Сущность и соотношение понятий "защита информации", "безопасность информации", "информационная безопасность"

**А. И. АЛЕКСЕНЦЕВ,**

кандидат исторических наук, профессор Российский государственный гуманитарный университет

Понятия защита ин­формации, безопасность информации, информа­ционная безопасность яв­ляются базовыми, по­скольку **их** сущность оп­ределяет в конечном ито­ге политику и деятель­ность в сфере защиты ин­формации. В то же время эти понятия взаимосвяза­ны и взаимообусловлены. Между тем и в норматив­ных документах, и в науч­ной литературе нет еди­ных подходов к определе­нию данных понятий, а, следовательно, и к рас­крытию их сущности, ибо определения должны в концентрированном виде выражать сущность по­нятий. В первую очередь это относится к понятию защита информации, где разброс мнений наиболее значителен. При этом различия касаются как со­держательной части понятия, так и способа ее реа­лизации.

По содержательной части защита информации рассматривается как: предупреждение несанкцио­нированного доступа к информации; создание ус­ловий, ограничивающих распространение инфор­мации; ограждение права собственника на владе­ние и распоряжение информацией; предотвраще­ние утечки, хищения, утраты, несанкционирован­ного уничтожения, копирования, модификации, искажения, блокирования, разглашения инфор­мации, несанкционированных и непреднамерен­ных воздействий на нее; сохранение полноты, на­дежности, целостности, достоверности, конфиден-*,.* циальности информации и т.д.

Способом реализации содержательной части понятия одни авторы называют совокупность ме-Si/роприятий, методов и средств, другие -деятель­ность, у третьих он вообще отсутствует.

Методологической основой для раскрытия сущности и определения понятия защиты инфор­мации должно быть определение понятия защита в целом, безотносительно к предмету защиты.

В толковых словарях термин защита интерпре­тируется двояко: как процесс охраны, сбережения, спасения от кого, чего-нибудь неприятного, враж­дебного, опасного и как совокупность методов, средств и мер, принимаемых для предотвращения, предупреждения чего-то. Таким образом, содержа­тельная часть в этих определениях по смыслу сов­падает - это предотвращение, предупреждение че­го-то опасного, враждебного. Если соотнести это положение с защитой информации, то самым опас­ным для собственника информации является нару­шение установленного статуса информации, и поэ­тому содержательной частью защиты должно быть , предотвращение такого нарушения.

Нарушение статуса любой информации заклю-

чается в нарушении ее физической сохранности вообще либо у данного собственника (в полном или частичном объеме), структурной целостно­сти, доступности для правомочных пользова­телей. Нарушение стату­са конфиденциальной информации, в том числе составляющей государ­ственную тайну, допол­нительно включает в се­бя нарушение ее конфи­денциальности (закры-тости для посторонних лиц).

Нарушение статуса информации обусловлено ее уязвимостью, которая означает неспособность информации самостоятельно противостоять деста­билизирующим воздействиям, сохранять при та­ких воздействиях свой статус.

Но уязвимость информации - понятие собира­тельное, она не существует вообще, а проявляется (выражается) в различных формах. В научной ли­тературе и нормативных документах не сформиро­вался термин форма проявления уязвимости ин­формации, но самих конкретных формназывается множество. При этом значительное количество пе­речисляемых форм являются синонимами или раз­новидностями одних и тех же явлений, некоторые не могут быть отнесены к формам по своей сущно­сти.

Представляется, что к формам проявления уяз­вимости информации, выражающим результаты дестабилизирующего воздействия на информа­цию, должны быть отнесены:\*)

- хищение носителя информации или отобра­женной в нем информации (кража);

- потеря носителя информации (утеря);

- несанкционированное уничтожение носителя информации или отображенной в неминформации (разрушение);

- искажение информации (несанкционирован­ное изменение, несанкционированная модифика­ция, подделка, фальсификация);

- блокирование информации;

- разглашение информации (несанкциониро­ванное распространение, раскрытие)

Хищение информации часто ставится в один ряд с ее несанкционированным копированием, размножением, съемом, перехватом. Однако пос­ледние являются не формами проявления уязви­мости информации, а способами хищения. ,

Термины модификация, подделка, фальсифи­кация не совсем адекватны термину искажение, они имеют нюансы, но суть их одна и та же - не­санкционированное частичное или полное измене-ниепервоначальной информации.

