КУРС: «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ:
сущность и понятие,
цели и значение,
теоретические и концептуальные основы

РАССМАТРИВАЕМЫЕ ВОПРОСЫ

- СУЩНОСТЬ И ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ
- ЦЕЛИ И ЗНАЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ
- ТЕОРЕТИЧЕСКИЕ И КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

СУЩНОСТЬ И ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ

ЮУрГУ

Рекомендуемая литература

- ГОСТ Р50922-96 «Защита информации. Основные термины и определения».
- Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. -1999. -№1.
- Алексенцев А.И. Защита информации: Словарь базовых терминов и определений. М.: РГГУ, 2000.
- Астахова Л.В. Теория информационной безопасности и методология защиты информации. – Челябинск: «ЗАО Челябинская межрайонная типография», 2006. – 361 с.
- Шиверский А.А Защита информации: проблемы теории и практика.-М.:Юрист,1996.

ЮУрГУ

Существующие подходы к содержательной части понятия защиты информации

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.

ЮУрГУ

Существующие подходы к содержательной части понятия защиты информации

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

ЮУрГУ

Методологическая основа для раскрытия сущности и определения понятия защиты информации – понятие «защита»

- Методологическая основа - определение понятия защита в целом, безотносительно к предмету защиты.

- В толковых словарях термин защита интерпретируется двояко:

процесс охраны, сбережения, спасения от кого-нибудь, чего-нибудь неприятного, враждебного, опасного

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.

ЮУрГУ

Методологическая основа для раскрытия сущности и определения понятия защиты информации – понятие «защита»

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).

ЮУрГУ

Понятие уязвимости информации и ее форм и видов

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.

ЮУрГУ

К формам проявления уязвимости информации, выражающим результаты дестабилизирующего воздействия на информацию, должны быть отнесены

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

ЮУрГУ

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.

ЮУрГУ

Виды уязвимости - утрата и утечка

- 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.

ЮУрГУ

Виды уязвимости - утрата и утечка

Термин утечка информации, более емко, чем другие термины, отражает суть явления, он давно уже закрепился в научной литературе и нормативных документах. Правда, единого подхода к определению этого термина нет. Наиболее распространенные определения утечки в обобщенном виде сводятся:

1. Либо к неправомерному (неконтролируемому) выходу конфиденциальной информации за пределы организаций и круга лиц, которым эта информация доверена,

2. Либо к несанкционированному завладению конфиденциальной информацией соперником.

ЮУрГУ

Виды уязвимости - утрата и утечка

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.

ЮУрГУ

Виды уязвимости - утрата и утечка

- 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.

ЮУрГУ

Определение «Утечка информации» А.И. Алексенцева

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.

ЮУрГУ

Соотношение понятий утечка, разглашение, распространение, передача информации

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.

ЮУрГУ

Соотношение понятий утечка, разглашение, распространение, передача информации

- 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. Утечка – результат разглашения.

- 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.

ЮУрГУ

Соотношение понятий утечка, разглашение, распространение, передача информации

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. 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.

Соотношение понятий утечка, разглашение, распространение, передача информации

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. 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.

ЮУрГУ

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.*

ЮУрГУ

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

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 защита информации", где одной из целей защиты названо: предотвращение утечки, хищения, утраты, искажения, подделки информации.

ЮУрГУ

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

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.**

ЮУрГУ

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 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. 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:

ЮУрГУ

Определение защиты информации (А.И. Алексенцев)

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.

Определения понятия защиты информации в ГОСТ Р50922-96

- ГОСТ Р50922-96 "Защита информации. Основные термины и определения": 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.

ЮУрГУ

Определения утечки в ГОСТ Р50922-96

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.*

ЮУрГУ

Соотношение определения понятия защиты информации А.И. Алексенцева и определения, сформулированного в ГОСТ Р50922-96.

Неконтролируемое распространение можно по смыслу приравнять к неправомерному выходу информации за пределы защищаемой зоны ее функционирования или установленного круга лиц. Но если в предложенном А.И. Алексенцевым 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.

