УДК 621.3

А.А. Замула[1], И.О. Жуков[1], Ю.В. Землянко[2]

[1] *Харьковский национальный университет радиоэлектроники, Харьков*
[2] *Харьковский государственный университет питания и торговли, Харьков*

ТЕХНОЛОГИИ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются вопросы, связанные с оценкой рисков информационной безопасности. Предлагаются и анализируются методы для оценки рисков информационной безопасности.

Ключевые слова: *информационная безопасность, оценка рисков, методы для оценки рисков.*

Актуальность проблемы

Современным информационным системам доверяют решение самых разнообразных и важных задач: автоматизированное управление технологическими процессами и промышленными предприятиями, автоматизацию деятельности банков, финансовых бирж, страховых компаний, торговых компаний и т.д. Растут масштабы и сложность корпоративных систем. Важность задачи обеспечения безопасности корпоративных информационных ресурсов осознана как руководством компаний, так и клиентами. Уже недостаточно ограничиваться защитой отдельных сегментов информационной системы.

Требования информационной безопасности должны быть направлены на обеспечение оптимального режима функционирования информационной системы в целом.

Построение любой системы информационной безопасности должно начинаться с анализа рисков. Прежде чем проектировать систему информационной безопасности, необходимо точно определить, какие угрозы существуют для данной информационной системы, насколько они потенциально опасны.

Грамотный учет существующих угроз и уязвимостей информационной системы, выполненный на этой основе анализ рисков закладывают основу для выбора решений с необходимым уровнем информационной безопасности при минимальных затратах.

Анализ и управление рисками применяется для оценки угроз, уязвимостей и рисков информационный системы, а также определения контрмер, обеспечивающих достаточный уровень защищенности этой информационной системы. Процесс оценивания рисков состоит в определении характеристик рисков информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства защиты.

При оценивании рисков учитываются многие факторы: ценность ресурсов, оценки значимости угроз, уязвимостей, эффективность существующих и планируемых средств защиты. Существуют различные подходы к оценке рисков, выбор которых зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности [1 – 5].

Цель статьи – проанализировать методы оценивания рисков информационной безопасности и на основе проведенного анализа предложить подход для выбора технологий управления рисками.

Анализ методов оценки рисков

Метод CORAS использует модель UML (унифицированный язык моделирования – язык графического описания для объектного моделирования в области разработки программного обеспечения). Для документирования промежуточных результатов и для того, чтобы представить полные заключения об анализе рисков информационной безопасности, используются специальные диаграммы CORAS, которые встроены в UML.

Метод CORAS – это компьютеризированный инструмент, который поддерживает документирование, создание отчетов о результатах анализа путем моделирования риска.

Все работы относительно рисков проводятся посредством следующих процедур:

1) подготовительные мероприятия – сбор общих сведений об объекте анализа;

2) представление клиентом объектов, которые необходимо проанализировать;

3) детализированное описание задачи аналитиком;

4) проверка корректности и полноты документация, представленной для анализа;

5) мероприятия по выявлению рисков, (осуществляется, например, в форме семинара) возглавляемые аналитиками;

6) оценка вероятностей и последствий инцидентов информационной безопасности;

7) выявление приемлемых рисков и рисков, которые должны быть представлены на дальнейшую оценку для возможного устранения;

8) устранение угроз, с целью сокращения вероятности и / или последствий инцидентов в области информационной безопасности [2].

В методе CRAMM анализ рисков включает в себя идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов.

Контроль рисков состоит в идентификации и выборе контрмер, позволяющих снизить риски до приемлемого уровня.

Формальный метод, основанный на этой концепции, должен позволить убедиться, что защита охватывает всю систему и существует уверенность в том, что:

- все возможные риски идентифицированы;
- уязвимости ресурсов идентифицированы и их уровни оценены;
- угрозы идентифицированы и их уровни оценены;
- контрмеры эффективны;
- расходы, связанные с информационной безопасностью, оправданы.

