УДК 004.056

АНАЛИЗ МЕТОДИК ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Абдулаев А., Медетбек кызы А., Мурзабек кызы Г.
Кыргызский государственный университет строительства, транспорта и архитектуры имени Н. Исанова

В статье описаны и проанализированы основные методики оценки рисков информационной безопасности. Отмечено, что наиболее эффективно использовать смешанный подход, сочетающий в себе как качественную, так и количественную оценку рисков. Проведен анализ нескольких существующих программных продуктов для методики оценки рисков информационной безопасности.

***Ключевые слова*:** информационная безопасность, риск информационной безопасности, анализ рисков, методика оценки рисков, количественная оценка, качественная оценка.

МААЛЫМАТТЫК КООПСУЗДУКТУН ТОБОКЕЛДИКТЕРИНИН УСУЛДАРЫН ТАЛДОО

Абдулаев А.А., Медетбек кызы А., Мурзабек кызы Г.
Н. Исанов атындагы Кыргыз мамлекеттик курулуш, транспорт жана архитектуры университети

Макалада маалыматтык коопсуздуктун тобокелдиктерин баалоонун негизги ыкмалары баяндалган жана талданган. Бул өзүндө да сапаттуу жана тобокелдиктерге сандык баа берүүнү камтыган аралаш мамилени абдан натыйжалуу пайдаланууга белгиленген. Маалыматтык коопсуздуктун тобокелдиктерин баалоо методикасы үчүн бир нече учурдагы программалык продукттарга талдоо жүргүзүлдү.

***Баштапркы сөздөр*:** маалыматтык коопсуздук, маалымат коопсуздугу, опурталдар, опурталдарды талдоо, опурталдарды баалоо методикасы, сандык баалоо, сапаттуу баалоо.

ANALYSIS OF METHODOLOGIES FOR ASSESSING INFORMATION SECURITY RISKS

Abdulaev A., Medetbek kyzy A., Murzabek kyzy G.
Kyrgyz State University of Construction, Transport and Architecture named after N. Isanov

The article describes and analyzes the main methods of information security risk assessment. It was noted that it is most effective to use a mixed approach that combines both qualitative and quantitative risk assessment. Several existing software products for information security risk assessment methodology have been analyzed.

Key words: information security, information security risk, risk analysis, risk assessment methodology, quantitative assessment, qualitative assessment.

Использование любых технологий наряду с положительным эффектом влечёт за собой возникновение неопределённости и связанных с этими технологиями рисков. Информационные технологии (ИТ) не исключение. Широкое применение информационных технологий как в системах управления компаниями, так и в технологических процессах привело к тому, что риски, связанные с ИТ, стали важной частью всех бизнес-рисков организации.

Методики оценки рисков для информационных систем преследуют одну и ту же цель: понять, какие риски наиболее актуальны для информационной системы данной организации. Но следовать к этой цели они могут разными способами, соответственно, будут и заметно отличаться получаемые результаты. Рассмотрим несколько наиболее актуальных методик, которые могут быть легко найдены как в интернете, так и в специальной литературе [1-4].

Методика FRAP

Методика FRAP (Facilitated Risk Analysis Process), разработанная компанией Peltier and Associates, описывает подход к качественной оценке рисков. Целью методики является выявление, оценка и документирование состава рисков информационной безопасности для заранее определенной области исследования. В качестве области исследования может быть

выбрана информационная система, приложение, бизнес-процесс или другая часть инфраструктуры организации, нуждающаяся в оценке рисков информационной безопасности.

В методике, обеспечение информационной безопасности предлагается рассматривать в рамках процесса управления рисками. Управление рисками в сфере информационной безопасности – процесс, позволяющий компаниям найти баланс между затратами средств и сил на средства защиты и получаемым эффектом.

Управление рисков должно начинается с оценки рисков: должным образом оформленные результаты оценки станут основой для принятия решений в области повышения безопасности системы в будущем.