Та или другая форма уязвимости информации

\*) В скобках даны существующие варианты названий форм

***16* Безопасность информационных технологий, 1999. .№ 1**

*А. И. Алексенцев. Сущность и соотношение понятий "защита информации"...*

может реализоваться при преднамеренном или случайном, непосредственном или опосредован­ном дестабилизирующем воздействии различны­ми способами на носитель информации или саму информацию со стороны определенных источни­ков воздействия.

Но результатами проявления форм уязвимости информации могут быть либо утрата, либо утечка информации, либо одновременно то и другое. *^*

К утрате как конфиденциальной, так и защи­щаемой части открытой информации приводят хи­щение и потеря носителей информации, несанкци­онированное уничтожение носителей информации или только отображенной в них информации, ис­кажение и блокирование информации. Утрата мо­жет быть полной или частичной, безвозвратной или временной (при блокировании информации), но в любом случае она наносит ущерб собственнику информации.

Термин утечка информации, вероятно, не са­мый благозвучный, однако он более емко, чем дру­гие термины, отражает суть явления, к тому же он давно уже закрепился в научной литературе и нор­мативных документах. Правда, единого подхода к определению этого термина нет. Наиболее распро-странные определения в обобщенном виде сводят­ся либо к неправомерному (неконтролируемому) выходу конфиденциальной информации за преде­лы организаций и круга лиц, которым эта инфор­мация доверена, либо к несанкционированному за-владению конфиденциальной информацией сопер­ником. При этот термин конфиденциальная ин­формация иногда неправомерно заменяется терми­ном защищаемая информация.

Первый вариант не раскрывает в полной мере сущности утечки, поскольку он не принимает во внимание последствий неправомерного выхода конфиденциальной информации. А они могут быть двоякими: или информация попала вруки лиц, не имеющих к ней санкционированного дос­тупа, или не попала. Например, потерянный носи­тель конфиденциальной информации означает не­правомерный выход информации за пределы лиц, имеющих к ней доступ, но он может попасть в чу­жие руки, а может быть и прихвачен мусороубо­рочной машиной и уничтожен в установленном для мусора порядке. В последнем случае утечки информации не происходит.

Второй вариант утечку информации связыва­ет с неправомерным завладением конфиденци­альной информацией только соперником. В та­ком варианте, к примеру, средства массовой ин­формации, которым нередко поставляют или они сами добывают конфиденциальную информа­цию, должны рассматриваться в качестве сопер­ников собственника информации, в этом случае настоящий соперник получает информацию пра­вомерно, через СМИ.

В то же время утечка информации не означает получение ее только лицами, не работающими на предприятии, к утечке приводит и несанкциониро­ванное ознакомление с конфиденциальной инфор­мацией лиц данного предприятия.

Исходя из изложенного, можно сформулиро­вать следующее определение:

Утечка информации - неправомерный выход конфиденциальной информации за пределы защи­щаемой зоны ее функционирования или установ­ленного круга лиц, результатом которого является получение информации лицами, не имеющими к ней санкционированного доступа.

Термин утечка информации нередко, в том чис­ле и в нормативных документах, заменяется или отождествляется с терминами разглашение инфор­мации, распространение информации и даже пере­дача информации. Такой подход представляется неправомерным. Термин разглашение информа­ции означает несанкционированное доведение конфиденциальной информации до потребителей, не имеющих права доступа к ней, таким образом, он предполагает, что разглашение исходит от кого-то, осуществляется кем-то. Результатом разглаше­ния является утечка информации, но утечка не сводится только к разглашению. Термин распро­странение применительно к конфиденциальной информации без слов несанкционированное или необоснованное ничего не выражает, поскольку распространение информации может быть и обос­нованным, к тому же он опять-таки предполагает, что информация исходит от кого-то. Термин пере­дача информации говорит сам за себя.

