Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
Vol. 5, Is. 3, pp. 82-88, 2015

DOI: 10.13187/vesp.2015.5.82
www.ejournal21.com

Theoretical Questions

UDC 004.056.53

The Justification of Requirements to the Security System Based on the Analysis of Information Risks

Yurii F. Katorin

State university of the sea and river fleet of the name of the Admiral S.O. Makarov,
Russian Federation
198035 Saint Petersburg, Dvinskaya Str., 5/7
Doctor of Military Sciences, Professor
E-mail: katorin@mail.ru

Abstract

The article describes the basic methods of the analysis of information risks and determination on this basis the necessary level of object security, stands the concept of "risk", studies the quantitative or qualitative assessment of potential risks, analyzes their advantages and disadvantages, and explores the method of justification of requirements to the security system, based on verifying the compliance level security requirements of one of standards in the field of information security.

Keywords: information security, risk, analysis, quantitative and qualitative evaluation, criteria, the protection level.

Введение

В настоящее время термин «информационный риск» нашел широкое применение. Однако пока не существует принятой большинством ученых и практиков трактовки понятия «информационный риск», более того, еще не сложилось общепринятого толкования этой категории. Отдельные специалисты в это понятие вкладывают следующий смысл: информационный риск – это возможное событие, в результате которого несанкционированно удаляется, искажается информация, нарушается ее конфиденциальность или доступность. То есть, понятие информационного риска используется как синоним понятия угроза безопасности информации. Необходимо отметить, что ставший уже привычным термин «угроза безопасности» хоть и звучит мелодично, на самом деле является идиомой (идиоматическим оборотом). Безопасности никто никогда не грозил! Угрожают не состоянию и не ситуации, а объекту.

Такой подход к определению рисков нельзя признать верным. Исторически риск понимался как неопределенность, связанная с вероятностью благоприятного или неблагоприятного исхода, причем к негативным последствиям по понятным причинам интерес был намного выше. В разное время риск изучался как аспект игры (например, у Б. Паскаля, Х. Гюйгенса), элемент задачи оценки в страховании (например, у Д. Бернулли).

Были введены функции полезности, как количественно (у того же Д. Бернулли, Г. Госсена, и позднее у Дж. фон Неймана и О. Моргенштерна), так и качественно (например, в работах В. Парето) описывавшие выбор определенного решения. Как и начальные работы, большинство из них основано на понятии риска и связанных с ним характеристиках системы. Более того, сам по себе риск отделялся от понятия случайного события, поскольку являлся оценочной величиной, указывающей на возможные потери (начиная с работ Ф. Найта и др.).

Обсуждение

Поэтому основным определением и сущностью понятия риска, как и ранее, остается следующее: «риск – это сочетание вероятности и последствий наступления некоторого события». Такое определение в разных вариациях и уточнениях предлагают различные авторы [1-3 и др. – для экономического риска, 4-6 и др. – для технических рисков, 7-9 и др. – для информационного риска]. В области информационного риска наблюдается стандартный подход к определению, который связывает в единую величину три составляющих – вероятность существования уязвимости, вероятность угрозы безопасности, вероятность негативного воздействия [9-11]. Очевидно, что в этом случае идет уточнение (декомпозиция) первого компонента риска – вероятности осуществления негативного события. Эта декомпозиция может быть более детальной, например, как в работе [12], или сводиться к простому вычислению вероятности из известного закона распределения случайной величины. Вместе с тем, именно определение уровня риска является принципиально важным моментом при формировании требований к системе безопасности информационных ресурсов.