После завершения оценки, проводится анализ соотношения затрат и получаемого эффекта, который позволяет определить те средства защиты, которые нужны, для снижения риска до приемлемого уровня.

FRAP один из наиболее распространенных методик качественной оценки рисков информационной безопасности. В наибольшей степени данный метод подходит организациям, осуществляющим первоначальное внедрение процессов управления рисками и не имеющим ресурсов или необходимости в покрытии этими процессами всей организации. Также метод подходит для небольших организаций или обособленных подразделений крупных организаций. Метод позволят выделить для управления рисками информационной безопасности отдельную область (информационную систему, бизнес-процесс, подразделение) и постепенно распространять процессы управления рисками на всю организацию.

Методика OCTAVE

Методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation - оценка критичных угроз, активов и уязвимостей), разработанная Университетом Карнеги-Мелон, описывает подход к качественной оценке рисков. Данная методика предназначена для формализации и оптимизации процесса оценки рисков информационной безопасности в организации и

обеспечения возможности получения необходимых организации результатов с минимальными затратами времени и ресурсов. Методика рассматривает людей, технологии, информационные системы, приложения, и другие объекты в контексте их отношения к информации и бизнес-процессам и услугам, которые они поддерживают.

Особенность данной методики заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная *группа*, включающая как технических специалистов, так и руководителей разного уровня, что позволяет всесторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры.

Оценка рисков осуществляется в три этапа, которым предшествует набор подготовительных мероприятий, включающих в себя согласования графика семинаров, назначения ролей, планирование, координация действий участников проектной группы.

На первом этапе, в ходе практических семинаров, осуществляется разработка профилей угроз, включающих в себя инвентаризацию и оценку ценности активов, идентификация применимых требований законодательства и нормативной базы, идентификацию угроз и оценку их вероятности, а также определение системы организационных мер по поддержанию режима ИБ.

На втором этапе производится технический анализ уязвимостей информационных систем организации в отношении угроз, чьи профили были разработаны на предыдущем этапе, который включает в себя идентификацию имеющихся уязвимостей информационных систем организации и оценку их величины.

На третьем этапе производится оценка и обработка рисков ИБ, включающая в себя определение величины и вероятности причинения ущерба в результате осуществления угроз безопасности с использованием уязвимостей, которые были идентифицированы на предыдущих этапах,

определение стратегии защиты, а также выбор вариантов и принятие решений по обработке рисков. Величина риска определяется как усредненная величина годовых потерь организации в результате реализации угроз безопасности.

Методика RiskWatch

Компания RiskWatch разработала собственную методику анализа рисков и семейство программных средств, и она может быть использована отдельно для анализа физических и программных рисков.

RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. Рекомендации в данном случае выдаются на основании известной аксиомы о том, что стоимость защиты не должна превышать стоимость потерь компании от реализации того или иного риска в реальной жизни. При этом сначала определяются категории защищаемых ресурсов, затем описываются возможные потери и классы инцидентов.

В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов.

Первый этап - *определение* предмета исследования. Здесь описываются такие параметры, как тип организации, состав исследуемой системы (в общих чертах), базовые требования в области безопасности. Для облегчения работы аналитика, в шаблонах, соответствующих типу организации ("коммерческая информационная система", "государственная/военная информационная система" и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации.

Второй этап - ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе, в частности, подробно описываются

ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов.

Третий этап - количественная *оценка риска*. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования. По сути, риск оценивается с помощью математического ожидания потерь за год.

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия [14,18].

Недостатки методики RiskWatch:

– методика RiskWatch подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов;

– полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска с системных позиций – метод не учитывает комплексный подход к информационной безопасности;

– программное обеспечение RiskWatch существует только на английском языке;

– высокая стоимость лицензии.

Методика CRAMM

Основу методики CRAMM (CCTA (Central Computer and Telecommunications Agency, Великобритании) Risk Analysis and Managment Method) составляет комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа, что, несомненно, можно

отнести к ее достоинствам. Методика является универсальной, ориентированная на разные типы организаций.

