УДК 004.413.4

Т. В. Савельєва, *к.т.н, доцент,*
e-mail: tam2003@ukr.net
О. М. Панаско, *к.т.н, доцент,*
e-mail: lena.pa@ukr.net
О. М. Пригодюк
e-mail: prigoduk@ukr.net
Черкаський державний технологічний університет,
б-р Шевченка, 460, Черкаси, 18006, Україна

АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ДЛЯ РЕАЛІЗАЦІЇ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Стаття присвячена актуальній проблемі сучасності – розвитку інформаційної безпеки з урахуванням ризик-орієнтованого підходу для вирішення задач управління інформаційною безпекою підприємства. Сучасні тенденції розвитку підприємств обумовлюють необхідність управління ризиками. Авторами досліджено методи та засоби, що дають можливість реалізувати ризик-орієнтований підхід у контексті забезпечення інформаційної безпеки підприємства і провести аналіз та оцінювання інформаційних ризиків системи захисту інформації. В роботі розглянуто серію представників інструментальних засобів, найбільш поширених в зазначеній сфері, а також проаналізовано кілька методологій, за допомогою яких здійснюється оцінювання ризиків, зокрема, методологія аналізу і управління ризиками CRAMM (Великобританія), оцінювання активів і уразливості інформаційної безпеки OCTAVE тощо, а також серію регулятивних документів, серед яких NIST SP800-30 (управління ризиками в системі інформаційних технологій); ISO/IEC 27005:2011 (методи управління ризиками інформаційної безпеки); ENISA (оцінювання ризиків інформаційної безпеки) і багато інших. В роботі представлено аналіз переваг та недоліків програмного забезпечення для визначення і оцінювання ризиків інформаційної безпеки (CRAMM, CORAS, Risk Watch, OCTAVE, Oracle Crystal Ball) і сформовано ряд рекомендацій щодо доцільності застосування розглянутих програмних засобів та управляючої документації з урахуванням відповідних потреб і критеріїв підприємств та організацій.

Ключові слова: *інформаційні технології, інформаційна безпека, загрози, вразливість, інформаційні ризики, оцінювання ризику.*

Постановка проблеми. Актуальність теми обумовлена тим, що протягом останніх років інформація стала відігравати важливу роль в усіх сферах людського життя, що пов'язано з поступовим становленням інформаційного суспільства.

В умовах сьогодення для підвищення показників ефективності і працездатності складних систем застосовують сучасні інформаційні технології та системи, внаслідок чого інформація виступає універсальним товаром для взаємовідносин між різними структурами підприємства чи організації. Питання її захисту набувають великої актуальності. Особливе значення відводиться оптимальному проектуванню систем захисту, що дозволяє з найбільшою ймовірністю вибирати найкращі рішення на множині альтернатив. В наші часи це стає актуальним для більшості підприємств, оскільки правильно спроектована і впроваджена система захисту буде запорукою успішного функціонування і конкурентоспроможності всієї організації.

Зважаючи на ускладнення комп'ютерних систем і збільшення кількості загроз, виникає потреба в оцінюванні інформаційної безпеки таких систем.

Оцінювання ризиків порушення інформаційної безпеки є однією з найважливіших складових процесу управління інформаційною безпекою. В результаті питання необхідності оцінювання ризиків інформаційної безпеки для побудови ефективних систем захисту інформації на підприємстві є актуальним. Згідно зі стандартом ISO/IES 17799:2000 [1] оцінювання ризиків інформаційної безпеки визначається як систематичний аналіз можливої шкоди, що завдається бізнесу в результаті

порушень інформаційної безпеки, з урахуванням можливих наслідків від втрати конфіденційності, цілісності або доступності інформації та інших ресурсів і ймовірності настання такого порушення, враховуючи існуючі загрози, вразливості, а також впроваджені заходи захисту [1].

Існує цілий ряд методів оцінювання ризиків, зокрема, *CRAMM, CORAS, Risk Watch, OCTAVE, Oracle Crystal Ball*.

Аналіз останніх досліджень і публікацій. На сьогоднішній день дослідженням в галузі забезпечення інформаційної безпеки в комп'ютерних системах та мережах приділяється велика увага. В цьому контексті слід відзначити роботи Замули А. А., Сєвєрінова О. В., Корнієнка М. О., Гарасима Ю. Р., Ромака В. А., Рибія М. М., Левадного С. М. та інших.