ЮУрГУ

Соотношение определения понятия защиты информации А.И. Алексенцева и определения, сформулированного в ГОСТ Р50922-96.

В один ряд поставлены разглашение, несанкционированный доступ к информации и ее получение.

А) Несанкционированный доступ к информации 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.

Б) Разглашение информации 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).

ЮУрГУ

Соотношение определения понятия защиты информации А.И. Алексенцева и определения, сформулированного в ГОСТ Р50922-96.

По второму компоненту содержательной части защиты информации, предложенное А.И. Алексенцевым, и гостированное определения расходятся **и по формулировке, и по существу**:

- У А.И. Алексенцева - это предотвращение утраты защищаемой информации.

- В ГОСТе - предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию.

ЮУрГУ

Соотношение определения понятия защиты информации А.И. Алексенцева и определения, сформулированного в ГОСТ Р50922-96.

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.

ЮУрГУ

Соотношение определения понятия защиты информации А.И. Алексенцева и определения, сформулированного в ГОСТ Р50922-96.

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.

ЮУрГУ

Соотношение определения понятия защиты информации А.И. Алексенцева и определения, сформулированного в ГОСТ Р50922-96.

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.

ЮУрГУ

Понятие безопасности информации

С понятием защиты информации тесно связано понятие безопасности информации.

Термин безопасность информации имеет двойное смысловое значение, его можно толковать:

- и как безопасность самой информации,

При этом безопасность самой информации не вписывается в однозначное понимание. С одной стороны, это может означать безопасность информации с точки зрения изначальной полноты и надежности информации (т.е. безопасность с точки зрения содержания), с другой стороны, — защищенность установленного статус-кво информации (безопасность с точки зрения формы информации).

- и как отсутствие угроз со стороны информации субъектам информационных отношений.

ЮУрГУ

Понятие безопасности 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. Общий подход: безопасность информации как состоянию защищенности (или защиты) информации. Это не вызывает возражений, ибо сам термин безопасность означает отсутствие опасностей, что определенным образом корреспондируется с термином состояние защищенности.

Понятие безопасности информации

Но определения существенно различаются между собой содержательной частью - защищенности от чего. Сюда относят:

- от внутренних и внешних угроз; *(непонятно)*
- от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.; *(перепутаны виды и формы уязвимости)*
- 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..

Понятие безопасности информации

Вторую часть определения А.И. Алексенцев сформулировал следующим образом:

- *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.

Т.о., Безопасность информации – это состояние защищенности информации от воздействий, нарушающих ее статус.

ЮУрГУ

Соотношение понятий «защита информации» и «безопасность информации»

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 (безопасность информации – результат ее защиты).**

ЮУрГУ

ЦЕЛИ И ЗНАЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

ЮУрГУ

Конституция Российской Федерации о защите информации

Информация в конституционном контексте связана, прежде всего, с реализацией основных прав и свобод человека и гражданина:

- право на информацию установлено в **ч. 4 ст. 29, ч. 2 ст. 24 и ст. 42 Конституции РФ**;
- право на защиту информации о частной жизни лица – в **ч. 1 ст. 24 Конституции РФ;**
- свобода мысли, мнений и слова закреплены в **ч. 1, 3 ст. 29 Конституции РФ**.
- Согласно **ч. 4 ст. 29 Конституции РФ** каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом".
- **Ч. 2 ст. 24 Конституции РФ** закрепляет общее право доступа каждого к информации, непосредственно затрагивающей его права и свободы. Этому праву корреспондирует общая обязанность органов государственной власти и местного самоуправления, располагающих такого рода информацией, ее предоставлять по соответствующим запросам.
    - **Ст. 42 Конституции РФ** говорит о праве каждого на «достоверную информацию» о состоянии окружающей Среды.

ЮУрГУ

Конституция Российской Федерации о защите информации

- **Возможные исключения из этого общего правила должны обязательно иметь форму закона. В ст. 29 ч. 4 Конституции указывается, что «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом».**

Формулировки этих норм Конституции РФ вполне адекватны соответствующим международно-правовым установлениям в этой специфической сфере общественных отношений.

