УДК 004.7(045)

В.В. Єрмошин, Я.В. Невойт

АНАЛІЗ І ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ БАНКІВСЬКИХ ТА КОМЕРЦІЙНИХ СИСТЕМ

Відповідно до вимог стандартів з управління інформаційною безпекою вимоги безпеки ідентифікуються систематичною оцінкою ризиків безпеки, а результати оцінки ризику допомагатимуть підприємству яке розробило та впровадило систему управління інформаційною безпекою спрямувати і визначити відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки і впровадити відповідні заходи безпеки, вибрані для захисту від цих ризиків.

В роботі автори поділяться своїм багаторічним практичним досвідом проведення оцінки ризиків інформаційної безпеки для банківських та комерційних систем шляхом розгляду способів реалізації завдань, які виникають під час проведення цих робіт.

Ключові слова: оцінка ризиків, загроза, вразливість

Вступ

Аналіз і оцінка ризиків інформаційної безпеки - обов'язковий етап як в рамках побудови комплексних систем захисту інформації (п. 6.1.3 НД ТЗІ 3.7-003-05) так і в рамках побудови систем управління інформаційної безпеки для банківської сфери та для підприємства іншого виду діяльності (вимоги п. 6.1.2 ISO/IEC 27001: 2013, п. 4.2.1 ISO/IEC 27001: 2005, п. 4.2.1 СОУ Н НБУ 65.1 СУІБ 1.0:2010).

Постановою Національного банку України №474 від 28.10.2010 року було введено в дію стандарти з управління інформаційною безпекою в банківській системі України, а листом НБУ від 03.03.2011 N 24-112/365 розроблено та оприлюднено Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та Методику оцінки ризиків. В наслідок прийняття та оприлюднення цих документів весь банківський сектор України зіткнувся з потребою оцінки ризиків інформаційної безпеки як складової оцінки операційного ризику.

Слід зазначити що на сьогоднішній день існують декілька світових і вітчизняних, в тому числі галузевих, методик та методологій оцінки ризиків інформаційної безпеки. З яких можна виділити FactorAnalysisofInformationRisk (FAIR), IS RISK ASSESSMENT MEASUREMENT, NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) та Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків оприлюднені листом НБУ від 03.03.2011 N 24-112/365 (далі – Методика НБУ) про які згадувалося вище. Однак жодна з існуючих методик та методологій не є «Методикою» в практичному/інженерному розумінні цього визначення (керівництво до дій або план дій). Кожна з методик містить ряд невизначеностей, які ускладняють процес оцінки, а в ряді випадків призводять до отримання непередбаченого з точки зору зіставного та відтворюваного результату.

Так при проведенні аналізу та оцінки ризиків інформаційної безпеки за Методикою НБУ актуальним стає питання складання і підтримки переліків загроз і вразливостей за якими можна провести оцінку, утворення на їх основі пар, оцінка ймовірності реалізації цих пар, а також їх вплив на конфіденційність, цілісність, доступність і спостережність по відношенню до банківських та комерційних систем. При цьому використання переліків і їх оцінок повинно дозволити отримати зіставний та відтворюваний результат, який не буде залежати від фахівця що проводить оцінку ризиків, його досвіду та кваліфікації. Відсутність кінцевих, робочих, готових для практичного використання, а не орієнтовних переліків загроз і вразливостей та пар, які вони можуть утворювати, попередньої аналітичної оцінки ймовірності їх виникнення та оцінки їх впливу на конфіденційність, цілісність, доступність та спостережність по відношенню до банківських та комерційним системам не дозволяють досягти такого результату , як в рамках однієї організації так і в рамках галузі або держави в цілому.

Вирішення цієї проблеми дозволило б стандартизувати та спростити по відношенню до кінцевих користувачів процес оцінки, знизити вимоги щодо його досвіду та кваліфікації, а також отримувати зіставний та відтворюваний результат як в рамках окремого підприємства, так і в рамках сектора/галузі економіки.