В [2] автори дослідили ризики інформаційної безпеки, провели аналіз моделей на основі матриці системи управління інформаційною безпекою, включаючи якісні й кількісні шкали, а також на базі теорії нечітких множин. Автори праці [3] займалися вирішенням задачі управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. Переваги та недоліки методів оцінювання інформаційних ризиків (ІР) можна спостерігати в праці [4] Левадного С. М.

В цьому напрямку також слід відзначити роботи Юдіна О. К., Горбенка І. Д., Домарьова В. В., Корченка О. Г., Луцького М. Г. Досліджувана проблематика знайшла своє відображення і в багатьох працях зарубіжних вчених, таких як Астахов А. М., Daniel Wentre, Thomas R., Whitman M. E. Abdallah, Vicki Chen, H. Sassanein, Sanjay Goel та ін.

Динамічність ринкового середовища, виникнення кризових ситуацій, зміни в системі функціонування і розвитку підприємств та організацій, поява нових серйозних загроз інформаційній безпеці спричиняють виникнення нових питань і проблем, які супроводжують запровадження інформаційних технологій та їх захист, а тому потребують більш глибокого аналізу та вивчення можливих шляхів їх подолання.

Метою роботи є дослідження та аналіз методів і засобів з метою реалізації ризик-орієнтованого підходу для проектування ефективної системи захисту інформації підприємств та організацій і забезпечення їх інформаційної безпеки.

Виклад основного матеріалу. Інформаційні системи і технології являють собою комплекс програмно-технічних засобів і методів виробництва, передачі, обробки та споживання інформації. Метою їх впровадження є створення системи, в якій інформаційні потоки налагоджені таким чином, що користувачі з мінімальними витратами одержують доступ до необхідної інформації в той час, коли вона потрібна, і там, де вона потрібна, а базовими принципами є: релевантність, час та місце [5, 6].

Оскільки інформація перестала бути просто необхідним допоміжним ресурсом для виробництва, а набула відчутної вартісної ваги, яка чітко визначається реальним прибутком, що одержується при її використанні, або розмірами збитку, з різним ступенем ймовірності завданого власнику інформації в разі її спотворення або втрати, проблема забезпечення інформаційної безпеки набула в умовах сьогодення виняткового значення.

Якщо інформація підприємства становить державну таємницю, то процес створення систем захисту інформації (СЗІ) полягає в задоволенні нормативним вимогам із застосуванням спеціального обладнання, програмного забезпечення та залученням спеціалізованих організацій. У комерційних організаціях, в яких наявна інформація, що становить комерційну та професійну таємниці, а також персональна інформація, процес побудови СЗІ повинен ґрунтуватися на аналізі ризиків.

Ризик – функція ймовірності реалізації певної загрози, що використовує деякі уразливості, і величини можливого збитку.

Аналіз інформаційних ризиків – це процес оцінювання ступеня захисту інформаційної системи (ІС) разом з визначенням кількісних (у формі грошових ресурсів) і якісних (рівні ризику: високий, середній, низький) показників ризику. Аналіз ІР здійснюється за допомогою різних інструментів і методів формування процесів захисту інформації. На основі його результатів виділяють найкритичніші ризики, які є небезпечною загрозою і потребують негайного вжиття додаткових захисних заходів.

Аналіз ІР є основою для побудови підсистеми управління інформаційною безпекою підприємства. В ході аналізу та оцінювання

рівня ІР слід дотримуватися таких кроків: ідентифікація інформаційних ресурсів (активів) компанії, що можуть бути об'єктом ризику, можливих загроз активу та визначення рівня загроз безпеці КІС підприємства; оцінювання рівня дієвості засобів контролю безпеки корпоративної системи; оцінювання вразливості корпоративної системи, що розглядається як результат впливу факторів вірогідного рівня сили загрози та рівня дієвості засобів контролю; оцінювання частоти подій втрат від інформаційних ризиків як результату впливу факторів частоти виникнення загрози та вразливості корпоративної системи; оцінювання величини можливих збитків від інформаційних ризиків в корпоративній системі; оцінювання рівня інформаційних ризиків в корпоративній системі як результуючій двох факторів: частоти подій втрат і величини можливих втрат від інформаційних ризиків [7].

