УДК 004:657

МОДЕЛЬ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Поліщук Д.В. – гр. БЧКІ-1-17, бакалавр, *darya.onischenko@gmail.com*
Захарова М.В. – к.т.н., доцент, *z.maria@ukr.net*
Люта М.В. – старший викладач, *lyuta.mv@knutd.com.ua*
Київський національний університет технологій та дизайну

У статті розглянута класифікація основних способів та методів оцінки ризиків інформаційної системи, описані моделі найефективніших засобів захисту інформації. Також, важливий акцент зосереджений на питанні дослідження основних принципів інформаційної безпеки, які обумовлені необхідністю забезпечення управління процесами формування та використання інформаційних ресурсів, а також створенням і застосуванням інформаційних систем. Нові моделі інформаційної безпеки в умовах розвитку суспільства будуть покликані протистояти різноманітним загрозам, небезпекам і викликам, як зовнішнім, так і внутрішнім.

The article considers the classification of the main methods and techniques of risk assessment of the information system, describes the models of the most effective means of information protection. Also, an important emphasis is placed on the study of the basic principles of information security, which are due to the need to manage the processes of formation and use of information resources, as well as the creation and application of information systems. New models of information security in the context of society will be designed to confront a variety of threats, dangers and challenges, both external and internal.

Вступ. Інформація в XXI столітті стала невід'ємною частиною людського життя. Вона стала рівноцінним ресурсом в порівнянні з іншими, наприклад, як із матеріальними (нафта, вугілля, електроенергія тощо). Френсіс Бекон ще в XVII столітті казав: «Інформація керує світом. Хто володіє нею, той може вирішувати долі народів». Тому на сьогоднішній день володіння інформацією пов'язане з ризиками її втратити. Інформаційні злочини стали дедалі частіше зустрічатись. Викрадення та продаж інформації в наш час є заробітком для великої кількості хакерів та злочинців [1]. Тому з'явилась необхідність якісно захищати інформацію. Для побудови якісної та ефективної системи захисту інформації використовують різні методи та способи аналізу можливих місць її витоку.

Інформаційний ризик – це імовірність виникнення втрат в зв'язку з зловмисним або випадковим виводом з ладу елементів інформаційної системи або викрадення інформації з інформаційної системи. Оцінка ризику – це визначення даної імовірності.

Ризик інформаційної безпеки - це потенційна можливість використання вразливостей активів конкретної загрози для заподіяння шкоди організації.

Постановка проблеми. Обговоривши в попередніх публікаціях основи інформаційної безпеки та законодавчі норми щодо захисту інформації, слід перейти до опису ризик-орієнтованого підходу для забезпечення кібербезпеки. В роботінеобхідно дослідити основи ризик-менеджменту, аналізу і розрахунку ризиків в області інформаційної безпеки, відповідні нормативні документи, а також застосування методів аналізу ризиків інформаційної безпеки.

Результати досліджень. Основними способами знаходження вразливостей в системі є такі способи: статичний аналіз кожного елементу, перевірка шляхом створення фіктивних атак, отримання інформації про вразливості від розробника ПЗ або моделювання ризиків [2]. Саме моделювання ризиків дозволяє продумати методи захисту системи ще в процесі її проектування. Моделювання ризиків – це неперервний процес, який допомагає знаходити та зменшувати кількість загроз у вашій системі шляхом прийняття певних дій.

Під величиною ризику умовно розуміють настання ймовірності негативної події і розміру збитку. У свою чергу під ймовірністю події розуміється настання ймовірності реалізації загрози інформаційній безпеці, а також вразливостей інформаційної безпеки, виражені в якісній або кількісній формі. Умовно можемо висловити це логічною формулою: величина_ризику = Ймовірність_події * Розмір_збитку, де Ймовірність_події = Ймовірність_загрози *Величину_вразливості.

