УДК 638.235.231

В.Щербина, А.А.Скопа

ПРОБЛЕМЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

I ВСТУПЛЕНИЕ

Постановка проблемы. Особенностью развития современных информационно-телекоммуникационных систем является взаимное проникновение средств вычислительной техники и связи. При этом одной из проблем, порождаемых данной тенденцией, является необходимость защиты информационных процессов, протекающих в таких системах. Она вытекает из высокого уровня автоматизации технологических процессов, обеспечивающих доставку сообщений к абонентам, широким внедрением методов цифровой обработки сигналов, а также применением в этих процессах современных технологий накопления, обработки, хранения и передачи информации. Отклонения в протекании этих процессов от нормы, возникающие в силу потенциальной возможности несанкционированного удаленного доступа к ресурсам систем передачи данных, как следствие, ведут за собой серьезные финансовые потери. Именно этим объясняется рост значимости вопросов, связанных с построением эффективных систем защиты информации (СЗИ). Их создание и внедрение в состав действующих информационно - телекоммуникационных систем на практике обходится очень дорого, поэтому особенно важным остается вопрос их экономической эффективности.

II ОСНОВНЫЕ НАПРАВЛЕНИЯ ПОСТРОЕНИЯ СИСТЕМЫ ОПРЕДЕЛЕНИЯ РИСКОВ

Цель исследований. Система защиты информации может быть эффективной лишь в случае точного учета уровня угроз, действующих в реальных условиях функционирования системы. Правильность определения их состава, а также количественных и качественных значений рисков от их реализации, определяет состав и стоимость необходимых функций защиты, включаемых в профиль безопасности. Это, в свою очередь, напрямую определяет расходы на реализацию защиты в целом.

Анализ исследований и публикаций. Деятельность, связанная с оценкой безопасности информационно - телекоммуникационных систем и реализацией функций защиты в таких системах, определяется соответствующими нормативно-правовыми документами государства и находится под контролем Департамента специальных телекоммуникационных систем и защиты информации СБ Украины. В этих документах достаточно полно отражены вопросы, связанные с построением защищенных систем. В частности, определены:

- *общие положения, в соответствии с которыми должны строиться системы защиты компьютерных систем (НДТЗИ 1.1-002-99) [1];*
- *термины и определения в области защиты компьютерных систем (НД ТЗИ 1.1-003-99) [2];*
- *критерии оценки защищенности компьютерных систем (НД ТЗИ 2.5-004-99) [3];*
- *классификация защищенных компьютерных систем и профили защиты (НД ТЗИ 2.5-004-99) [4].*

Рис. 1. Диаграмма, иллюстрирующая взаимосвязь элементов оценки безопасности

Нерешенные проблемы. Существует также целый ряд других нормативных документов, регламентирующих отдельные аспекты информационной безопасности. В некоторых из них, процедуры, связанные с анализом рисков упоминаются, но не детализируются. И это составляет серьезную проблему в процессе решения вопросов, связанных с созданием систем защиты, адекватных существующим угрозам.

В частности такой нормативный документ как НД ТЗИ 3.7-001-99 [5], в котором приведены методические указания по составлению технического задания на создание комплексной системы защиты, в принципе выводит процедуры анализа рисков за пределы аудита безопасности. В нем говориться о том, что разработчик системы накануне составления технического задания, среди прочих работ, должен выполнить следующие:

- *классифицировать и описать ресурсы автоматизированной системы (АС);*
- *разработать информационную модель АС;*
- *определить перечень угроз и каналов утечки информации;*
- *определить требования к мерам защиты;*
- *сформировать функциональный профиль защищенности;*
- *выполнить оценку стоимости и эффективности выбранных средств защиты.*

Каждый из перечисленных этапов работ, в соответствии с положениями документов, принятых Международной организацией по стандартизации ISO, является составной частью процедуры анализа рисков.

Цель статьи. В соответствующих нормативных документах Украины никак не разъясняется, каким образом перечисленные результаты могут быть получены. Неясно, например, каким образом должна осуществляться декомпозиция оцениваемой системы с целью выделения, классификации и описания ресурсов, требующих защиты.

