УДК 004.056.53

О.Є. Ананченко

ПИТАННЯ ФОРМУВАННЯ ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Тема статті актуальна для діяльності підприємств, компаній та акціонерних товариств державної та приватної власності. Основний наголос зроблено на висвітленні та обґрунтуванні різних питань формування організаційної структури системи управління інформаційною безпекою. Побіжно охарактеризовано визначення принципів і методів забезпечення інформаційної безпеки, виконання вимог законодавства держави стосовно цих питань та відповідальність за їх впровадження. Пропонується і обґрунтовується доцільність створення різних підрозділів що будуть розробляти та реалізовувати комплекс правових, організаційних та технічних засобів і заходів, спрямованих на запобігання та недопущення неправомочних та несанкціонованих дій з будь-якою інформацією на підприємствах.

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

Вступ

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.

Основні труднощі реалізації систем захисту полягають в тому що вони повинні задовольняти двом групам суперечливих вимог. З одного боку повинен бути забезпечений надійний захист інформації в системі, що в більш конкретному вираженні формулюється у вигляді двох узагальнених задач: виключення випадкової та навмисної видачі інформації стороннім особам і розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговуючого персоналу. З іншого боку, системи захисту не повинні створювати великих незручностей в процесі роботи з використанням ресурсів системи [2].

Основна частина

Забезпечення інформаційної безпеки є стратегічним завданням керівництва будь-якого підприємства, компанії або акціонерного товариства. В цій роботі розглядаються питання формування організаційної структури системи управління інформаційною безпекою в основному тих підприємств, що надають інфо-комунікаційні послуги різним користувачам. В даному випадку інформаційна безпека(ІБ) ідентифікується як стан інформації, інформаційних ресурсів та інформаційних систем при якому забезпечується захист інформації(даних) від витоку, крадіжки, втрат, несанкціонованого знищення, викривлення, модифікації(підробки), копіювання, блокування бази даних тощо. Тому захист інформації повинен включати комплекс правових, організаційних і технічних засобів на заходів, спрямованих на запобігання неправомірних дій з інформацією.

Метою діяльності підприємства в сфері ІБ повинно бути забезпечення збалансованого і успішного виконання своїх функцій, досягнення сталого ведення бізнесу в умовах ризиків, що можуть привести до порушення конфіденційності, цілісності, доступності інформації, а також до порушення стійкості функціонування її мереж зв'язку та інформаційних систем.

За результатами опитування, однією з основних проблем, що стоять перед підприємствами є створення чіткої стратегії розвитку IT-інфраструктури з стратегією інформаційної безпеки в її серці. Компанії та підприємстваз більшою рішучістю ставляться до забезпечення інформаційної безпеки своєї IT-інфраструктуру в світлі зростаючого числа інцидентів і значних фінансових втрат, пов'язаних з ними.Основними результатами опитування стало:

- Підтримка інформаційної безпеки є основною проблемою з якою стикаються IT-менеджмент компанії;
- За останні 12 місяців, 91% опитаних компаній мали принаймні один випадок зовнішнього інциденту IT-безпеки і 85%повідомили про внутрішні інциденти;
- Серйозний інцидент може коштувати великій компанії в середньому $ 649000; для малих і середніх компаній рахунок в середньому становить близько $ 50000;
- Успішна спрямована атака на велику компанію може коштувати їй $ 2,4 млн прямих фінансових втрат і додаткових витрат;
- Для компанії середнього або невеликого розміру, цільова атака може означати близько $ 92000 за моральну шкоду - майже вдвічі більше, ніж в середньому атаки;
- Значна частина інцидентів, що призводять до втрати цінних даних були внутрішніми, викликані такими питаннями як незакриті уразливості в програмному забезпеченні, які використовуються компанією, навмисних або недбалих дій співробітників, втрати чи крадіжки мобільних пристроїв;
- Персональні мобільні пристрої, що використовуються для цілей, пов'язаних з роботою залишаються однією з головних небезпек для бізнесу: 65% опитаних бачили загрозу вBringYourOwnDevice політики;
- Витік інформації, що здійснюються з використанням мобільних пристроїв навмисно або випадково - складають основну внутрішню загрозу, майбутнім якої компанії стурбовані [3].

Поряд з виконанням принципів і методів забезпечення ІБ важливим фактором є визначення організаційної структури системи управління інформаційної системи(СУІБ) підприємства. В загальному вигляді СУІБ включає в себе систему організаційно-технічних засобів, здійснюваних для досягнення нормальної діяльності в сфері ІБ.

