Економічні науки

УДК 004.056.53

Ю.О. Русіна
к.е.н., доцент,
Київський національний університет технологій та дизайну
І.О.Щеглов
студент,
Київський національний університет технологій та дизайну
Ю.А. Русина
к.э.н., доцент,
Киевский национальный университет технологий и дизайна
И.О.Щеглов
студент,
Киевский национальный университет технологий и дизайна
Y. Rusina
Ph.D., Associate Professor,
Kyiv National University of Technology and Design
I.Schehlov
student,
Kyiv National University of Technology and Design

УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА
СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ
IMPROVEMENT OF ENTERPRISE INFORMATION SECURITY MANAGEMENT

Анотація: У статті визначено сутність системи управління інформаційною безпекою підприємства, викладено основні цілі та складові елементи. Наведено рекомендації щодо вдосконалення системи управління інформаційною безпекою на підприємстві.

Ключові слова: інформаційна безпека, інформаційна система, управління інформаційною безпекою.

Аннотация: В статье определена сущность системы управления информационной безопасностью предприятия, изложены основные цели и составляющие элементы. Приведены рекомендации по совершенствованию системы управления информационной безопасностью на предприятии.

Ключевые слова: информационная безопасность, информационная система, управление информационной безопасностью.

Summary: In the article the essence of information security management company, set out the main objectives and components. Recommendations for improving information security management system in the enterprise.

Keywords: information security, information system, information security management.

Постановка проблеми. Актуальність проблеми захисту інформації сьогодні не викликає сумнівів. Успіх сучасного підприємства та його розвиток в умовах гострої конкуренції в значній мірі залежать від застосування інформаційних технологій, а отже, від ступеня забезпечення інформаційної безпеки.

З кожним роком зростає кількість інцидентів інформаційної безпеки, з'являються нові методи та засоби незаконного втручання в інформаційну систему підприємств. Інформація в сучасному суспільстві стає пріоритетним активом та фактором успіху роботи підприємства незалежно від галузі та форми його власності. У зв'язку з цим значно виросла кількість спроб несанкціонованого доступу до інформаційних ресурсів.

Телекомунікаційна галузь завжди була найбільш технологічно розвинутою та динамічним драйвером впровадження інноваційних рішень для забезпечення інформаційної безпеки [1].

Управління інформаційною безпекою повинно бути невід'ємною складовою управління сучасним підприємством і являти собою систему

заходів, спрямованих не тільки на подолання загроз та ризиків, але й на передбачення та запобігання їх настання.

Проблема інформаційної безпеки набула особливої значущості в сучасних умовах широкого застосування автоматизованихних інформаційних систем, заснованих на використанні комп'ютерних і телекомунікаційних засобах. При забезпеченні інформаційної безпеки стали цілком реальними загрози, викликані навмисними (зловмисними) діями людей. Перші повідомлення про факти несанкціонованого доступу до інформації були пов'язані, в основному, з хакерами, або «електронними розбійниками». Останнім десятиліттям порушення захисту інформації прогресує з використанням програмних засобів і через глобальну мережу Інтернет. Досить поширеною загрозою інформаційної безпеки стало також зараження комп'ютерних систем вірусами[8].

Таким чином, у зв'язку із зростаючою роллю інформаційних ресурсів в житті сучасного суспільства, а також через реальність численних загроз з точки зору їх захищеності, проблема інформаційної безпеки вимагає до себе постійної і більшої уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставини, які мають до того ж різну фізичну природу, що переслідують різні цілі і викликають різні наслідки, призводять до необхідності комплексного підходу при вирішенні даної проблеми.

Метою статті є дослідження концептуальних основ економічної безпеки підприємств у сучасних умовах функціонування.

Аналіз останніх досліджень та публікацій. Серед праць, котрі присвячені дослідженням методологічних, сутнісних та змістовних основ інформаційної безпеки особливе місце займають теоретичні розробки Е. Бєляєва, М. Бусленка, С. Гриняєва, О. Данильяна, О. Дзьобаня, Г. Ємельянова, В. Лопатіна, О. Позднякова, Л. Сергієнка, В. Циганкова, М. Чеснокова та інших дослідників. Авторами робіт у яких розкриваються особливості забезпечення інформаційної безпеки є праці О.Дзьобаня,

А.Колодюка, В.Копилова, А.Кубишкіна, Є.Мануйлова, В.Ніцевича, А.Стрельцова, М.Якушева та ін.

Виклад основного матеріалу дослідження.

Згідно з міжнародним стандартом [7], система управління інформаційною безпекою - це «частина загальної системи управління організації, що заснована на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід та вдосконалення інформаційної безпеки».

