- створити узгоджений понятійний апарат і єдину термінологію з надання послуг у СЗІБ, яка буде зрозумілою постачальникам та споживачам послуг;
- створити загальновизнану систему класифікації послуг у СЗІБ, що дозволить забезпечити єдиний правовий режим їх надання;
- розробити та впровадити методологію розрахунку цін на надання послуг у СЗІБ.

Література: ***1.*** *Соглашение о сотрудничестве государств–участников Содружества Независимых Государств в области обеспечения информационной безопасности [Електронний ресурс]. – Режим доступу: http://adilet.minjust.kz/rus/docs/P1200000692* ***2.*** *Закон України Про ліцензування певних видів господарської діяльності [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1775-14* ***3.*** *Постанова КМУ від 25.05.2011 № 543 Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/543-2011-%D0%BF* ***4.*** *Постанова КМУ від 18.05.2011 № 517 Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/517-2011-%D0%BF* ***5.*** *DiaWest: в 2011 году рынок корпоративных услуг вырос на 35% [Електронний ресурс]. – Режим доступу: http://www.apitu.org.ua/node/2341* ***6.*** *Закон України Про ціни і ціноутворення [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/5007-17* ***7.*** *Наказ ДСТСЗІ СБУ від 14.07.2004 № 56 Про затвердження Граничних тарифів на послуги конфіденційного зв'язку [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0909-04* ***8.*** *В Україні лише третина населення має доступ до інтернет [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2012/09/25/6973396/* ***9.*** *Исследование: 17,6 млн украинцев регулярно пользуются интернетом [Електронний ресурс]. – Режим доступу: http://biz.liga.net/all/it/novosti/2262042-17-6-mln-ukraintsev-polzuyutsya-internetom-issledovanie.htm* ***10.*** *Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – [проект]. - К.: Національний банк України 2010. – 49 с.: табл. – (Галузевий стандарт України).* ***11.*** *Валерий Васильев Услуги в области ИТ-безопасности [Електронний ресурс]. – Режим доступу: http://www.pcweek.ru/security/article/detail.php?ID=141643* ***12.*** *Ткаченко В. В. Дорожная карта специалиста по ИБ [Електронний ресурс]. – Режим доступу: http://www.trn.ua/articles/2144/* ***13.*** *Постанова КМУ від 11.04.2012 № 295 Про затвердження Правил надання та отримання телекомунікаційних послуг [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/295-2012-%D0%BF* ***14.*** *Копитін Ю. В. Модель страхування ризиків інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://digitech.onat.edu.ua/files/13.pdf* ***15.*** *А. А. Анисимов Менеджмент в сфере информационной безопасности [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/department/itmngt/manofis/* ***16.*** *Рекомендация МСЭ-Т X.1205 Обзор кибербезопасности [Електронний ресурс]. – Режим доступу: http://www.itu.int/* ***17.*** Анна Кожина *Основной движущей силой рынка ИБ будут мобильные и облачные технологии [Електронний ресурс]. – Режим доступу: http://www.itbestsellers.ru/experts/detail.php?ID=19880*

УДК 004.056.53(045)

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА БАЗІ МІЖНАРОДНИХ СТАНДАРТІВ СЕРІЇ ISO

Анна Чунарьова, Андрій Чунарьов
Національний авіаційний університет

Анотація: **Проведено аналіз сучасних заходів управління інформаційною безпекою інформаційних мереж на базі міжнародних стандартів серії ISO. Виділено ряд переваг застосування системи управління інформаційною безпекою. Запропоновано сценарій управління ризиками інформаційної безпеки та розроблену структурну схему оцінки інформаційних ризиків інформаційної мережі підприємства.**

Summary: **An analysis of contemporary events information security management of information networks based on international standards of series ISO. Highlighted a number of advantages of information security management system. We propose a scenario of risk management information security and developed a structural block diagram of information risk assessment information network.**

Ключові слова: **Інформаційна безпека, оцінка ризиків, управління інформаційною безпекою, модель**

порушника, модель загроз.

