Ущерб, S_i, наносимый і-ой угрозой, может определяться в абсолютных единицах: экономических потерях, временных затратах, снижении уровня защищенности, объеме уничтоженной или испорченной информации и т. д. Здесь можно воспользоваться подходом из [6].

IV Выводы

В статье рассмотрена постановка формальной задачи оптимального выбора СФПЗ для защищенных АС, а также показаны возможности детального описания основных показателей, необходимых для этого – вероятность появления угроз, вероятность устранения угроз, предотвращенный ущерб за счет ликвидации угроз. Основными этапами решения этой задачи являются:

- сбор и обработка экспертной информации об угрозах – ущерб, частота появления;
- оценка стоимости СЗИ для конкретного СФПЗ, т. е. учет ограничения $C(P_0) \le C_г$.

Литература: ***1.*** *Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с.* ***2.*** *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.* ***3.*** *Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2. 2–005–99. – Київ: ДСТСЗІ СБ України, 1999. – 23 с.* ***4.*** *Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – Київ: ДСТСЗІ СБ України, 1999. – 26 с.* ***5.*** *Антонюк А., Берестов Д. С., Пустовіт С. М. Аналіз складу профілів захищеності інформації Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2005. - №10. – 46-51 С.* ***6.*** *Кудин Д., Корольков В. Количественные оценки качества функционирования системы защиты информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2005. – №6. – 35-37 С.* ***7.*** *Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах /Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. - №3. – 156-160 С.* ***8.*** *Герасименко В. А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат.-1994.-тт.1, 2.* ***9****. А. А. Антонюк, Е. Н. Боровская, В. Ю. Суслов Модель угроз информации в защищенных автоматизированных системах // Безопасность информации. – № 2. – 2001. – 25-28 С.*

УДК 681.3:519.872

ОБОБЩЕНИЕ МОДЕЛИ УГРОЗ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

Анатолий Антонюк, Виктор Жора*
Академия ГНС Украины
**Институт программных систем НАНУ*

Аннотация: **Рассматриваются вопросы построения модели угроз в информационно-телекоммуникационной системе. Предлагается определение и классификация компонентов модели угроз, а также типовые алгоритмы реализации угроз. Приводится пример обобщенной модели угроз в информационно-телекоммуникационной системе.**

Summary: **The issues of developing threat model in information and telecommunication system are considered. Determination and classification of threat model components as well as typical algorithms of threat realization are offered. The example of generalized threat model in information and telecommunication system is given.**

Ключевые слова: **Информационно-телекоммуникационная система, угроза, атака, уязвимость, дестабилизирующий фактор.**

I Введение

Анализ угроз информации является одним из важнейших этапов при разработке комплексных систем защиты информации (КСЗИ) в информационно-телекоммуникационных системах (ИТС) и проводится на основании предварительно разработанной модели угроз. Согласно [1], модель угроз – это абстракное формализованное или неформализованное описание методов и способов осуществления угроз. На основании модели угроз также формируется политика безопасности (ПБ), в которой находят отражение

вопросы защиты от сформулированных угроз с учетом рисков их реализации.

От четкости и полноты модели угроз, прежде всего, зависят правильный выбор средств, технологий и мер по защите информации, а, соответственно, и уровень защищенности ИТС.

Существующие подходы и рекомендации к построению модели угроз в основной своей массе являются частными, противоречивыми, разнородными, оперирующими различной терминологией и понятиями. Ниже рассматривается попытка внести ясность в процесс построения модели угроз и, возможно, заложить некую научно-методологическую базу для дальнейшего использования при разработке КСЗИ в ИТС.

Приведенное в [1] определение угрозы предлагается рассмотреть с несколько иной точки зрения. В дальнейшем в этой статье под *угрозой* будем понимать *цель* нарушения безопасности информации в случае умышленных действий нарушителя либо *результат* неблагоприятных для безопасности информации неумышленных действий. Ниже рассматриваются необходимые и наиболее важные условия и средства для достижения цели.

