УДК 638.235.231

ПРИНЦИПЫ ПОСТРОЕНИЯ МОДЕЛЕЙ УГРОЗ ИНФОРМАЦИОННЫМ РЕСУРСАМ СИСТЕМ И СЕТЕЙ СВЯЗИ

Петр Воробиенко, Олег Нечипорук, Юрий Щербина
Одесская национальная академия связи им. А. С. Попова

Аннотация: **Определены основные параметры угроз информационным объектам систем передачи и обработки информации, описан общий подход к построению формальной модели угроз информации, позволяющей производить выбор функциональных услуг защиты.**
Summary: **Key parameters of threats to information objects of systems of transfer and processing of the information are determined, the common approach to construction of formal model of threats of the information is described, allowing to make a choice of functional services of protection.**
Ключові слова: **Угрозы информации, анализ рисков.**

I Введение

В последние десятилетия наблюдается тенденция взаимного проникновения средств вычислительной техники и средств связи. 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. Как показывает опыт, стоимость такого рода систем чрезвычайно высока, и поэтому от правильного учета рисков, имеющих место в условиях эксплуатации, зависит эффективность их функционирования. Таким образом, актуальность выработки методологии оценки угроз информационным ресурсам в настоящее время высока как никогда. Создание такой методологии представляет собой сложную задачу.

II Основная часть

Сложность задачи 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.

Этой проблеме в последние годы 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.

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;
- оценку рисков от отдельных угроз;
- определение функциональных услуг защиты;
- определение остаточного риска.

Однако, что касается методик выполнения каждого из перечисленных пунктов, то право их выбора остается за разработчиком системы. Разумность такого подхода очевидна. Тем не менее, авторы считают, что имело бы смысл закрепить на уровне нормативного документа способ построения модели угроз как метода их универсального описания. В соответствии с принятой в Украине терминологией [1], 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 [2], формальная модель угроз должна представлять собой такой набор их параметров, который позволял бы разработчику оптимальным образом выбирать услуги защиты из предлагаемого перечня.

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 [3]. Это означает, что такие объекты должны быть классифицированы, описаны и строго учтены. Исходя из этого, 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.

Для того, чтобы можно было выбрать средство защиты от угрозы, она должна быть оценена количественно. В качестве такой оценки используют показатель риска [1], 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 і-тый 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 следующим правилом:

- 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:

$$C_k = C_0 + \sum_i^n \lambda_i C_{CBi} \quad для\ всех\ C_{CBi} > C_0 \,,$$

$$C_k = C_0 \qquad\qquad для\ всех\ C_{CBi} < C_0 \,,$$

где $C_к$ – комплексная оценка объекта, подлежащего защите, C_0 – обычная оценка объекта, подлежащего защите, C_{CBi} – обычная оценка объекта, связанного с объектом, который рассматривается в данный момент, 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

$$P_y = \sum_{j=1}^{m} P_j^A (1 - P_2^A)...(1 - P_{j-1}^A)(1 - P_{j+1}^A)...(1 - P_m^A),$$

где m – общее количество возможных атак на данный информационный объект, P_j^A – вероятность успешной реализации j-той 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. Разработчик системы защиты может иметь свою методику 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, которые 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:

$$W = \sum_{i}^{n} P_{3i} C_i$$

где n – общее число существенных угроз.

III Выводы

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:

1 код, однозначно идентифицирующий информационный объект в исследуемой информационной системе;
2 стоимость информационного объекта в условных единицах;
3 перечень объектов, доступ к которым открывается в случае несанкционированного доступа к данному объекту, их стоимости и коэффициенты связи с оцениваемым объектом;
4 описание уязвимостей и сценариев атак с их использованием, а также вычисленные вероятности их успешной реализации;
5 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.

Формальная модель угроз должна представлять собой совокупность записей в базе данных угроз (БДУ), 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.

*Литература: **1.** НД ТЗИ 1.1-002-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины. **2.** НД ТЗИ 1.1-003-99. Критерии оценки защищенности в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины. **3.** НД ТЗИ 1.1-001-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. ДСТСЗИ СБ Украины.*