УДК 625.05

О.А. Замула, В.І. Черниш

Харківський національний університет радіоелектроніки, Харків

АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ В ГАЛУЗІ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглянута технологія оцінювання ризиків інформаційної безпеки на основі стандартів ISO/IEC 27001 та BS 7799-3. *Проведений аналіз існуючих методів оцінювання та управління ризиками інформаційної системи.*

Ключові слова: *інформаційна безпека, ризик, аналіз ризиків, моніторинг.*

Вступ

В останні кілька років у світі спостерігається тенденція до стандартизації складових систем управління в організаціях. Ініціатива виходить як на державному рівні, так і на рівні окремо взятих галузей. Серед нормативних актів, що підштовхують організації перебудовувати свою систему інформаційної безпеки (ІБ) та отримали найбільше поширення і популярність, можна відзначити акт Sarbanes-Oxley та угоду з банківського нагляду Basel II.

Sarbanes-Oxley був прийнятий в США з метою контролю за фінансовою звітністю організацій, і в даний час застосовується переважно в цій країні. Стандарт використовують, головним чином, ті компанії, що виходять зі своїми акціями на американські біржі. З боку заходів, які вживаються такими компаніями з точки зору вдосконалення системи ІБ, це передбачає запровадження контролю цілісності, захист від несанкціонованого доступу (НСД), шифрування даних і т.д.

Угода Basel II має більш широку географію розповсюдження: його положення застосовуються в країнах Євросоюзу, США, Японії та ін. Основною метою, сприяти досягненню якої покликаний цей документ, є контроль банківських ризиків. Оцінка ризиків є зараз одним з актуальних напрямків у сфері регулювання банківської діяльності. Головним чином це стосується операційних ризиків, які несуть банки [1]. Серед найбільш значущих з них є ризики ІБ, такі як неадекватні або помилкові дії персоналу та внутрішні процеси.

У загальному випадку можна виділити наступні складові управління ризиками:

– моніторинг та оцінювання організаційних ризиків функціонування системи;

– моніторинг та оцінювання ризиків технічних засобів;

– прийняття рішення з управління ризиками на основі наявних оцінок;

– проведення безпосередньої роботи з управління ризиками [2].

Поступово відходить у минуле підхід, коли окремі вимоги нормативних актів та окремі проблеми інформаційної безпеки вирішуються в порядку виникнення. Багато компаній сьогодні приходять до того, що система захисту інформаційних ресурсів повинна будуватися, виходячи із загальноприйнятих норм і з урахуванням напрацьованих практик. Це допомагає уникнути розбудови інфраструктури інформаційної системи (ІС) в «авральному режимі» під будь-які вимоги і знижує рівень незапланованих витрат на обслуговування системи (у тому числі і ризик витрат, пов'язаних з втратою або крадіжкою інформації).

Аналіз сучасних стандартів в галузі управління інформаційною безпекою систем

Сімейство Міжнародних Стандартів на Системи Управління Інформаційною Безпекою 27000 розробляється ISO/IEC JTC 1/SC 27. Це сімейство включає в себе Міжнародні стандарти, що визначають вимоги до системи управління інформаційної безпеки (СУІБ), управління ризиками, метрики і вимірювання, а також керівництво з впровадження.

Для цього сімейства стандартів використовується послідовна схема нумерації, починаючи з 27000 і далі. ISO 27000 ISO/IEC 27000:2009 Information technology. Security techniques. Information security management systems. Overview and vocabulary (Визначення і основні принципи). Випущений в липні 2009 р.

ISO 27001 ISO/IEC 27001:2005/BS 7799-2:2005 Information technology. Security techniques. Information security management systems. Requirements Інформаційні технології (Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги). Випущений в жовтні 2005 р.

ISO 27002 ISO/IEC 27002:2005, BS 7799-1:2005, BS ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management (Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою (УІБ)). Випущений в червні 2005 р.

ISO 27003 ISO/IEC 27003:2010 Information Technology – Security Techniques – Information Security Management Systems Implementation Guidance (Керівництво з впровадження СУІБ). Випущений в січні 2010 р.