Используется количественная или качественная оценка возможных рисков. Наиболее распространенной на практике остается качественная оценка информационных рисков, когда при отсутствии точных данных значения параметров устанавливает проводящий анализ рисков эксперт. Суть методики заключается в определении посредством экспертных оценок зависимости значения риска от определенных факторов – вероятности наступления события и ущерба от наступления данного события. Формула, чаще всего используемая в этом случае при расчете рисков, представляет собой произведение трех параметров:

- стоимость ресурса (Asset Value, AV). Указанная величина характеризует ценность ресурса. При качественной оценке рисков стоимость ресурса чаще всего ранжируется в диапазоне от 1 до 3, где 1 — минимальная стоимость ресурса, 2 — средняя стоимость ресурса и 3 — максимальная стоимость ресурса;

- мера уязвимости ресурса к угрозе (Exposure Factor, EF). Этот параметр показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе. При качественной оценке рисков данная величина также ранжируется в диапазоне от 1 до 3, где 1 — минимальная мера уязвимости (слабое воздействие), 2 — средняя (подвергшийся воздействию ресурс подлежит восстановлению), 3 — максимальная (ресурс требует полной замены после реализации угрозы);

- оценка вероятности реализации угрозы (Annual Rate of Occurrence, ARO) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая).

На основании полученных данных выводится оценка ожидаемых потерь (уровень риска):

- оценка ожидаемого возможного ущерба от единичной реализации определенной угрозы (Single Loss Exposure, SLE) рассчитывается по формуле:

SLE = AV x EF; (1)

- итоговые ожидаемые потери от конкретной угрозы за определенный период времени (Annual Loss Exposure, ALE) характеризуют величину риска и рассчитывается по формуле:

ALE = SLE x ARO. (2)

Таким образом, конечная формула расчета рисков представляет собой произведение:

ALE = ((AV x EF = SLE) x ARO). (3)

Полученные результаты излагаются в табличной форме. После ранжирования рисков определяются требующие первоочередного внимания; основным методом управления

такими рисками является снижение, реже — передача. Риски среднего ранга могут передаваться или снижаться наравне с высокими рисками. Риски низшего ранга, как правило, принимаются и исключаются из дальнейшего анализа.

Диапазон ранжирования рисков принимается исходя из проведенного расчета их качественных величин. Так, например, если величины рассчитанных рисков лежат в диапазоне от 1 до 18, низкие риски находятся в диапазоне от 1 до 7, средние — в диапазоне от 8 до 14, высокие — в диапазоне свыше 14 [7]. Управление рисками сводится к снижению величин высоких и средних рисков до характерных для низких рисков значений. Снижение величины риска достигается за счет уменьшения одной или нескольких составляющих (AV, EF, SLE) путем принятия определенных мер. В основном это возможно применительно к EF и SLE, так как AV (стоимость ресурса) — фиксированный параметр. Снижение параметра SLE, т. е. вероятности реализации угрозы, может быть достигнуто за счет технических мер защиты информации [17].

Как видим, при качественной оценке большинство из описанных параметров принимается на основе мнения эксперта. Распространенность этого метода связана с тем, что количественная оценка вероятности реализации угрозы весьма затруднена ввиду относительной новизны информационных технологий и, как следствие, отсутствия универсальных методик оценки, и достаточного количества статистических данных. Однако в случае экспертной оценки стоимости ресурса (AV) точная количественная оценка (например, в денежном эквиваленте) чаще всего не проводится, и тогда определение параметра SLE в абсолютных величинах невозможно. Вместе с тем, только существенно и качественно выполненный анализ информационных рисков позволяет в дальнейшем провести сравнительный оценку по критерию «эффективность-стоимость» различных вариантов защиты. Таким образом, сама по себе качественная оценка рисков не позволяет аргументировать размер инвестиций в безопасность, так как не содержит конкретных цифр для определения затрат в случае реализации угроз, а значит и аргументировать стоимость работ, направленных на снижение рисков.