Основна частина

В якості загального підходу до вирішення зазначеної проблеми оцінки ризиків інформаційної безпеки доцільно використовувати наступну послідовність:

1. Розробити загальний підхід , який дозволить проводити практичну оцінку ризиків інформаційної безпеки;
2. На базі підходу розробити методику оцінки ризиків інформаційної безпеки (включаючи єдину термінологію, що буде використовуватися під час оцінки ризиків);
3. Розробити переліки загроз та вразливостей та перелік пар, які можуть утворитися на їх базі;
4. По відношенню до всіх визначених пар загроза/вразливість оцінити ймовірності їх виникнення та вплив на конфіденційність, цілісність, доступність та спостережність по відношенню до банківських та комерційних систем;
5. Визначити напрямки щодо подальших дій по підтримці в актуальному стані переліку загроз, вразливостей їх пар та оцінок;
6. Провести автоматизацію розробленого підходу та методики.

При використанні методології НБУ перший та другий пункти послідовності регулятором вирішені. Ним визначається наступний порядок проведення робіт з оцінки ризиків інформаційної безпеки:

1. Створюються загальні переліки загроз та можливих вразливостей.
2. Створюються актуальні для банку пари загроза/вразливість (з врахуванням особливостей бізнес-процесу та ієрархії вимог).
3. Оцінюється (за визначеною шкалою оцінки) умовна ймовірність реалізації загрози з використанням вказаної вразливості.
4. Оцінюється (за визначеною шкалою оцінки) вплив реалізації загрози на цілісність, конфіденційність, доступність та спостережність.
5. Розраховуються ризики за бізнес-процесом (відповідно до п.6.2 Методики НБУ).

При розгляді поняття «Загроза» доцільно використовувати визначення, що це потенційна причина небажаного інциденту, який може призвести до шкоди для системи або банку/підприємства. При формулюванні загрози доцільно використовувати двоскладову конструкцію - де перша частина описує дію небажаного інциденту та об’єкт цієї дії, а друга частина описує в наслідок чого ця дія відбулася.

Дією небажаного інциденту може бути пошкодження, втрата, компрометація, викривлення, неправильна робота, зупинка.

Об’єктом дії може бути програмно-технічний комплекс (далі – ПТК), будівлі, обладнання, інформація.

В ряді випадків для банківської системи в якості об’єкту дії доцільно розглядати кошти.

На базі дії та її об’єкту може бути складено матрицю дії (таблиця 1).

Таблиця 1

Матриця дії

	ПТК	будівля	обладнання	інформація
Пошкодження	1	1	1	1
Втрата	1		1	1
Компрометація				1
Викривлення				1
Неправильна робота	1		1	
Зупинка	1		1	

Таким чином на базі матриці утворюється загальний перелік дії загроз, який являє собою першу частину конструкції «Загроза», а саме: Пошкодження ПТК; Втрата ПТК; Неправильна робота ПТК; Зупинка ПТК; Пошкодження будівлі; Пошкодження обладнання; Втрата обладнання; Неправильна робота обладнання; Зупинка обладнання; Пошкодження інформації; Втрата інформації; Компрометація інформації; Викривлення інформації.

В разі розгляду в якості об’єкту кошти, додатково утвориться ще одна дія загрози – втрата коштів.

При описі в наслідок чого дія загрози відбулася доцільно використовувати наступну класифікацію загроз [1, 2]:

*Клас 1.*Загрози, пов'язані з несприятливими подіями природного, техногенного характеру;

Клас 2. Загрози, пов'язані з діяльністю терористів і осіб, які вчиняють злочини та правопорушення;

Клас 3. Загрози, пов'язані з діяльністю постачальників / провайдерів / партнерів;

Клас 4. Загрози, пов'язані зі збоями, відмовами, руйнуваннями / ушкодженнями програмних і технічних засобів;

Клас 5. Загрози, пов'язані з діяльністю внутрішніх порушників ІБ;

Клас 6. Загрози, пов'язані з діяльністю зовнішніх порушників ІБ;

Клас 7. Загрози, пов'язані з невідповідністю вимогам наглядових та регулюючих органів, чинному законодавству;

Клас 8. Загрози,пов’язані з дистанційним банківським обслуговуванням клієнтів.