Помимо разглашения, утечка может произой­ти и в результате потери и хищения носителя кон­фиденциальной информации, а также хищения отображенной в носителе информации при сохран­ности носителя у собственника (владельца). Может произойти не означает, что произойдет. Выше уже отмечалось, что потеря носителя не всегда приво­дит к утечке информации. Хищение конфиденци­альной информации также не всегда связано с по­лучением ее лицами, не имеющими к ней доступа. Имелось немало случаев, когда хищение носите­лей конфиденциальной информации осуществля­лось у коллег по работе допущенными к этой ин­формации лицами с целью подсидки, причинения вреда коллеге. Такие носители, как правило, унич­тожались лицами, похитившими их. Но в любом случае потеря и хищение если и не приводят к утечке информации, то создают угрозу утечки. По­этому можно сказать, что к утечке конфиденци­альной информации приводит ее разглашение и могут привести хищение и потеря. Сложность со­стоит в том, что зачастую невозможно определить, во-первых, сам факт разглашения или хищения информации при сохранности носителя информа­ции у собственника (владельца), во-вторых, попала ли информация вследствие ее хищения или потери посторонним лицам. При этом не следует отожде­ствлять хищение с разглашением, как это иногда делается. Хищение может привести и часто приво­дит к разглашению и в последнем случае выступа­ет в роли опосредованного способа разглашения, но, во-первых, результатом хищения не всегда бы­вает разглашение, во-вторых, разглашение конфи­денциальной информации осуществляется не только посредством ее хищения.

Безопасность информационных технологий, 1999. ,№ **1 *17***

***Специальный* выпуск"**

Утрата и утечка информации могут рассматри­ваться как виды уязвимости информации.

Суммируя соотношение форм и видов уязвимо­сти защищаемой информации, можно констатиро­вать:

1.Формы проявления уязвимости информации выражают результаты дестабилизирующего воз­действия на информацию, а виды уязвимости - ко­нечный суммарный итог реализации форм уязви­мости.

2.Утрата информации включает в себя, по срав­нению с утечкой, большее число форм проявления уязвимости информации, но она не поглощает утечку, т.к., во-первых, не все формы проявления уязвимости информации, которые приводят или могут привести к утечке, совпадают с формами, приводящими к утрате, во-вторых, если к утрате информации приводит хищение носителей, то к утечке может привести хищение и носителей, и отображенной в них информации при сохранности носителей.

3. Наиболее опасными формами проявления уязвимости конфиденциальной информации явля­ются потеря, хищение и разглашение - первые две одновременно могут привести и к утрате, и к утеч­ке информации, вторая (хищение информации при сохранности носителя) и третья могут не обна­ружиться со всеми вытекающими из этого послед­ствиями.

4. Неправомерно отождествлять виды и отдель­ные формы проявления уязвимости информации (утрата^потеря, утрата= хищение, утечка=разгла-шение (распространение), заменять формы прояв­ления уязвимости информации способами дестаби­лизирующего воздействия на информацию, а так­же ставить в один ряд формы и виды уязвимости защищаемой информации, как это, в частности, сделано в законе "Об информации, информатиза­ции и защитой нформации", где одной из целей за­щиты названо: предотвращение утечки, хищения, утраты, искажения, подделки информации.

Поскольку нарушение статуса информации вы­ражается в различных формах проявления уязви­мости информации, а все формы сводятся к двум видам уязвимости, содержательную часть понятия защита информации можно определить как пре­дотвращение утраты и утечки конфиденциальной информации и утраты защищаемой открытой ин­формации.

Вторая составляющая сущности защиты ин­формации - способ реализации содержательной части - в толковых словарях, как уже отмечалось, представлена как процесс или как совокупность методов, средств и мероприятий.