Управління ризиками – процес, що включає аналіз ризиків, вибір, реалізацію та оцінювання ефективних і економічних контрзаходів, перевірку встановлення ризиків на прийнятному рівні.

Ризик-орієнтований підхід висвітлює перелік небезпек, робить запобіжні заходи їх уникнення більш осмисленими і цілеспрямованими [8]. Основним завданням ризик-орієнтованого підходу є створення реальних наукових основ організації безпеки складних технічних систем. За оцінками експертів, його впровадження дає змогу за рахунок підвищення ефективності заходів на порядок скоротити витрати на створення безпечних систем (рис. 1).

Ризик-орієнтований підхід до вирішення задач управління інформаційною безпекою лежить в основі всіх міжнародних і галузевих стандартів на системи менеджменту (ISO 27001, ГОСТ Р 27001, СТО БР ІББС, Basel II, UK Turnbull Guidance, SOX, COSO ERM-Integrated Framework і т. д.) і забезпечує суттєві переваги організації, що його застосовує.

Для організацій, які не застосовують ризик-орієнтований підхід до управління інформаційною безпекою, характерні особливості, що зображені на рис. 2.

Мета аналізу ризиків: визначити цілі управління ІБ; оцінити основні критичні області, що негативно впливають на ключові бізнес-процеси організації; розробити ефективні і обґрунтовані рішення для контролю або мінімізації виявлених ризиків; визначити баланс між можливими збитками від витоку інформації та розміром витрат на ІБ; наочно представити і обґрунтувати структуру витрат на інформаційну безпеку для керівництва.

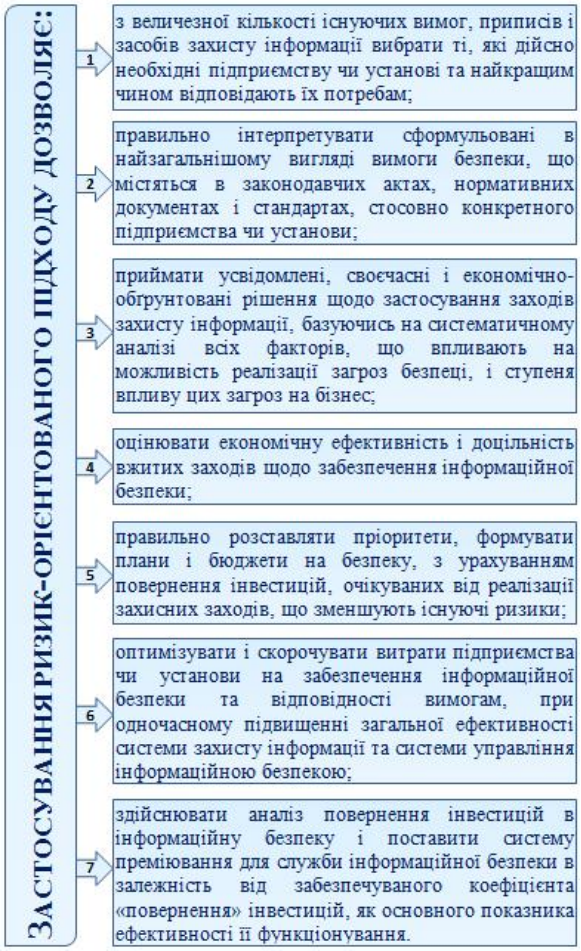

Рис. 1. Переваги ризик-орієнтованого підходу до управління інформаційною безпекою

Методи та засоби оцінювання ІР у систематизованому вигляді зображено на рис. 3.

Метод – систематизована сукупність кроків, дій, які необхідно виконати для розв'язання певного завдання чи досягнення поставленої мети, дати оцінку ризиків [9], тобто метод – це покрокова інструкція у поєднанні з інструментом (програмним продуктом) для оцінювання ризиків. Усі методи оцінювання ризиків можна поділити на кількісні, якісні або комбіновані (поєднання кількісних і якісних методів).

Кількісна оцінка (метод) – величина ризиків, які виражаються в цифрах, наприклад, грошах, часі простою сервера, втраченій вигоді.

Якісна оцінка (метод) – величини ризиків, що характеризуються відносно, наприклад «високий», «середній», «низький» ризик.

Кількісне управління ризиками, пов'язане зазвичай із надзвичайно трудомісткою роботою, яка зрештою не дає відчутного виграшу, все більше поступається місцем якісним методам оцінювання ризиків у сфері захисту інформації. Щодо комбінації кількісних і якісних методів, то вона, вочевидь, поєднує в собі як переваги, так і недоліки обох груп методів [9].

