com/isms/
4. Verhun A. M. Informacijno-analitychne zabezpechennja monitorynghu rivnja finansovoji bezpeky promyslovykh pidpryjemstv / A. M. Verhun // Formuvannja rynkovykh vidnosyn v Ukrajini. 2016. # 11. S. 28-32.