Непонятно также, что считать информационной моделью АС. В документе «Терминология в области защиты информации в компьютерных системах от несанкционированного доступа» НД ТЗИ 1.1-003-99 вообще не дано исчерпывающего определения этого понятия.

Такое положение обычно объясняют тем, что эти вопросы не рассматриваются и в аналогичных международных документах. Однако это не совсем так.

Освещение упомянутых вопросов определяет цель статьи.

Изложение основного материала. Осенью 1999 года в поддержку «Общим критериям» [6-8] организация ISO выпустила проект документов под названием «Общая методология оценки безопасности информационных технологий» (Common Evaluation Methodology for Information Technology Security), состоящий из двух частей: «Часть 1. Введение и общая модель» и «Часть 2. Методология испытаний». В этом документе, в качестве одной из важнейших проблем, ставиться задача построения такой методологии испытаний, которая

обеспечивала бы сравнимость результатов оценки, получаемых различными группами независимых экспертов. Речь идет об оценке защищенности систем и, в том числе, об оценке параметров угроз.

Главная трудность проведения таких оценок связана со сложностью формализации процессов, протекающих в информационно - телекоммуникационных системах. В большинстве случаев, оценки вероятностей реализации угроз, величин наносимого в случае их реализации ущерба и ожидаемых рисков, выполняются экспертными методами. И субъективный фактор здесь играет значительную роль. Для сведения субъективного фактора к минимуму, предлагается выполнять оценку защищенности на единой методологической основе с использованием надежных и апробированных схем и методик.

Под схемой оценки обычно понимают совокупность нормативных и руководящих документов, обеспечивающих получение оценки защищенности определенной группой экспертов в рамках определенных критериев. При проведении таких оценок используют программно-методический аппарат и инструментальные средства, специально создаваемые для этих целей. Взаимосвязь элементов оценки безопасности приведена на рисунке 1. Предполагается, что для получения конкретных результатов оценки, в том числе и рисков от реализации угроз, необходимы:

- *критерии, в соответствии с которыми определяются результаты проводимых испытаний;*
- *методологические материалы, содержащие методики контроля заданных требований, охватывающие все аспекты безопасности;*
- *программы оценки, определяющие порядок и последовательность использования инструментальных средств для определения качественных и количественных показателей.*

Наличие перечисленных компонент, апробированных и имеющих статус нормативных документов должно обеспечить сравнимость результатов получаемых в процессе оценки и сертификации.

Предложенная в упомянутом документе ISO схема, применима и в условиях нашего государства, поскольку она не противоречит положениям отечественной нормативно-правовой базы в области защиты информации.

Что касается такого элемента как критерии оценки, то они изложены в НД ТЗИ 2.5-004-99. Содержащиеся в них требования к реализации функций защиты должны приниматься во внимание при построении моделей угроз. Эти функции разделены на четыре группы, в зависимости от вида наносимого информационным ресурсам ущерба: потерей конфиденциальности, целостности, доступности или наблюдаемости и ранжируются по уровням реализации в соответствии надежностью обеспечиваемой защиты. Инструментальные средства и методики, используемые при определении параметров угроз, должны содержать достаточный арсенал возможностей для определения стойкости всего диапазона функций защиты, предлагаемого этим документом.

Поскольку нормативные документы не содержат методик, определяющих практический порядок проведения анализа угроз и стойкости реализованных функций безопасности, их предполагается разрабатывать отдельно в процессе разработки конкретных систем защиты и согласовывать их с ДСГС ЗИ. В принципе это правильный подход. Слабость такого подхода заключается в том, что при проведении повторных проверок защищенности другими группами экспертов и применении ими своих собственных методик и программ испытаний, сравнимость получаемых не гарантируется. С этой точки зрения, целесообразно было бы иметь в наличии для типовых сред опробованные типовые методики. Это обеспечивало бы доказательность и сопоставимость результатов оценки.

Разрабатываемое методическое обеспечение должно обеспечивать функциональное тестирование механизмов безопасности, заложенных в профиль защиты. С этой целью в его состав должны быть включены программа и методика тестирования, а также контрольные

результаты. К числу аспектов, определяющих качество тестирования, относят его достаточность и глубину.