Исследование состояния информационной безопасности системы с помощью метода CRAMM проводится в три стадии:

1) на первой стадии исследования производится идентификация и определение ценности защищаемых ресурсов. По завершению стадии заказчик исследования должен знать, достаточно ли для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или необходимо проведение более детального анализа;

2) на второй рассматриваются вопросы, относящиеся оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии 2 заказчик получает идентифицированные и оцененные уровни рисков для своей системы;

3) на третьей производится поиск адекватных контрмер. По существу это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. В конце стадии 3 заказчик будет знать, как следует модифицировать систему в терминах мер уклонения от риска, а также выбора и проработки, специальных мер противодействия, ведущих к снижению или минимизации оставшихся рисков [3].

Метод OCTAVE – это метод оперативной оценки критических угроз, активов и уязвимостей. Методика подразумевает создание группы анализа, которая изучает безопасность. Группа анализа (ГА) включает сотрудников бизнес-подразделений, эксплуатирующих систему, и сотрудников отдела информационных технологий [4].

Метод OCTAVE – это трехэтапный подход оценки рисков информационной безопасности.

На первой стадии осуществляется оценка организационных аспектов. Во время выполнения этой стадии ГА определяет критерии (показатели) оценки ущерба (неблагоприятных последствий), которые позже будут использоваться при оценке рисков. Здесь же осуществляется определение наиболее важных организационных ресурсов и оценка текущего состояния практики обеспечения безопасности в организации.

На завершающем этапе первой стадии определяются требования безопасности, и строится профиль угроз для каждого критического ресурса.

На второй стадии проводится высокоуровневый анализ ИТ-инфраструктуры организации, при этом обращается внимание на степень, с которой вопросы безопасности решаются и поддерживаются подразделениями и сотрудниками, отвечающими за эксплуатацию инфраструктуры.

На третьей стадии проводится разработка стратегии обеспечения безопасности и плана защиты информации.

Этот этап складывается из определения и анализа рисков и разработки стратегии обеспечения безопасности и плана сокращения рисков. В процессе определения и анализа рисков оценивают ущерб от реализации угроз, устанавливают вероятностные критерии оценки угроз, оценивают вероятность реализации угроз.

В процессе разработки стратегии обеспечения безопасности и плана сокращения рисков:

- описывают текущую стратегию безопасности,
- выбирают подходы сокращения рисков,
- разрабатывают план сокращения рисков,
- определяют изменения в стратегии обеспечения безопасности,
- определяют перспективные направления обеспечения безопасности.

Оценка методов

Для оценки и сравнения представленных методов управления ИТ-рисков используется стандарт COBIT [5] – пакет открытых документов, описывающих универсальную модель управления информационными технологиями.

В статье представлена таблица, которая отображает возможности рассматриваемых стандартов с точки зрения используемых категорий сравнения (табл. 1).

Жирным и курсивным начертанием в таблице обозначены разделы (группы) категорий. В таблице знак “+” обозначает, что данный пункт соответствует критерию, а знак “–” не соответствует критерию, представленному в стандарте COBIT. Знак “!” обозначает, что соответствие критериев зависит от других факторов.

Таблица 1

Возможности рассматриваемых стандартов
с точки зрения используемых категорий сравнения

Категории сравнения	CRM	OCT	CRS
Риски			
Использование категорий рисков	+	+	+
Использование понятия макс. допустимого риска	+	+	+
Подготовка плана мероприятий по снижению рисков	+	+	+
Управление			
Использование понятия ” владелец риска”	+	+	+
План работ по снижению рисков	–	+	–
Включает проведение тренингов	–	+	–
Включает проведение собраний, семинаров	–	+	–
Оценка бизнес-, операционных-, ИТ - рисков	–	+	+
Оценка рисков на техническом уровне	+	–	+
Оценка рисков на организационном уровне	+	+	+
Информирование руководителя	+	+	+
Предлагаемые способы снижения рисков			
Исключение (обход) риска	–	–	+
Снижение риска	+	+	+
Принятие риска	–	+	+
Использование элементов риска			
Материальные активы, нематериальные активы, ценность активов	+	+	+
Угрозы, уязвимости	+	+	+
Меры безопасности	+	+	–
Потенциальный ущерб, вероятность реализации угроз	+	+	+
Рассматриваемые типы рисков			
Бизнес-риски	!	!	!
Риски, связанные с нарушением законодательных актов	!	+	!
Риски, связанные с использованием технологий	!	+	!
Коммерческие риски	!	!	!
Риски, связанные с привлечением третьих лиц	!	!	!
Риски, связанные с привлечением персонала	!	!	!
Повторные оценки рисков	–	+	–
Определение правил принятия рисков	–	+	+
Способы измерения величин рисков			
Качественная оценка, качественное ранжирование рисков	+	+	+
Количественная оценка, количественное ранжирование рисков	+	–	+
Использование независимой оценки	+	–	+
Расчет возврата на инвестиции	!	–	–
Расчет оптимального баланса между различными типами мер безопасности, такими как:			
Меры предотвращения	+	–	–
Меры по исправлению	+	–	–
Меры по восстановлению	+	–	–
Интеграция способов управления	+	+	–
Описание назначения способов управления	–	–	–
Процедура принятия остаточных рисков	–	+	+
Управление остаточными рисками	–	–	–
Мониторинг рисков			
Применение мониторинга мер безопасности	–	–	–
Присутствие процесса реагирования на инциденты ИБ	–	+	–
Проведение мероприятий по снижению рисков	+	+	–
Структурированное документирование результатов оценок рисков	+	+	–