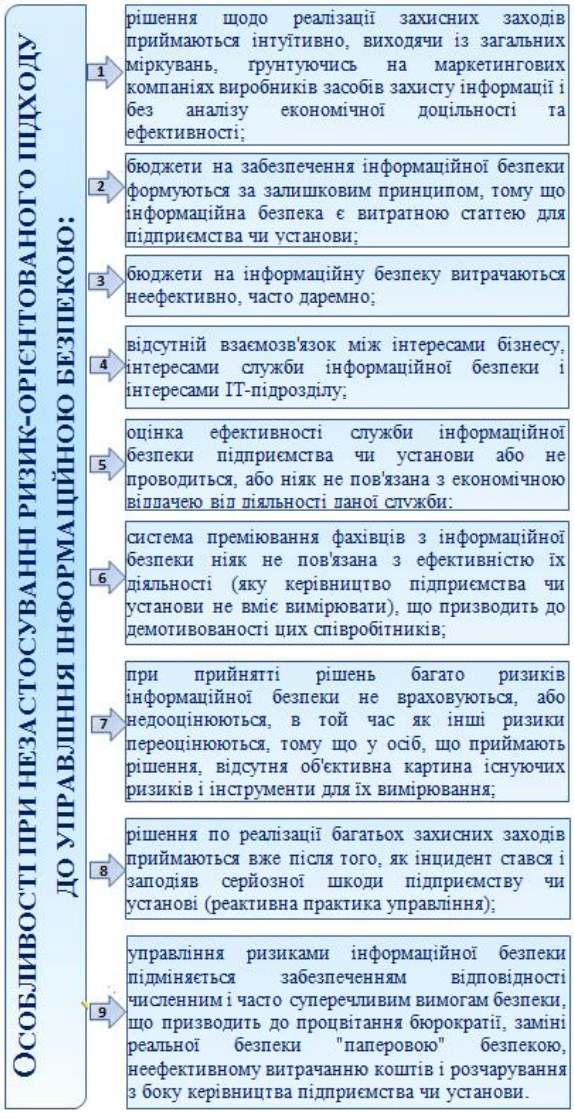

Рис. 2. Наслідки відсутності ризик-орієнтованого підходу при забезпеченні інформаційної безпеки підприємства чи організації

Програмні засоби та методики аналізу ризиків. Інформаційні технології удосконалюються з кожним днем, тому доводиться підвищувати і якість управління ризиками. Неминуче застарівають одні методики, інші – виникають і удосконалюються, в зв'язку з чим дуже важливо працювати з максимально актуальними на даний момент. В результаті на ринку програм оцінювання ризиків закріплюються лише затребувані аналоги, витісняючи неефективні або такі, що рідко оновлюються.

CRAMM (Великобританія) – британський метод, що має відомий підхід до кількісного і якісного розрахунку ІР. Його основними цілями є: автоматизація управління ризиками, оптимізація фінансових витрат на управління, оптимізація часу на супровід систем безпеки компанії, підтримка безперервності бізнесу [10].

Переваги: метод використовує комплексний підхід до оцінювання ризиків державних і комерційних організацій, застосовує технології оцінювання загроз і вразливостей за непрямими факторами з можливістю верифікації результатів, має широку базу знань по контрзаходах і володіє універсальністю і адаптованістю під профілі різних організацій. Розроблено програмні продукти, що реалізують цю методику.

Недоліки: використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора, процес є досить трудомістким і може обраховуватись місяцями безперервної роботи аудитора, не дозволяє створювати власні шаблони звітів або модифікувати існуючі. Ця методика припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як «уникнення» або «прийняття», не розглядаються. Програмне забезпечення існує тільки англійською мовою.

CORAS – інструмент, що дозволяє документувати, створювати звіти про результати аналізу шляхом моделювання ризику. У цій методології інформаційні системи представлені як складний комплекс з урахуванням людського фактора, а не тільки на основі використовуваних технологій.

Переваги: програмний продукт, що реалізує цю методологію, є безкоштовним і не потребує значних ресурсів для установки. Методика проста у використанні і не вимагає спеціальних знань.