Количественная оценка риска рассчитывается либо аналитически, но тогда для ее точного расчета требуется очень большой объем исходных данных, что вызывает скептическое отношение к таким оценкам ряда специалистов по анализу риска, ориентированных на практические задачи [7, 13]. Либо графически, с построением в заданном пространстве зависимости потерь от вероятности реализации угроз. Прогнозирование отдельных параметров риска с приемлемой точностью является весьма трудоемкой задачей, и получить точную количественную оценку сложно. При этом стоимость ресурса рассчитывается с использованием экономических методик, а для расчета вероятности реализации угрозы требуется владеть методами, используемыми специалистами по информационной безопасности. Что еще больше усложняет задачу.

Результаты

Поэтому в реальных случаях организации чаще всего идут от имеющегося негативного опыта, что и является главной проблемой анализа информационных рисков. Ибо в том случае, когда действие происходит раньше анализа, эффективность предпринятых мер также отдается на волю случая. Кроме того, поскольку при создании системы информационной безопасности неизменно решается вопрос о целесообразности затрат на предлагаемые контрмеры, процесс ее формирования тормозится до принятия руководством решений о целесообразности (или нецелесообразности) затрат на защиту информации. Избежать такой ситуации поможет стандартная процедура коммуникации риска, представленная на (Рис. 1) и разработанная на основе [14, 15].

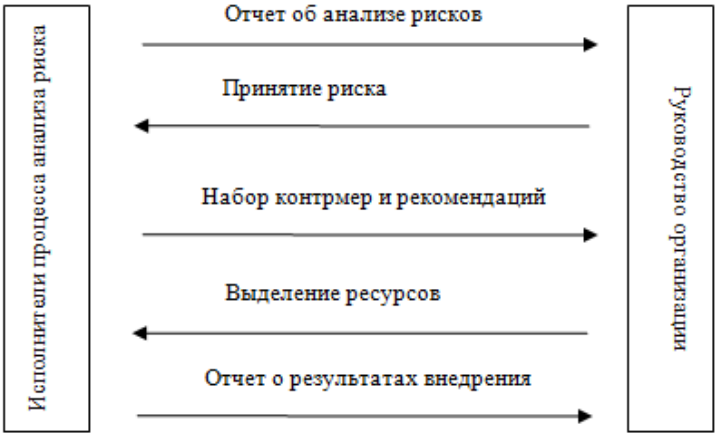

Рис. 1. Коммуникации риска

Как уже было сказано выше, риск – возможность ущерба, которая возникает как результат взаимодействия пары «угроза» и «уязвимость». Для каждой угрозы требуется оценить убытки, которые будут иметь место при ее реализации [14]. Постановка задачи анализа рисков в теоретических исследованиях, как правило, заключена в получении на основе статистических и вероятностных исследований математической модели информационных рисков для объекта исследования (например, актива или группы активов организации). Такая постановка задачи апробирована во многих задачах анализа информационных рисков. В качестве примера можно привести модели, полученные с использованием экспертных оценок и перечисленные в [16].

Основными этапами этой модели, применяемыми при количественной оценке информационных рисков, являются:

- первичный анализ рисков;
- планирование;
- внедрение мер защиты информации;
- мониторинг и тестирование уровня остаточного риска.

Естественно приведенная модель не является единственной (широко известна, например, модель Carnegy Mellon University [13]. Количественная оценка рисков позволяет четко рассчитать и аргументировать инвестиции в безопасность, но она крайне трудоемка.

Таким образом, анализ рисков в «чистом виде» является или слишком трудоемким, или не дает в дальнейшем эффективно этими рисками управлять. Поэтому на практике наибольшее распространение получили два упрощенных подхода к обоснованию проекта подсистемы обеспечения безопасности, не требующие расчета рисков для конкретного объекта.