Достаточность характеризует полноту охвата функций безопасности и объем проводимого тестирования. При определении достаточности должно быть продемонстрировано соответствие между параметрами функций безопасности и контрольными результатами.

Глубина тестирования характеризует уровень его детализации. Она определяет вероятность выявления ошибок, допущенных в ходе реализации механизмов безопасности и наличие закладных элементов.

Для правильного определения соответствия между включенными в профиль функциями защиты и действующими в среде эксплуатации угрозами, процедуры проверки должны включать:

- *анализ уязвимостей;*
- *оценку мощности функций безопасности;*
- *оценку возможности неправильного применения функций безопасности;*
- *анализ тайных каналов.*

Уязвимостями считают любой параметр системы, делающий возможной реализацию потенциальных угроз. Задача, заключающаяся в их определении, решается методами аналитического исследования проектных материалов и путем натурного моделирования предполагаемых угроз. В зависимости от заданного уровня гарантий, предполагается и различный уровень возможностей предполагаемых нарушителей.

Оценка мощности функций безопасности предполагает определение вероятности выполнения ими своих задач при непосредственном воздействии угроз. Оценка возможности неправильного применения функций безопасности предполагает анализ эксплуатационных документов на предмет отсутствия противоречивых положений в инструкциях. Наличие таких противоречий может приводить к возможности их неоднозначного толкования и, как следствие, создавать предпосылки для реализации угроз.

Анализ скрытых каналов является одной из наиболее сложных задач и предполагает определение наличия потенциальных возможностей проникновения нарушителем в систему, минуя установленные правила разграничения доступа.

Необходимость создания типового методологического обеспечения, удовлетворяющего перечисленным требованиям, определяется достаточно большим числом однотипных информационных сред. В составе современных информационно – телекоммуникационных системах такие среды содержаться в большом количестве. Это будет способствовать сравнимости получаемых результатов оценки.

Практическая реализация программ, закладываемых в содержание методического обеспечения, выполняется специально разрабатываемыми с этой целью инструментальными средствами. Такие средства применяются в следующих направлениях:

- *для выполнения генерации тестов;*
- *для имитации угроз;*
- *для анализа текстов программ.*

Генераторы тестов могут быть либо стохастическими, либо осуществлять только целенаправленное тестирование. Они применяются, в первую очередь, при исследовании качества и надежности реализованных функций защиты. Наибольшее распространение в практике анализа средств защиты получили генераторы последнего типа. Они, кроме прочего, применяются и для анализа текстов программ, на предмет выявления скрытых в их недекларированных возможностей и закладных элементов.

Проверка механизмов защиты от программных вирусов, средств сетевого экранирования от атак из внешних сетей, а также других видов угроз осуществляется при помощи специальных имитаторов угроз. С этой целью используются методы натурного моделирования. Результатом моделирования атак со стороны среды эксплуатации должны стать показатели реальных остаточных рисков.

Наиболее сложной задачей является поиск недекларированных возможностей в программном обеспечении. В большинстве испытательных лабораторий тексты программ анализируются вручную без применения средств автоматизации. Это отнимает чрезвычайно много времени и интеллектуальных ресурсов. Разработка инструментальных средств в этой области сейчас находится на самом начальном этапе.

Еще одним видом инструментальных средств, которые стали очень популярны, являются информационные и экспертные системы. Их применение позволяет осуществлять выбор механизмов безопасности в соответствии с заданными требованиям. Однако они требуют постоянного совершенствования и обновления баз данных, входящих в их состав.

Создание современных инструментальных средств для анализа защищенности АС, это наиболее сложная область, связанная с защитой информации. Именно от ее качества зависит практическая деятельность по оценке Решение проблем, связанных с созданием эффективных технологий в этой сфере, требует хороших знаний в области вычислительной техники, телекоммуникаций и специальных разделов математики.