ISO 27004 ISO/IEC 27004:2009 Information technology. Security techniques. Information security man-

agement. Measurement (Вимірювання ефективності СУІБ). Випущений в січні 2010 р.

ISO 27005 ISO/IEC 27005:2008 Information technology. Security techniques. Information security risk management (Інформаційні технології. Методи забезпечення безпеки. Управління ризиками ІБ). Випущений в червні 2008 р.

ISO 27006 ISO/IEC 27006:2007 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems (Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту та сертифікації СУІБ). Випущений в березні 2007 р.

ISO 27007 Керівництво для аудитора СУІБ (в розробці).

ISO 27011 ISO/IEC 27011:2008 Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Керівництво з управління ІБ для телекомунікацій). Випущений в травні 2009 р.

ISO 27033-1 ISO/IEC 27033-1:2009 Information technology. Security techniques. Network security. Overview and concept (Основні концепції управління мережевою безпекою). Випущений в січні 2010 р.

Стандарт ISO/IEC 27001:2005 описує загальну методологію підходу до забезпечення ІБ в організації і акцентує увагу на найбільш критичних складових ІС. Він охоплює елементи управління системою ІБ, актуальні для всіх без винятку сфер бізнесу, такі як: політика ІБ, розподіл відповідальності за ІБ, проведення навчання в цій області, звітність по інцидентах, захист від вірусів, забезпечення безперервності роботи, контроль копіювання ліцензійного програмного забезпечення (ПЗ), захист архівної документації та захист персональних даних. Цей стандарт дає компанії інструмент, що дозволяє управляти конфіденційністю, цілісністю і збереженням такого важливого активу компанії як інформація. Елементи управління системою ІБ розділені в стандарті по декількох груп, і включають в себе розділи:

– політика безпеки – підтримка політики у сфері ІБ з боку керівництва підприємства;

– інфраструктура системи безпеки – створення організаційної структури, яка буде забезпечувати працездатність системи ІБ в організації;

– класифікація ресурсів і управління – пріоритезація інформаційних ресурсів за ступенем їх цінності і розподіл відповідальності за них;

– співробітники – зниження ризику людських помилок, крадіжки і неправильного використання устаткування (навчання співробітників та відстеження інцидентів);

– фізична і зовнішня безпека – запобігання НСД та порушення роботи ІС організації;

– управління мережами і комп'ютерними ресурсами – забезпечення безпечного функціонування комп'ютерів та мереж;

– управління доступом – управління доступом до бізнес-інформації;

– розвиток та обслуговування системи – виконання вимог безпеки при створенні або розвитку інформаційної системи організації, підтримку безпеки додатків і даних;

– забезпечення безперервності бізнесу – план дій у разі надзвичайних обставин для забезпечення безперервності роботи організації;

– відповідність вимогам законодавства – виконання вимог відповідного громадянського та кримінального законодавства, включаючи закони про авторські права і захист даних.

Стандарт складається з двох частин: в першій частині описані механізми контролю (всього їх 127), необхідні для побудови СУІБ. Ця частина використовується в якості основи для проведення аудиту СУІБ в організації. У другій частині стандарту описуються ті критерії, по яких проводиться сертифікація СУІБ. Виходячи з ідеології стандарту ключовим елементом СУІБ є система управління ризиками, найважливішою частина яких є аналіз цих ризиків з метою визначення, які ресурси від яких загроз необхідно захищати, а також якою мірою ресурси потребують захисту. Проведення аналізу ризиків дозволяє організації оцінити можливі збитки в кількісних і якісних показниках. Цей міжнародний стандарт був підготовлений для того, щоб надати модель для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення СУІБ. Передбачається, що прийняття СУІБ є стратегічним для організації [3]. Стандарт приймає процесний підхід для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення СУІБ організації.

