С. В. Конявская

К ВОПРОСУ О КЛАССИФИКАЦИИ ОБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ[1]

Актуальной на сегодняшний день методологической проблемой является обоснование эффективности (и шире — целесообразности) применения тех или иных решений защиты информации в тех или иных конкретных системах. Поскольку в значительной мере это вопрос бизнеса, то за счет многообразия применяемых технологий и инфраструктур дроблением объектов защиты сегодня удается мотивировать применение в любой системе любого набора средств защиты информации. Это перегружает системы, делает их плохо управляемыми и ненадежными (растет количество возможных точек отказа, функции многократно дублируются, что ведет к неизбежным ошибкам настроек и возникновению конфликтов). В каждом конкретном случае можно доказывать, что нужно защищать — ключи или справочники сертификатов и что лучше — отражать атаки виртуальных машин на виртуальные машины или обеспечивать невозможность осуществления такой атаки, однако это всякий раз будут точечные выводы, не меняющие основного подхода: выделить новую сущность и предложить новое решение для ее защиты. Этот подход требует в качестве необходимого условия неясности предмета, позволяющей предельно «усложнять» задачи, повышая тем самым стоимость их решения.

Альтернативой представляется методологический прием — возведение каждого явления, предполагаемого к защите, к классификации объектов защиты информации.

В области защиты информации классифицируют, как правило, следующее:

- собственно информацию (по огромному количеству критериев, и классификации в основном получаются не сводимыми одна к другой)[2];
- объекты информатизации (также довольно много актуальных и авторитетных на сегодняшний день классификаций, различающихся, впрочем, в меньшей степени, чем классификации информации как таковой)[3];
- объекты защиты информации (как правило, приводятся в виде факультативных по отношению к первым двум видам классификаций и редко кладутся в основу дальнейших построений, являясь просто видом справочного материала)[4].

Почему из перечисленных возможностей именно классификацию объектов защиты представляется целесообразным положить в основу методологии определения оптимального

[1] Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно с ООО «ОКБ САПР».

[2] Представляется нецелесообразным приводить ссылки на конкретные примеры классификаций, поскольку перечень будет либо несоразмерно велик, либо катастрофически неполон — в том или ином виде классификация информации есть в абсолютном большинстве относительно объемных и в значительном количестве небольших работ на тему защиты информации.

[3] Как правило, объекты информатизации классифицируются с нормативными методическими целями, поэтому так или иначе сводятся (или восходят) к классификации СТР-К [1] либо создаются в дружественных странах (например, в Республике Беларусь [2]).

[4] В качестве примера можно привести классификацию, растиражированную в широком спектре методических и дидактических материалов по информационной безопасности и представленную, в частности, в [3], где выделяются следующие объекты:

- информация (так! — *С. К.*);
- ресурсные объекты (это аппаратное и программное обеспечение, процессы и процедуры обработки информации. — *С. К.*);
- физические объекты (территории, помещения, здания, техническое оборудование, средства и каналы связи. — *С. К.*);
- пользовательские объекты (пользователи информации, субъекты информации, собственники информации, обслуживающий персонал. — *С. К.*).

Не останавливаясь на не вполне удачных формулировках типа «пользовательские объекты», стоит только отметить, что эта классификация никак не используется автором в дальнейшем изложении материала и во всех других обнаруженных случаях приведения данной классификации имеет место та же самая ситуация. Думается, что связано это именно с тем, что такая классификация непродуктивна — она не решает никаких задач.

подхода к решению прикладных задач — вполне очевидно: именно это и есть целевая функция данной классификации.

Информация классифицируется с самыми разными целями, но в основном все эти классификации либо слишком абстрактны для прикладных применений, либо, наоборот, настолько ограничены конкретной областью действия, что не могут стать источником получения знания, а могут быть только инструментом описания.

Объекты информатизации классифицируются, как правило, с целью формализации проверки их соответствия тем или иным требованиям. И если брать классификацию СТР-К, то она, по сути дела не является инструментом разделения объектов по некоему признаку, поэтому использовать ее для определения правильности или неправильности подхода к защите в общем-то невозможно. По ней можно только установить, должны ли какие-либо меры приниматься в принципе.

Сущность же «объект защиты» принципиально формируется (должна формироваться) на основании дифференциальных признаков, связанных с тем, как защищается объект того или иного класса и чем способы и методы его защиты отличают его от объектов других классов.

Наиболее высокой степенью абстрагированности от инфраструктур различных типов характеризуется классификация, предложенная В. А. Конявским [4]. Предельно коротко ее можно свести к следующему тезису.