Защита информации включает в себя опреде­ленный набор методов, средств и мероприятий, од­нако ограничивать способ реализации только этим было бы неверно. Защита информации должна быть системной, а в систему помимо методов, средств и мероприятий входят и другие компонен­ты: объекты защиты, органы защиты, пользовате­ли информации. При этом защита не должна пред­ставлять собой нечто статичное, а являться непре­

рывным процессом. Но этот процесс не осуществ­ляется сам по себе, а происходит в результате дея­тельности людей. Деятельность же, по определе­нию, включает в себя не только процесс, но и цели, средства и результат. Защита информации не мо­жет быть бесцельной, безрезультатной и осуществ­ляться без помощи определенных средств. Поэто­му именно деятельность и должна быть способом реализации содержательной части защиты.

Объединив содержательную часть защиты ин­формации и способ реализации содержательнойча-сти, можно сформулировать следующее определе­ние:

Защита информации - деятельность по предот­вращению утраты и утечки конфиденциальной ин­формации и утраты защищаемой открытой инфор­мации.

Учитывая, что определение должно быть лако­ничным, а термин утрата и утечка защищаемой информации поглощаетвсе формы проявления уязвимости конфиденциальной и защищаемой ча­сти открытой информации, можно ограничиться более кратким определением при условии диффе­ренцированного его преломления в практической работе: Защита информации - деятельность по предотвращению утраты и утечки защищаемой информации.

'—" А теперь проанализируем определение этого понятия, содержащееся в ГОСТ Р50922-96 "Защи­та информации. Основные термины и определе­ния", поскольку это определение официальное, имеющее в смысловом значении обязательный ха­рактер. Оно сформулировано так: Защита инфор­мации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Как видно, это определение совпадает с предло­женным по способу реализации содержательной части защиты и по одной из ее составляющих -предотвращению утечки защищаемой информа­ции. Однако определение утечки в ГОСТе дано дру­гое - оно не сформулировано отдельно, а вмонтиро­вано в определение термина Защита информации от утечки, которое звучит так: Защита информа­ции от утечки: деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкциониро­ванного доступа к защищаемойинформации и от получения защищаемой информации (иностран­ными} разведками. Из этого определения вытека­ет, что утечка информации - это неконтролируе­мое распространение защищаемой информации.

Неконтролируемое распространение можно по смыслу приравнять к неправомерному выходу ин­формации за пределы защищаемой зоны ее функ­ционирования или установленного круга лиц. Но если в предложенном в данной статье определении утечки далее обозначен результат такого выхода -получение информации лицами, не имеющими к ней санкционированного доступа, то в стандарте неконтролируемое распространение выступает уже как результат, к которому приводят разглаше-

***18* Безопасность информационных технологий, 1999. № 1**

*А. И. Алексенцев. Сущность и соотношение понятий "защита информации"...*

ние, получение информации разведками и несанк­ционированный доступ к ней. Т.е., в первом случае неконтролируемое распространение приводит к несанкционированному получению, во втором -все наоборот. Но различия не ограничиваются этим. Вызывает недоумение, почему в один ряд по­ставлены разглашение, несанкционированный до­ступ к информации и ее получение. Разве несанк­ционированный доступ к информации не может привести к ее разглашению и получению? Если нет, то как он влияет на неконтролируемое распро­странение информации? Только как возможность с его помощью похитить ее. Но хищение в итоге опять приводит к получению информации. С дру­гой стороны, разве разглашение информации не приводит к ее получению иностранными разведка­ми и не только ими?

Такая путаница в ГОСТе вызвана тем, что на одну доску поставлены понятия с разными значе­ниями: форма проявления уязвимости защищае­мой информации (разглашение), механизм полу­чения информации (несанкционированный дос­туп) и результат неконтролируемого распростране­ния информации (получение разведками).

По второму компоненту содержательной части защиты информации предложенное в данной ста­тье и гостированное определения расходятся и по формулировке, и по существу. В статье - это пре­дотвращение утраты защищаемой информации, В ГОСТе - предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Таким образом, если в первой части определения содержательной части ГОСТ называ­ет вид уязвимости информации (утечку), то во вто­рой - не вид (утрату), а воздействия, которые могут привести к этому виду уязвимости. Конечно, утра­та не может произойти без несанкционированных или непреднамеренных воздействий на информа­цию, но зачем понадобился разный подход к обо­значению двух видов уязвимости информации, по­чему один называется, другой подразумевается?