Данная методика заключается в описании защищаемых ресурсов с помощью выражения их денежной ценности, после чего определяется необходимый уровень защиты системы в соответствии с ценностью защищаемых данных.

Далее проводится комплексная оценка угроз для каждого из ресурсов, а также уровня данных угроз, после чего используются стандартные рекомендации исходя из уровня угроз и требуемого уровня защиты данного ресурса, т.е. проводится идентификация ресурсов: физических, программных и информационных, содержащихся внутри границ системы, построив при этом модели системы, с деревом связи ресурсов. Эта схема позволяет выделить критичные элементы. Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения. Оцениваются зависимость пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей, вычисляются уровни рисков и анализируются результаты.

Таким образом, CRAMM первоначально определяет качественный уровень, а потом производит количественную оценку (в баллах). В методике отсутствуют: процесс интеграции способов управления, мониторинг эффективности используемых способов управления и способов управления остаточными рисками, процесс реагирования на инциденты.

Сильная сторона методики CRAMM — идентификация элементов риска информационной безопасности: материальных и нематериальных активов, их ценности, угроз, мер безопасности, величины потенциального ущерба и вероятности реализации рискового события. Её основной недостаток - он разработан для аудита и анализа уже эксплуатирующихся информационных систем и поэтому она не всегда подходит для этапа проектирования системы.

Методика Гриф

Для проведения полного анализа информационных рисков, прежде всего, необходимо построить полную модель информационной системы с точки зрения ИБ. Для решения этой задачи ГРИФ, в отличие от представленных на рынке западных систем анализа рисков, которые громоздки, сложны в использовании и часто не предполагают самостоятельного применения ИТ-менеджерами и системными администраторами, ответственными за обеспечение безопасности информационных систем компаний, обладает простым и интуитивно понятным для пользователя интерфейсом. Основная задача методики ГРИФ – дать возможность ИТ менеджеру самостоятельно оценить уровень рисков в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании и иметь возможность доказательно (в цифрах) убедить руководство компании в необходимости инвестиций в сферу ее информационной безопасности.

На первом этапе метода ГРИФ проводится опрос ИТ-менеджера с целью определения полного списка информационных ресурсов, представляющих ценность для компании.

На втором этапе проводится опрос ИТ-менеджера с целью ввода в систему ГРИФ всех видов информации, представляющей ценность для компании. Введенные группы ценной информации должны быть размещены пользователем на указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и т. д.). Заключительная фаза — указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

На третьем этапе проходит определение всех видов пользовательских групп с указанием числа пользователей в каждой группе. Затем фиксируется, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяются виды (локальный и/или

удаленный) и права (чтение, запись, удаление) доступа пользователей ко всем ресурсам, содержащим ценную информацию.

На четвертом этапе проводится опрос ИТ-менеджера для определения средств защиты ценной информации на ресурсах. Кроме того, в систему вводится информация о разовых затратах на приобретение всех применяющихся средств защиты информации и ежегодные затраты на их техническую поддержку, а также ежегодные затраты на сопровождение системы информационной безопасности компании.

На завершающем этапе необходимо ответить на вопросы по политике безопасности, реализованной в системе, что позволит оценить реальный уровень защищенности системы и детализировать оценки рисков.

В результате выполнения всех действий по данным этапам, на выходе будет сформирована полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволит перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

К недостаткам ГРИФ можно отнести:

- Отсутствие привязки к бизнесс-процессам (запланировано в следующей версии).

- Отсутствие возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности (запланировано в следующей версии).

- Отсутствие возможности добавления специфичных для данной компании требований политики безопасности.

Методика Microsoft

Методика управления рисками информационной безопасности, предложенная корпорацией Microsoft, изложена в ее «Руководстве по управлению рисками безопасности». Эта комбинированная методика объединяет элементы количественного и качественного подходов. При этом

качественный подход используется для быстрого упорядочивания перечня всех рисков информационной безопасности, а количественный подход позволяет в дальнейшем выполнить более глубокий анализ наиболее значимых рисков. Это дает возможность сформировать относительно небольшой перечень основных рисков, требующих глубокого изучения, и сконцентрировать усилия на этих рисках.