I Вступ

Сучасний етап розвитку інформаційної безпеки потребує комплексного підходу до розробки та впровадження методів і засобів захисту ресурсів інформаційно-комунікаційних систем та мереж (ІКСМ) як на технічному, так і організаційному рівні, тобто реалізації комплексного процесу. Комплексний процес організації безпеки в першу чергу має включати заходи управління інформаційною безпекою. Зазначений процес забезпечує механізми та методи, які дозволяють реалізувати комплексну політику інформаційної безпеки організації ІКСМ. Інформаційна безпека – реалізація процесу захисту інформації від широкого діапазону загроз (внутрішніх та зовнішніх), що здійснюється з метою забезпечення ефективності та надійності функціонування ІКСМ.

II Постановка задачі

Міжнародні стандарти серії ISO (ISO/IEC 17799, ISO 27001, ISO 27002) є основоположними в сфері управління інформаційною безпекою. Вони являють собою модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування та удосконалення системи безпеки, відповідальність співробітників і оцінку ризику.

Основна ідея стандартів серії ISO – забезпечення надійного захисту інформаційних ресурсів ІКСМ та організація ефективного доступу до даних й процесу їх обробки згідно з визначеними послугами.

Метою даною статті є аналіз сучасних заходів управління інформаційною безпекою ІКСМ на базі міжнародних стандартів ISO, виділення переваг застосування системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO і на основі проведеного аналізу розробити сценарій управління ризиками інформаційного об'єкту корпоративної мережі та структурну схему оцінювання інформаційних ризиків на базі міжнародних стандартів серії ISO.

III Основна частина

Заходи управління інформаційною безпекою

Сучасні ІКСМ уразливі до низки мережних загроз, які можуть бути результатом реалізації несанкціонованого доступу, а також розкриття, викривлення або модифікації інформації. Щоб захистити сучасні інформаційні ресурси та послуги від загроз, необхідно застосовувати відповідні заходи управління безпекою.

Під ***управлінням інформаційною безпекою*** будемо розуміти циклічний процес, що включає: постановку задачі захисту інформації; збір та аналіз даних про стан інформаційної безпеки в ІКСМ; оцінку інформаційних ризиків; планування заходів з обробки ризиків; реалізацію і впровадження відповідних механізмів контролю; розподіл ролей і відповідальності; політику безпеки; навчання та мотивацію персоналу, оперативну роботу зі здійснення захисних заходів; моніторинг (аудит) функціонування механізмів контролю, оцінку їх ефективності та надійності. Процес впровадження системи управління інформаційною безпекою включає оцінку поточного стану інформаційного забезпечення захисту інформації ІКСМ, формування комплексу заходів щодо забезпечення оптимального рівня на основі оцінки ризиків.

Після ідентифікації вимог безпеки варто вибирати й застосовувати заходи управління таким чином, щоб забезпечувати впевненість у зменшенні ризиків від реалізації несанкціонованого доступу. Засоби управління можуть бути обрані зі стандартів або з безлічі інших документів та заходів управління, визначених для даного класу систем, або можуть бути розроблені, щоб задовольнити потреби компанії відповідно до обраної політики інформаційної безпеки. Згідно з міжнародним стандартом ISO 27001, система управління інформаційною безпекою – це «*частина загальної системи управління організації, яка заснована на оцінці ризиків, створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення загальної інформаційної безпеки*».

Відповідно до вимог ISO/IEC 27001 система управління інформаційною безпекою повинна містити такі етапи [1, 2] :

1 етап - *планування* - фаза створення: створення переліку інформації, оцінки ризиків і вибору заходів та механізмів захисту;

2 етап - *дія* - етап реалізації та впровадження відповідних заходів;

3 етап - *перевірка* - фаза оцінки ефективності та надійності функціонування створеної системи. Проведення внутрішнього аудиту системи, виявлення недоліків.

4 етап - *удосконалення* - виконання коригувальних дій з покращення функціонування системи;

При створенні системи управління інформаційною безпекою потрібно керуватися відповідними заходами

з метою підвищення ефективності захищеності сучасних ІКСМ. Заходи управління варто вибирати, ґрунтуючись на відношенні вартості реалізації послуг та впровадження систем безпеки й зниження ризиків і можливих втрат, якщо відбудеться порушення безпеки ІКСМ. Деякі з заходів управління в стандартах та нормативних документах можуть розглядатися як керівні принципи для управління інформаційною безпекою й можуть бути застосовані для організації політики безпеки. Розглянемо заходи управління інформаційною безпекою із законодавчої точки зору та узагальнені для сучасних ІКСМ [3].