Отчасти это объясняется, вероятно, тем, что ре­зультаты воздействия на информацию ГОСТ не сводит только к ееутрате. Это видно из расшифров­ки понятий несанкционированного и непреднаме­ренного воздействий на информацию.

К несанкционированному воздействию ГОСТ относит воздействие на защищаемую информацию с нарушением установленных прав или правил на изменение информации, приводящее к искаже­нию, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничто­жению или сбою функционирования носителя ин­формации.

Непреднамеренное воздействие определяется ГОСТом как воздействие на защищаемую инфор­мацию ошибок пользователя информацией, сбоя технических и программных средств информаци­онных систем, а также природных явлений или иных нецеленаправленных на изменение инфор­мации воздействий, связанных с функционирова­нием технических средств, систем или с деятельно­стью людей, приводящих к искажению, уничто­

жению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Таким образом, результатом воздействия на информацию или ее носитель являются и вид уяз­вимости (утрата), и формы проявления уязвимости (искажение, уничтожение, блокирование), и спо­соб воздействия (копирование). Если в данном слу­чае копирование заменяет хищение, то это невер­но, поскольку есть и другие способы хищения. К тому же непонятно, в чем смысл в определении по­нятия отделять носитель информации от самой ин­формации, ведь в итоге названные утрата и унич­тожение носителя (без учета неправомерности по­становки их в один ряд) являются одновременно утратой и уничтожением отображенной в них ин­формации, а сбой функционирования носителя приводит к блокированию информации.

Может показаться, что все это - частности. Но определение любого понятия, помимо всего проче­го, требует точности формулировки. \_

С понятием защиты информации тесно связано понятие безопасности информации.

Термин безопасность информации имеет двой­ное смысловое значение, его можно толковать и как безопасность самой информации, и как отсут­ствие угроз со стороны информации субъектам ин­формационных отношений.При этом безопасность самой информации также не вписываетсяв одно­значное понимание. С одной стороны, это может означать безопасность информации с точки зрения изначальной полноты и надежности информации, с другой стороны, — защищенность установленного статус-кво информации.

В нормативных документах и литературе безо­пасность информации рассматривается только в разрезе ее защищенности, и это, вероятно, оправ­дано при наличии термина информационная безо­пасность.

Существует несколько определений понятия безопасность информации. При общем подходе к безопасности информации как состоянию защи­щенности (или защиты) информации эти определе­ния существенно различаются между собой содер­жательной частью - защищенности от чего. Сюда относят: от внутренних и внешних угроз; от утеч­ки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (поддел­ки), несанкционированного копирования, блоки­рования информации и т.п.; от случайных или преднамеренных несанкционированных воздейст­вий на информацию или несанкционированного ее получения; от случайного или преднамеренного доступа лиц, не имеющих права на получение ин­формации, ее раскрытие, модификацию или раз­рушение, и др.

Не вызывает возражений подход к определе­нию безопасности информации как к состоянию защищенности информации, ибо сам термин безо­пасность означает отсутствие опасностей, что опре­деленным образом корреспондируется с термином состояние защищенности.

Вторую часть определения можно сформулиро-

**Безопасность информационных технологий, 1999. № 1 *19***

***Специальный выпуск***

вать и как от воздействий, нарушающих ее статус, **и как** от утраты и утечки, поскольку в конечном итоге они выражают одно и то же, т.к. предотвра­щение утраты и утечки информации осуществля­ется посредством предотвращения дестабилизиру­ющих воздействий на информацию. Первый вари­ант представляется более предпочтительным, т.к. непосредственной целью защищенности информа­ции является противодействие дестабилизирую­щим воздействиям.

Из определений понятий защита информации и безопасность информации вытекает и соотноше­ние между ними: защита информации направлена на обеспечение безопасности информации или, другими словами, безопасность информации обес­печивается с помощьюее защиты.

