УДК 681.14

Щербина Ю. В., *к.т.н.*; **Кунах Н. И.,** *д.т.н.*

ПРИНЦИПЫ ПОСТРОЕНИЯ МОДЕЛЕЙ УГРОЗ ИНФОРМАЦИОННЫМ РЕСУРСАМ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Щербина Ю. В., Кунах Н. І. Принципи побудови моделей загроз інформаційним ресурсам розподілених обчислювальних систем. Визначені основні параметри загроз інформаційним об'єктам систем передачі і обробки інформації, а також приведений загальний підхід до побудови формальної моделі загроз, що дозволяє здійснювати вибір функціональних послуг захисту.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ПОГРОЗ, ОБЧИСЛЮВАЛЬНА СИСТЕМА, НОРМАТИВНА ДОКУМЕНТАЦІЯ

Щербина Ю. В., Кунах Н. И. Принципы построения моделей угроз информационным ресурсам распределенных вычислительных систем. Определены основные параметры угроз информационным объектам систем передачи и обработки информации, а также приведен общий подход к построению формальной модели угроз, позволяющей осуществлять выбор функциональных услуг защиты.

Ключевые слова: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МОДЕЛЬ УГРОЗ, ВЫЧИСЛИТЕЛЬНАЯ СИСТЕМА, НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ

Shcherbyna Yu. V., Kunakh N. I. Construction principles of the models of threats to the informative resources of the distributed computer systems. In the article defined the main parameters of threats to information objects of communications systems and data processing, described the common approach to the building of formal threat model information, allowing making choice of functional protection services.

Key words: INFORMATIVE SAFETY, THREATS MODEL, COMPUTER SYSTEM, NORMATIVE DOCUMENT

Постановка задачи. В последние десятилетия наблюдается тенденция повсеместного перехода к безбумажному документообороту, основанному на использовании распределенных вычислительных систем. Это объясняется высоким уровнем автоматизации технологических процессов, обеспечивающих доставку информации к абонентам, широким распространением современных технологий накопления, хранения и обработки информации, а также применением цифровых методов обработки сигналов. В этих условиях требования к корректности информационных процессов, протекающих в системах передачи и обработки информации, постоянно растут, и для их удовлетворения приходится создавать системы защиты информации, способные противостоять внешним и внутренним угрозам. Учитывая высокую стоимость такого рода систем, приходится принимать специальные меры для повышения их эффективности, которая, в первую очередь, определяется правильным учетом рисков от реализации угроз, имеющих место в условиях эксплуатации. Это делает задачу выработки методологии оценки угроз информационным ресурсам особенно актуальной.

Создание методологии, которая обозначена выше, представляет собой сложную задачу. Эта сложность объясняется, во-первых, субъективным подходом в оценке стоимости самих информационных объектов и, во-вторых, постоянным изменением среды эксплуатации защищаемых систем. Оба этих обстоятельства определяют необходимость постоянного мониторинга состояния безопасности системы и актуальности угроз, выявленных на момент ввода ее в эксплуатацию.

В последние годы проблеме выработки методологии оценки угроз информационным ресурсам было посвящено достаточно много публикаций, однако, большинство из них чаще всего отражает подход к решению частных задач. Кроме того, одни и те же термины не всегда одинаково понимается различными авторами. Отсюда вытекает еще одна проблема, которая связана с отсутствием строгого закрепления соответствующих понятий, связанных с деятельностью по защите информации в нормативно-правовых актах, регулирующих отношения между заказчиками и разработчиками средств ее защиты.

Для дальнейшего понимания сути решаемой проблемы приведем понятие *угрозы* [1]: под *угрозой* будем понимать потенциально существующая возможность случайного или преднамеренного действия (бездействия), в результате которого могут быть нарушены основные свойства информации и систем ее обработки: *доступность, целостность и*

конфиденциальность. Знание спектра потенциальных угроз защищаемой информации, умение квалифицированно и объективно оценить возможность их реализации и степень опасности каждой из них, является важным этапом сложного процесса организации и обеспечения защиты.

