УДК 338

Гриджук Г.С.

СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА: ЕКОНОМІЧНО ЕФЕКТИВНИЙ ПІДХІД ДО ПРОЕКТУВАННЯ ТА ФУНКЦІОНУВАННЯ

В статті розглянуто питання системи безпеки підприємства. Викладено основні вимоги до підготовки та проектування економічно ефективної системи безпеки, адекватної загрозам бізнесу.

Ключові слова: інформаційна безпека,проектування системи інформаційної безпеки, система захист, інформаційний ресурс.

In the article the question of the security company. The basic training requirements and design cost-effective security system, adequate business challenges.

Keywords: information security, information security system design, system protection, information resource.

В статье рассмотрены вопросы системы безопасности предприятия. Изложены основные требования к подготовке и проектирования экономически эффективной системы безопасности, адекватной угрозам бизнеса.

Ключевые слова: информационная безопасность, проектирование системы информационной безопасности, система защита, информационный ресурс.

Постановка проблеми. В наш час – час кризи та нестабільності керівництво будь-якого підприємства розуміє, що неможливо виділити необмежений обсяг фінансів та людських ресурсів на забезпечення інформаційної безпеки. З економічної точки зору відрахування в безпеку повинні показати прибуток або скорочення можливих витрат. Політика забезпечення інформаційної безпеки повинна визначати пріоритети інвестицій в напрямку найбільшої уразливості. Неможливо створити абсолютно надійну систему безпеки. В основному через те, що постійно з'являються нові види загроз, яким система не зможе протистояти, а також через те, що ефективність системи захисту залежить від обслуговуючого персоналу, а людині властиво помилятися. У будь-якому випадку вартість засобів забезпечення безпеки повинна відповідати ризику і прибутку для середовища, що оточує суб'єкт господарювання.

Аналіз останніх досліджень та публікацій. Необхідність побудови системи інформаційної безпеки на підприємстві доводилась такими українськими науковцями, як Кормичем Б.А., Низенком Е.І., Кузьменком Б.В., Лужецьким В.А., Северином Л.І., Гульчаком Ю.П. Кожухівським А.Д. [1-4].Проте їхні дослідження розкривають лише організаційно-правові або програмно-технічні основи впровадження системи.

Формулювання цілі статті. Дана стаття покликана відповісти на питання, як спроектувати економічно ефективну систему безпеки, адекватну загрозам бізнесу.

Виклад основного матеріалу. На більшості сучасних підприємств система інформаційної безпеки зводиться в основному до безпеки його комп'ютерної мережі та призначена для того, щоб мережа підприємства постійно перебувала в безпечному стані. Проте не слід виключати важливий людський фактор, який у 80% випадків стає джерелом витоку цінної інформації підприємства. Для того, щоб інформаційна мережа перебувала в безпечному стані, вона повинна відповідати ряду властивостей, серед яких основними є конфіденційність, цілісність і доступність.

Перед тим, як приступити до проектування системи безпеки, необхідно сформулювати вимоги до розроблюваної системи. Зробити це найкращим чином допоможе організаційно-нормативна документація. На підприємстві повинна бути розроблена внутрішня нормативна документація: політика інформаційної безпеки, методика визначення цінності або критичності для бізнесу різних даних, правила реагування на інциденти в області порушення інформаційної безпеки тощо. Сформулювати вимоги також допоможуть вітчизняні та міжнародні стандарти. При цьому слід пам'ятати, що вони розробляються як універсальне керівництво, яке не завжди може застосовуватися в оригінальному вигляді на конкретному підприємстві, де сильно розвинена індивідуальність ведення бізнесу. З економічної точки зору ефективно сформулювати власні вимоги до конкретного унікального інформаційного середовища кожного підприємства. До виконання цього завдання слід залучати як фахівців з інформаційної безпеки (у тому числі консультантами з сторонніх спеціалізуються підприємств), так і аналітиків, юристів, технічних фахівців, що обслуговують обчислювальну мережу, і,безумовно, керівництво підприємства.

Спочатку необхідно сформулювати, яку саме інформацію необхідно захищати, потім - від кого, і на аналізі отриманого матеріалу визначити, як найефективніше це зробити. Потім реалізувати розроблену систему безпеки на технічному, організаційному і правовому рівнях.

Необхідно оцінити збиток, який може мати місце у разі витоку інформації або при будь-якому іншому порушенні системи безпеки, а також вірогідність нанесення такої шкоди. Для визначення адекватності вартості системи захисту слід зіставити розміри збитку і ймовірність його нанесення з розмірами витрат на забезпечення захисту. На жаль, отримати реальну вартість інформації досить складно, тому часто застосовуються якісні експертні оцінки; інформаційні ресурси класифікують як критичні для ведення бізнесу, особливої важливості і т. д.

Знання «що захищати» і від «кого» дозволяють точно сформулювати вимоги до системи інформаційної безпеки. На питання, «як захищатися» по кожній з вимог, відповіді вже готові у фахівців з інформаційної безпеки. Сьогодні на ринку представлений цілий ряд спеціальних засобів

інформаційної безпеки, що володіють певним набором властивостей, вартістю, захищеністю.