Організаційна структура системи управління будується на основі розмежування функціональних повноважень між різними підрозділами, а основними елементами організаційної СУІБ можуть бути в залежності від розміру та статусу підприємства: генеральний директор, начальник департаменту безпеки, директора по напрямам діяльності, директора територіальних управлінь, відділ інформаційної безпеки, підрядчики, співробітники. Під аутсорсинговими компаніями розуміються сторонні організації які на основі укладених договорів виконують певні роботи або надають послуги підприємству в інформаційній сфері. Поняття інформаційної сфери містить в собі сукупність інформації, інформаційної інфраструктури, суб’єктів, що здійснюють збирання, формування, розповсюдження і використання інформації.

Генеральний директор як перша особа, є власником усіх інформаційних активів, визначає склад і обсяг відомостей що складають інформаційну таємницю, а бо іншу інформацію обмеженого доступу, а також їх захисту та збереження у відповідності з існуючим законодавством України. При цьому інформаційними активами є все що має цінність в інформаційній сфері – інформація, програмне забезпечення, технічні засоби обробки інформації, засоби зв’язку, персонал тощо.

В загальному вигляді основними класами активів підприємств, захист яких необхідно забезпечувати є:

- Інформація, що зберігається і опрацьовується в корпоративній інформаційній системі;
- Відомості та повідомлення, що передаються по мережам електрозв'язку;
- Програмне забезпечення, що входить в корпоративну інформаційну систему;
- Технічні засоби обробки інформації в корпоративній інформаційній системі;
- Безпосередньо засоби зв'язку;

- Інформаційні та комунікаційні сервіси, що надаються як користувачам так і штатним співробітникам;
- Будівлі, спеціальні споруди, серверні приміщення тощо.;
- Ліцензії, репутація, імідж підприємства, його співробітники зі своєю кваліфікацією, знаннями, досвідом.

Якщо в штаті є посада начальника департаменту безпеки то в його обов'язки можуть входити санкціонування дій по забезпеченню ІБ та визначення пріоритетних напрямів розвитку забезпечення інформаційної безпеки.

Але основним підрозділом, що безпосередньо організовує і відповідає за забезпечення ІБ в рамках своїх повноважень є відділ інформаційної безпеки(ВІБ). Саме співробітники ВІБ відповідно до затверджених функціональних обов'язків виконують низку робіт, зокрема:

- Розробляють проекти і реалізують стратегію забезпечення інформаційної безпеки;
- Визначають вимоги з ІБ до бізнес проектів та до засобів їх реалізації та автоматизації;
- Розробляють внутрішню нормативну базу в сфері забезпечення ІБ;
- Координують діяльність різних виробничих підрозділів в царині забезпечення ІБ з урахуванням певних пріоритетних напрямів розвитку інформаційної безпеки;
- Формулюють і обґрунтовують свої пропозиції до проекту бюджету або фінансового плану підприємства для забезпечення ІБ;
- Виконують роботу по виявленню та оцінці загроз ІБ, аналізують ризики і підтримки їх в актуальному стані, реалізують заходи по запобіганню можливих загроз ІБ;
- Приймають участь у визначенні господарів економічних ризиків, розраховують результати оцінки цих ризиків для керівництва, а також пропонують шляхи і засоби обробки ризиків з урахуванням їх ефективності. В даному випадку ризик ІБ це функція вірогідності реалізації певної загрози, в тому числі економічної, а також виду та величини можливого збитку;
- Розробляють пропозиції по удосконаленню механізмів забезпечення ІБ та контролюють реалізацію вимог до інформаційної безпеки;
- Ініціюють та проводять розслідування за фактами інцидентів ІБ;
- Визначають і контролюють виконання вимог до процесу управління доступом до інформаційних систем і ресурсів користувачів, штатного персоналу, впровадження і підтримки систем. Тобто в їх компетенції знаходиться надання права доступу або навіть цілковитого позбавлення доступу через певні причини.

В організаційну структуру системи управління інформаційною безпекою включаються і інші суб'єкти, що займають певні ніші цього процесу. Так директори підрозділів, що здійснюють закупку і розробку інформаційних систем, керівники, розробники проектів відповідають персонально за забезпечення інформаційної безпеки на всіх етапах виконання проектних робіт у відповідності з вимогами діючої нормативної документації. Керівники підрозділів експлуатації та моніторингу інформаційних систем несуть відповідальність за забезпечення інформаційної безпеки на всіх етапах життєвого циклу інформаційних систем. Окремі співробітники в межах своїх повноважень зобов'язані виконувати вимоги по забезпеченню ІБ, визначені відповідними нормативними документами та повідомляти про всі відомі їм інциденти інформаційної безпеки своєму безпосередньому керівнику або підрозділу, відповідальному за управління такими інцидентами.