Определение полного множества угроз информационной безопасности практически невозможно, но относительно полное описание их может быть достигнуто при детальном составлении модели угроз. В связи с этим возникает вопрос: что такое модель угроз?

Модель угроз [2] – это документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности информации (данных, файлов, и т.д.) и уязвимостей при их обработке в информационных системах, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности данных.

Цель разработки модели угроз – определение актуальных для конкретной информационной системы угроз безопасности, источников угроз и уязвимостей. Результаты моделирования должны использоваться для классификации информационных систем передачи (обработки) данных, а также в качестве исходных данных для построения (проектирования) обоснованной и эффективной системы их защиты.

В зарубежной нормативной базе достаточно хорошо прописана процедура анализа рисков, т.е. приводится последовательность обязательных этапов, выполняемых при оценке угроз, к которым, чаще всего, относят:

- определение границ защищаемой системы;
- определение перечня защищаемых информационных объектов;
- выявление слабых мест в системе защиты и угроз;
- оценка рисков от отдельных угроз;
- определение функциональных услуг защиты;
- определение остаточного риска.

Цель статьи. К настоящему моменту у нас в стране отсутствуют нормативно закрепленные методики оценки защищенности автоматизированных систем, а также методики построения формальных моделей угроз, на основании которых делается вывод об истинном уровне такой защищенности. Разработчику системы предоставляется известная свобода действий.

В соответствии с принятой в Украине терминологией [3], понятие «модель угроз» предполагает формальное или неформальное описание методов их реализации. Учитывая, что при составлении профиля защиты функциональные услуги защиты выбираются из перечня, оговоренного нормативным документом [4], формальная модель угроз должна представлять собой такой набор их параметров, который позволял бы разработчику оптимальным образом выбирать услуги защиты из предлагаемого перечня.

Формирование модели угроз. До того как определить модель угроз, важно оговорить, что является информационным объектом, требующим защиты. Далее под информационными объектами будем понимать источники/приемники информации, а также информационные потоки безотносительно к их физическим носителям [5]. Это означает, что реальными объектами, которые подлежат строгому учету, являются файлы, хранящиеся в различных видах памяти и данные, хранящиеся в аппаратной части интерфейсов используемой вычислительной системы. Последние могут быть идентифицированы своими адресами портов. Все они должны быть классифицированы, описаны и строго учтены.

Из сказанного следует, что работы по формированию модели угроз должны начинаться с пространственной и функциональной структуризации защищаемой системы, которая задает многоуровневые координаты любого из идентифицируемых объектов.

Пространственная структуризация системы предполагает выделение локальных сред – отдельных частей системы, которые расположены в отдельных зданиях или помещениях и требуют своих особых средств защиты. Глубина такой структуризации определяется выбранным уровнем гарантий защищенности. Функциональная структуризация предполагает разделение системы на функциональные подсистемы, которые, в свою очередь, должны быть структурированы до уровня конкретных средств или программ, выполняющих разнообразные функции. Качество проведенной декомпозиции защищаемой автоматизированной системы.

Количественная оценка угроз. Для того чтобы можно было выбрать средство защиты от угрозы, она должна быть оценена количественно. В качестве такой оценки используют показатель риска [3], определяемый как функция вероятности реализации конкретной угрозы, а также вида и величины нанесенного ущерба. В простейшем случае, риск можно представить как $W = P_y C_i$, где P_y – вероятность удачной атаки на *i*-й информационный объект; C_i – стоимость данного объекта в относительных единицах, определяемая заказчиком.

Поскольку точной и объективной процедуры определения стоимости информационных объектов не существует даже при квалифицированной экспертизе, определяют стоимость наименее ценного (но требующего защиты), с точки зрения владельца системы, объекта за единицу, а стоимость остальных объектов определяют по отношению к нему.

