Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.054

Караткевич

ВалерийВалерьевич

Методика оценки рисков информационной безопасности типовой информационной системы

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

Научный руководитель
Голиков Владимир Федорович
д.т.н., профессор

Минск 2015

ВВЕДЕНИЕ

Современная нормативная база в области обеспечения информационной безопасности (ИБ) прямо указывает на необходимость постоянного использования оценок проявления потенциальных факторов угроз и уязвимостей информации в информационных системах для организации целенаправленных действий по их минимизации и устранению. Международное сообщество специалистов определяет такие действия как процесс менеджмента (управления) ИБ, а процедуры анализа и оценивания названных факторов - как менеджмент риска ИБ.

В соответствии с требованиями нормативной базы реализация процесса управления ИБ может осуществляться только в рамках документированной системы управления информационной безопасностью (СУИБ), построенной на основе менеджмента риска ИБ. Таким образом, базовым компонентом СУИБ согласно установившемуся подходу становится система менеджмента риска ИБ.

Практика обеспечения безопасности информационных систем также постепенно осознает необходимость применения процедур анализа и оценки риска ИБ. Так, деятельность по достижению требуемого уровня ИБ помимо основного и вспомогательного процессов (реакции на инциденты и обеспечение ресурсами безопасности) все чаще включает процесс управления ИБ, который охватывает не только правила управления (политики, инструкции и регламенты безопасности), разработанные на основе выявленных угроз и уязвимостей, но и контроль их результативности, осуществляемый путем проведения аудита ИБ на базе анализа риска, с последующей корректировкой управляющих механизмов. Сегодня очевидно, что настраивать СУИБ информационных систем только по фактам проявления угроз и уязвимостей сложно и ресурсоемко, а следовательно, малоэффективно.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность данной работы заключается в том, что важнейшей проблемой, определяющей подходы к построению, совершенствованию и перспективному развитию информационных систем, становится их безопасность. Анализ современных тенденций обеспечения безопасности в сфере информационных систем государственного и специального назначения показывает, что в основе повышения их защищенности лежит выявление потенциальных факторов угроз и уязвимостей информации, количество которых постоянно растет.

Цели данной магистерской работы работы является – разработка методики оценки рисков информационной безопасности в типовой информационной системе.

Для достижения данных целей были решены следующие задачи:

- обзор и анализ существующих стандартов;
- обзор и анализ инстументальных средств анализа рисков;
- разработка методики оценки рисков для типовых информационных систем.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются объект и предмет исследования, цель и задачи.

Первая глава«Управление рисками и международные стандарты»носит теоретический характер и состоит из шести подразделов.

В подразделах 1.1. «Международный стандарт ISO 17799» и 1.2 «Обзор стандарта ISO 17799» рассматривается история создания стандартаISO 17799» и приведен его обзор. Стандарт ISO17799 определяет следующие аспекты организации режима ИБ:

- политика безопасности;
- организация защиты;
- классификация информационных ресурсов и управление ими;
- управление персоналом;
- физическая безопасность;
- администрирование компьютерных систем и сетей;
- управление доступом к системам;
- разработка и сопровождение систем;
- планирование бесперебойной работы организации;
- проверка системы на соответствие требованиям ИБ.

В подразделе 1.3. рассматривается Германский стандарт BSI «Руководство по защите информационных технологий для базового уровня защищенности». Оно представляет собой гипертекстовый справочник объемом около 4 Мб (в формате HTML). Особенностью данного стандарта является наличие каталогов угроз и контрмер, содержащие около 600 позиций в каждом.

Каталоги являются наиболее подробными из общедоступных.

В подразделе 1.4 приведено сравнение стандартов ISO 17799 и BSI. В стандарте ISO 17799 (BS 7799) декларируются общие принципы, которые предлагается конкретизировать применительно к исследуемым информационным технологиям. Во второй части основное внимание уделено сертификации информационной системы на соответствие стандарту, то есть формальной процедуре, позволяющей убедиться, что декларируемые принципы реализованы. Объем стандарта сравнительно невелик - менее 120 страниц в обеих частях.

В германском стандарте BSI, напротив, обсуждается много «частных случаев» - различных элементов информационных технологий. Объем документа очень велик - несколько тысяч страниц; несомненно, он будет возрастать.

Подраздел 1.5 содержит описание стандарта США NIST 800-30, который включает следующие стадии управления рисками:

- описание системы;

- идентификация угроз;
- идентификация уязвимостей;
- анализ системы управления ИС;
- оценка параметров угроз;
- анализ возможных последствий нарушения режима ИБ;
- определение рисков;
- выработка рекомендаций по управлению рисками;
- разработка отчетных документов.

В подразделе 1.6 приводится описание ведомственных и корпоративных стандартов. Организацией MITRE была разработана концепция управления рисками при построении различных систем (не только информационных). В данной концепции риск не разделяется на составляющие его части (угрозы и уязвимости), что в некоторых случаях может оказаться более удобным с точки зрения владельцев информационных ресурсов.

Вторая глава «Инструментальные средства анализа рисков» описывает По базового уровня и средства полного анализа рисков. Инструментальные средства анализа рисков позволяют автоматизировать работу специалистов в области защиты информации, осуществляющих оценку или переоценку информационных рисков предприятия.

К ПО базового уровня относятся такие программные продукты, как COBRA. Программный продукт для анализа и управления рисками COBRA, производитель - C & A SystemsSecurityLtd., позволяет формализовать и ускорить процесс проверки на соответствие режима информационной безопасности требованиям Британского стандарта BS 7799 (ISO 17799) и провести простейший анализ рисков. COBRA позволяет представить требования стандарта в виде тематических «вопросников» по отдельным аспектам деятельности организации.