Первый из них основан на проверке соответствия уровня защищенности объекта требованиям одного из стандартов в области информационной безопасности. Это может быть класс защищенности в соответствии с требованиями руководящих документов ФСТЭК России, например, профиль защиты, разработанный в соответствии со стандартом ISO-15408, или какой-либо другой набор требований. Тогда показатель достижения цели в области безопасности – это выполнение заданного набора требований. Показатель эффективности – минимальные суммарные затраты на выполнение поставленных функциональных требований. Методика достаточно эффективная, ибо ясно, что ФСТЭК, при разработке требований, учитывал среднестатистические риски для каждого класса объектов. Основной недостаток данного подхода заключается в том, что в случае, когда требуемый уровень защищенности жестко не задан (например, через законодательные требования или хотя бы приказы ФСТЭК) определить «наиболее эффективный» уровень защищенности объекта достаточно сложно. Кроме того «отнесение» конкретного объекта к определенному стандарту требует привлечение высококвалифицированных специалистов по ИБ.

Второй подход к построению системы обеспечения ИБ связан с оценкой и управлением рисками. Изначально он произошел из принципа «разумной достаточности» примененного к сфере обеспечения ИБ. Этот принцип быть описан следующим набором утверждений:

- необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в т.ч. и экономическим, заключающимся в снижении потерь от нарушений безопасности;
- стоимость средств защиты не должна превышать стоимости защищаемой информации (или других ресурсов – аппаратных, программных);
- затраты нарушителя на НСД к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

Если представить некоторую идеальную ситуацию, то идею такого подхода отображает приведенный график (рис. 2), позволяющий оптимизировать уровень защищенности объекта системой информационной безопасности на основе сравнения показателей стоимости совокупных потенциальных потерь без использования системы информационной безопасности и показателя стоимости реальных потерь при ее использовании.

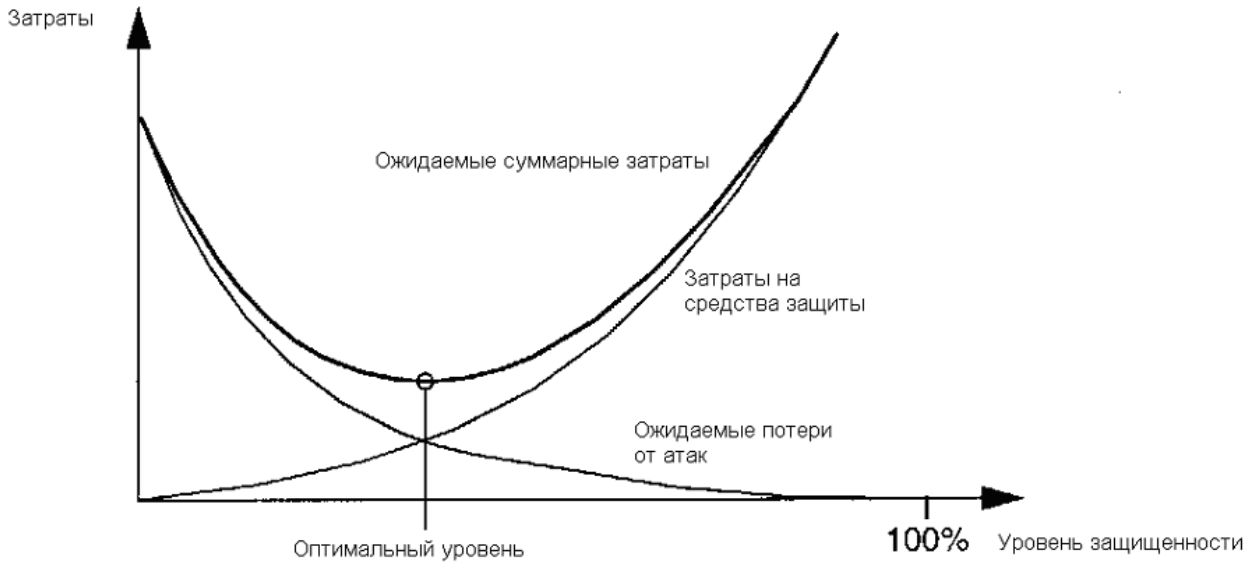

Рис. 2. Соотношение уровня затрат на средства защиты и ожидаемого ущерба.