Рассмотрение базируется на модели ИТС, аналогичной [2]. Там, в частности, принимается, что компоненты, составляющие любую ИТС, являются переменными с течением времени. В связи с этим естественно предположить, что с течением времени и угрозы могут возникать и исчезать. Это означает, что каждой угрозе можно ставить в соответствие нечто вроде ее жизненного цикла – от зарождения угрозы до полной ее реализации. Возникает естественный вопрос о конкретных этапах, которые должны включаться в такой жизненный цикл, а также о любых других понятиях, которые могут иметь какое-то отношение к угрозам. Как показывает практический опыт и теоретические исследования [3, 4], кроме понятия угрозы, исторически сформировались и определены в литературе такие важные понятия как атака, уязвимость ИТС, дестабилизирующий фактор и др.

II Базовые понятия

Для рассмотрения процесса реализации угроз определим наиболее важные понятия, без которых не может реализоваться угроза.

Поскольку предполагается, что в любой ИТС все компоненты меняются во времени, введем Ω – продолжительность жизненного цикла ИТС, t – значения дискретного времени, t=1, …, Ω.

Обозначим множество угроз в некоторый момент времени t через $\mathbf{T}(t)$, т. е. $T_l(t)\in\mathbf{T}(t)$, l=1, …, L.

Очевидно, что в процессе реализации угрозы ее осуществлению может предшествовать некоторая подготовительная деятельность злоумышленника. *Атакой* будем называть совокупность действий нарушителя, направленных на реализацию угрозы. Пусть $\boldsymbol{A}(t)$ – множество атак в некоторый момент времени t, $A_i(t)\in\mathbf{A}(t)$, i=1, …, I.

Атака всегда направлена на получение конкретного результата в конкретной ИТС. Это означает, что для этого нарушитель может воспользоваться какими-либо недостатками или уязвимостями системы защиты информации в ИТС, которые всегда имеют место. Последнее вытекает из принципа невозможности создания абсолютной защиты. Именно активизация (или использование) некоторой уязвимости в ИТС позволяет преодолеть существующие механизмы защиты информации и выполнять операции, направленные на нарушение ее безопасности. *Уязвимостью* будем называть качественную и/или количественную недостаточность компонентов ИТС, отвечающих за защиту информации. Обозначим множество уязвимостей в некоторый момент времени t через $\mathbf{V}(t)$, $V_k(t)\in\mathbf{V}(t)$, k=1, …, K.

Заметим, однако, что не только уязвимости в системе мер и средств защиты информации позволяют осуществлять угрозы, а и случайные либо объективные обстоятельства, факторы или события, которые препятствуют реализации защитных механизмов и мероприятий. В связи с этим в [4] и [5] вводится понятие *дестабилизирующего фактора* (ДФ) – явления или события, возникновение которого на некотором этапе жизненного цикла ИТС может привести к реализации угрозы. Следует отметить, что в данном контексте можно рассматривать ДФ как инструментарий внешнего воздействия на ИТС, что может привести к активизации уязвимости и реализации угрозы. Множество ДФ в некоторый момент времени t обозначим через $\mathbf{D}(t)$, $D_j(t)\in\mathbf{D}(t)$, j=1, …, J.

Очевидно, что кроме приведенных понятий, имеющих непосредственное отношение к процессу реализации угрозы, следует определить, кто и кому угрожает. Это достигается путем определения понятий *объект* и *субъект* угрозы. Под *объектом* угрозы будем понимать пассивный объект или объект-процесс [6], на вывод которого из защищенного состояния (состояния “безопасности” [7]) направлена угроза. *Субъектом* угрозы в таком случае является объект-пользователь либо объект-процесс, непостредственно реализующий угрозу. Очевидно, что множества $\mathbf{O}(t)$ объектов угроз и $\mathbf{S}(t)$ субъектов угроз являются подмножествами множества объектов ИТС в некоторый момент времени. Заметим, что в такой схеме исключаются из рассмотрения субъекты, не являющиеся объектами рассматриваемой ИТС. Для того

чтобы включить все возможные причины нарушения безопасности, целесообразно расширить множество субъектов угроз за пределы ИТС. В таком случае в модели угроз могут фигурировать элементы среды функционирования ИТС, физические объекты, внешние программные и аппаратные средства.