Якщо розглядати заходи управління з законодавчої точки зору, *то вони включають*:

- захист даних і таємність особистої інформації;
- охорону інформаційних ресурсів організації;
- права на інтелектуальну власність.

Заходи управління сучасних ІКСМ включають :

- документи, що стосується політики інформаційної безпеки;
- розподіл обов'язків, пов'язаних з інформаційною безпекою;
- структура підрозділів й навчання, пов'язані з інформаційною безпекою ;
- повідомлення про інциденти, пов'язані з безпекою ;
- управління безперервністю.

Слід зазначити, що всі заходи управління в стандартах та нормативних документах є важливими, але застосування якого-небудь засобу управління має відповідати ризикам та можливим загрозам даної ІКСМ.

В загальному випадку система управління безпекою повинна включати (рис. 1) :

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

Переваги застосування системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO:

- *Забезпечення неперервності.* Від якості застосовуваних новітніх технологій захисту інформації залежить не тільки збереження конфіденційності та цілісності інформації, а й взагалі існування конкретних інформаційних і телекомунікаційних сервісів, послуг та програм.
- *Мінімізація ризиків.* Впровадження системи управління інформаційною безпекою дозволяє зменшити інформаційні ризики, розкрадання і неправильне використання обладнання, пошкодження та порушення роботи інформаційної системи організації за рахунок розмежування фізичного доступу та впровадження механізму моніторингу (аудиту) стану інформаційної безпеки. Оцінка та мінімізація ризиків дозволяє ідентифікувати загрози інформаційним ресурсам та послугам, оцінити їх уразливість і ймовірність виникнення загроз, а також можливий руйнівний вплив при реалізації несанкціонованого доступу.
- *Зниження витрат на інформаційну безпеку.* Застосування передових технологій зі створення, моніторингу та поліпшення інформаційної безпеки дозволяє знизити витратну частину бюджету, що спрямована на забезпечення інформаційної безпеки.
- *Забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів ІКСМ.*
- *Забезпечення комплексного та централізованого контролю рівня захисту інформації.*

Система управління інформаційною безпекою.

Підхід до управління ризиками інформаційної безпеки на базі міжнародних стандартів серії ISO є проактивним та здатним допомогти інформаційним системам організацій різних рівнів та будь-якого розміру у вирішенні проблем, що виникають в процесі забезпечення відповідності інформаційної безпеки регулятивним нормам. Найбільш значними стандартами інформаційної безпеки у сфері управляння інформаційної безпеки є: критерії безпеки комп'ютерних систем, європейські критерії безпеки інформаційних технологій, федеральні критерії безпеки інформаційних технологій, канадські критерії безпеки комп'ютерних систем, загальні критерії безпеки інформаційних технологій та сім'я стандартів ISO. Усі вони визнають значення процесу управління ризиками, базові методи та затверджують концепцію процесу створення, впровадження, використання, моніторингу, перевірки, підтримання та вдосконалення системи захисту організації.

Для ефективного функціонування організації доводиться ідентифікувати та управляти багатьма процесами, а саме процесом управління ризиками інформаційного об'єкту. Процес управління ризиками безпеки дозволяє організаціям досягти поєднання максимальної економічної ефективності з відомим та прийнятним рівнем ризику та надає керівникам різних рівнів зрозумілий метод організації та пріоритизації ресурсів з обмеженим доступом для реалізації управління ризиками. Реалізація управління ризиками безпеки дозволяє організаціям з розподіленими корпоративними мережами використовувати економічно ефективний

контроль, що знижує ризик до прийнятного рівня. Визначення допустимого ризику та підхід до управління ризиками залежать від структури конкретної інформаційної системи, її розподіленості, оскільки не існує універсального рішення, а різні організації використовують різні моделі управління ризиками. Кожна модель пропонує власне поєднання точності, ресурсів, часу, складності та суб'єктивності. Інвестиції в процес управління ризиками заснований на перевіреній концепції та чіткому визначенні ролей та обов'язків. Крім того, ефективна програма управління ризиками допоможе розподіленим корпоративним мережам забезпечити дотримання чинних законодавчих вимог з забезпечення гідного рівня інформаційної безпеки. Оцінювання ризиків організації є первинним етапом при розробці та експлуатації захищених інформаційних систем. Через оцінки ризиків ідентифікуються загрози активам, оцінюються їх уразливість й імовірність виникнення загроз, а також можливий руйнівний вплив під час реалізації несанкціонованих дій. Далі запропоновано сценарій управління ризиками інформаційного об’єкту (рис. 1).