Недоліки: не передбачена періодичність проведення оцінювання ризиків і оновлення їх величин. CORAS не дозволяє оцінити ефекти-

вність інвестицій, вкладених у впровадження заходів безпеки, так само як не дає можливості знайти необхідний баланс між заходами, спрямованими на запобігання, виявлення, виправлення або відновлення інформаційних активів.

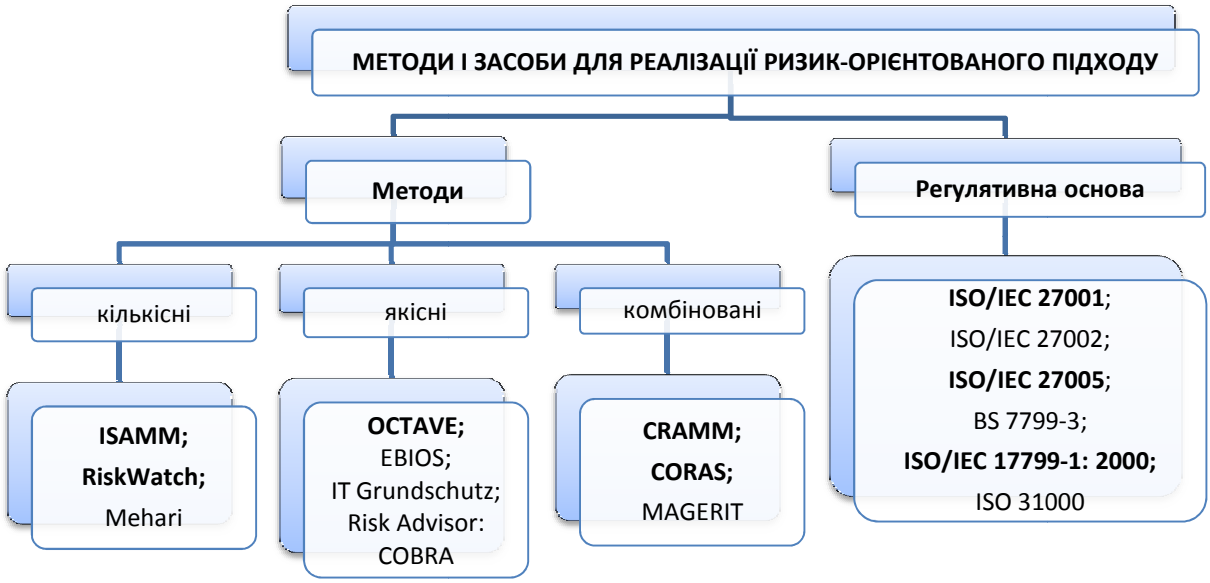

Рис. 3. Методи і засоби для ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства

Risk Watch (США) являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів.

Переваги: у Risk Watch як критерії для оцінювання та управління ризиками використовуються «очікувані річні втрати» та оцінка «повернення інвестицій». Risk Watch орієнтована на точне кількісне оцінювання співвідношення втрат від загроз безпеці і затрат на створення системи захисту.

Недоліки: Отримані оцінки ризиків (математичне очікування втрат) далеко не вичерпують розуміння ризику з системних позицій – метод не враховує комплексний підхід до інформаційної безпеки [9].

OCTAVE (США) – метод оперативного оцінювання критичних загроз, активів і вразливостей і вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації.

Переваги: простота у використанні і наочність вихідних даних; швидке впровадження і використання в організаціях і установах різного профілю; регулярне проведення оцінювання ризиків та оновлення їх величин як частини процесу оцінювання ризиків. Існує програмний продукт, що реалізує положення цієї методики.

Недоліки: не використовується такий спосіб управління ризиками, як обхід (виключення). Метод OCTAVE не дає кількісного оцінювання ризиків інформаційній безпеці, проте якісне оцінювання може бути використане у визначенні кількісної шкали їх ранжування.

Oracle Crystal Ball – додаток до Microsoft Excel для моделювання бізнес-процесів, визначення ризиків, прогнозування невизначених даних і оптимізації результатів. Використання моделювання за методом Монте Карло дає додаткові можливості по оптимізації. Crystal Ball забезпечує можливість моделювання та імітації для здійснення «What-If» аналізу.

Переваги: простота у використанні і наочність вихідних даних [11].