Для каждого из перечисленных множеств может быть предложена произвольная классификация. К примеру, угрозы могут различаться:

- по цели реализации (нарушение конфиденциальности, целостности, доступности либо наблюдаемости);
- по степени ущерба, который может быть нанесен вследствие реализации угрозы;
- по типу проявления (сбой, отказ, ошибка, утечка, модификация, др.) и т. д.

Атаки можно класифицировать по следующим признакам:

- по продолжительности (единократная либо повторяющаяся);
- по местонахождению источника (локализованная либо распределенная);
- по используемым средствам (с использованием штатных средств ИТС либо с привлечением вспомогательных);
- по принципу реализации (локальная либо удаленная);
- по объекту воздействия.

Уязвимости могут различаться:

- по причине возникновения (качественная либо количественная недостаточность);
- по признаку преднамеренности (случайная либо преднамеренная);
- по продолжительности существования (временная либо систематическая);
- по времени возникновения относительно этапа жизненного цикла ИТС (технологическая, эксплуатационная);
- по характеру (программная, аппаратная, программно-аппаратная, административная, организационно-правовая).

Дестабилизирующие факторы могут иметь как объективную, так и субъективную природу. Последние также можно классифицировать по признаку преднамеренности (случайные либо умышленные). По типу проявления ДФ могут выражаться как в стихийных бедствиях, так и отказе компонентов ИТС, сбоях оборудования, ошибках персонала и т. д.

Субъекты и объекты угроз прежде всего различаются по степени активности. Детальная классификация данных сущностей зависит от классификации, принятой в конкретной ИТС. Тем не менее, в качестве субъектов угрозы можно выделить людей, технические средства, программные средства, внешнюю среду. Данная задача в полной мере решается в процессе построения модели нарушителя.

Приведенная классификация является весьма условной и естественно не учитывает все возможные признаки разграничения тех или иных сущностей, однако эксперт в области безопасности информации вправе использовать любую удобную для него классификацию при построении модели угроз для конкретной ИТС.

III Алгоритм реализации угрозы

Теперь необходимо выяснить, каким образом взаимодействуют элементы введенных выше множеств в процессе реализации угрозы, т. е. формально определить возможные последовательности взаимодействий элементов множеств $\mathbf{T}(t)$, $\mathbf{A}(t)$, $\mathbf{D}(t)$, $\mathbf{V}(t)$, $\mathbf{O}(t)$, $\mathbf{S}(t)$ в некоторый момент времени $t=\tau$.

Для определения возможных и имеющих реальный практический смысл последовательностей (схем) этих элементов будем пользоваться следующими соображениями, основанными на практическом опыте:

- в любой схеме совсем не обязательно должны принимать участие элементы всех без исключения множеств – могут использоваться лишь некоторые из множеств;
- порядок взаимодействия элементов не устанавливается – могут быть схемы с произвольным порядком следования элементов;
- в любой схеме может использоваться не один, а несколько элементов любого множества;
- некоторые множества могут принимать участие в схемах повторно.

С целью подтверждения возможной практической реальности для каждой из рассмотренных ниже схем приводится конкретный пример с соответствующими комментариями.

Итак, рассмотрим следующую схему:

1) $A_i(\tau) \rightarrow D_j(\tau) \rightarrow V_k(\tau) \rightarrow T_l(\tau)$.

В данной схеме атака нарушителя, используя ДФ, активизировала уязвимость, что привело к реализации угрозы. В качестве иллюстрации рассмотрим пример: атака нарушителя состоит из действий по выведению из строя системы энергоснабжения ИТС. Отсутствие электропитания в таком случае будет ДФ. При этом может активизироваться такая уязвимость системы защиты информации, как отсутствие

бесперебойных источников питания либо исчерпание их ресурса в связи с длительным использованием. Это может привести к неработоспособности компонентов ИТС и, как следствие, к реализации угрозы доступности, а возможно и целостности информации.

2) $A_i(\tau) \rightarrow V_k(\tau) \rightarrow D_j(\tau) \rightarrow T_l(\tau)$.

В данной схеме нарушитель использует существующую уязвимость и ДФ для реализации угрозы. В качестве примера приведем спуфинг пакетов в сети передачи данных. Атакой считаем действия нарушителя по подключению к сети передачи данных и мониторингу трафика. При этом используется уязвимость, выражающаяся в несовершенстве протоколов передачи данных и отсутствии систем обнаружения и предотвращения вторжений. ДФ будет то, что по сети передается информация в открытом виде (например, атрибуты доступа). В случае перехвата этих данных нарушитель реализует угрозу конфиденциальности информации.

3) $A_i(\tau) \rightarrow V_k(\tau) \rightarrow T_l(\tau)$.

Угрозы могут реализовываться и без активизации ДФ. Примером данной ситуации может быть DoS-атака нарушителя на публичный веб-ресурс. Уязвимость средств защиты от атак типа «отказ в обслуживании» может привести к реализации угрозы доступности информации.

4) $A_i(\tau) \rightarrow D_j(\tau) \rightarrow T_l(\tau)$.

Такая схема иллюстрирует реализацию угрозы посредством активизации злоумышленником ДФ при видимом отсутствии уязвимостей. Уместным примером здесь кажется ситуация, когда нарушитель осуществляет деятельность по подглядыванию пароля, вводимого пользователем с клавиатуры. Вследствие случайности пароль может быть набран в другом поле, что позволит считать его с экрана монитора в открытом виде. Таким способом может реализоваться угроза конфиденциальности.

5) $A_i(\tau) \rightarrow T_l(\tau)$.

Данная ситуация характеризует возможность реализации угрозы без активизации уязвимостей и ДФ. Например, если пользователь обладает полномочиями администратора или суперпользователя, он может реализовать любую угрозу информации. Предотвратить реализацию подобных угроз можно лишь организационными мероприятиями, тем не менее, человеческий фактор является определяющим.

6) $D_j(\tau) \rightarrow V_k(\tau) \rightarrow T_l(\tau)$.

Данная схема иллюстрирует реализацию угрозы при отсутствии нарушителя, т. е. неумышленные действия по нарушению безопасности информации. Возникновение ДФ при условии наличия определенной уязвимости может привести к осуществлению угрозы. Например, в качестве ДФ можно рассматривать стихийное бедствие в виде пожара. Уязвимость, проявившаяся в отсутствии системы пожаротушения и резервного копирования, может привести к реализации угрозы целостности либо доступности информации.

7) $D_j(\tau) \rightarrow T_l(\tau)$.

Эта схема подобна предыдущей за исключением отсутствия уязвимости при реализации угрозы. В качестве ДФ можно рассмотреть ошибку системного либо прикладного программного обеспечения (например, «зависание»). В результате может реализоваться угроза доступности информации.

Приведенные выше схемы иллюстрируют варианты взаимодействия множеств в случаях реализации угрозы. Однако, подобные соображения справедливы и в тех случаях, когда угроза не реализуется, например в схемах типа $A_i(\tau) \rightarrow V_k(\tau) \rightarrow D_j(\tau)$ (обстоятельства либо средства защиты позволили предотвратить угрозу). Кроме этого, данные цепочки являются базовыми, и на их основе могут формироваться более сложные схемы, использующие комбинации сущностей, например: $A_i(\tau) \rightarrow V_k(\tau) \rightarrow D_j(\tau) \rightarrow D_{j+1}(\tau) \rightarrow V_{k+1}(\tau) \rightarrow T_l(\tau)$.

Включение в рассмотренные схемы объектов угроз, от которых преимущественно исходят информационные потоки, и субъектов угроз, к которым эти потоки направлены, позволит описать процесс реализации угрозы в рамках формализма объектно-субъектной модели ИТС: $S_m(\tau) \rightarrow A_i(\tau) \rightarrow V_k(\tau) \rightarrow D_j(\tau) \rightarrow T_l(\tau) \rightarrow O_n(\tau)$. Интерпретация атаки как последовательности процессов, а уязвимости – как некоторого объекта, – позволит в некотором приближении перейти к представлению процесса реализации угрозы в виде цепочки доступов [8].

IV Общая структура модели угроз

Процесс построения модели угроз можно условно разбить на следующие этапы:

1) определение перечня ДФ, которые могут возникать на протяжении жизненного цикла ИТС;

2) определение источников ДФ и возможных инициаторов атак;

3) определение и анализ возможных уязвимостей системы защиты ИТС;

4) формирование перечня всех возможных угроз информации в ИТС, субъектов и объектов угроз;

5) определение отношений между множествами ДФ, уязвимостей и угроз.

Для формирования множеств сущностей, фигурирующих в процессе реализации угрозы, необходимо выбрать удобную для представления этих множеств классификацию. При этом целесообразно учитывать специфику конкретной ИТС и отдавать предпочтение наиболее актуальной классификации. Модель угроз представляется в виде таблицы, которая также может сопровождаться таблицами, характеризующими множества сущностей, содержащихся в модели угроз, и снабженных соответсвующими идентификаторами.

Таблица – Пример обобщенной модели угроз в ИТС

№ п/п	Название и тип угрозы	Субъект угрозы	Объект угрозы	Возможная атака	ДФ	Используемая уязвимость
1	$T_l(\tau)$	$S_m(\tau)$	$O_n(\tau)$	$A_i(\tau)$	$D_j(\tau)$	$V_k(\tau)$

V Выводы

Предложенные соображения позволяют существенно упростить процесс построения модели угроз при создании защищенных ИТС. В частности, приведенный подход:

- инвариантен относительно применения к разным классам и типам ИТС;
- позволяет описать любую реальную ситуацию;
- является открытым, поскольку предусматривает добавление новых сущностей;
- учитывает любые классификации входящих сущностей.

Однако, формальное описание рассматриваемых множеств может быть неоднозначным, так как на практике зачастую сложно определить четкую грань между понятиями ДФ, уязвимости и угрозы. Кроме того, данный подход изначально не предполагает возможности построения универсальной модели угроз, поскольку все возможные угрозы перечислить невозможно вследствие появления новых, возникающих по мере развития технологий. Поэтому приоритетной задачей эксперта в сфере безопасности информации при разработке модели угроз является выделение наиболее существенных угроз для конкретной ИТС.

Литература: ***1****. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. - НД ТЗІ 1.1–003–99, ДСТСЗІ СБ України, Київ, 1999. – 26 с..* ***2****. Антонюк А. О., Жора В. В. Загрози інформації і канали витоку. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип. 2 - К.:2001, с. 42-46.* ***3****. Сердюк В. А. Классификация угроз информационной безопасности сетей связи, их уязвимостей и атак нарушителя. // Информационные технологии, № 9. - М.:2002, с. 7-12.* ***4****. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат.-1994.-тт.1, 2.* ***5****. А. А. Антонюк, Е. Н. Боровская, В. Ю. Суслов Модель угроз информации в защищенных автоматизированных системах // Безопасность информации. – № 2. – 2001. – 17-22 с.* ***6****. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. - НД ТЗІ 1.1–002–99, ДСТСЗІ СБ України, Київ, 1999. – 16 с.* ***7****. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Изд. Молгачева С. В., 2001. – 352 с.* ***8****. Антонюк А. О., Жора В. В. Моделювання доступу та каналів витоку в інформаційних системах. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип. 3 - К.:2001, с. 156-160.*

УДК 681.3

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ. ФОРМАЛЬНЫЙ ПОДХОД

Игорь Павлов
ВИТИ НТУУ «КПИ»

Анотация: **Раскрывается понятие процесса проектирования систем защиты информации и дано его математическое описание.**

Summary: **In article the concept of process of systems designing of information protection is opened, and its mathematical description is given.**

*Ключевые слова: П***роектирование систем защиты информации.**

I Введение

Существующие нормативные документы по оценке защищённости определяют гарантии безопасности,