В процессе информационного взаимодействия на разных его этапах заняты люди (**операторы, пользователи**) и используются средства информатизации — технические (**ПЭВМ, ЛВС**) и программные (**ОС, ППО**). Информация (сведения) порождается людьми, затем преобразовывается в **данные** и представляется в АС в виде **информационных ресурсов**. Данные между компьютерами передаются по **каналам** связи. В процессе работы АС данные преобразовываются в соответствии с реализуемой **информационной технологией**.

На основании этого положения выделено четыре объекта защиты:

- компьютеры,
- данные,
- каналы,
- информационные технологии.

Задачей формирования этой классификации было выявление и обоснование информационной технологии как отдельного объекта защиты. Эта задача была решена, сейчас сложно себе представить, что этот объект не выделяется или считается несущественным.

Однако на сегодняшний день возникло понимание необходимости уточнения этой классификации.

Этому и посвящены приведенные ниже выкладки.

Понятие «информационная технология» описывает процесс *изменения* данных.

Тезис этот может показаться неочевидным, если исходить из определения, данного в ГОСТ: «Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных» [5]. Однако обратим внимание, что это определение не касается сущности понятия, а описывает его через обстоятельства, в которых оно проявляется. Это «приемы, способы и методы» даже не *выполнения* перечисленного ряда действий, а *используемые при* их выполнении. То есть *тогда, когда* они выполняются. В какой еще зависимости они находятся, кроме временной, ГОСТом не определяется.

Таким образом, это определение не дает ни явного подтверждения, ни опровержения тому, что результатом действия технологии обязательно является изменение данных.

Кроме обращения к ГОСТу, можно прибегнуть к методу выведения содержания из определения понятия, родового по отношению к рассматриваемому. То есть из определения понятия «технология» (так как информационная технология — это точно технология, просто не любая).

«Технология — всегда процесс производства продукта. Информационная технология (ИТ) — процесс производства информационного продукта. Та или иная совокупность информационных продуктов называется информационным ресурсом. В процессе производства продуктов используются материалы, средства производства и технологии производства. В информационном производстве средства производства — это средства вычислительной техники (СВТ) и информационные системы (ИС) на их основе, технологии — это ИТ, а материалы — информация в том или ином виде — преимущественно в виде **сообщений** в электронной форме» [6]. Такая длинная цитата приведена для того, чтобы сделать акцент на следующем: у информационной технологии входные и выходные данные — различны (одни являются материалом, а вторые — продуктом), в противном случае применение технологии необоснованно. В процессе производства должно быть что-то произведено, иначе процесс определенно поставлен неверно.

Интуитивно именно это обычно понимается под «обработкой» данных и не это — под «хранением»[5]. Интуитивно, потому что общепринятого терминологического определения обработки данных на сегодняшний день нет (в техническом смысле, а не в смысле регулировки отношений граждан, как, в частности, в Федеральном законе № 152-ФЗ, — такого рода определения для классификации технической стороны вопроса неприменимы).

Итак, обработка данных — это процесс, в ходе которого они как-то меняются.

В общем случае — предсказуемо меняются. По определению Н. А. Кузнецова, «информация — это сущность, сохраняющаяся при вычислимом изоморфизме» [7]. Если преобразование не изоморфно — информация утрачена.

Поэтому, как правило, результат разрушительного программного воздействия на данные «обработкой» не называется. А вот преобразование из одного формата в другой — называется, хотя изменения «содержания» данных не происходит.

Таким образом, обработка данных — это процесс исполнения информационной технологии, которая, в свою очередь, напомним, является упорядоченной последовательностью операций над данными.

Кроме обработки данных, возможно еще их хранение. В отличие от обработки — когда данные меняются, хранение — это когда данные *не* меняются. Это, однако, не единственная полезная для классификации характеристика хранения. Важно также то, что при хранении данные остаются там же, где были *сохранены*. Они не перемещаются.

Стало быть, есть третий случай — когда данные перемещаются, не изменяясь — это передача. В таком контексте невозможно игнорировать тот факт, что защищенная передача данных предполагает в качестве обязательного требования их неизменность. То есть данные перемещаются, но не изменяются.

Логика классификации детерминирует и четвертый случай — данные одновременно и перемещаются, и изменяются. Видимо, это говорит о том, что информационная технология может включать, а может и не включать в себя передачу данных между инфраструктурными элементами (на которых функционируют инструменты, выполняющие операции над данными).

Итого.