Оценка стоимости каждого защищаемого информационного объекта должна быть комплексной. Она должна учитывать зависимость между различными информационными объектами, поскольку доступ, полученный злоумышленником к некоторому информационному объекту, может косвенно влиять на безопасность других, связанных с ним объектов. Такой учет должен выполняться в соответствии со следующими правилами:

– комплексная стоимость оцениваемого объекта равна обычной стоимости, если связанные с ним объекты имеют меньшую стоимость;

– комплексная стоимость объекта равна сумме его собственной стоимости и величины, которая характеризует степень зависимости объектов, умноженной на стоимость зависимого объекта, если стоимость зависимого объекта больше стоимости оцениваемого объекта.

Это правило может быть выражено следующим образом:

$$C_k = C_0 + \sum_i^n \lambda_i C_{CB_i}, \text{ для всех } C_{CB_i} > C_0; \qquad C_k = C_0, \text{ для всех } C_{CB_i} < C_0,$$

где C_k – комплексная оценка объекта, подлежащего защите; C_0 – обычная оценка объекта, подлежащего защите; C_{CB_i} – обычная оценка объекта, связанного с рассматриваемым в данный момент объектом; λ_i – коэффициент, характеризующий связь между объектами.

Чаще всего угрозы классифицируют по виду нанесенного ущерба: нарушению конфиденциальности, целостности или доступности. Из этого следует, что одна и та же угроза может быть реализована различными сценариями атак. Под атакой, обычно понимают целенаправленную последовательность действий, приводящих к реализации *угрозы*. Сценарий атаки предполагает использование слабого места (уязвимости) в системе защиты. Наличие нескольких уязвимостей предполагает возможность реализации различных сценариев атак. Поэтому, при определении риска от реализации угрозы, необходимо учитывать их общую вероятность реализации. Если допустить, что в некоторый момент времени реализуется лишь один из возможных сценариев, то общая вероятность может быть определена как $P_y = \sum_{j-1}^{m} P_j^A (1-P_1^A)(1-P_2^A)...(1-P_{j-1}^A)(1-P_{j+1}^A)...(1-P_m^A)$, где m – общее

количество возможных атак на данный информационный объект; P_j^A – вероятность успешной реализации j-й атаки.

Определение вероятностей реализации атак – одна из наиболее ответственных задач. Отдельно должны быть оценены умышленные и неумышленные угрозы, а также угрозы, осуществляемые из внешней среды и внутренние угрозы. В каждом случае предполагается применение отдельной методики с привлечением специалистов в этой области. Такую методику разработчик системы защиты может иметь свою или может воспользоваться готовым пакетом прикладных программ по своему выбору. Исходные данные для определения вероятностей угроз получают от владельца системы или от организаций, профессионально занимающихся деятельностью в данной области.

Когда риск от всех отдельных угроз определен, угрозы для однотипных объектов ранжируют (составляют ряд в порядке возрастания рисков). Это дает возможность, учитывая мнение заказчика системы, выделить те из них, что не являются существенными, т. е. те, которые можно не учитывать при выборе средств защиты.

Общий риск от реализации угроз, признанных существенными может быть определен по правилу: $W = \sum_{i=1}^{n} P_{y_i} C_i$, где n – общее число существенных угроз.

Таким образом, исходя из сказанного, формальную модель угроз можно определить как перечень обязательных параметров, определяемых на этапе анализа рисков, которых достаточно для выбора адекватных функциональных услуг защиты. К их числу относят:

– код, однозначно идентифицирующий информационный объект в исследуемой информационной системе;

– стоимость информационного объекта в условных единицах;

– перечень объектов, доступ к которым открывается в случае несанкционированного доступа к данному объекту, их стоимости и коэффициенты связи с оцениваемым объектом;

– описание уязвимостей и сценариев атак с их использованием, а также вычисленные вероятности их успешной реализации;

– вычисленное значение риска от реализации данной угрозы и выводы ее существенности.