Программные средства, позволяющие провести полный анализ рисков, создаются с использованием структурных методов системного анализа и проектирования (SSADM - StructuredSystemsAnalysisandDesign) и относятся к категории средств автоматизации разработки или CASE-средств (ComputerAidedSystemEngineering).

Такие методы представляют собой инструментарий для:

- построения модели ИС с позиции ИБ;
- оценки ценности ресурсов;
- составления списка угроз и оценки их вероятностей;
- выбора контрмер и анализа их эффективности;
- анализа вариантов построения защиты;
- документирования (генерации отчетов).

Один из наиболее известных продуктов этого класса, CRAMM.

Целью разработки метода являлось создание формализованной процедуры,

позволяющей:

- убедиться, что требования, связанные с безопасностью, полностью проанализированы и документированы;
- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
- оказывать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем:
- обеспечить проведение работ в сжатые сроки;
- автоматизировать процесс анализа требований безопасности;
- представить обоснование для мер противодействия;
- оценивать эффективность контрмер, сравнивать различные их варианты;
- генерировать отчеты.

В третьей главе «Методика оценки рисков для типовой информационной системы» приводится описание высокоуровневого и детального подходов к оценке рисков.

Оценка рисков ИБ с помощью высокоуровневого подхода может быть обеспечена путем использования справочных материалов (каталогов), где можно подобрать наиболее актуальные угрозы для конкретной ИС.

Детальный процесс оценки рисков ИБ включает в себя тщательную идентификацию и определение ценности активов, оценку угроз этим активам и оценку уязвимостей.

Далее описывается процесс оценки рисков информационной безопасности типовой информационной системы, который включает в себя:

- идентификацию активов;
- идентификацию угроз;
- идентификацию уязвимостей;
- идентификацию мер защиты;
- оценка вероятности реализации угрозы;
- оценка влияния угроз;
- оценка рисков;
- документирование результатов.

В главе 4 приводятся общие положения по выбору метода оценки рисков.

После того как принято решение о проведении оценки риска, определены цели и область применения, должен быть выбран метод или методы оценки, исходя из приемлемости следующих факторов (СТБ ISO/IEC 31010):

а) стадия разработки ИС. На ранней стадии развития системы могут применяться менее детализированные методы. Они должны совершенствоваться по мере увеличения объема информации;

б) задачи оценки. Цели и задачи анализа должны иметь прямое отношение к

используемым методам. Например в том случае, если предпринимается сопоставительное исследование различных вариантов, может оказаться приемлемым использование довольно грубых моделей последствий для частей ИС, не подверженных изменениям;

в) уровень детализации. Решение относительно глубины проведения оценки должно отражать первоначальное восприятие последствий (несмотря на то, что оно может измениться после получения предварительной оценки);

г) требования к людским ресурсам, степени компетентности персонала и другим необходимым ресурсам. Простой, хорошо разработанный метод обеспечит лучшие результаты по сравнению с более усложненной процедурой, которая разработана недостаточно хорошо, поскольку он соответствует задачам и области определения анализа;

д) наличие и доступность информации о ИС.

ЗАКЛЮЧЕНИЕ

Базируясь на проведенных в диссертационной работе теоретических исследованиях, касающихся выбора подхода к оценке рисков:

- разработаны методика оценки рисков информационной безопасности в информационных системах;
- разработаны рекомендации по выбору метода оценки на каждом этапе процесса оценки рисков;
- приведен пример применения разработанной методики для оценки рисков типовой информационной системы.
- получены результаты в виде графиков и таблиц. Имеют хорошее совпадение с экспериментальными данными.

Основываясь на результатах работы сделаны выводы:

Основной проблемой, на которой следует остановиться, является определение качественных и количественных показателей рисков и угроз, на основании которых выбираются функции защиты. Большинство технологий, создаваемых для оценки защищенности автоматизированных систем, предполагает использование совокупности определенным образом упорядоченных качественных показателей. Практически, ни в одном из существующих нормативных документов, посвященных оценке информационной безопасности, количественные показатели не применяются. Однако вопрос о необходимости использования количественных показателей ставится постоянно.

Употребление количественных показателей оправдано только тогда, когда они могут быть определены с достаточной точностью и когда речь идет о параметрах, сохраняющих свои значения неизменными. Когда же речь идет о таких понятиях как риск и угроза, говорить об их точном учете не следует. Более того, эти величины не могут быть определены точно еще и потому, что они постоянно изменяются под влиянием среды функционирования.

Из вышесказанного следует, что в настоящее время для оценки вероятности рекомендуется применять экспертные мнения. Экспертные суждения должны основываться на всей имеющейся информации об ИС. Использование соответствующих накопленных данных для выявления событий или ситуаций, которые возникали в прошлом, дает возможность предположить вероятность их возникновения в будущем. Используемые данные должны соответствовать рассматриваемому типу ИС, оборудования, организации и ее деятельности. Если в прошлом риск возникал очень редко, то любая оценка вероятности будет весьма неопределенной. Это особенно касается тех случаев, когда событие, ситуация или обстоятельство в прошлом никогда не возникали, что не позволяет обоснованно предполагать, что они не произойдут в будущем. А применение количественных показателей не имеет смысла из-за недостаточного количества статистической

информации. Поэтому основная нагрузка при оценке рисков ложится на экспертов, и результат оценки будет напрямую зависеть от знаний и опыта эксперта.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

–Караткевич В.В. Проблема оценки рисков информационной безопасности в информационных системах / В.В.Караткевич, В.Голикоф// Научно-практическая конференция по вопросам информационной безопасности Союзного государства – Псков, 2014 – с.