ОЦЕНКА РИСКОВ В ФУНКЦИОНИРУЮЩЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

RISK ASSESSMENT IN THE FUNCTIONING INFORMATION SYSTEM

A. Klyuev
A. Fajzenger
D. Yuriev

Summary. For any information system, the risk is the likelihood of destructive impact on its components through the implementation of a threat to information security. Accordingly, one of the most necessary components underlying the creation of an information security system is the methodology for risk assessment. This article is devoted to the investigation of the methodology for assessing information security risks. The methodological base of the terminology of information security is considered, which shows the relationship of risks with other components of the information security process. An example of a typical information system of the organization is also given. The methodology used is based on the expert methodology for risk analysis in accordance with ISO / IEC27005–2011, which includes: asset identification, threat identification, vulnerability identification, identification of countermeasures taken, identification of consequences, risk measurement, impact assessment, risk measurement. The relevance of the topic at the moment is due to the ever-increasing number of cyberthreats, the activity of intruders in the information environment, as well as the transition from a threat-oriented method of developing information security systems to a risk-oriented approach. The result of the work can be used in the construction of information security systems in various organizations, regardless of their scale and scope.

Keywords: risk, threat, vulnerability, incident, asset, confidentiality, integrity, accessibility, probability, consequences, countermeasure.

Клюев Андрей Сергеевич
Аспирант, Дальневосточный федеральный университет, г. Владивосток, kozerog1991@gmail.com
Файзенгер Алексей Аркадьевич
Аспирант, Дальневосточный федеральный университет, г. Владивосток
Юрьев Дмитрий Русланович
Аспирант, Дальневосточный федеральный университет, г. Владивосток

Аннотация. Для любой информационной системы риском является вероятность нанесения деструктивного воздействия ее компонентам посредством реализации угрозы информационной безопасности. Соответственно одним из самых необходимых компонентов, лежащих в основе создания системы информационной безопасности, является методология оценки рисков. Настоящая статья посвящена исследованию методологии оценки рисков информационной безопасности. Рассматривается методологическая база терминологии информационной безопасности, в которой показывается взаимосвязь рисков с другими составляющими процесса информационной безопасности. Также приводится пример типовой информационной системы организации. Исследуемая методология базируется на экспертной методике анализа рисков в соответствии со стандартом ИСО/МЭК 27005–2011, включающей в себя: идентификацию активов, идентификацию угроз, идентификацию уязвимостей, идентификацию принятых контрмер, идентификацию последствий, измерение риска, оценку последствий, измерение уровня риска. Актуальность темы в настоящий момент обусловлена постоянно растущим количеством киберугроз, активностью злоумышленников в информационной среде, а также переходом от угрозо-ориентированной методике разработки систем информационной безопасности к риск-ориентированному подходу. Результат работ может быть использован при построении систем обеспечения информационной безопасности в различных организациях, независимо от их масштаба и сферы деятельности.

Ключевые слова: риск, угроза, уязвимость, инцидент, актив, конфиденциальность, целостность доступность, вероятность, последствия, контрмера.

Вне зависимости от сферы деятельности и масштабов предприятия его функционирование невозможно без нормальной работоспособности информационных систем, обеспечивающих реализацию и поддержку бизнес-процессов. Однако информационные технологии позволяют не только повысить эффективность бизнес-процессов, но и являются источниками критичных для информационной инфраструктуры рисков. [1]

Для любой информационной системы риском является вероятность нанесения деструктивного воздействия ее компонентам посредством реализации угрозы информационной безопасности. Соответственно одним из самых необходимых компонентов, лежащих в основе создания системы информационной безопасности, является методология оценки рисков. [2]

Место рисков в структуре терминологии информационной безопасности и их взаимосвязь с остальными понятиями показана на рисунке 1.

Нарушители (источники угроз) реализуют угрозы на уязвимости информационных технологий ведут, что ведет к увеличению рисков.