Понятие информационная безопасность в науч­ной литературе сначала отождествлялось с поняти­ем безопасность информации. Затем к этому приба­вилось или это заменилось на защищенность субъе­ктов информационных отношений от негативных информационных воздействий. В различных опре­делениях присутствуют те или другие нюансы, но они не меняют сути названных подходов. Такое толкование информационной безопасности пред­ставляется неполным. Методологической основой определения этого понятия должно быть отнесение его не к самой информации, хотя информационная безопасность и сопряжена с информацией, а к субъ­ектам информационной среды - физическим и юридическим лицам, участвующим в информаци­онном процессе. Из этого, кстати, следует, что в практическом преломлении информационная безо­пасность не существует вообще, безотносительно к субъекту информационной среды, именно субъект диктует показатели такой безопасности. Это отно­сится не только к конкретным субъектам, но и к личности, обществу и государству в целом.

Смысловое содержание понятия информацион­ная безопасность предполагает и в какой-то мере предопределяет включение в него трех составляю­щих.

Первой составляющей является удовлетворе­ние информационных потребностей субъектов, включенных в информационную среду. Здравый смысл подсказывает, что не может быть обеспечена информационная безопасность субъекта без нали­чия у него необходимой информации. Информаци­онные потребности различных субъектов не одина­ковы, однаков любом случае отсутствие необходи­мой информации может иметь и, как правило, име­ет отрицательные последствия. Эти последствия могут носить различный характер, их тяжесть за­висит от состава отсутствующей информации.

Необходимая для удовлетворения информаци­онных потребностей информация должна отвечать определенным требованиям. Во-первых, информа­ция должна быть относительно полной. Относи­тельно потому, что абсолютно полной информации ни один субъект иметь не может. Полнота инфор­мации характеризуется ее достаточностью для принятия правильных решений. Во-вторых, ин­формация должна быть достоверной, ибо искажен­

ная информация приводит к принятию неправиль­ных решений. В-третьих, информация должна быть своевременной, т.к. необходимые решения эффективны лишь тогда, когда они принимаются вовремя.

Но требования полноты, достоверности и свое­временности информации относятся не только к ее первоначальному статусу. Эти требования имеют силу на все время циркулирования информации, потому что **их** нарушение на стадии последующего использования информации также может привес­ти к неправильным решениям или вообще к невоз­можности принятия решений, как и нарушение статуса конфиденциальности может обесценить информацию. Поэтому информация должна быть защищена от воздействий, нарушающих еестатус. А это относится к сфере безопасности информации. Стало быть, обеспечение безопасности информа­ции должно являться второй составляющей ин­формационной безопасности.

К принятию неверных решений может привес­ти не только отсутствие необходимой информации, но и наличие вредной, опасной для субъекта ин­формации, которая чаще всего целенаправленно навязывается. Это требует обеспечения защиты субъектов информационных отношений от нега­тивного информационного воздействия, что долж­но являться третьей составляющей информацион­ной безопасности.

При таком подходе можно сформулировать следующее определение:

Информационная безопасность - состояние ин­формационной среды, обеспечивающее удовлетво­рение информационных потребностей субъектов информационных отношений, безопасность ин­формации и защиту субъектов от негативного ин­формационного воздействия.

При этом под информационной средой, соглас­но закону Об участии в международном информа­ционном обмене, понимается сфера деятельности субъектов, связанная с созданием, преобразовани­ем и потреблением информации. В законе дано и определение информационной безопасности как состояния защищенности информационной среды общества, обеспечивающего ее формирование, ис­пользование и развитие в интересах граждан, орга­низаций, государства.

Этому определению не хватает конкретности. В него можно вписать и содержательную часть пред­ложенного определения, а можно свести его только к безопасности информационных систем, что не­правомерно, т.к. информационная безопасность не ограничивается безопасностью информационных систем.

Из предложенных в данной статье определений понятий защита информации, безопасность ин­формации, информационная безопасность видно, что существует прямая связь и зависимость между понятиями защита информации - безопасность информации, безопасность информации - инфор­мационная безопасность и опосредованная - меж­ду понятиями защита информации - информаци­онная безопасность.

***20* Безопасность информационных технологий, 1999. *№ 1***