Існує також умовна класифікація ризиків: за джерелом ризику (наприклад, атаки хакерів або інсайдерів, фінансові помилки, вплив державних регуляторів, юридичні претензії контрагентів, негативний інформаційний вплив конкурентів); по цілі (інформаційні активи, фізичні активи, репутація, бізнес-процеси); за тривалістю впливу (операційні, тактичні,стратегічні)

Цілі процесу аналізу ризиків ІБ такі:

1. Ідентифікувати активи і оцінити їх цінність.
2. Ідентифікувати загрози активам і уразливості в системі захисту.
3. Прорахувати ймовірність реалізації загроз і їх вплив на бізнес (англ. Businessimpact).
4. Дотримати баланс між вартістю можливих негативних наслідків і вартістю заходів захисту, дати рекомендації керівництву компанії по обробці виявлених ризиків.

Етапи 1-3є оцінкою ризику (англ. Riskassessment) і являють собою збір наявної інформації. Етап 4 вдає із себе вже безпосередньо аналіз ризиків (англ. Riskanalysis), тобто вивчення зібраних даних і видачу результатів / вказівок для подальших дій; при цьому також важливо розуміти власний рівень впевненості в коректності проведеної оцінки. На етапі 4 також пропонуються методи обробки для кожного з актуальних ризиків: передача (наприклад, шляхом страхування), уникнення (наприклад, відмова від впровадженнях тієї чи іншої технології або сервісу), прийняттях (свідома готовність понести збитки в разі реалізації ризику), мінімізаціях (застосування заходів для зниження ризику ІБ і ймовірності негативної події, що приводить до реалізації ризиків інформаційної безпеки). Після завершення всіх етапів аналізу ризиків слід вибрати прийнятний для компанії рівень ризиків (англ. Acceptablerisklevel), встановити мінімально можливий рівень безпеки (англ. Baselinesofperformance), потім впровадити контрзаходи і надалі оцінювати їх з точки зору досяжності встановленого мінімально можливого рівня безпеки з їх допомогою.

Збиток від реалізації атаки може бути прямим або непрямим. Прямий збиток – це безпосередні очевидні і легко прогнозовані втрати компанії, такі як втрата прав інтелектуальної власності, розголошення секретів виробництва, зниження вартості активів або їх часткове або повне руйнування, судові витрати і виплата штрафів і компенсацій.

Непрямий збиток може означати якісні або непрямі втрати. Якісними втратами можуть бути припинення або зниження ефективності діяльності компанії, втрата клієнтів, зниження якості вироблених товарів або послуг, що надаються. Непрямі втрати - це, наприклад, недоотриманий прибуток, втрата ділової репутації, додатково понесені витрати. Крім цього, в зарубіжній літературі зустрічаються також такі поняття, як тотальний ризик (англ. Totalrisk), який присутній, якщо взагалі ніяких заходів захисту не впроваджується, а також залишковий ризик (англ. Residualrisk), який присутній, якщо загрози реалізувалися, незважаючи на запроваджені заходи захисту.

Аналіз ризиків інформаційної безпеки може бути як кількісними, так і якісними.

Розглянемо один із способів кількісного аналізу ризиків. Основними показниками будемо вважати такі величини:

- ALE – annuallossexpectancy, очікувані річні втрати, тобто «Вартість» всіх інцидентів за рік.
- SLE – singlelossexpectancy, очікувані разові втрати, тобто «Вартість» одного інциденту.

- EF – exposurefactor, фактор відкритості перед загрозою, тобто який відсоток активу зруйнує загроза при її успішної реалізації.
- ARO – annualizedrateofoccurrence, середня кількість інцидентів на рік відповідно до статистичних даних.

Значення SLE обчислюється як добуток розрахункової вартості активу і значення EF, тобто SLE = AssetValue * EF. При цьому у вартість активу слід включати і штрафні санкції за його недостатній захист.