В свою очередь владельцы информационных активов предпринимают контрмеры для предотвращения

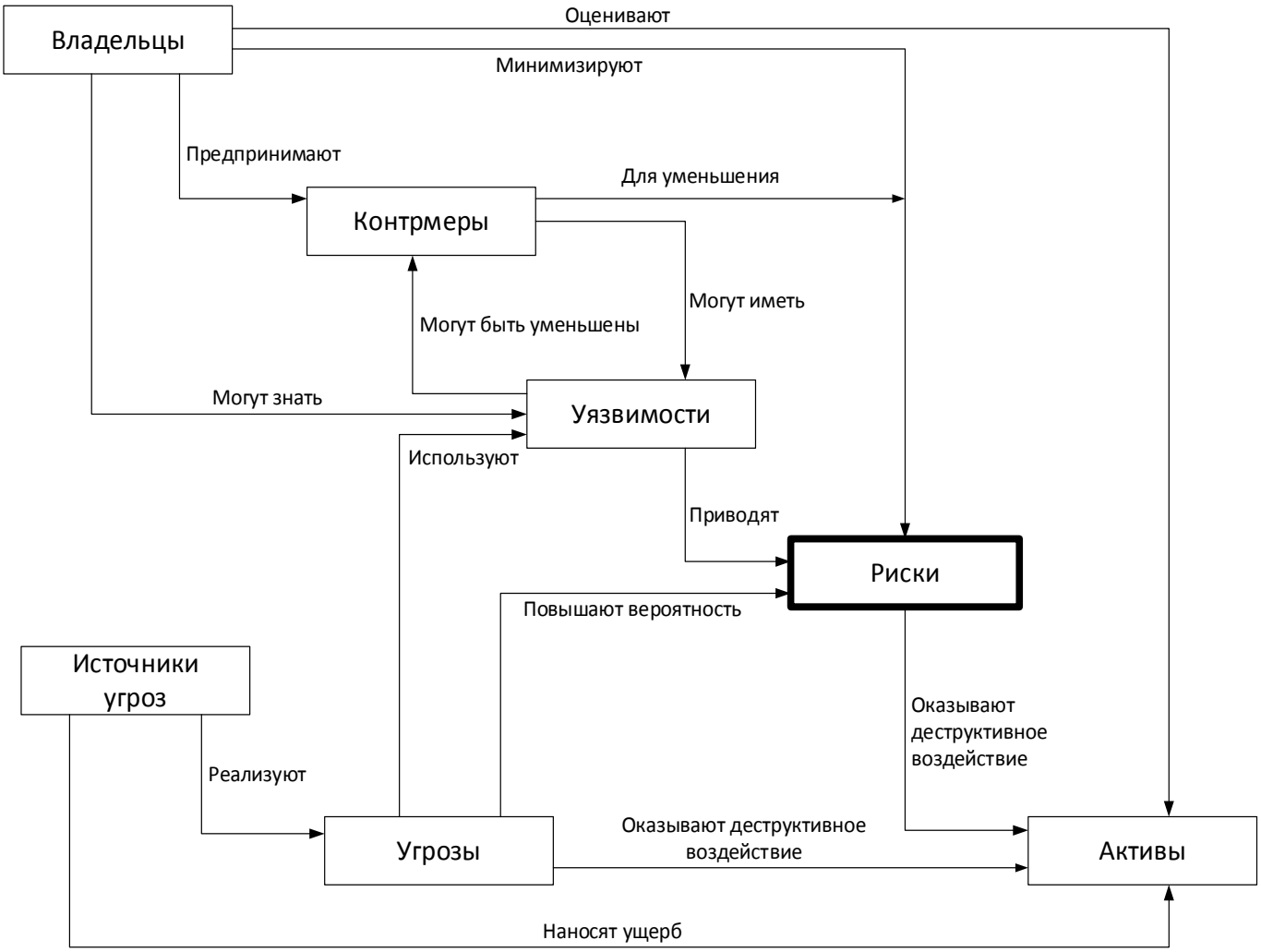

Рис. 1. Место рисков в структуре понятий информационной безопасности

риска или стараются минимизировать риски информационной безопасности.