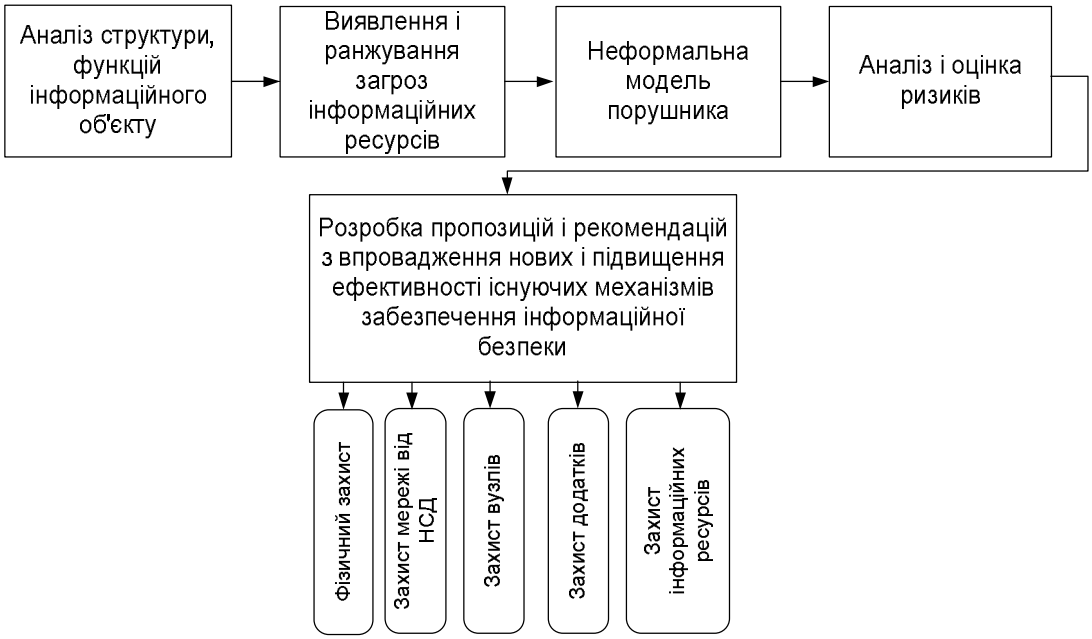

Рисунок 1 – Сценарій управління інформаційною безпекою підприємства

Запропонований сценарій розрахунку ризиків складається з наступних базових складових, а саме:

– визначення методології оцінювання ризику для інформаційної системи;

– розроблення критеріїв ухвалення ризиків та визначення прийнятого рівня ризику;

– визначення активів;

– виявлення небезпеки для активів;

– виявлення вразливих місць в системі захисту;

– виявлення дій, які порушують конфіденційність, цілісність та доступність активів та інформаційної ситсеми;

– визначення ймовірності провалу системи безпеки за наявності переважних небезпек та вразливостей;

– оцінювання рівнів ризику;

– визначення прийнятності ризику або проведення процедури скорочення, використовуючи встановлені критерії допустимості та прийнятності ризику;

– вибір завдань та засобів управління для скорочення ризиків з умов забезпечення ефективності захисту.

Завдання та засоби управління мають бути вибрані та впроваджені відповідно до вимог, встановлених процесом оцінки ризиків та скорочення ризиків згідно з ISO 27002. Цей вибір повинен враховувати як критерії з допустимості ризику, так і юридичні, регулятивні та договірні вимоги. Впровадження даного сценарію дозволяє підвищити ефективність та надійність створеної системи захисту інформації на базі проведення оцінки ризиків, яка визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, методи забезпечення безпеки, практичні правила та вимоги, відповідальність співробітників, використання оцінювання ризику в контексті інформаційної безпеки підприємств. У процесі

впровадження даного сценарію створюється система менеджменту інформаційної безпеки. Метою створеної системи менеджменту інформаційної безпеки є скорочення матеріальних втрат, пов'язаних з порушенням інформаційної безпеки. На основі запропонованого сценарію розроблена структурна схема оцінювання інформаційних ризиків (рис. 2)