Серед основних її цілей можна виділити:

- забезпечення безпеки найважливішої корпоративної інформації;
- захист основних активів і критичних бізнес-процесів організації;
- мінімізація ризиків інформаційної безпеки при веденні операційної діяльності організації;
- забезпечення безперервності основної діяльності організації;
- підвищення загального рівня управління організації.

Інформаційна безпека підприємства включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою – комплексність[6].

Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Слід зазначити, що ключовим фактором, у забезпеченні інформаційної безпеки підприємства є його персонал. Основними заходами при роботі з яким є: проведення аналітичних процедур при прийомі і звільненні; навчання і інструктаж практичним діям по захисту інформації; контроль за виконанням вимог по захисту інформації,

стимулювання відповідального відношення до збереження інформації та ін.

Система управління інформаційною безпекою є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки. Систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси[3].

Основними цілями інформаційної безпеки є:

- конфіденційність інформації, тобто необхідність введення обмежень доступу до даної інформації для певного кола осіб;
- неможливість несанкціонованого доступу до інформації, тобто ознайомлення з конфіденційною інформацією сторонніх осіб;
- цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка і виведення), яка полягає в її існуванні в неспотвореному вигляді (незміненому по відношенню до деякому фіксованому її станом);
- доступність інформації, тобто здатність забезпечувати своєчасний і безперешкодний доступ осіб до інформації;
- мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів;
- облік усіх процесів, пов'язаних з ризиками.

Досягнення заданих цілей здійснюється в ході вирішення наступних завдань:

- введення в систему термінів інформаційної безпеки;
- класифікації інформаційних ресурсів підприємства;
- визначення власників процесів, відповідальних за інформаційну безпеку;
- розробки спектра ризиків інформаційної безпеки та проведення їх експертних оцінок;

- визначення групи доступу до інформаційних ресурсів;
- розробки системи управління ризиками інформаційної безпеки (методи та їх оцінка);
- складання переліків адміністративних і технічних заходів для мінімізації та компенсації ризиків;
- здійснення заходів інформаційної безпеки та періодичного контролю за станом ризиків;
- забезпечення фізичної безпеки та безпеки персоналу;
- розробки вимог до інформаційної системи з нагляду інформаційної безпеки;
- контролінгу інформаційної безпеки на підприємстві.

Виділяються чотири стадії реалізації системи управління інформаційною безпекою:

1) формування політики в галузі ризиків;
2) аналіз бізнес-процесів;
3) аналіз ризиків;
4) формування цільової концепції.

Система управління інформаційною безпекою підприємства повинна включати (рис.1) :

- аутентифікацію (користувачів, даних, додатків, послуг, тощо);
- авторизацію (авторизований перелік цін, ключових торговельних документів, партнерів, користувачів, керівництва);
- аудит інформаційних ресурсів та послуг.

Рис. 1. Базова система управління інформаційної безпеки (складено автором на основі джерела [2])

При удосконаленні системи управління інформаційною безпекою, необхідно зазначити, що ефективне управління інформаційною безпекою підприємства характеризується за наступними ознаками[4]:

- охоплення всього підприємства;
- відповідальність керівників;
- інформаційна безпека розглядається в якості вимоги бізнесу;
- інформаційна безпека забезпечується з урахуванням ризиків;
- адекватна політика інформаційної безпеки;
- достатність виділених ресурсів;
- персонал навчений і проінформований;
- безпечний життєвий цикл програмного забезпечення;
- планована, керована і вимірювана інформаційна безпека;
- регулярний аудит.

Процес управління інформаційною безпекою відбувається в масштабі всього підприємства. Система управління інформаційною безпекою підприємства охоплює людей, продукти, виробництва, процеси, політику, процедури, системи, технології, мережі та інформацію.

Керівники усвідомлюють свою відповідальність та підзвітність у сфері інформаційної безпеки перед організацією, акціонерами, співтовариствами і державою. Топ-менеджери задіяні в процесах управління інформаційною безпекою фірми і підтримують їх адекватними фінансовими ресурсами, ефективними методами контролю, політикою, розробленою з урахуванням актуальних ризиків, а також щорічним аудитом. У випадках реалізації ризиків інформаційної безпеки керівники підприємства беруть на себе відповідальність.

Інформаційна безпека розглядається в якості вимоги бізнесу. Забезпечення інформаційної безпеки розглядається як обов'язкова бізнес-вимога, яка має безпосередній вплив на виконання стратегічних цілей, тактичних завдань, планів управління ризиками і високорівневих політик, а також на дотримання вимог регуляторів. Всі менеджери розуміють, яким

чином і чому безпека виступає як необхідна умова існування і розвитку бізнесу.