Поскольку риск представляет из себя комбинацию последствий, которые происходят из-за деструктивного воздействия и вероятности реализации такого воздействия все риски информационной безопасности информационной системы должны быть идентифицированы, количественно определены, качественно показаны и приоритезированы в соответствии с критериями оценки рисков организации.

Оценка риска является процессом, позволяющим определить потенциальные угрозы и уязвимости активов, а также понять какими контрмерами они могут быть нейтрализованы.

Процесс оценки рисков состоит из следующих шагов:

- идентификация активов;
- идентификация угроз;
- идентификация уязвимостей;
- идентификация принятых контрмер;
- идентификация последствий;
- измерение риска;
- оценка последствий;
- измерение уровня риска.

Идентификация активов выполняется в целях выявления ресурсов, нуждающихся в защите.

В целях более точной идентификации активов рассмотрим типовую архитектуру информационной системы (рисунок 2). [3]

В приведенной архитектуре активами являются: информация, хранимая в базе данных; операционные системы; программное обеспечение приложения; средства вычислительной техники, сетевой трафик, сетевое оборудование.

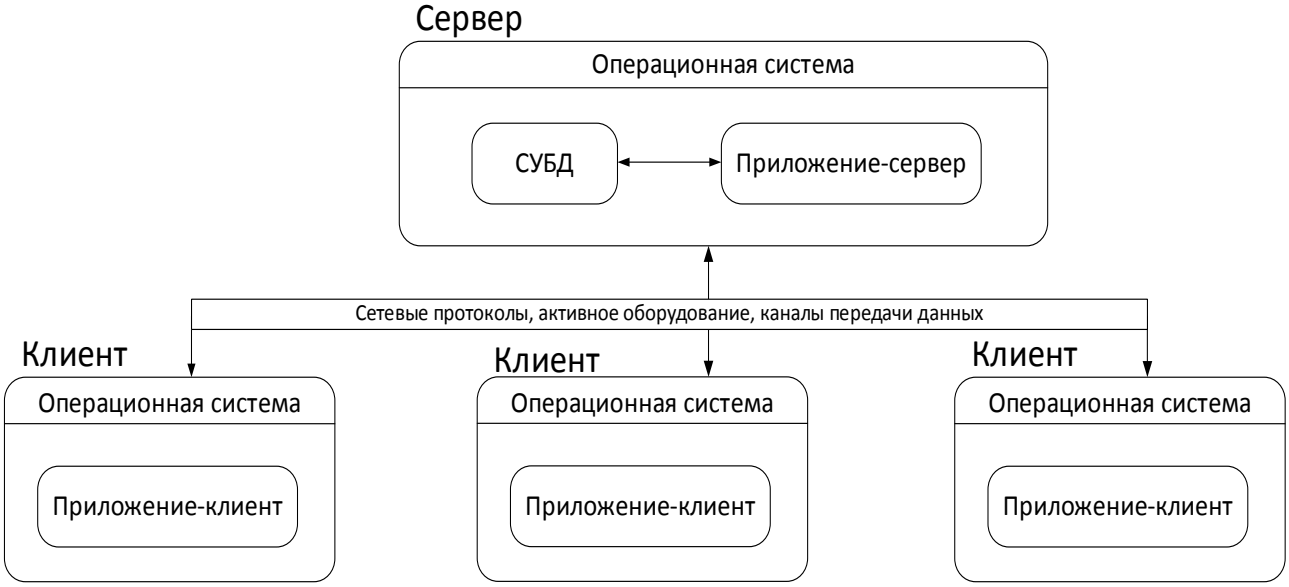

Рис. 2. Типовая архитектура информационной системы

Вместе с идентификацией активов производится оценка их ценности, которая может носить количественную (финансовую) характеристику или качественную.

Идентифицированные активы необходимо ранжировать по шкале от 1 до 5 в соответствии с ценностью актива для организации. [4]

Идентификация угроз. Угроза обладает потенциалом оказания деструктивного воздействия на актив. На данном этапе идентифицируются все источники угроз и каналы их реализаций.