Організація для того, щоб задовольнити вимоги даного стандарту, повинна зробити наступне: визначити область програми і межі СУІБ в термінах характеристик бізнесу, її місця розташування, активів і технологій, також включаючи подробиці та обґрунтування будь-яких винятків з області застосування; визначити політику щодо СУІБ в термінах характеристик бізнесу, організації, її місця розташування, активів і технологій; захистом інформації, враховувати законодавчі, нормативні вимоги, визначати стратегії управління інформаційними ризиками; визначити підхід до оцінки ризику в організації; виявити ризики; проаналізувати ризик та оцінити значущість ризику; виявити та оцінити можливості для обробки ризиків; вибрати цілі та засоби керування для обробки ризику. Стандарт рекомендує проводити постійний контроль результативності СУІБ, аналіз цілей управління, беручи до уваги результати аудиту та статистику виникнення порушень.

У відповідності з стандартом ISO/IEC 27001 документація, яка визначає управління інформаційними ризиками організації, повинна включати в себе: документовану заяву про політику та цілі СУІБ; область програми СУІБ; процедури і засоби управління на підтримку СУІБ; опис методології оцінки ризиків; звіт про оцінки ризиків; план обробки ризиків [3]. В стандарті наголошується відповідальність керівництва в організації управління інформаційними ризиками. У розділі розглядаються види зобов'язань керівництва, деякі принципи менеджменту ресурсів і забезпечення

необхідного рівня компетентності персоналу. Стандарт розглядає основні цілі та принципи проведення аудиту захищеності організації від загроз в інформаційній сфері, а також аналіз СУІБ з точки зору керівництва. У стандарті зазначено основні вхідні і вихідні дані для внутрішнього аудиту. В якості важливих результатів аудиту можна виділити оновлення оцінки ризиків для організації та відповідно зміну методів управління ними. Заключна частина стандарту присвячена принципу постійного поліпшення в СУІБ.

Стандарт Великобританії BS 7799 присвячений УІБ організації. Цей стандарт є одним з найбільш авторитетних в світі. На його базі розроблено міжнародний стандарт ISO/IEC 17799, котрий згодом еволюціонував в ISO/IEC 27002. Третя частина даного стандарту присвячена питанням управління інформаційними ризиками.

Стандарт BS 7799-3:2006 гармонізований з ISO/IEC 17799:2005 щодо прикладів по компонентах системи захисту. Стандарт допускає використання будь-яких стратегій організації оцінки ризиків, зокрема викладених у ISO 13335-3.

Стандарт BS 7799-3 містить вступну частину, розділи з оцінки ризиків, обробці ризиків, безперервним дій з управління ризиками, а також має додаток з прикладами активів, погроз, вразливостей, методів оцінки ризиків. Стандарт дотримується самого загального поняття ризику, під яким розуміють комбінацію ймовірності події і його наслідків. Управління ризиків сформульовано як скоординовані безперервні дії з управління та контролю ризиків в організації.

Оцінка ризиків – перший етап в управлінні системи ІБ, призначеної для ідентифікації джерел ризиків і визначення його рівня значущості. Оцінку розбивають на аналіз ризиків та оцінювання ризиків. У рамках аналізу проводиться інвентаризація та категоризація ресурсів, що захищаються, з'ясовуються нормативні, технічні, договірні вимоги до ресурсів в сфері ІБ, а потім, з урахуванням цих вимог, визначається вартість ресурсів. Наступним етапом аналізу ризиків є складання переліку значущих загроз та вразливостей для кожного ресурсу та обчислення ймовірності їх реалізації. Стандарт допускає двояке тлумачення поняття загрози ІБ: як умова реалізації вразливості ресурсу, і, як загальне, потенційна подія, здатна призвести до компрометації ресурсу. Оцінювання ризику проводиться шляхом його обчислення і порівняння з заданою шкалою. Обчислення ризику полягає в множенні ймовірності компрометації ресурсу на значення величини збитку, пов'язаного з його компрометацією. BS 7799-3 допускає використання як кількісних, так і якісних методів оцінки ризиків, але, на жаль, в документі немає обґрунтування та рекомендацій по вибору математичного і методичного апарату оцінки ризиків ІБ. Додаток до стандарту містить єдиний приклад, який умовно можна віднести до якісного методу оцінки. Даний приклад використовує трьох-і п'ятибальні оціночні шкали:

– оцінюються рівні вартості ідентифікованого ресурсу за п'ятибальною шкалою: «незначний», «низький», «середній », «високий», «дуже високий»;

– оцінюються рівні можливості загрози за трибальною шкалою: «низький», «середній », «високий»;

– оцінюються рівні ймовірності вразливості: «низький», «середній », «високий»;

– за заданою таблицею розраховуються рівні ризику;

– проводиться ранжування інцидентів за рівнем ризику.