ЮУрГУ

Конституция Российской Федерации о защите информации

Таким образом, для информации в РФ действует принцип изначальной открытости. Ограничение доступа к информации есть исключение из общего принципа открытости информации, и осуществляется только на основе федерального законодательства. Однако его реализация, без каких либо ограничений, может принести ущерб собственникам, владельцам и пользователям информации. Этот тезис подтверждается частью 3 статьи 55 Конституции, согласно которой права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

ЮУрГУ

Конституция Российской Федерации о защите информации

Поэтому в Конституции вводятся **ограничивающие нормы на принцип открытости**. К таким нормам относятся:

- признание и защита равным образом частной, государственной, муниципальной и иных форм собственности, в том числе собственности на информационные ресурсы (ч. 1 ст. 8). - Право частной собственности охраняется законом. Каждый вправе иметь имущество в собственности, владеть, пользоваться и распоряжаться им как единолично, так и совместно с другими лицами (ст. 35.);

- право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23). - Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ч. 1 ст. 24);

ЮУрГУ

Конституция Российской Федерации о защите информации

- право каждого на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (ч. 2 ст. 23);

- право государства иметь государственную тайну. - Перечень сведений, составляющих государственную тайну, определяется федеральным законом (ч. 4 ст. 29).

Таким образом, в Конституции устанавливается баланс между открытостью информации и ограничением доступа к ней.

ЮУрГУ

Существующие подходы к определению целей защиты информации

ЮУрГУ

Статья 20 Закона «Об информации, информатизации и защите информации» определяет основные цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;
- обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

ГОСТ Р 50922-96 ГОСУДАРСТВЕННЫЙ СТАНДАРТ РФ Защита информации ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ:

Цель защиты информации - желаемый результат защиты информации. Примечание: Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

ЮУрГУ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Защита информации АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ГОСТ Р 51624-2000

В настоящем стандарте реализованы нормы Законов РФ в информационной сфере и в областях защиты информации:

Общей целью ЗИ в АСЗИ является предотвращение или снижение величины ущерба, наносимого владельцу и/или пользователю этой системы, вследствие реализации угроз безопасности информации.

Цели защиты информации в АСЗИ должны включать:

- содержательную формулировку цели защиты;
- показатель эффективности достижения цели и требуемое его значение;
- время актуальности каждой цели защиты информации (этапы жизненного цикла, в течение которых цель должна достигаться).

ЮУрГУ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Защита информации АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ГОСТ Р 51624-2000

Частными целями ЗИ обеспечивающими достижение общей АСЗИ, являются:

- предотвращение утечки информации по техническим каналам;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечения полноты, целостности, достоверности информации в системах обработки;
- сохранение возможности управления процессом обработки и использования информации условиях несанкционированных воздействий на защищаемую информацию.

ЮУрГУ

Понятие целей защиты информации, их отличие от задач

ЮУрГУ

Часто цель и задачи ЗИ отождествляют, что неверно.

Цель защиты информации – это то, ради чего она должна защищаться (предполагаемый результат деятельности по защите информации).

Задачи защиты информации - это, что необходимо сделать для реализации цели (результата защиты информации).

ЮУрГУ

Структура целей защиты информации (А.И.Алексенцев)

ЗАЩИТА ИНФОРМАЦИИ ИМЕЕТ ДВА УРОВНЯ ЦЕЛЕЙ:

Первый уровень – непосредственные цели, которые должны быть привязаны к самой информации как непосредственному объекту защиты.

Цель защиты информации – безопасность информации.

Второй уровень – конечные цели (опосредованные), которые должны быть привязаны к субъектам информационных отношений (государству, обществу, личности, конкретному хозяйствующему субъекту).

Цель защиты информации – безопасность субъектов информационных отношений.