Источниками угроз могут быть: нарушитель, воздействующий на актив из внешних границ (внешний нарушитель); нарушитель, воздействующий на актив из внутренних границ (внутренний нарушитель); техногенный источник; стихийный источник.

Каналами реализации могут быть: физические каналы (каналы непосредственного доступа к активам), каналы связи (линии связи и каналообразующее оборудование), технические каналы (оптические, видовые, акустические и др.).

Угрозы необходимо идентифицировать по показателям «низкая», «средняя», «высокая» в соответствии с вероятностью ее реализации.

Идентификация уязвимостей производится в целях определения уязвимостей, которые могут быть использованы угрозами для нанесения деструктивного воздействия на актив.

В качестве уязвимостей могут быть рассмотрены: уязвимости операционных систем, уязвимости СУБД, уязвимости приложений, уязвимости протоколов передачи данных, уязвимости сетевых устройств, уязвимости организации функционирования информационной системы.

Важно понимать, что как наличие угрозы, так и наличие уязвимости не причиняет само по себе вреда активам, а лишь делает такую возможность потенциальной.

Уязвимости необходимо идентифицировать по показателям «низкая», «средняя», «высокая» в соответствии с вероятностью их реализации.

Идентификация принятых контрмер проводится в целях выявления актуальных угроз и уязвимостей, а также для оптимизации расходов на построение системы информационной безопасности. Кроме того, идентификация контрмер проводится, чтобы определить — работают ли штатно принятые контрмеры, отсутствие штатного функционирования может послужить наличием уязвимости в системе безопасности.

Обычно к принятым контрмерам относятся: сведения об охране объекта и его элементов, сведения о физической защищенности активов, сведения о технических средствах охраны, штатные механизмы безопасности операционных систем и приложений, механизмы безопасности сетевого оборудования.

Идентификация последствий. К последствиям реализации угроз относят нарушение конфиденциально-

Таблица 1. Определение вероятности реализации риска

	Уровни угроз	Низкая			Средняя			Высокая		
	Уровни уязвимостей	Н	С	В	Н	С	В	Н	С	В
Ценность актива	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

Таблица 2. Совокупность результатов оценки рисков

№	Риск	Актив	Вероятность реализации	Последствия	Уровень риска
1	Атака отказа в обслуживании	Каналообразующее оборудование	6	Недоступность сервисов для клиентов	200000 руб. в день
2	Атака вируса-шифровальщика	Средства вычислительной техники, программное обеспечение, СУБД	8	Недоступность сервисов для клиентов и сотрудников	600000 руб. в день

сти, целостности и доступности функционирования информационной системы.

По своей направленности на актив последствия могут быть:

- прямыми: стоимость восстановления актива, стоимость приобретения нового актива, стоимость приостановленных операций;
- косвенными: упущенные возможности, нарушение установленных законодательством обязанностей, нарушение этических норм.

Учитывая особенности функционирующих систем весьма критичными угрозами являются угрозы нарушения доступности.

Измерение риска базируется на оцененных последствиях и вероятностях реализации инцидентов информационной безопасности применительно к активам. Измеренный риск является комбинацией вероятности инцидента информационной безопасности и его последствий.

В процессе измерения риска активы организации оцениваются с точки зрения замены или восстановления, затем полученная стоимость переводится в качественный показатель.

Ценность активов организации, уровни угроз и уязвимостей, относящиеся к каждому виду последствий, приводятся в матричной форме (таблица 1). Для каждой комбинации идентифицируется мера риска на основе шкалы от 0 до 8. Для каждого актива рассматриваются соответствующие угрозы и уязвимости, и в соответствии с ценностью актива устанавливается вероятность риска. Например: если актив имеет ценность 3, угроза является «средней», а уязвимость «низкой», то мера риска = 3 [5].

Оценка последствий начинается с классификации активов в соответствии с их критичностью, с точки зрения важности активов для осуществления бизнес-процессов организации.