Після того як ризик оцінений, повинно бути ухвалено рішення щодо його обробки – точніше, вибору та реалізації заходів та засобів з мінімізації ризику. Крім оціненого рівня ризику, при прийнятті рішення можуть бути враховані витрати на впровадження та супровід механізмів безпеки, політика керівництва, простота реалізації, думка експертів та ін.

У результаті обробки ризику залишається так званий залишковий ризик, щодо якого приймається рішення про завершення етапу відпрацювання ризику. На жаль, в стандарті BS 7799-3 нічого не сказано про ефективність заходів, засобів і сервісів, які можуть бути використані при обробці ризику.

Розділ 7 BS 7799-3 «Безперервна діяльність з управління ризиками» відповідає на наступні дві фази менеджменту системи: контроль ризику та оптимізація ризику. Для контролю ризику рекомендуються технічні заходи (моніторинг, аналіз системних журналів та виконання перевірок), аналіз з боку керівництва, незалежні внутрішні аудити ІБ. Фаза оптимізації ризику містить переоцінку ризику і, відповідно, перегляд політик, керівництва з управління ризиками, корегування та оновлення механізмів забезпечення безпеки.

Процедури контролю ризиків і оптимізації, включаючи використання політик, заходів і засобів безпеки, ідентифікацію ресурсів, загроз та вразливостей, документування, гармонізовані з ISO/IEC 27001 та 27002. Відмінною рисою стандарту є принцип обізнаності про процеси оцінки, відпрацювання, контролю та оптимізації ризиків в організації. На кожному етапі управління ризиками передбачено інформування всіх учасників процесу управління безпекою, а також фіксування подій СУІБ. Стандарт перераховує обов'язки і задає вимоги до категорії осіб, що безпосередньо беруть участь при управлінні ризиками, а саме: експертам з оцінки ризиків, менеджерам з безпеки, менеджерам ризиків безпеки, а також власникам ресурсів і навіть керівництву організації [4].

Основними видами інформаційних активів, які зачіпаються при управлінні інформаційними ризиками, відповідно до документа, є: процеси та служби інформаційної системи; програмне забезпечення; технічні засоби; людські ресурси; нематеріальні ресурси – репутація, імідж організації, а також інші нематеріальні фактори, що впливають на ведення бізнесу.

Наведений у стандарті метод оцінки ризиків є універсальним, але при цьому не передбачає використання якоїсь певної методології оцінки ризиків. Це породжує певну неоднозначність у виборі методів управління ризиками.

В основі наведеного в стандарті методу оцінки зазвичай лежать зважені якісні оцінки. Природно, такий метод не позбавлений недоліків, а саме:

– проблеми завдання масштабу при побудові якісних шкал;

– проблеми адекватності експертної оцінки;

– неможливості визначити, які параметри системи і якою мірою впливають на загальний рівень ризику.

Це ускладнює управління ризиками та говорить про актуальність розробки універсальної методології оцінки та управління інформаційними ризиками, яка б дозволяла спільно використовувати аналітичні та якісні методи.

Аналіз існуючих методів оцінювання та управління ризиками інформаційної системи

Як показує огляд інформаційних джерел, у галузі оцінки та управління інформаційними ризиками на даний момент переважають експертні методи їх оцінки. Це обумовлено, перш за все, відсутністю узагальнених статистичних даних по реалізації загроз в інформаційній сфері для систем. Часто доводиться використовувати достовірну статистику спільно з експертними оцінками. Експертні оцінки зазвичай є оцінки ймовірності настання подій, а також приблизні значення збитку відповідні цим подіям. На основі цих даних проводиться розрахунок ризику системи. Таким чином, для управління ризиками оцінка суб'єктивної ймовірності є ключовим моментом [5].