Управляючі документи. Крім методів оцінювання ризиків, використовують управляючі документи, де теоретично описуються і даються методичні вказівки процесу оцінювання ризиків, але не дається конкретних технологій. Найвідоміші стандарти, які використовуються на території України: ISO 27001, ISO 27005, ISO 17799.

ISO/IEC 27001 – міжнародний стандарт, що визначає інформаційну безпеку як збереження конфіденційності, цілісності та доступності інформації та представляє перелік вимог

до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації. Цей стандарт визначає процеси, що дають можливість бізнесу встановлювати, використовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки; встановлює вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації [12].

ISO/IEC 27005 – стандарт, що забезпечує рекомендації для менеджменту ризиків інформаційній безпеці, які включають інформацію і менеджмент ризиків безпеці технологій телекомунікації. Методи, описані в цьому стандарті, відповідають загальним поняттям, моделям і процесам, зазначеним в ISO/IEC 27001. Ці рекомендації призначені, щоб допомогти реалізувати достатню інформаційну безпеку, що ґрунтується на підході менеджменту ризиками. Стандарт є придатним до всіх типів організацій (наприклад комерційні підприємства, урядові агентства, некомерційні організації), що мають намір здійснювати менеджмент ризиками, які ставлять під загрозу інформаційну безпеку організації.

ISO/IEC 17799 – «Управління інформаційною безпекою – Інформаційні технології. – Information technology – Information security management» є найбільш відомим стандартом в сфері захисту інформації.

Цей міжнародний стандарт встановлює рекомендації та загальні принципи для ініціалізації, здійснення, підтримки і поліпшення управління безпекою інформації в установі. Цілі, виділені в цьому міжнародному стандарті, забезпечують загальне керівництво управління безпекою інформації на загальноприйнятих показниках. Цілі управління і контролю цього міжнародного стандарту призначені, щоб виконати і здійснити захист інформації відповідно до ідентифікованої оцінки ризику [1, 12].

Розглянуті методології дозволяють досить лаконічно оцінити весь асортимент пропонованих засобів оцінювання ризиків в інформаційному середовищі. Всі вони добре справляються з оцінюванням ризиків та їх управлінням, але мають свої недоліки, пов'язані з моніторингом. У жодній системі не передбачається розрахунок оптимального балансу способів управління, не проводиться обробка залишкових ризиків, не даються вказівки щодо подальших аналізів ризиків у мережі, не враховується мінливість факторів ризику.

Критерію «Простота використання» не відповідають лише CRAMM і Risk Watch, для успішної і продуктивної роботи з якими необхідне навчання або залучення експертів. До того ж, CRAMM припускає більше часу для аналізу. Решта розглянутих комплексів таких проблем не виявляють, а Crystal Ball навіть є занадто простим у використанні.

Методологія OCTAVE є гнучкою, підприємства та організації можуть використовувати ряд критеріїв для «приладження» програми під свої потреби. OCTAVE не використовує кількісне оцінювання ризиків, але якісне оцінювання досить легко описує кількісний показник.

Дуже важливою повинна бути наявність «What-If» аналізу, тобто оцінювання ситуації при використанні профілю захисту. Це дозволяє підприємству заглянути вперед і оцінити можливі вигоди при використанні спеціальних засобів і дій по захисту інформації. Таке оцінювання дають лише Crystal Ball і Risk Watch.

У методології CRAMM відсутні: інтеграція способів управління і опису їх призначення; перерахунок максимально допустимих величин ризиків; реагування на інциденти. При роботі з ризиками CRAMM використовує тільки методи їх зниження, а такі методи управління ризиками, як «обхід» або «прийняття», не розглядаються.

Однією з переваг для підприємств з обмеженими фінансовими можливостями є безкоштовність використання. CORAS і OCTAVE не вимагають значних ресурсів при застосуванні.

На відміну від CRAMM, програма Risk Watch більш орієнтована на кількісне оцінювання і дає змогу проводити аналіз тільки на програмно-технічному рівні, але не враховує адміністративних чинників, а отже, одержувана оцінка не є повною і не враховує комплексний підхід до безпеки.