По мере того, как затраты на защиту растут, размер ожидаемый потерь падает и если обе функции имеют вид, представленный на рисунке, то можно определить минимум функции «Ожидаемые суммарные затраты», который нам и требуется.

Заключение

К сожалению, на практике точные зависимости между затратами и уровнем защищенности определить далеко не всегда представляется возможным, поэтому аналитический метод анализа рисков в представленном виде используется довольно редко. Вместе с тем, количественная оценка рисков позволяет четко рассчитать и аргументировать инвестиции в безопасность, но она крайне трудоемка. Она рассчитывается либо аналитически, но тогда для ее точного расчета требуется очень большой объем исходных данных, что вызывает скептическое отношение к таким оценкам ряда специалистов по анализу риска, ориентированных на практические задачи. Либо графически, с построением в заданном пространстве зависимости потерь от вероятности реализации угроз. Прогнозирование отдельных параметров риска с приемлемой точностью является весьма трудоемкой задачей, и получить точную количественную оценку сложно.

Примечания:

1. Долматов А.С. Математические методы риск-менеджмента: учеб. пособие. М.: Экзамен, 2007. 320 с.

2. Лобанов А.А. Энциклопедия финансового риск-менеджмента. 2-е изд. / А.А. Лобанов, М.В. Чугунов. М.: Альпина, 2006. 878 с.

3. Соложенцев Е.Д. Сценарное логико-вероятностное управление риском в бизнесе и технике. М.: Бизнес-пресса, 2006. 530 с.

4. Половко А.М. Основы теории надежности / А.М. Половко, С.В. Гуров. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2006. 704 с.

5. Рябинин И.А. Основы теории и расчета надежности судовых электроэнергетических систем. Л.: Судостроение, 1971. 456 с.

6. Сугак Е.В. и др. Надежность технических систем / под общей ред. Е.В. Сугака, Н.В. Василенко. Красноярск: МГП «Раско», 2001. 608 с.

7. Астахов А.М. Искусство управления информационными рисками. М.: ДМК-Пресс, 2010. 312 с.

8. Peltier T.L. Information security risk analysis / T.L. Peltier. 2 ed. Auerbach Publications, 2005. 361 p.

9. Tipton, H.F. Information security management handbook / H.F. Tipton, M. Krause. 6 ed. Auerbach Publications, 2007. 328 p.

10. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. // Федеральное агентство по техническому регулированию и метрологии: сайт. URL: http://protect.gost.ru/document.aspx?control=7&id=129018 (дата обращения: 20.05.2010).

11. Jones A. Risk management for computer security / A. Jones, D. Ashenden. Elsevier Butterworth-Heinemann, 2005. 297 p.

12. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. 2-е изд. М.: Горячая линия-Телеком, 2004. 148 с.

13. Петренко, С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. М.: Компания АйТи, ДМК-Пресс, 2004. 384 с.

14. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. М.: Стандартинформ, 2006. 20 с.

15. Суханов А. Анализ информационных рисков в управлении информационной безопасностью [электронный ресурс] / А. Суханов // Журнал BYTE #11, 2008. // Безопасность: торговый каталог: сайт. URL: http://sec.bl.by/articles/detail177766

16. Золотарев В.В., Данилова Е.А. Управление информационной безопасностью. Часть 1. Анализ информационных рисков / В.В. Золотарев, Е.А. Данилова. Красноярск: изд-во Сиб. гос. аэрокос. ун-та, 2010. 136 с.

References:

1. Dolmatov A.S. Matematicheskie metody risk-menedzhmenta: ucheb. posobie. M.: Ekzamen, 2007. 320 s.

2. Lobanov A.A. Entsiklopediya finansovogo risk-menedzhmenta. 2-e izd. / A.A. Lobanov, M.V. Chugunov. M.: Al'pina, 2006. 878 c.