Для проектування системи безпеки потрібно використовувати наукові, точні математичні методи, для особливо важливих об'єктів - формалізовані моделі безпеки і формальні політики безпеки. Перевагою формального опису політики безпеки є відсутність в ній суперечностей і можливість теоретично довести безпеку системи при дотриманні всіх умов політики безпеки.

Базою для створення системи безпеки служать коректно вироблені вимоги до неї. Коли всі показники, що описують властивості захищаються ресурсами і засобами захисту, виражені кількісно, проектування системи безпеки зводиться до математичної моделі. Для перетворення якісних показників у кількісні можна використовувати експертні оцінки. Коли отримано кількісну оцінку рівня захищеності з даного критерію, є можливість порівнювати різні комплекси засобів захисту. Для побудови економічно ефективної системи захисту необхідно вирішити задачу оптимального вибору засобів реалізації системи захисту від комплексу можливих загроз інформації, що відповідають заданим обмеженням (вартість всієї системи, загальний рівень безпеки, швидкість роботи і т. п.).

Для скорочення розмірності задачі оптимізації, спрощення формалізації політики безпеки та з огляду на специфіку і багатофункціональність інформаційної безпеки пропонується розглядати систему захисту у вигляді сукупності взаємодіючих підсистем. Декомпозиція системи захисту проводиться з метою розподілу різних слабозв'язаних функцій захисту з різних підсистем. У результаті вони можуть проектуватися, реалізовуватися і управлятися в процесі експлуатації роздільно. Число підсистем визначається, виходячи з практичних потреб та мінімізації витрат на проектування і побудову системи безпеки. Інформаційна взаємодія підсистем здійснюється на основі аутентифікації взаємодіючих сторін з встановленням захищеного з'єднання. Подібна побудова дозволяє комплексно використовувати різні засоби і методи захисту, підвищити загальну ефективність системи в цілому при зниженні витрат на проектування і реалізацію, а також скоротити розмірності задачі оптимізації і спростити формалізацію правил функціонування підсистем захисту. Кожна підсистема, у свою чергу, може ділитися на вкладені підрівні захисту. Зв'язок між підсистемами захисту здійснюється за допомогою засобів електронного цифрового підпису.

Усі підсистеми повинні мати однакову ступінь захищеності, що дозволяє ефективно розподілити ресурси системи захисту. У міру проектування системи захисту проводиться поетапна деталізація і конкретизація цілей, завдань і структури підсистем захисту. На етапі експлуатації системи в міру виявлення необлікованих загроз здійснюється уточнення структури і складу підсистем безпеки. Проектування й побудова

систем захисту з апріорно заданими властивостями, відповідними необхідного рівня безпеки, досить трудомістке завдання. Проектування оптимальної системи утруднене через безліч параметрів, які треба врахувати, і через неадекватність моделей безпеки, модифікованих для опису розподілених обчислювальних мереж.

Висновки. З огляду на вищесказане, пропонується методика оптимальної побудови системи захисту, яка описує специфіку розподіленої віддаленої взаємодії компонентів інформаційної системи та багатокритеріального розв'язання задачі вибору комплексу засобів захисту. Методика дозволяє формалізувати архітектуру мережі і правила розмежування доступу в ній, сформулювати вимоги, що ставляться до системи захисту (до компонентів мережі та процедур взаємодії між ними), здійснити проектування системи захисту з необхідним рівнем захищеності з мінімізацією витрат на її проектування, побудову та обслуговування з урахуванням використовуваних інформаційних технологій. Вирішується завдання вибору такої сукупності методів захисту (зі списку всіх доступних методів за кожною з вимог), при якій виконувалися задані обмеження на частину параметрів системи і максимізувалися або мінімізувалися б інші параметри (рівень захищеності і вартість).

ЛІТЕРАТУРА

1. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України [Текст] : монографія / Б.А. Кормич ; Одеськ. нац. юрид. акад. - О. : Юрид. літ., 2003. - 471 с.
2. Кузьменко Б.В. Організаційно-правові та програмно-технічні засоби забезпечення інформаційної безпеки [Текст] : навч. посіб. для студ. спец. 6.050101 "Комп'ют. науки" / Кузьменко Б.В. ; Кабмін України, Нац. аграр. ун-т, Каф. автоматиз. с.-г. вир-ва. - К. : [б. и.], 2008. - 164с.
3. Низенко Э. И. Обеспечение безопасности предпринимательской деятельности [Текст] : учеб. пособие / Э.И. Низенко ; Межрегион. акад. упр. персоналом. МАУП. - К. : [б. и.], 2003. - 122 с.
4. Основи організаційного захисту інформації [Текст] : навч. посіб. Для студ. напр. підготовки 1601 - "Інформ. безпека" / В.А. Лужецький, Л.І. Северин, Ю.П. Гульчак, А.Д. Кожухівський ; Вінницьк. нац. техн. ун-т. - Вінниця : ВНТУ, 2005. - 147 с.

УДК 339.137.2

О.О. Железняк, О.С. Кузьменко

ВПЛИВ КОНКУРЕНТНОГО СЕРЕДОВИЩА НА ДИНАМІКУ ЗБУТУ ТОВАРУ У РИНКОВИХ УМОВАХ

У статті проведено дослідження впливу конкурентного середовища на динаміку збуту товару у ринкових умовах. Розглянуто основні показники, які