Якщо потрібно оцінити ризики одноразово, то доречно застосувати методологію CORAS, а в разі періодичного використання доцільнішою є система CRAMM. OCTAVE буде актуальною у великих організаціях, де постійне оцінювання ризиків є невід'ємною частиною роботи. З низки критеріїв неможливо встановити перевагу того чи іншого засобу оцінювання ризиків, але кожне підприємство

визначає для себе пріоритетні напрямки, за якими і вибирає методику. В ідеалі необхідно отримати не тільки задовільні результати оцінювання, а й зручний у використанні програмний комплекс, який би був інструментом при такому оцінюванні. Природним є бажання отримати ясні результати дослідження, а також рекомендації щодо зниження ризиків. Інструмент зобов'язаний простежити зв'язок між ризиками і причинами, що призводять до цих ризиків. Саме цим вимогам найбільш задовольняє OCTAVE.

Порівняльну характеристику основних систем аналізу ризиків подано в табл. 1.

Таблиця 1

Порівняння методологій управління інформаційними ризиками

Критерії	CRAMM	CORAS	Risk Watch	OCTAVE	Oracle Crystal Ball
Загальні характеристики					
Розрахованість на організації різного розміру і сфери діяльності	+	+	+	+	+
Автоматизація «What-if»	–	?	+	–	+
Зручність сприйняття графіків і звітів	–	+	–	+	+
Простота використання	–	+	–	+	+
Безкоштовне використання	–	+	–	+	–
Підтримка	+	+	+	+	+
Кількісна оцінка	+	+	+	–	?
Якісна оцінка	+	+	–	+	?
Російська локалізація	–	?	+	?	–
Підвищення інформованості співробітників	–	–	–	+	?
Придатність до регулярного використання	+	–	?	+	?
Використання незалежної оцінки	+	+	?	–	?
Вхідні дані					
Ресурси	+	+	+	+	+
Тип інформаційної системи	+	?	+	+	–
Цінність ресурсів	+	+	+	+	?
Загрози	+	+	+	+	+
Уразливості системи	+	+	+	+	+
Вибір контрзаходів	+	?	+	–	–
Базові вимоги в сфері безпеки	–	?	+	–	–
Втрати	–	?	+	–	–
Заходи захисту	+	–	+	+	–
Частота виникнення загроз	–	?	+	–	–
Мережеве обладнання	–	?	–	+	–
Види інформації	–	?	–	?	–
Групи користувачів	–	?	–	–	–
Засоби захисту	–	?	–	+	–

ПРИМІТКА: + відповідає критерію; – не відповідає критерію; ? – відповідність критерію залежить від інших факторів.

Усі перелічені методології спрямовані на проведення оцінювання ризиків інформаційної безпеки, що дає можливість сконцентрувати увагу на найбільш актуальних проблемах та запобігти нанесенню шкоди підприємству чи організації.

Висновки. В роботі здійснено аналіз найпоширеніших методик у сфері управління ризиками ІБ для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємств, що дало змогу визначити їх основні особливості,

встановити переваги та недоліки кожної з методологій аналізу ризиків на основі найбільш поширених на сьогоднішній день інструментальних засобів. В роботі представлено ряд рекомендацій щодо доцільності застосування розглянутих програмних засобів та управляючої документації з урахуванням відповідних потреб і критеріїв підприємств та організацій.

Список літератури

1. ISO/IEC 17799:2000 Международный стандарт Информационные технологии – практические правила управления информационной безопасностью. С. 87.
2. Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации. *Наука і техніка Повітряних Сил Збройних Сил України*. 2014. № 2 (15). С. 133–138.
3. Гарасим Ю. Р., Ромака В. А., Рибій М. М. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. *Вісник Національного університету "Львівська політехніка". Сер.: Автоматика, вимірювання та керування*. 2013. № 753. С. 90–99.
4. Левадний С. М. Оцінка інформаційних ризиків. URL: http://www.rusnauka.com/21_SEN_2014/Informatica/4_174674.doc.htm
5. IT ринок. Дослідження та рекомендації. *IT Ukraine Association.* URL: http://itukraine. org.ua/it-rynok
6. Левченко М. О. Використання інформаційних технологій в управлінні ризиками машинобудівних підприємств. *Актуальні проблеми економіки*. 2012. № 4. С. 305–311.
7. Мельник Г. Модель оценивания уровня информационных рисков в корпоративных системах. *Вісник Київського національного університету імені Тараса Шевченка. Сер.: Економіка*. 2015. № 6 (171). С. 48–54.
8. Астахов А. Искусство управления информационными рисками. Москва: ДМК Пресс Год, 2010. 312 с.
9. Гловацький В. В., Методи оцінювання стану безпеки та загроз інформаційних ресурсів. *Зв'язок*. 2016. № 5. С. 13–16.
10. Медведовский И. С. Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, Risk Watch и ГРИФ (Опубликовано на "SecurityLab"). 2004. URL: http://www.ixbt.com/cm/informationsystem-risks012004.shtml
11. Axoft. Oracle Crystal Ball. URL: http://oracle.axoft.ru/catalog/rubric.php?RUBRIC_ID=488
12. Сертифікація систем менеджменту ISO 27001:2005. URL: http://www.qmsc.com.ua/index.php/iso-27001