Последствия влияния рисков на активы определяются путем моделирования результатов событий либо совокупности событий, или экстраполяции экспериментальных исследований или данных за прошедшее время. Последствия могут быть выражены с точки зрения финансовых, технических, репутационный или иных критериев, значимых для организации.

Измерение уровня риска базируется на оцененных последствиях и вероятности реализации риска. Измеренный риск является комбинацией вероятности риска информационной безопасности и его последствий.

Как правило на данном этапе заканчивается процесс оценки рисков. Выходными данными после проведенной работы являются: совокупность рисков информационной безопасности, активы подверженные рискам, значения вероятности реализации риска и последствия реализации риска (таблица 2).

Однако процесс менеджмента рисков на данном этапе не заканчивается.

Далее организация должна выработать по каждому риску стратегию его обработки: отказ от риска, снижение риска, передача (делегирование) риска, принятие риска. В соответствии с данной концепцией должна быть

реализован процесс управления рисками информационной безопасности.

Одним из примеров методов управления рисков информационной безопасности является метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation — Оценка оперативной критической угрозы, активов и уязвимостей).

Особенность метода OCTAVE заключается в том, что процедура анализа рисков производится исключительно силами сотрудников предприятия, без привлечения сторонних консультантов. В этих целях создается рабочая группа, включающая как технических специалистов, так и управленческий персонал разного уровня, что позволяет многогранно оценить последствия реализации инцидентов информационной безопасности и разработать контрмеры.

Структурно OCTAVE предполагает следующие уровни управления рисками:

1) Разработка профиля угроз активу.
2) Идентификация инфраструктурных уязвимостей.
3) Разработка концепции и политики безопасности.

На первом этапе, в ходе проведения практических семинаров внутри предприятия, осуществляется разработка профилей угроз безопасности, включающих в себя аудит активов и оценку их ценности, идентификацию применимых требований нормативной базы и действующего законодательства, выявление угроз и оценку вероятности их реализации, а также определение комплекса действующих мер по поддержанию режима информационной безопасности.

На втором этапе проводится технический аудит уязвимостей информационных активов предприятия в отношении угроз информационной безопасности, чьи профили были определены на предыдущем этапе, который включает в себя идентификацию имеющихся уязвимостей информационных систем организации и оценку их величины.

На третьем этапе производится оценка рисков и обработка рисков информационной безопасности, включающая в себя расчёт величин и вероятностей нанесения ущерба в результате реализации угроз информационной безопасности с использованием уязвимостей, которые были идентифицированы ранее. Определение стратегии защиты, а также выбор вариантов и принятие решений по реагированию на риски. Величина риска определяется как усредненная величина годовых потерь организации в результате реализации угроз безопасности.

Выбор качественного или количественного подходов к оценке рисков, определяется характером бизнеса организации и уровнем его информатизации, т.е. важностью для него информационных активов, а также уровнем зрелости организации.

Эффективность процесса управления рисками информационной безопасности определяется точностью и полнотой анализа и оценки факторов риска, а также эффективностью используемых в организации механизмов принятия управленческих решений и контроля их исполнения.

ЛИТЕРАТУРА

1. ГОСТ Р ИСО/МЭК 13335–1 «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».— М.: Стандартинформ.—2008.—18с.
2. ГОСТ Р ИСО/МЭК 15408–1–2008. «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» — М.: Стандартинформ.—2009.—41с.
3. Международный стандарт ИСО/МЭК 27005–2011. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».—К.: АО «Ситроникс информационные технологии Украина».—2012.—94с.
4. Гаспарян М. С. Информационные системы и технологии / Гаспарян М. С., Лихачева Г. Н.—М.: Издат. центр ЕАОИ.—2008.—384с.
5. Пастоев А. Методологии управления ИТ-рисками [Электронный ресурс].— Режим доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/metodologii-upravleniya-it-riskami (дата обращения 16.01.2018).
6. Астахов А. Как управлять рисками информационной безопасности? [Электронный ресурс].— Режим доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/kak-upravlyat-riskami-informacionnoi-bezopasnosti (дата обращения 17.01.2018)