Значення ALE обчислюється як добуток SLE і ARO, тобто ALE = SLE * ARO. Значення ALE допоможе проранжувати ризики – ризик з високим ALE буде самим критичним. Далі, розраховане значення ALE можна буде використовувати для визначення максимальної вартості реалізованих заходів захисту, оскільки, згідно із загальноприйнятою підходу, вартість захисних заходів не повинна перевищувати вартості активу або величини прогнозованого збитку, а розрахункові доцільні витрати на атаку для зловмисника повинні бути менше, ніж очікувана їм прибуток від реалізації цієї атаки. Цінність заходів захисту також можна визначити, вирахувавши з розрахункового значення ALE до впровадження заходів захисту значення розрахункового значення ALE після впровадження заходів захисту, а також віднявши щорічні витрати на реалізацію цих заходів. Умовно записати цей вислів можна наступним чином:(Цінність заходів захисту для компанії) = (ALE до впровадження заходів захисту) – (ALE після впровадження заходів захисту) - (Щорічні витрати на реалізацію заходів захисту).

Прикладами якісного аналізу ризиків можуть бути, наприклад, метод Делфі, в якому проводиться анонімне опитування експертів в кілька ітерацій до досягнення консенсусу, а також мозковий штурм і інші приклади оцінки «Експертним методом» [4].

Перевага моделювання інформаційних ризиків полягає в тому, що ми отримуємо розуміння реальних атак, чітко визначаємо зв’язок компонентів системи, отримуємо сценарії та ймовірності використання вразливостей та отримуємо розуміння впливу на систему проведення атаки. На сьогоднішній день існує багато різних методологій для моделювання інформаційних ризиків.

Основними є:

1. STRIDE
2. PASTA
3. Trike
4. VAST
5. OCTAVE

Висновки. Отже, одним з важливіших кроків при побудовісистеми захисту інформації є обрання методів, управляючих документів та інструментів. Як правило, компанії не знають, які з існуючих способів оцінки ризиків кращі саме для їх установи. Процес оцінки повинен бути пристосований до індивідуальних, персональних та приватних особливостей організації, але в той же час узгоджений з найкращими стандартами та досвідченими, провідними практиками. У данійроботі було розглянуто класифікацію основних способів та методів оцінки інформаційних ризиків. Також проведено аналіз одних із кращих методів, провідних документів та інструментів. Обрати кращий засіб оцінки ризику полягає в їх детальному порівнянні, використовуючи різні стандарти та критерії. Якщо критерії, які використовуються, застосовані до всіх моделей оцінки ризиків, підприємство може порівняти різні моделі оцінки і об'єктивно прийняти рішення про запровадження найкращих з тих, які задовольняють їх потреби.

Список використаних джерел

1. Хорошко В.О. «Проєктування комплексних систем захисту інформації», 2020. – 317с.
2. Когут Ю.І. «Кібертероризм: історія, цілі, об'єкти. Практичний посібник», 2021. – 304 с.
3. Когут Ю.І. «Кібербезпека та ризики цифрової трансформації компаній», 2021. – 372 с.
4. Бобало Ю.Я., Горбатий І.В. та інші «Інформаційна безпека» 2019. – 580 с.
5. Астрахов А.М. Мистецтво управління інформаційними ризиками – М: ДМК Пресс, 2010. – 312 с.
6. Лекції І.Б. Родіонов. - «Системний аналіз. Теорія систем і системний аналіз», 2008. – 122 с.
7. Макаревич Л.М. Управління підприємницькими ризиками: монографія / Л.М. Макаревич. – М .: Річ навіть і Сервіс, 2006. – 443 с.
8. Луцький М.Г. Базові поняття управління ризиком в сфері інформаційної безпеки / Іваненко Є.В. // Захист інформації – 2011. – №2. – С. 86-94.
9. Красилівська О.О. Розробка комплексної системи захисту інформації на об’єкті інформаційної діяльності [Електронний ресурс]. – Режим доступу: http://o53xo.oj2xg3tbovvwcltdn5wq.nblk.ru/3_SND_2010/Informatica/58042.doc.htm – Назва з екрану.
10. Побудова комплексних систем захисту інформації [Електронний ресурс]. Режим доступу: http://iqusion.com/ua/sistemi-zakhistu-informatsiji – Назва з екрану.