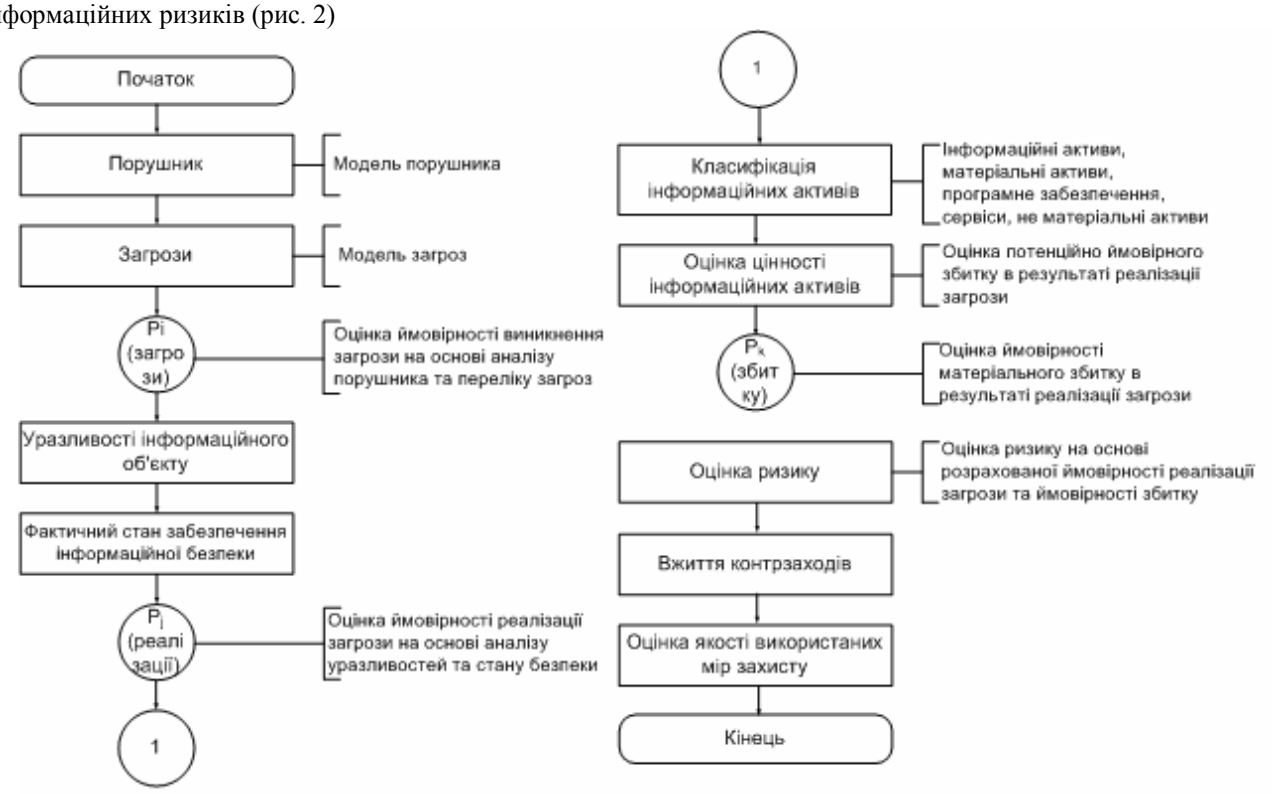

Рисунок 2 – Структурна схема оцінювання інформаційних ризиків

IV Висновки

На основі проведеного аналізу сучасних заходів управління інформаційною безпекою ІКСМ на базі міжнародних стандартів ISO виявлено, що управління безпекою ІКСМ є важливим аспектом забезпечення безпеки властивостей інформаційних ресурсів та послуг в мережах передачі даних. Для досягнення й підтримки безпеки в інформаційно-комунікаційних системах та мережах потрібен певний діапазон засобів та заходів управління. В роботі виділено ряд переваг застосування системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO в сучасних ІКСМ.

Також запропоновано сценарій управління ризиками інформаційної безпеки та розроблену структурну схему оцінювання інформаційних ризиків корпоративної мережі підприємства.

Література: ***1.*** *ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management.* ***2.*** *ISO/IEC 27001:2005, Information Security Management - Specification With Guidance for Use.* ***3.*** *Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.* ***4.*** *Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. – М.: Горячая линия – Телеком, 2004. – 280 с.*