ЮУрГУ

Структура целей защиты информации (А.А. Шиверский)

Защита информации — это деятельность собственника информации или уполномоченных им лиц по:

- обеспечению своих прав на владение, распоряжение и управление защищаемой информацией;
- предотвращению утечки и утраты информации;
- сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки;
- сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

В общем виде цели защиты информации сводятся к режимно-секретному информационному обеспечению деятельности государства, отрасли, предприятия, фирмы.

ЮУрГУ

Задачи защиты информации

Первый уровень – задачи общеконцептуального плана:

- **на предупреждение угроз**. Предупреждение угроз — это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- **на выявление угроз**. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
- **на обнаружение угроз.** Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;
- **на локализацию** преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
    - **на ликвидацию последствий** угроз и преступных действий **и восстановление** статус-кво.

ЮУрГУ

Первый уровень – задачи общеконцептуального плана

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными **мерами и средствами**, начиная от создания климата *глубоко осознанного отношения сотрудников к проблеме* безопасности и защиты информации до *создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.*

Предупреждение угроз возможно и путем *получения информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях* и других элементах преступных деяний.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

ЮУрГУ

Первый уровень – задачи общеконцептуального плана

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции.

Обнаружение угроз — это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов.

ЮУрГУ

Первый уровень – задачи общеконцептуального плана

Пресечение или локализация угроз — это действия, направленные наустранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного здания от подрыва и др.

ЮУрГУ

Задачи защиты информации

Второй уровень задач защиты информации зависит от конкретного предприятия (прикладные задачи). Они зависят:

- от видов защищаемой на предприятии информации;
- степени ее конфиденциальности;
- состава носителей защищаемой информации.

ЮУрГУ

По мнению А.А.Шиверского, защита информации разбивается на решение двух основных групп задач:

1. Своевременное и полное удовлетворение информационных потребностей, возникающих в процессе управленческой, инженерно-технической, маркетинговой и иной деятельности, то есть обеспечение специалистов организаций, предприятий и фирм секретной или конфиденциальной информацией.

2. Ограждение засекреченной информации от несанкционированного доступа к ней соперника, других субъектов в злонамеренных целях.

ЮУрГУ

Вторая группа задач — это ограждение защищаемой информации от несанкционированного доступа к ней соперника, включает такие условия, как:

- Защита информационного суверенитета страны и расширение возможности государства по укреплению своего могущества за счет формирования и управления развитием своего информационного потенциала.

- Создание условий эффективного использования информационных ресурсов общества, отрасли, предприятия, фирмы, структурного подразделения, индивида.

- Обеспечение безопасности защищаемой информации: пред отвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации и т.п., вмешательства в информацию и информационные системы.

- Сохранение секретности или конфиденциальности засекреченной информации в соответствии с установленными правилами ее защиты, в том числе предупреждения ее утечки и несанкционированного доступа к ее носителям, предотвращению ее копирования, фотографирования и др.

ЮУрГУ

Вторая группа задач — это ограждение защищаемой информации от несанкционированного доступа к ней соперника, включает такие условия, как:

- Сохранение полноты, достоверности, целостности информации и ее массивов и программ обработки, установленных собственником информации или уполномоченными им лицами.

- Обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальной персональной информации, в том числе накапливаемой в банках данных.

- Недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности, принадлежащей государству, предприятиям и фирмам, частным лицам.

ЮУрГУ

ТЕОРЕТИЧЕСКИЕ И КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

ЮУрГУ

Понятие теории и ее соотношение с понятием концепции

Наука – это сфера человеческой деятельности, функцией которой является выработка и систематизация объективных знаний о действительности.

Эмпирический уровень.
Цель и результат – описание явлений, фактов, объектов, их свойств и признаков (фактографическая информация).

Теоретический уровень.
Цель – объяснение фактов и явлений, предсказание процессов действительности, отражение объективных закономерностей развития природы и общества независимо от исторического периода (выявление сущности и существенных взаимосвязей между объектами, выявление генезиса и эволюции объекта, открытие законов и закономерностей).