Выводы

Анализ представленных методов показывает, что методы соответствуют требованиям групп «Риски» и «Менеджмент» в стандарте COBIT, но не в полной мере отвечают требованиям разделов «Мониторинг» и «Управление».

Методы оценки информационной безопасности, описанные в работе, не рассматривают механизмов управления рисками остаточного уровня, не производится оценка качества процесса реагирования на инциденты в области информационной безопасности.

Кроме того, ни один из методов не дает подробных рекомендаций по поводу периодичности проведения оценок ИТ-рисков.

В методах CRAMM и CORAS упущен из виду пересмотр величин рисков после реализации контрмер.

В случае если требуется выполнить только разовую оценку уровня ИТ-рисков в компании любого масштаба, целесообразно применять метод CORAS.

Для управления ИТ-рисками на базе периодических оценок на техническом уровне более предпочтительным является метод CRAMM.

Метод OCTAVE целесообразно применять в крупных компаниях, где предполагается внедрение управления ИТ-рисками на базе регулярных оценок на уровне не ниже организационного и когда требуется разработка обоснованного плана мероприятий по их снижению.

На практике заказчик всегда хочет получить не только результаты первоначальной оценки ИТ-рисков и рекомендации по их снижению, но и простой в использовании инструмент такой оценки. Большое внимание заказчик уделяет ясности получаемых результатов оценки ИТ-рисков и их связи с рекомендуемыми действиями по снижению последних.

Инструмент оценки ИТ-рисков должен позволять отследить связи между выявленными рисками и причинами, которые ведут к ним.

Проанализировав данные, представленные в табл. 1, можно сделать вывод, что этим требованиям лучше всего отвечает метод OCTAVE.

Направление дальнейших исследований – разработать автоматизированный метод выбора соответствующей технологии управления рисками информационной безопасности.

Список литературы

1. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 616 с.

2. Метод CORAS [Электронный ресурс]. – Режим доступа к ресурсу: http://coras.sourceforge.net.

3. Метод CRAMM [Электронный ресурс]. – Режим доступа к ресурсу: www.cramm.com.

4. Потий А.В. Методика оценки критических ресурсов, угроз и уязвимостей безопасности информации для малых предприятий (описание и руководство по применению методики: технический отчет). OCTAVE-S / А.В. Потий, Ю.А. Избенко, А.В. Леншин и др. – Х. ХНУРЭ, 2006. – Т. 1. – 144 с.

5. Метод COBIT [Электронный ресурс]. – Режим доступа к ресурсу: www.cobit.org.

Поступила в редколлегию 20.01.2011

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков.

ТЕХНОЛОГІЇ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

О.А. Замула, І.О. Жуков, Ю.В. Землянко

Розглядаються питання, пов'язані з оцінкою ризиків інформаційної безпеки. Пропонуються і аналізуються методи для оцінки ризиків інформаційної безпеки.

Ключові слова: *інформаційна безпека, оцінка ризику, методи для оцінки ризиків.*

TECHNOLOGIES OF RISK MANAGEMENT OF THE INFORMATION SECURITY

O.A. Zamula, I.O Zhukov, U.V. Zemlyanko

The questions connected to a risks assessment of information security are considered. Methods for an information security risks assessment are offered and analyzed.

Keywords: *information security, a risks assessment, methods for a risks assessment.*