Політика інформаційної безпеки бізнесу розробляється на верхніх рівнях управління і співробітники не мають права в односторонньому порядку вирішувати, скільки інформаційної безпеки вони «хочуть». При цьому гнучкі виключення з правил дозволяють виконувати необхідні бізнес-процеси, а керівники забезпечені засобами належного контролю[5].

Інформаційна безпека забезпечується з урахуванням ризиків. Оцінка достатності рівня захищеності заснована на розрахунку допустимих інформаційних ризиків, у тому числі ризиків порушення вимог регуляторів, збоїв у поточній роботі, репутаційного збитку і фінансових втрат. Вивчається вплив внутрішніх і зовнішніх ризиків, на основі чого, за необхідності, перераховуються допустимі рівні інформаційної безпеки бізнесу. Це невід'ємна частина ризик-менеджменту організації.

Вимоги до інформаційної безпеки реалізуються через ясно і точно сформульовану політику ІБ, підтримувану персоналом і забезпечену всіма необхідними організаційними і технічними заходами.

Проводиться адекватне і стале фінансування, виділення ресурсів на інформаційну безпеку. Ключовий персонал, у тому числі IT-фахівці та офіцери безпеки, мають достатні ресурси, повноваження і час для того, щоб підтримувати систему інформаційної безпеки підприємства в необхідному стані.

Всі співробітники, що мають доступ до активів, знають свої щоденні обов'язки з підтримання достатнього рівня інформаційної безпеки. Поінформованість, мотивованість і дотримання прийнятих правил вважаються нормою корпоративної культури. Персонал проходить регулярні тренінги в області інформаційної безпеки. Політика інформаційної безпеки відображена в посадових інструкціях.

Вимоги до інформаційної безпеки виконуються протягом всього життєвого циклу програмного забезпечення, включаючи його придбання,

проектування, розробку, тестування, експлуатацію, технічне обслуговування та списання.

Безпека є невід'ємною частиною стратегічного, фінансового та оперативного планування. В системі інформаційної безпеки у підприємства є досяжні, вимірні цілі, інтегровані в стратегічні та оперативні плани. Реалізація даних цілей контролюється з використанням метрик. Аудит існуючих планів дозволяє визначати слабкі місця системи інформаційної безпеки, вимоги безперервності бізнес-процесів і виконання запланованого. Рівень інформаційної безпеки бізнесу є одним з показників роботи менеджерів і завжди враховується при запуску нових проектів, у взаєминах з іншими учасниками ринку, а також в ході поточного управління проектами.

Проводиться регулярний аудит і, за необхідності, перегляд корпоративної системи інформаційної безпеки чи окремих її компонентів. Це дозволяє підтримувати бажаний рівень інформаційної безпеки в організації.

Висновки. Отже, в сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

Література:

1. Данчук В.Д. Удосконалення методів забезпечення інформаційної безпеки корпоративних інформаційних систем [Текст] / Данчук В.Д., Ананченко В.Є., Ананченко О.Є. // Збірник наукових доповідей та тез науково-технічної конференції «Інформаційна безпека України» Київського національного університету ім. Т.Шевченка 12-13 березня 2015.— Київ. — С. 96-97.
2. Семененко В.А. Информационная безопасность: Учебное пособие. 2-е изд., стереот. —М.: МГИУ, 2005. — 215 с.
3. Корнюшин, П.Н. Информационная безопасность [Текст] / П.Н. Корнюшин, С.С. Костерин. — Владивосток: ТИДОТ ДВГУ, 2003. — 154 с.
4. Конев И. Р. Информационная безопасность предприятия [Текст] / И. Р. Конев, А. В. Беляев. — СПб. : БХВ-Петербург, 2003. — 747 с.
5. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1[Текст] / С.В. Кавун, В.В. Носов, О.В. Мажай. — Харків: Вид. ХНЕУ, 2008. — 352 с.
6. Аникин И.В. Теория информационной безопасности и методология защиты информации [Текст] /И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина . — Казань : Изд-во Казан. гос. техн. ун-та, 2008. — 358с.
7. ISO/IEC 17799:2005 RU; ISO/IEC 27001:2005 RU. — [Електрон. ресурс]. — Режим доступу : http://iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1/.
8. Зегжда, Д.П., Івашко, А.М. Основи безпеки інформаційних систем. - М .: Інтуїт, 2006.