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, конфиденциальности информации и т.д.

Способом реализации содержательной части понятия одни авторы называют совокупность мероприятий, 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 заключается 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 (закрытости 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 форм называется 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 нем информации (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 изменение первоначальной информации.

Та или другая форма уязвимости 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 распространённые 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 завладению 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 в руки 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. По-этому 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.

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=разглашение (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 информации", 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 непрерывным 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 содержательной части, 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 поглощает все 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 защищаемой информации 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 разглашение, 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 ее утрате. 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, уничтожению, 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 вписывается в 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, блоки-

рования 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 сформулировать 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 помощью ее 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, однако в 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 ее статус. 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.