1) Хранение — нет изменения, нет перемещения (00)

2) Передача — нет изменения, есть перемещение (01)

3) Обработка в рамках одного инфраструктурного элемента — есть изменение, нет перемещения (10)

[5] В этом смысле можно, безусловно, определить «хранение» как «тождественное преобразование». Но за исключением сомнительной задачи мотивировать устоявшееся словосочетание «технология хранения» это определение ничего не дает, кроме смешения очевидно различных сущностей. Контекстуальный же анализ идиомы «технология хранения» показывает, что она метафорична (как большинство идиом) и описывает цепочку «технология сохранения» (преобразования данных в формат, в котором они будут храниться) и дальнейшее «хранение» уже без применения какой-либо технологии.

4) Обработка в рамках разных инфраструктурных элементов — есть изменение, есть перемещение (11)

Так, данные могут храниться, передаваться и обрабатываться. Отражая это на приведенную выше классификацию, получаем две точки, в которых отражение происходит не идеально:

1) компьютеры,

2) данные.

Казалось бы, две из четырех — это слишком много несоответствия (или слишком мало соответствия), чтобы можно было вообще говорить о сводимости классификаций.

Однако несоответствия эти имеют совершенно разную природу, что существенно снижает их критичность.

Очевидно, что «данные» выпадают из этого ряда ровно по той причине, что это *предмет*, общий для всех выделяемых *объектов*:

- каналы — это каналы *передачи данных*;
- информационные технологии — это технологии *обработки данных*;
- компьютеры — это...

Логика классификации ведет к тому, что это средство (место) *хранения данных*.

Однако компьютер — это, конечно, не только место хранения. Это с тем же успехом и место (и что важнее — средство) их обработки. Он содержит и инструменты, и хранилища, и даже каналы передачи в общем-то.

Видимо, в контексте данной классификации компьютер (или СВТ) необходимо заменить на «носитель». Это позволит избежать нарушения правила единого основания, обязательного для классификации, с одной стороны, а с другой — отражение «хранения» на «носитель» — абсолютно точно. Носитель — это средство хранения данных.

В результате получаем следующую обобщающую классификацию объектов защиты, относящихся к предмету защиты — «данные»:

1. Носители (хранение);
2. Технологии (обработка);
3. Каналы (передача).

Отдельно данные как самостоятельный объект защиты не имеют смысла, поскольку защищать данные оказывается возможно только при хранении, обработке или передаче. Других состояний у них просто нет. И все это состояния именно *данных*.

Практическая польза этой, как и всякой другой, классификации заключается в возможности проверки ею концептуальных основ подсистем защиты тех или иных систем и инфраструктур — как на предмет полноты, так и на предмет избыточности.

В частности, такая проверка делает предельно наглядной необоснованность тезиса о том, что в терминальных системах необходимо защищать только терминальный сервер и в лучшем случае — каналы, а на терминальном клиенте достаточно только относительно надежно аутентифицировать пользователя, так как *на терминальных клиентах* не хранятся и не обрабатываются данные.

Делает возможным это утверждение именно неопределенность понятия обработки данных, которую в «бытовом» смысле очень привлекательно свести к изменению *содержания*.

Однако если проверить эту логику тем, реализуют ли терминальные клиенты какую-нибудь *технологию*, становится очевидным, что да, реализуют: именно ОС терминального клиента поддерживает работу оборудования терминала (сетевая карта, видеокарта и так далее), именно в ней исполняется (как приложение) само ПО терминального клиента ICA или RDP, поддерживается работа протокола.

Ясно, что эти функции имеют значение с точки зрения обеспечения безопасности информации в системе и ОС терминального клиента должна быть контролируемой. Таким образом, вопрос из

области доказательства целесообразности принятия защитных мер в отношении того или иного инфраструктурного элемента можно свести к прояснению его участия в жизненном цикле данных, что является намного более простой и однозначной процедурой.

СПИСОК ЛИТЕРАТУРЫ:

1. Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
2. *Деев Н. А., Мартинович Т. С.* Критерии классификации объектов информатизации по требованиям защиты информации. URL: http://www.ITsec.ru/doc/deev_martinovich.doc (дата обращения: 25.07.2013).
3. Общие вопросы технической защиты информации. Электронный курс. М.: Интернет-университет информационных технологий «Интуит», 2003. URL: http://www.intuit.ru/studies/courses/2291/591/info (дата обращения: 25.07.2013).
4. *Конявский В. А.* Информационные технологии как объект защиты и классификация антивирусных программ // Безопасность сетей и средств связи. 2007. Вып. 2. С. 52–54.
5. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», приложение 1, статья 4.
6. *Конявский В. А.* Научно-методические проблемы создания защищенных информационных технологий // ВКСС Connect! 2006. № 1 (34). С. 41.
7. *Кузнецов Н. А., Мусхелишвили Н. Л., Шрейдер Ю. А.* Информационное взаимодействие как объект научного исследования (перспективы информатики) // Вопросы философии. 1999. № 1. С. 77–87.