В свою чергу кожний з класів розділяється на події в наслідок чого ця загроза може бути реалізована. Для класу 1 вона буде мати наступний вигляд:

Таблиця 2

Клас загроз

Клас загроз	**В наслідок чого ця загроза може бути реалізована**
Клас 1. Загрози, пов'язані з несприятливими подіями природного, техногенного характеру	пожежі
	природних явищ руйнівного характеру
	порушення в роботі системи клімат-контролю
	збоїв електроживлення
	електромагнітної радіації
	техногенної аварії

На базі цієї інформації можна утворити перелік загроз (скласти конструкцію загроз заповнивши відповідну матрицю, позначка «1» означає, що така загроза може існувати).

Таблиця 3

Перелік загроз

Клас загроз	↓[в наслідок чого ця загроза може бути реалізована]↓	пошкодження ПТК	втрата ПТК	неправильна робота ПТК	зупинка ПТК	пошкодження будівлі	втрата будівлі	пошкодження обладнання	втрата обладнання	зупинка обладнання	пошкодження інформації	втрата інформації	компрометація інформації	викривлення інформації
Клас 1. Загрози, пов'язані з несприятливими подіями природного, техногенного характеру	пожежі	1	1		1	1	1	1	1	1	1	1		
	природних явищ руйнівного характеру	1	1		1	1	1	1	1	1	1	1		
	порушення в роботі системи клімат-контролю	1	1		1	1		1	1	1	1	1		
	збоїв електроживлення	1	1		1			1		1	1	1		
	електромагнітної радіації	1	1		1			1		1	1	1		
	техногенної аварії	1	1		1	1	1	1	1	1	1	1		

Висновок

Таким чином банком чи підприємством буде вирішена перша частина задачі оцінки ризиків інформаційної безпеки - створено загальний перелік загроз. Подальші дії в оцінці ризиків інформаційної безпеки буде розглянуто в подальших роботах.

Література

1.Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України введених в дію листом НБУ від 03.03.2011 N 24-112/365.

2.Єрмошин В. Методологія оцінки ризиків у відповідності до вимог міжнародного стандарту ISO/IEC 27001 // Одиннадцатая Международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах", Тезисы докладов. –К: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ" . –2008. - С.63.

3. Ермошин В.В. Методика оценки информационных рисков предприятия // Захист інформації. – 2009. – №4(45), С. 80-88.

4. Єрмошин В.В., Хорошко В.О., Капустян М.В. Методика оцінки інформаційних ризиків системи управління інформаційною безпекою // Сучасний захист інформації. – 2010. – №3, С. 95-104.

5. СОУ Н НБУ 65.1 СУІБ 1.0:2010 “Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги” (ISO/IEC 27001:2005, MOD).

6. СОУ Н НБУ 65.1 СУІБ 2.0:2010 “Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою” (ISO/IEC 27002:2005, MOD).

7. BS ISO/IEC 27005:2008 Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности.

8. РС БР ИББС-2.2-2009 Методика оценки рисков нарушения информационной безопасности.

9. Factor Analysis of Information Risk (FAIR) http://www.riskmanagementinsight.com/.

10. IS RISK ASSESSMENT MEASUREMENT http://www.isaca.org.

11. NIST SpecialPublication 800-30 Risk Management Guide for Information Technology Systems http://www.nist.gov.

12. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach http://www.cert.org/octave/.

Надійшла 04.08.2014 р. Рецензент: д.т.н., проф. Богданович В.Ю.