Современный рынок предлагает множество технологий, автоматизирующих процедуры связанные с оценкой рисков и анализом защищенности. К их числу следует отнести такие зарубежные инструментальные средства как CRAMM, «COBRA», «КОНДОР+», «Авангард» и другие. Все они ориентированы на оценку информационных технологий, выполняемую в рамках «Общих критериев». Их приобретение и использование на территории нашего государства в принципе возможно. Они содержат общие программы анализа рисков, определяют принципы декомпозиции систем, и классификации активов, подлежащих защите. Однако они не включают генераторов, позволяющих осуществлять тестирование механизмов безопасности, реализованных в системе в соответствии с критериями, изложенными в НД ТЗИ 2.5-004-99.

Еще одной 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 в периодической печати ставится постоянно. Более того, их использование в принципе не считается запрещенным.

На самом деле эта проблема достаточно условна. Все дело заключается в том, что 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, которые сами по себе четко и однозначно не определены, 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.

Каким же образом должна решаться данная проблема. На практике это делается введением относительных шкал, каждому делению которых приписывается совокупность признаков, в соответствии с которыми определяется их отношение к измеряемой величине.

Так, например, для определения стоимости активов автоматизированной системы, подлежащей защите, все опии нумеруются, и за единицу измерения принимается стоимость самого дешевого из них. Стоимость остальных активов определяется по отношению к самому дешевому в целых числах. Понятно, что такая оценка будет достаточно приблизительной, однако, учитывая то, как быстро изменяются цены на программно - аппаратное обеспечение, об абсолютной точности говорить нет смысла.

Другим примером является определение вероятности успешной реализации угроз. Для их определения строиться модель угрозы, а затем аналитическим путем или способом натурного моделирования определяют, насколько вероятно будет преодоление средств

защиты в случае ее реализации. При этом модель угрозы должна включать все возможные сценарии атак, осуществление которых приводит к достижению цели, поставленной нарушителем. В рассмотренном примере, как и в предыдущем, точность оценки будет зависеть от полноты учета всех уязвимостей в системе безопасности и от мастерства эксперта, выполняющего оценку. И, таким образом, для определения вероятности тоже можно ограничиться относительной шкалой с фиксированным значением уровней.

То же самое относится и к рискам, которые определяются как произведение вероятности реализации угрозы на стоимость ожидаемых потерь.

Сложность в этом вопросе заключается в том, каким образом, при описанном выше подходе, обеспечить достоверность и сопоставимость величин, получаемых в процессе оценки защищенности системы и в процессе ее сертификации. Решение этого вопроса заключается в использовании единых шкал, в соответствии с которыми определяются величины искомых показателей. Кроме того, важным является качество подготовки экспертов, выполняющих оценку. О том, насколько это важно, свидетельствует тот факт, что целая группа стран, принявших «Единые критерии» в качестве национальных документов и заключивших соглашение о взаимном признании результатов оценки и сертификации информационных технологий, централизовано готовит специалистов, которые такую оценку могут осуществлять.

III ВЫВОДЫ

Из сказанного следует, что в настоящее время существует необходимость в создании нормативного документа, определяющего требования к процедурам анализа рисков от реализации угроз информации в информационно-телекоммуникационных системах. Кроме того, с учетом принципов построения таких систем, их программно-аппаратного состава и реализуемых ими информационных процессов, должны быть созданы методики и инструментальные средства, позволяющие на практике получать значения показателей рисков от реализации угроз, имеющих место в конкретной среде эксплуатации.

Начинать решение этой задачи следует с анализа статистических данных об угрозах, реализация которых уже имела место, и об экономических потерях они приводили. Это позволит определить основные цели безопасности и вытекающие задачи, стоящие перед системами и службами безопасности.

Список литературы

1. НД ТЗИ 2.5-004-99. Критерии оценки защищенности в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины, 1999.

2. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины, 1999.

3. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины, 1999.

4. НД ТЗИ 2.5-004-99. Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа, 1999.

5. НД ТЗИ 3.7-001-99. Методические указания по разработке технического задания на создание комплексной системы защиты информации в автоматизированной системе, 1999.

6. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. – ISO/IEC 15408-1.1999.

7. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. – ISO/IEC 15408-2.1999.

8. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. – ISO/IEC 15408-3.1999.