Суммарный риск является обобщенным показателем, характеризующим возможные потери в случае нарушения принятой в системе политики безопасности. С учетом мнения заказчика, выбирают средства защиты от каждой угрозы по критерию «эффективность – стоимость». После этого определяют остаточную общую величину риска и, если, по мнению заказчика, эта величина достаточно велика, усиливают средства защиты.

Приведенный список параметров может быть расширен по желанию разработчика. Но их минимальное число должно быть закреплено нормативным документом.

Предложеня. Как показано в [1], на основе построенной модели угроз строится модель защиты. Для примера рассмотрим приведенную там же модель защиты, которая построена по принципу «нарушитель-злоумышленник». Модель включает в себя механизмы защиты как со стороны внешних, так и внутренних нарушителей и предусматривает организационные и технические меры. Так, для нейтрализации угроз, связанных с использованием программно-аппаратных средств информационного воздействия предлагаются такие мероприятия:

– блокирование команд, направленных на несанкционированный доступ;

– блокирование управляющих команд и протоколов от нелегальных ресурсов;

– использование и разработка средств, предотвращающих несанкционированное копирование и уничтожение информации, т.е идентификация и аутентификация;

– использование сертифицированных средств криптографической защиты информации на абонентском и линейном уровнях, а также в системе управления; использование средств разграничения доступа к информационным и сетевым ресурсам;

– разработка автоматизированных процедур тестирования составных частей (ресурсов);

– разработка и использование средств, обслуживающих информационные и сетевые ресурсы;

– разработка и использование эффективных шлюзовых экранирующих систем разграничения сетей;

– разработка и использования доверенных защищенных протоколов информационного и сетевого обмена;

– разработка и создание резервной системы;

– распознавание и идентификация легальных доверенных пользователей.

Что же касается нейтрализации угроз, связанных с нейтрализацией оперативных средств и методов, используемых нарушителем, предлагается ряд мероприятий по выработке соответствующих предложений, а именно:

– дополнение перечня сведений, составляющих конфиденциальную информацию;

– оперативное обслуживание окружения (т.е. абонентов, пользователей и т.д.);

– оперативное реагирование персонала, обеспечивающего эксплуатацию оборудования;

– сбор и анализ данных о фактах несанкционированных нелегитимных действий и о признаках информационного воздействия со стороны внешних и внутренних абонентов и пользователей;

– сбор информации о фирмах поставщиках сетевого оборудования и программного обеспечения;

– соблюдению оперативных требований по обращению с носителями и информационными ресурсами, а также требований нормативной документации по обеспечению безопасности.

Вывод. Формальная модель угроз должна представлять собой совокупность записей в базе данных угроз, поля которой содержат информацию обо всех их параметрах для каждого защищаемого информационного объекта. При таком способе ее организации удобно ее поддерживать в актуальном состоянии: дополнять новыми записями и удалять сведения об угрозах утративших свою актуальность.

В целом, после определения некоторого множества угроз информационной безопасности, защиту можно условно разделить на решение следующих проблем: *а)* теоретических; *б)* системных; *в)* защиты программного обеспечения сетевых и информационных ресурсов; *г)* защиты технических средств информационных и сетевых ресурсов; *д)* использование сертифицированных средств комплексной защиты информации и фильтрующих шлюзовых средств.

Литература

1. Модель угроз и классификация несанкционированных воздействий в Автоматизированных Системах / [Электронный ресурс] // Режим доступу : http://www.m-g.ru/about/articles/105.html

2. Что такое модель угроз? [Электронный ресурс] // Режим доступу : http://www.volgablob.ru/pages/cons/pd/q5.php

3. НД ТЗИ 1.1-002-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины.

4. НД ТЗИ 1.1-003-99. Критерии оценки защищенности в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины.

5. НД ТЗИ 1.1-001-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины.