Г. В. Фролов

ТИПИЗАЦИЯ ПРОЕКТНЫХ И ПРИКЛАДНЫХ РЕШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ РАЗРАБОТКЕ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Информационные технологии (ИТ) стали неотъемлемой частью повседневной жизни. На их основе удовлетворяются базовые потребности государства, бизнеса и гражданского общества по формированию, распространению, накоплению и потреблению информации.

ИТ эффективны тогда, когда они соответствуют потребностям текущего времени. Быстро изменяющиеся методы работы, появление на рынке новых ИТ-продуктов обусловливают потребность в создании новых и постоянной модификации и адаптации эксплуатирующихся информационных систем.

Для реализации новых общественных потребностей созданы высокоэффективные средства создания и развития ИТ. В частности, все большее развитие получает практика использования типовых решений, которые облегчают процесс разработки ИТ и снижают временные затраты.

В то же время практические подходы к разработке подсистем безопасности современных ИТ принципиально не изменились за последние десятилетия.

До недавнего времени практика разработки систем безопасности ИТ основывалась на нормативно-методологической базе, образованной Руководящими документами Гостехкомиссии России [1—5], которые были приняты в 90-х годах прошлого столетия. По мнению ряда авторов, они отражают «военный» подход к вопросу защиты информации, направленный на обеспечение ее конфиденциальности.

Анализ данных документов позволяет утверждать, что лежащий в их основе подход к разработке систем безопасности ИТ содержит элементы типизации проектных и прикладных решений в области защиты информации. В основе типизации лежит понятие «класс защищенности». Группировка ИТ по различным классам осуществляется на основании определяющих признаков, к которым относятся:

· наличие в ИТ информации различного уровня конфиденциальности;

· уровень полномочий субъектов доступа ИТ на доступ к конфиденциальной информации;

· режим обработки данных в ИТ — коллективный или индивидуальный.

На основании этих признаков выделены три типа ИТ:

· ИТ, в которых работает один пользователь, допущенный ко всей информации, размещенной на носителях одного уровня конфиденциальности;

· многопользовательские ИТ, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности;

· многопользовательские ИТ, в которых одновременно обрабатывается или хранится информация различных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации.

Эти три типа, представляющие собой верхний уровень типизации, в свою очередь разделены на классы защищенности, иерархичные между собой в пределах своей группы. Каждый класс характеризуется типовой совокупностью требований по защите. Таким образом, идентифицировав на основании определяющих признаков тип разрабатываемой ИТ, разработчик получает типовой набор требований по защите, которым должна удовлетворять система безопасности ИТ, чтобы последняя считалась защищенной.

Традиционная нормативно-методологическая база содержит и элементы типизации прикладных решений в области защиты информации. В их основе также лежат классы защищенности с соответствующими типовыми наборами требований по защите. При этом нормативные документы Гостехкомиссии устанавливают, какого класса защищенности должны применяться средства ИТ и средства защиты, чтобы обеспечить необходимый класс защищенности ИТ в целом. Если средство ИТ или средство защиты относится к определенному классу защищенности, оно может считаться типовым прикладным решением для построения ИТ соответствующих классов защищенности.

Рассмотренный подход к разработке защищенных ИТ обладает несомненными преимуществами, такими как простота практического применения, высокая скорость разработки, применение опробованных проектных и прикладных решений. Однако у данного подхода существует и недостаток — он учитывает в основном задачи обеспечения конфиденциальности информации, оставляя без должного внимания вопросы обеспечения ее целостности и доступности. Поэтому его применение для разработки систем безопасности ИТ не соответствует современным требованиям.

С принятием в 2004 г. ГОСТ Р ИСО/МЭК 15408-2002 г., являющегося российским вариантом «Общих критериев» (ОК), появился новый стандартизированный подход к разработке защищенных ИТ. Однако он до сих пор не получил широкого практического применения. Отсутствие в ОК конкретных требований и критериев для различных типов систем информационных технологий вынуждает разработчиков проектировать системы безопасности «с нуля». При этом при отсутствии развитого методического обеспечения каждый разработчик реализует свой, неформализованный метод решения поставленной задачи. Как результат, в большинстве случаев системы безопасности создаются «под ключ», исключая их дальнейшее развитие без участия разработчиков. При этом процесс разработки имеет высокую стоимость и занимает довольно много времени.

Возникает противоречие между потребностью общества в быстром развитии ИТ и практикой проектирования подсистем безопасности «с нуля», связанной с большими временными затратами. Данное противоречие может быть снято при создании методики разработки подсистем безопасности ИТ на основе типовых решений.

Наиболее важным моментом при использовании технологий, основанных на применении типовых решений, является базовое определение типового элемента [6]. Основной идеей настоящей статьи является выделение типовых решений в области защиты информации на основе технологии «полного перекрытия угроз».

В технологии «перекрытия угроз» [7] рассматривается взаимодействие «области угроз», «защищаемой области» (ресурсов АС) и «системы защиты» (механизмов безопасности ИТ). Для описания системы защиты используется графовая модель, представленная на рис. 1.

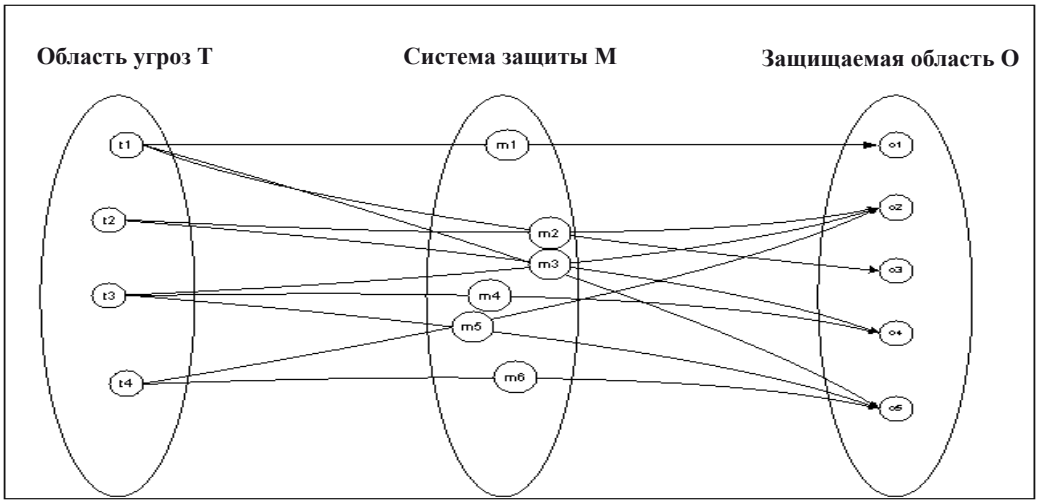

Рис. 1. Графовая модель системы защиты

Согласно технологии перекрытия угроз, решение задачи разработки системы защиты ИТ требует создания модели угроз объекта ИТ и модели защищаемой области. На практике построение таких моделей затруднено, так как эти понятия недостаточно формализованы и систематизированы, что не гарантирует качества результата.

В литературе [8–11], посвященной проблемам защиты информации, понятие «объект защиты» ассоциируется с корпоративной сетью, автоматизированной информационной системой, отдельным компьютером или каким-либо устройством, информацией, информационным процессом. Отсутствие четкого понимания в таком принципиальном вопросе, определяющем направления основных усилий в создании системы безопасности ИТ, препятствует разработке защищенных информационных технологий.

В различных источниках понятие «угроза» имеет большое количество трактовок, характеризующих ту или иную грань такого сложного явления. Практика свидетельствует о том, что, решая задачу идентификации угроз безопасности при разработке защищенной ИТ, большинство разработчиков использует свои неформализованные методы. Поэтому отсутствует повторимость результата, его значимость и возможность использования в других разработках. Гарантией качественного решения задачи построения моделей угроз для реальной сложной системы было бы использование соответствующих справочных баз данных (БДУ). В настоящее время разработаны и поддерживаются, в том числе и международными специализированными организациями, ряд БДУ безопасности ИТ. Однако сравнение содержащихся в существующих реализациях БДУ решений показывает значительную разницу как в подходах к классификации угроз, так и в полученных результатах.

В связи с этим первым этапом решения поставленной задачи было выделение объектов защиты в современных ИТ, классификация и описание множества угроз безопасности ИТ.

В настоящее время при решении практических задач защиты информации в качестве объектов защиты выступают технические и программные средства обработки информации, каналы связи и данные. В работе [12] рассматриваются вопросы защиты информационных технологий электронного документооборота. В ней обосновано выделение нового объекта защиты в системах электронного документооборота — информационной (компьютерной) технологии как упорядоченной последовательности операций обработки данных. На наш взгляд, это утверждение может быть распространено на все типы ИТ. Однако в литературе по защите информации термин «информационная технология» используется в более широком смысле. Последовательность операций традиционно обозначается термином «технологический процесс».

Поэтому представляется целесообразным для обозначения нового объекта защиты использовать термин «технологический процесс».

Таким образом, в данной работе в качестве объектов защиты ИТ выделены:

· технические средства ИТ (ТС);

· программные средства ИТ (ПС);

· каналы связи (КС);

· данные (Д);

· технологический процесс (ТП).

Достаточный уровень защищенности ИТ в целом может быть обеспечен только при обеспечении достаточного уровня защищенности каждого из выделенных объектов защиты. Данное утверждение следует из мультипликативной парадигмы защиты, согласно которой уровень информационной безопасности в ИТ не выше обеспечиваемой самым слабым звеном защиты [13].

В основу определения угроз безопасности ИТ положена идея взаимоувязывания угроз с объектами защиты ИТ, что предполагает наличие пяти классов угроз, соответствующих выделенным объектам защиты ИТ. Описание угроз безопасности должно обеспечить возможность идентификации угроз безопасности в среде функционирования ИТ различных масштабов, архитектуры и области применения, т. е. описанные угрозы должны быть типовыми. Для этого предлагается описывать угрозы на уровне детализации, соответствующем пяти выделенным структурным компонентам ИТ.

Помимо построения моделей угроз и защищаемой области разработчик защищенной ИТ описывает множество мер противодействия, которые должны перекрыть пути осуществления угроз безопасности к защищаемым объектам. Как правило, угроза может быть реализована несколькими способами, поэтому следует говорить о множестве путей осуществления, связанных с угрозой безопасности ИТ. Отсюда следует, что каждой угрозе должны быть сопоставлены соответствующие множества мер противодействия. Так как в нашем случае описываются типовые угрозы ИТ, то им можно сопоставить типовые меры противодействия.

Систему защиты ИТ предлагается трактовать как совокупность сервисов (услуг) безопасности, предоставляемых прикладной подсистеме ИТ. В данной работе сервис рассматривается как способность системы безопасности ИТ реализовать определенную типовую меру противодействия угрозе. Следовательно, для противодействия угрозе должно быть реализовано множество типовых сервисов безопасности, соответствующее множеству типовых мер противодействия.

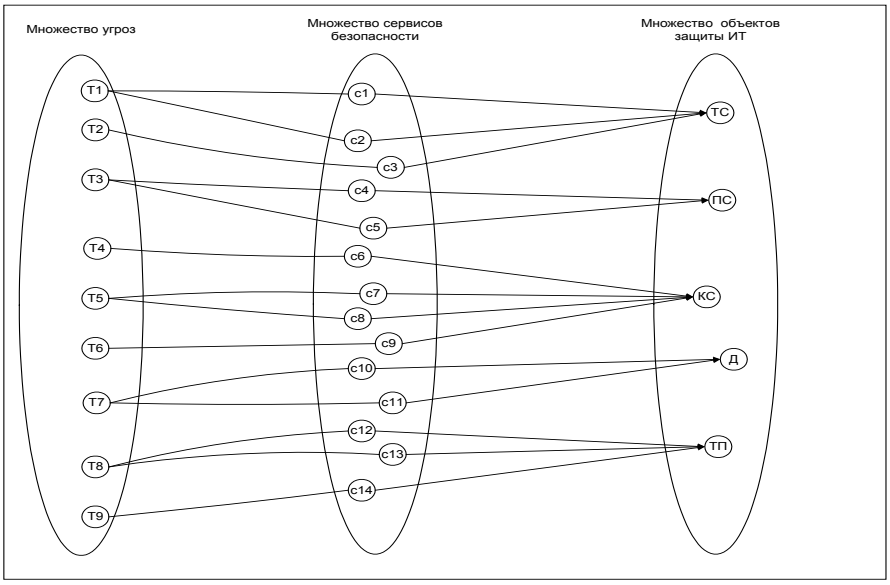

Рис. 2. Модель системы защиты, содержащей сервисы безопасности и объекты защиты ИТ

В результате получаем модель, описывающую систему защиты с учетом наличия в ней пяти объектов защиты и взаимоувязанных с ними угроз безопасности и сервисов безопасности (Рис. 2).

Система защиты ИТ представляет собой совокупность сервисов безопасности, которые могут быть реализованы в среде функционирования ИТ, в самой ИТ (путем использования защищенных средств ИТ) или средствами защиты информации. Поэтому модель системы защиты можно представить в следующем виде (Рис. 3).

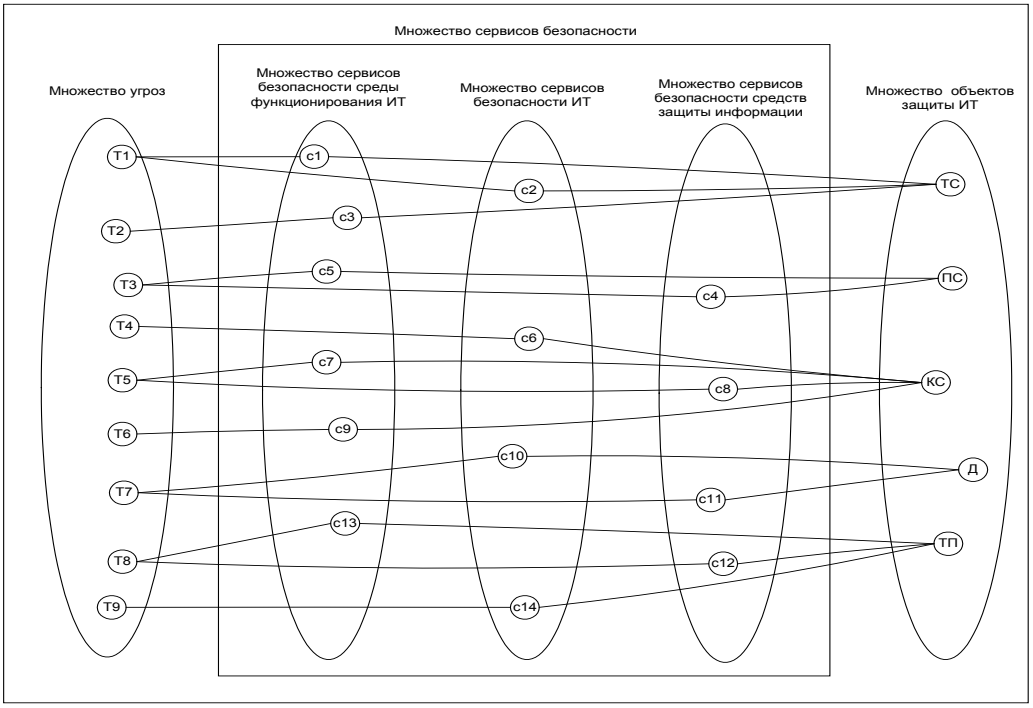

Рис. 3. Модель системы защиты, содержащей три подмножества сервисов безопасности

Каждому типовому сервису безопасности сопоставлены множества требований безопасности. Эти множества разработаны на основе каталога требований безопасности, содержащегося в ОК.

Из подхода к моделированию системы безопасности ИТ как совокупности типовых сервисов безопасности следует, что сервисный подход целесообразно применить и к описанию прикладных решений в области защиты информации. Средство ИТ или средство защиты, реализующее типовой сервис безопасности, в данном случае можно рассматривать как типовое. Для оценки способности средств ИТ или средств защиты информации реализовывать сервисы безопасности каждому сервису безопасности сопоставлены множества требований безопасности, разработанные на основании каталога функциональных требований безопасности ОК.

Процесс разработки защищенных ИТ с применением типовых решений предлагается проводить в соответствии с методикой, разработанной на основе методологии ОК. Методика предполагает выполнение трех основных этапов: разработка профиля защиты (ПЗ) ИТ, разработка задания по безопасности (ЗБ) ИТ и оценка защищенности ИТ.

Основной идеей предлагаемой методики является выделение в качестве типового элемента проектного и прикладного решения в области защиты информации сервиса безопасности. В связи с этим цели разработки профиля защиты ИТ, задания по безопасности ИТ и оценки защищенности ИТ можно сформулировать следующим образом. Цель разработки ПЗ ИТ – определение множества сервисов безопасности, которые должны быть реализованы в ИТ и среде

ее функционирования, для того чтобы была обеспечена защищенность ИТ. Цель разработки задания по безопасности ИТ — выбор средств ИТ и средств защиты информации, которые реализуют сервисы безопасности ИТ, заданные в ПЗ. Цель проведения оценки защищенности ИТ — подтверждение того, что в ИТ фактически реализованы все необходимые сервисы безопасности. В процессе разработки используются базы данных угроз, сервисов безопасности, требований безопасности, средств ИТ и средств защиты информации.

Алгоритм разработки ПЗ ИТ, согласно предлагаемой методике, будет следующим. На первом этапе разработчик определяет объекты ИТ, соответствующие каждому из пяти определенных ранее обобщенных объектов ИТ, подлежащих защите. В случае если идентифицируется хотя бы один объект соответствующего типа, необходимо описать для него угрозы безопасности на основании перечня типовых угроз для объектов данного класса. Далее на основании множества типовых сервисов безопасности описываются сервисы безопасности, которые должны быть реализованы, чтобы обеспечить защищенность ИТ. Сервисы безопасности могут быть реализованы как самой ИТ, так и средой ее функционирования. Для разграничения «ответственности» за их реализацию разработчик формулирует предположения безопасности, каждое из которых представляет собой утверждение, что определенный сервис безопасности реализуется средой функционирования ИТ. По окончании этого этапа на основании множества предположений безопасности формируется раздел ПЗ «Цели безопасности для среды ИТ». Сервисы безопасности, не попавшие в этот раздел, формируют раздел ПЗ «Цели безопасности для ИТ».

Согласно ОК, ПЗ включает разделы, содержащие требования безопасности. В рамках предлагаемой методики разработчик определяет требования безопасности на основании множеств требований безопасности, сопоставленных каждому из сервисов безопасности. Ранее отмечалось, что в нашем случае при разработке ПЗ основную роль играют сервисы безопасности. Требования безопасности необходимы для того, чтобы разработчик смог определить параметры (атрибуты) сервисов безопасности, таких как реализуемые криптографические алгоритмы, модели управления доступом, роли безопасности пользователей и т. д. Эти параметры задаются путем формулировки правил политики безопасности организации на основании базы данных правил, взаимоувязанных с требованиями безопасности.

Помимо функциональных требований безопасности ПЗ ИТ должен включать и требования доверия, представленные в виде оценочного уровня доверия (ОУД). ОК дают самые общие рекомендации по выбору разработчиком ИТ оценочного уровня доверия, увязывая его выбор со стоимостью проведения оценки либо со стоимостью защищаемых активов. Однако в рамках технологии «полного перекрытия угроз» было бы логично увязать выбор требований доверия с наличием в среде функционирования ИТ определенных угроз безопасности.

Далее рассмотрим алгоритм разработки задания по безопасности ИТ. При выполнении этой работы разработчик использует базу данных средств ИТ и средств защиты информации, оцененных по сервисам безопасности. В базе данных содержится информация по двум категориям: реализуемые объектом оценки сервисы безопасности и параметры сервиса безопасности, обеспечиваемые объектом. В процессе разработки ЗБ ИТ разработчик должен выбрать средства ИТ и средства защиты, которые реализуют определенные в ПЗ сервисы безопасности и способны обеспечить заданные параметры сервисов безопасности.

В процессе разработки ЗБ может возникнуть ситуация, когда невозможно выбрать средства ИТ или средства защиты информации, реализующие все необходимые сервисы безопасности, либо, наоборот, выбранные средства реализуют избыточные сервисы безопасности. Первая ситуация требует обязательной доработки ПЗ ИТ путем переноса недостающих сервисов безопасности в среду функционирования ИТ. Вторая с точки зрения защищенности ИТ не критична, однако

по каким-либо другим соображениям разработчик может удалить «лишние» сервисы из среды функционирования ИТ.

В рамках рассматриваемой методики используется метод качественной оценки защищенности путем сравнения заданного в ПЗ ИТ множества сервисов безопасности с перечнем фактически реализованных сервисов безопасности, указанных в ЗБ ИТ. Помимо этого оценщик проводит анализ того, обеспечивают ли реализованные сервисы безопасности параметры, определенные правилами политики безопасности организации. Оценка наиболее актуальна в случае использования средств ИТ или средств защиты информации, не включенных в базу данных средств, оцененных по сервисам безопасности.

Оценка защищенности ИТ не ограничивается определением множества фактически реализованных системой безопасности ИТ сервисов безопасности и возможностью выполнения правил политики безопасности организации. Необходимо подтвердить, что обеспечен заданный оценочный уровень доверия.

Использование рассмотренной методики разработки защищенных ИТ позволит значительно ускорить и упростить процесс создания ИТ за счет применения типовых проектных и прикладных решений в области защиты информации. Кроме того, использование разработанных баз данных апробированных типовых решений позволит гарантировать качество конечного результата.

СПИСОК ЛИТЕРАТУРЫ:

1. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. 1992 г.
2. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. 1992 г.
3. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. 1992 г.
4. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. 1997 г.
5. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. 1999 г.
6. *Чернов А. Г.* Технология создания систем поддержки принятия решений в интегрированных САПР // Media-planning.ru, 2000 г. URL: http://www.media-planning.ru/atchernov/rus/docs/rus-dic.htm.
7. *Астахов А.* Анализ защищенности автоматизированных систем // ISACA.RU, 2002 г. URL: http://www.isaca.ru/security/Pubs/Pub1 AAM SecEval.htm.
8. *Петренко С. А., Петренко А. А.* Аудит безопасности Intranet. М., 2002.
9. *Тихонов В. А., Райх В. В.* Основы защиты информации. М., 2004.
10. *Домарев В. В.* Защита информации и безопасность компьютерных систем. К.: Диа-Софт, 1999.
11. *Леонов А. П., Леонов К. А., Фролов Г. В.* Безопасность автоматизированных банковских и офисных систем. Мн., 1996.
12. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. Мн.: Беллитфонд, 2004.
13. *Конявский В. А., Фролов Г. В.* Гарантированная защита информации от несанкционированного доступа в автоматизированных системах // Компьютерная преступность и информационная безопасность / Под ред. А. П. Леонова. Мн., 2000. С. 508–547.