Підрядчики, в рамках виконання договірних відносин, можуть надавати послуги та реалізувати роботи, але несуть відповідальність за розголошення будь яких відомостей по інформаційній безпеці.[4]

Проводячи удосконалення або формування організаційної структури системи управління інформаційною безпекою слід притримуватись низки певних принципів і положень.

В першу чергу це законність. Забезпечення ІБ безумовно повинно здійснюватися в суворій відповідності до положень законодавства країни, стандартів, керівних документів у сфері ІБ, локальних нормативних документів. Основними зовнішніми документами є закони України «Про інформацію» від 02.10.1992 №2657-XII, «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 №80/94-ВР, «Про телекомунікації» від 18.11.2003 №1280-IV, «Про захист персональних даних» від 01.06.2010 №2297-VI. Крім того діють Постанови Кабінету Міністрів України від 22.05.1996 р. №558 «Про охорону держсекретів і інформації с обмеженим доступом, що є власністю держави», від 26.02.1998р. №180 «Про забезпечення режиму секретності при обробці інформації з обмеженим доступом в автоматизованих системах», від 13.03.2002р. №281 «Про деякі питання захисту інформації, охорона якої забезпечується державою», від 12.04.2002р. №522 «Про затвердження Порядку підключення до глобальних мереж передачі даних». Існують і відомчі нормативні обов'язкові документи. Наприклад 24.01.2001р. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України видав наказ №76 «Про захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах».[5]

Положення централізації передбачають що процес забезпечення ІБ здійснюється за єдиними організаційними, функціональними та методичними принципами. Доступ до інформації варто надавати тільки в обсягах необхідних для виконання своїх функціональних обов'язків штатним співробітником. При цьому важливим є принцип персональної відповідальності. Це значить що відповідальність за забезпечення ІБ покладається на кожного співробітника в межах його функціональних обов'язків. Об'єктивно потрібна загальна підтримка колективом запропонованих заходив, тобто лояльність керівництва і штатних працівників до різних заходів інформаційної безпеки, взаємне розуміння необхідності їх проведення та персональної відповідальності.

Позитивний ефект досягається безперервністю забезпечення ІБ, це визначається як безперервний процес що включає в себе етапи планування, впровадження, оцінки ефективності та покращення контролю, приведення можливих ризиків до прийнятного рівня у відповідності з пріоритетною діяльністю підприємства. Принцип комплексності встановлює погоджене застосування різноманітних і уніфікованих методів та механізмів забезпечення ІБ в рамках усіх процесів та інформаційних активів підприємства. Дуже важливим є економічний принцип розумної достатності. Він збалансовує рівень витрат на забезпечення інформаційної безпеки з рівнем оплати ризиків інформаційних активів, тобто вартість намічених заходів не може перевищувати вартості реалізації ризиків по відношенню до будь-якого з інформаційних активів.

Підприємству, компанії чи акціонерному товариству, для підтримки свого іміджу та збереження довіри клієнтів, варто мати такий технічний стан, щоб всі засоби забезпечення критичних процесів і сервісів передбачали резервування потужностей з урахуванням їх постійної готовності до збоїв та форс-мажорних обставин.

Висновки

Обґрунтовано, що інформаційна безпека забезпечується створенням на підприємстві, в компанії або в акціонерному товаристві ефективної структури управління інформаційною безпекою.

При цьому необхідно досягти погодженого застосування різноманітних та уніфікованих методів і механізмів забезпечення інформаційної безпеки в межах усіх процесів та інформаційних активів. Наведена класифікація зазначених активів.

Запропонована низка принципів та положень для формування організаційної структури загальної системи управління інформаційною безпекою.

Література

1. Данчук В.Д. Удосконалення методів забезпечення інформаційної безпеки корпоративних інформаційних систем./ 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. Домарев В.В. Безопасность информационных технологий. Системный поход / ТИД "ДС ISBN 966-7992-36-5; 2004 г.. – 29 с.

3. GlobalCorporate IT SecurityRisks: 2013 [Електронний ресурс]. – Режим доступу: http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

4. Брягин О.В. Безопасность вашего бизнеса. Системный подход. Аналитические материалы, практические рекомендации. – К.: КНТ, 2006. – 228 с.

5. Офіційний веб-портал Верховної Ради України [Електронний ресурс] – Режим доступу. http://zakon.rada.gov.uaє

Надійшла 27.01.2016 р. Рецензент: д.т.н., проф. Єрохін В.Ф.