References

1. ISO/IEC 17799:2000 Information technology – Code of practice for information security management, p. 87 [in Russian].
2. Zamula, A., Severinov, A. and Kornienko, M. (2014) Analysis of information security risks assessment models for building a data protection system. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*, No. 2 (15), pp. 133–138 [in Russian].
3. Garasim, Yu., Romaka, V. and Rybiy, M. (2013) Analysis of the process of information security risk management in the process of ensuring the properties of system survivability. *Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Ser.: Avtomatyka, vymiriuvannia ta keruvannia*, No. 753, pp. 90–99 [in Ukranian].
4. Levadny, S. (2014) Assessment of information risks. URL: http://www.rusnauka.com/21_SEN_2014/Informatica/4_174674.doc.htm
5. IT market. Research and recommendations. *IT Ukraine Association*. URL: http://itukraine.org.ua/it-rynok
6. Levchenko, M. (2012) Application of information technologies in risk management at machine-builing enterprises. *Aktualni problemy ekonomiky*, No. 4, pp. 305–311 [in Ukranian].
7. Melnyk, H. (2015) Model of information risk measurement in corporate systems. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Ser.: Ekonomika,* No. 6 (171), pp. 48–54 [in Ukranian].
8. Astahov, A. (2010) The art of information risks management. Moscow: DMK Press

God, 312 p. [in Russian].
9. Glovatskyi, V. (2016) Methods of assessing information resources security condition and threats. *Zviazok,* No. 5, pp. 13–16 [in Ukranian].
10. Medvedovskyi, I. (2004) Modern methods and tools for the analysis and control of the risks of information systems of companies CRAMM, Risk Watch and GRIF. URL: http://www.ixbt.com/cm/informationsystem-risks012004.shtml
11. Axoft. Oracle Crystal Ball. URL: http://oracle.axoft.ru/catalog/rubric.php?RUBRIC_ID=488
12. Certification of management systems ISO 27001:2005. URL: http://www.qmsc.com.ua/index.php/iso-27001

T. V. Savelieva, *Ph.D., associate professor,*
e-mail: tam2003@ukr.net
O. M. Panasko, *Ph.D., associate professor,*
e-mail: lena.pa@ukr.net
O.M. Prigodyuk
e-mail: prigoduk@ukr.net
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

ANALYSIS OF METHODS AND MEANS TO IMPLEMENT A RISK-ORIENTED APPROACH IN THE CONTEXT OF PROVIDING ENTERPRISE INFORMATION SECURITY

The article is devoted to the actual problem of the present – the information security development on the base of risk-oriented approach for solving the problems of information security management for an enterprise. Modern business development trends require the need for risk management. The authors research methods and tools that allow to implement a risk-oriented approach in the context of providing enterprise information security and to analyze and evaluate information risks of information security system. The paper considers a series of the tools representatives, most commonly used in this area, and analyzes several risk assessment methodologies, in particular CRAMM (UK) – the methodology for analysis and risk management, OCTAVE for assessing assets and vulnerability of information security, etc., and a series of regulatory documents, among which NIST SP800-30 (risk management in information technology system); ISO/IEC 27005:2011 (information security risk management methods); ENISA (information security risk assessment) and many others. The analysis of the software advantages and disadvantages for the determination and assessment of information security risks (CRAMM, CORAS, Risk Watch, OCTAVE, Oracle Crystal Ball) is presented and a number of recommendations according to the feasibility of using the considered software and management documentation taking into account relevant requirements and criteria of enterprises and organizations is formed.

Key words: *information technologies, information security, threats, vulnerability, information risks, risk assessment.*

Стаття надійшла 01.03.2018.

Рецензенти: Т. О. Прокопенко, д.т.н., доцент,
Ю. М. Тесля, д.т.н., професор.