В соответствии с данной методикой, управление рисками информационной безопасности (ИБ) представляет собой непрерывный процесс, включающий следующие этапы:

– планирование сбора данных (создание базы для оценки рисков ИБ);

– взаимосвязанный сбор данных (информации о рисках ИБ);

– приоритизация рисков (ранжирование выявленных рисков).

Информация о уязвимых местах, угрозах ИБ, системе и механизмах ИБ, о физических и нефизических активах компании позволяет провести оценку рисков ИБ согласно методике компании, Microsoft на достаточно высоком уровне.

Методика Microsoft содержит детальное описание инструкций по реализации каждого из перечисленных этапов оценки рисков ИБ, обзор ключевых факторов успеха, а также типовые перечни ИТ-активов, угроз, уязвимостей и шаблоны документов, необходимых для реализации процесса оценки рисков информационной безопасности.

С точки зрения практического применения можно выделить следующие достоинства методики Microsoft:

- комбинирование качественного и количественного подхода к оценке рисков позволяет производить более ресурсоемкую количественную оценку только в тех случаях, в которых это необходимо для эффективного управления рисками информационной безопасности;

- наличие средств автоматизации анализа рисков позволяет минимизировать трудозатраты и время выполнения мероприятий по анализу и оценке рисков ИБ;

- наличие детального описания каждого из этапов процесса оценки рисков информационной безопасности позволяет уменьшить вероятность ошибок исполнителей;

- использование непрерывного цикла позволяет организовать регулярную непрерывную оценку рисков и поддержание в актуальном состоянии информации о текущем уровне рисков, так и о необходимых действиях по управлению рисками;

- возможность оценки рисков информационной безопасности в деньгах делает возможным использование результатов оценки рисков при технико-экономическом обосновании инвестиций, необходимых для внедрения средств и методов защиты информации;

- наличие вспомогательных материалов, поддерживающих процесс анализа рисков, позволяет свести к минимуму требования к специальным знаниям и компетентности непосредственных исполнителей мероприятий.

Методика Microsoft присущи следующие недостатки:

- высокая трудоемкость требует привлечения значительных ресурсов внутри организации или извне;

- отсутствие типовых рисковых сценариев требует дополнительных трудозатрат участников проектной команды в процессе определения актуальных для организации сценариев рисков информационной безопасности.

Рассмотренные методики в той или иной степени позволяют показать примерную оценку информационного риска для предприятия. Невозможно дать точную оценку риску, ввиду сложности представления ущерба для системы из-за большого количества компонентов вычислительной среды и различных топологий локальных и корпоративных сетей с их программно-аппаратным наполнением и управлением.

Как видно, каждый из программных продуктов имеет свои достоинства и недостатки. Ни одна из методик не предлагает оценку рисков в корпоративной среде предприятия, кроме методики анализа корпоративных

рисков от Microsoft. Современный бизнес диктует скорость развития технологий, как с экономической, так и с технической стороны.

Заключение

В статье описаны и проанализированы основные методики оценки рисков информационной безопасности. Отмечено, что наиболее эффективно использовать смешанный подход, сочетающий в себе как качественную, так и количественную оценку рисков. Проведен анализ нескольких существующих программных продуктов для методики оценки рисков информационной безопасности. Каждый из продуктов имеет свои достоинства и недостатки, но сфера их применения зависит от самого предприятия.

ЛИТЕРАТУРА

1. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность // Петренко С.А., Симонов С.В. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.
2. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009. № 1(49). С. 15–26.
3. Международный стандарт ISO/IEC 27005:2008. Информационная технология – Методы защиты – Менеджмент рисков информационной безопасности BS ISO/IEC 27005:2008.
4. Левченко В.Н. Этапы анализа рисков. URL: http://www.cfin.ru/finanalysis/risk/ stages.shtml