3. Solozhentsev E.D. Stsenarnoe logiko-veroyatnostnoe upravlenie riskom v biznese i tekhnike. M.: Biznes-pressa, 2006. 530 s.

4. Polovko A.M. Osnovy teorii nadezhnosti / A.M. Polovko, S.V. Gurov. 2-e izd., pererab. i dop. SPb.: BKhV-Peterburg, 2006. 704 s.

5. Ryabinin I.A. Osnovy teorii i rascheta nadezhnosti sudovykh elektroenergeticheskikh sistem. L.: Sudostroenie, 1971. 456 s.

6. Sugak E.V. i dr. Nadezhnost' tekhnicheskikh sistem / pod obshchei red. E.V. Sugaka, N.V. Vasilenko. Krasnoyarsk: MGP «Rasko», 2001. 608 s.

7. Astakhov A.M. Iskusstvo upravleniya informatsionnymi riskami. M.: DMK-Press, 2010. 312 s.

8. Peltier T.L. Information security risk analysis / T.L. Peltier. 2 ed. Auerbach Publications, 2005. 361 p.

9. Tipton, H.F. Information security management handbook / H.F. Tipton, M. Krause. 6 ed. Auerbach Publications, 2007. 328 p.

10. GOST R ISO/MEK 27001-2006. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoi bezopasnosti. Trebovaniya. // Federal'noe agentstvo po tekhnicheskomu regulirovaniyu i metrologii: sait. URL: http://protect.gost.ru/document.aspx?control=7&id=129018 (data obrashcheniya: 20.05.2010).

11. Jones A. Risk management for computer security / A. Jones, D. Ashenden. Elsevier Butterworth-Heinemann, 2005. 297 p.

12. Malyuk A.A., Pazizin S.V., Pogozhin N.S. Vvedenie v zashchitu informatsii v avtomatizirovannykh sistemakh. 2-e izd. M.: Goryachaya liniya-Telekom, 2004. 148 s.

13. Petrenko, S.A. Upravlenie informatsionnymi riskami. Ekonomicheski opravdannaya bezopasnost' / S.A. Petrenko, S.V. Simonov. M.: Kompaniya AiTi, DMK-Press, 2004. 384 s.

14. GOST R ISO/MEK 17799-2005. Informatsionnaya tekhnologiya. Prakticheskie pravila upravleniya informatsionnoi bezopasnost'yu. M.: Standartinform, 2006. 20 s.

15. Sukhanov A. Analiz informatsionnykh riskov v upravlenii informatsionnoi bezopasnost'yu [elektronnyi resurs] / A. Sukhanov // Zhurnal BYTE #11, 2008. // Bezopasnost': torgovyi katalog: sait. URL: http://sec.bl.by/articles/detail177766

16. Zolotarev V.V., Danilova E.A. Upravlenie informatsionnoi bezopasnost'yu. Chast' 1. Analiz informatsionnykh riskov / V.V. Zolotarev, E.A. Danilova. Krasnoyarsk: izd-vo Sib. gos. aerokos. un-ta, 2010. 136 s.

УДК 004.056.53

Обоснования требований к системе безопасности на основе анализа информационных рисков

Юрий Федорович Каторин

Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Российская Федерация
198035 Санкт-Петербург, ул. Двинская, 5/7
Доктор военных наук, профессор
E-mail: katorin@mail.ru

Аннотация.

В статье рассказывается об основных методах анализа информационных рисков и определении на этой основе необходимого уровня защиты объекта, расшифровывается само понятие «риск», исследуются количественная или качественная оценка возможных рисков, анализируются их недостатки и преимущества, а также описан метод обоснования требований к системе безопасности, основанный на проверке соответствия уровня защищенности объекта требованиям одного из стандартов в области информационной безопасности.

Ключевые слова: информационная безопасность, риск, анализ, количественная и качественная оценка, критерий, уровень защиты.