Застосування методів експертної оцінки має очевидні недоліки, такі, як їх суб'єктивність, великі похибки при використанні їх в аналітичних розрахунках.

Необхідно відзначити також існуючі кількісні методи, що існують для оцінок ризику. Вони зазвичай використовують накопичену статистику і оперують з ймовірностями, отриманими в результаті статистичних розрахунків [6]. Недоліком таких методів є необхідність накопичення досить великих обсягів статистичних даних для отримання точних прогнозів щодо рівня ризику.

Оцінка ризику експертними методами має перевагу у вигляді достатньої простоти застосування в умовах відсутності об'єктивних даних про величини ймовірностей виникнення подій, і величинах збитку. Ефективністю такого способу оцінки інформаційних ризиків можна керувати шляхом зміни складу експертної групи, а також підвищенням рівня підготовки її учасників.

Висновки

Застосування згаданих нормативних актів передбачає, як правило, часткову зміну IT-інфраструктури організації і, в тому числі, перебудову системи ІБ як частини цієї інфраструктури, а також зміну підходу до її побудови. Вплив даних нормативних актів на формування СУІБ компаній має непрямий характер, але підштовхує керівництво замислитися про те, наскільки дії і засоби, що застосовуються в цілях захисту інформації, адекватні та ефективні. Будь-який стандарт робить компанію більш прозорою для взаємодіючих з нею контрагентів, так як повідомляє про те, що параметри в цій організації відповідають певним нормативам – перевірено та підтверджено авторитетним джерелом. Це може відноситися до якості продукції, методів управління, і, в тому числі, до системи ІБ. Стандартизуючи свою систему, компанія забезпечує необхідну і достатню ступінь прозорості її структури для своїх партнерів і клієнтів, що, у свою чергу, дає їм упевненість у забезпеченні належного рівня захисту тієї інформації, яку вони довіряють цій організації: персональних даних, ділової інформації і т. д. Це підвищує лояльність всіх взаємодіючих контрагентів один до одного, і позитивно позначається на веденні бізнесу.

Список літератури

1. Северинов А.В. Анализ угроз и рисков безопасности информации в беспроводных сетях / А.В. Северинов, В.И. Черныш //Системи управління, навігації та зв'язку. – К.: ЦНДІ НіУ, 2011. – Вип. 1(17). – С. 229-232.

2. ГОСТ Р ИСО/МЭК 17799-2005.

3. ГОСТ Р ИСО/МЭК 27001.

4. Марков А. Нормативный вакуум информационной безопасности / А. Марков, В. Цирлов // Открытые системы. – 2007. – №8.

5.Петренко С.А. Управление информационными рисками: Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: АйТи-Пресс, 2004. – 381 с.

6. Федотов Н.С. Оценка и нейтрализация рисков в информационных системах: метод. пос. / Н.С. Федотов, В.С. Алешин. – М.: МГТУ им. Н.Э.Баумана, 2004. – 52 с.

Надійшла до редколегії 1.03.2011

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Харківський національний технічний університет сільського господарства ім. П. Василенка, Харків.

АНАЛИЗ МЕЖДУНАРОДНЫХ СТАНДАРТОВ В ОБЛАСТИ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Замула, В.И. Черныш

Рассмотрена технология оценки рисков информационной безопасности на основе стандартов ISO/IEC 27001 и BS 7799-3. Проведенный анализ существующих методов оценки и управления рисками информационной системы.

Ключевые слова: *информационная безопасность, риск, анализ, стандарты ISO/IEC 27001 и BS 7799-3.*

ANALYSIS OF INTERNATIONAL STANDARTS IN RISK ASSESSMENT OF INFORMATION SECURITY

A.A. Zamula, V.I. Chernish

The general methodology for risk assessment of information security standards based on ISO/IEC 27001 and BS 7799-3. The analysis there exist methods of risk assessment and management information system.

Keywords: *information security, risk analysis, standards of ISO/IEC 27001 and BS 7799-3.*