ЮУрГУ

Результатом теоретического научного исследования могут быть:

- Теория – форма научного знания, раскрывающая сущность изучаемых явлений, существенные взаимосвязи между фактами;

- Концепция – это форма научного знания, представляющая собой систему взглядов, то или иное понимание явлений, процессов разными субъектами, обусловленные спецификой его целей, задач, их оценку. Концепция разрабатывается на основе общепризнанных, логически доказанных положений, отражающих объективные законы и закономерности окружающей действительности, т.е. - на основе теории.

ЮУрГУ

Теория защиты информации

– это форма научного знания, дающая целостное представление о закономерностях и существенных связях объектов и явлений в области защиты информации.

Цель теории защиты информации – определить и объяснить сущность, цели, задачи, принципы, закономерности, методы, средства защиты информации и связи между ними.

ЮУрГУ

Основные положения теории защиты информации: общетеоретические положения:

- Объективная необходимость и общественная потребность в ЗИ;
- Зависимость системы и состояния ЗИ от политико-правовых и социально-экономических реальностей;
- Тесная взаимосвязь ЗИ с информатизацией общества;
- Баланс между потребностью в свободном обмене информацией и ограничениями на ее распространение;
- Соблюдение баланса интересов государства, общества и личности (теория интересов);
- Влияние ЗИ на права, свободы и безопасность граждан;
- Сходство и различия в межгосударственных, государственных и ведомственном подходах к ЗИ и ИБ;
- Социальные последствия ЗИ.

Методологические принципы защиты информации:

- Обеспечение единства, взаимосвязи и сбалансированности в решении задач производственной деятельности и ЗИ;
- Сочетание общих норм защиты с нормами, обусловленными спецификой деятельности предприятий различного профиля;
- Обеспечение сбалансированного соотношения объективной необходимости с экономической целесообразностью ЗИ;
- Сочетание максимального ограничения доступа к ЗИ с качественным выполнением служебных обязанностей;
- Обеспечение персональной ответственности за ЗИ и др.

ЮУрГУ

Названные общетеоретические и методологические положения являются основами национальной политики в сфере защиты информации и основой концепции защиты информации

ЮУрГУ

Понятие и назначение концепции защиты информации

Концепция защиты информации - это система взглядов на сущность, цели, принципы и организацию защиты информации.

ЮУрГУ

Понятие и назначение концепции защиты информации

Концепция должна:

- отображать политику государства в области защиты информационных ресурсов страны;
- подчинять цели и задачи ЗИ потребностям общественно-политического и социально-экономического развития страны;
- предусматривать режимное информационное обеспечение национальной безопасности государства;

ЮУрГУ

Понятие и назначение концепции защиты информации

Концепция должна:

- определять систему засекречивания-рассекречивания информации, обеспечивающую выделение для защиты действительно ценной для государства, общества и личности информации и исключающей использование секретности в узко корыстных отраслевых или личных интересах;

- создать структуру режимных мер и обеспечить ее функционирование в соответствии с принципами строительства правового государства и современного хозяйственного механизма, базирующегося на предприятиях различных форм собственности.

ЮУрГУ

Концепция защиты информации предполагает:

- Определение понятия, сущности и целей защиты информации.
- Какую информацию необходимо защищать, каковы критерии отнесения ее к защищаемой.
- Дифференциация защищаемой информации: а) по степеням конфиденциальности, б) по собственникам и владельцам.
- Определение состава и классификация носителей защищаемой информации.

ЮУрГУ

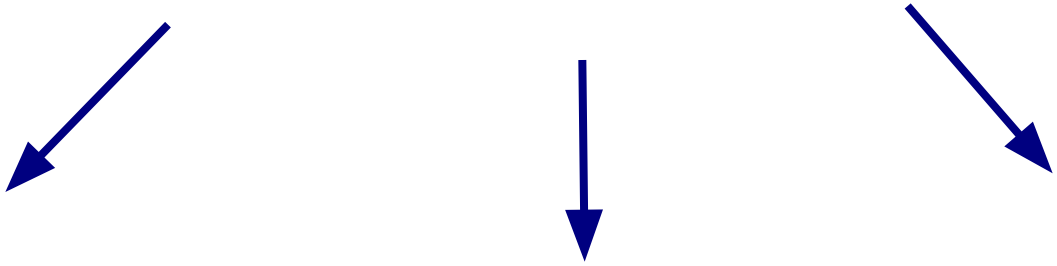
Концепция защиты информации предполагает:

- Определение состава угроз безопасности информации.
- Определение источников, видов и способов дестабилизирующего воздействия на информацию, причин, обстоятельств и условий воздействий, каналов, методов и средств несанкционированного доступа к информации.
- Определение методов и средств защиты информации.
- Кадровое обеспечение защиты информации.

ЮУрГУ

Уровни концепции защиты информации

А.А. Шиверский выделяет три уровня защиты информации в государстве:



социально-политический

стратегический

оперативный

ЮУрГУ

Социально-политический уровень защиты информации

ЮУрГУ

Социально-политический уровень защиты информации

связан с проведением единой государственной информационной политики и политики информационной безопасности, защитой различных видов охраняемых тайн, объектов интеллектуальной собственности.

Это положение нашло отражение, например, в:

- Доктрине информационной безопасности РФ, в которой защита информационных ресурсов названа одной из составляющих национальных интересов РФ в информационной сфере;

- Указ Президента РФ № 170 от 20 января1994 г. «Об основах государственной политики в сфере информатизации», где в частности в п. 1 указывается, что «...основными направлениями государственной политики в сфере информатизации являются ... формирование и защита информационных ресурсов как национального достояния...» и др.

ЮУрГУ

Социально-политический уровень защиты информации

Концепцию (доктрину) целесообразно разрабатывать для конкретного исторического этапа развития государства специалистами — научными и практическими работниками, и после одобрения высшим руководством страны реализовывать в виде законов, других нормативных актов и практических мер по всей иерархии систем защиты информации.

Социально-политический уровень защиты информации

Действовавшая в 70 — 80-х гг. концепция защиты информации являлась воплощением политики отражения угроз нашему государству со стороны зарубежных государств, борьбы с разведывательно-подрывной деятельностью спецслужб этих государств. В качестве средств и методов борьбы с империализмом были: гонка вооружения, защита государственных секретов и т.п. Следствием реализации этой концепции являются многочисленные перечни сведений, подлежащих засекречиванию и не подлежащих опубликованию в открытой печати. Населению выдавалась строго дозированная информация.

ЮУрГУ

Основные положения современной концепции защиты информации

Во-первых, ЗИ в РФ является частью деятельности по обеспечению ИБ личности, общества и государства.

ЮУрГУ

Основные положения современной концепции защиты информации

Во-вторых, ЗИ должна обеспечить соблюдение конституционных прав и свобод личности в области информации: на доступ к информации (в т.ч. - о государственной политике РФ), на полную, достоверную и оперативную информацию, на личную тайну, на интеллектуальную собственность и др.

ЮУрГУ

Основные положения современной концепции защиты информации

В-третьих, ЗИ должна обеспечить охрану и развитие информационных ресурсов страны, ее защищенной информационной инфраструктуры в целом.

Информационные ресурсы РФ являются ее национальным достоянием, национальным богатством и включены в качестве информационных составляющих в инфраструктуру страны. Информационные ресурсы, призванные обслуживать деятельность различных государственных структур, обеспечивающих национальные интересы РФ и ее безопасность, не являются однородными. Их защита организуется и осуществляется на основе различных законодательных и других нормативных актов, различных организационных мерах, хотя используются в основном общие принципы ЗИ и схожие порядок и правила защиты.

ЮУрГУ

Организационно-правовой (стратегический) уровень защиты информации

ЮУрГУ

Организационно-правовой (стратегический) уровень защиты информации

- На этом уровне разрабатывается система законодательных актов и других нормативно-правовых документов, директив, стандартов, которые составляют организационно-правовую базу и условия для построения систем защиты информации в отрасли, на предприятии, в учреждениях и фирмах.

- Стратегия защиты информации отражает идеи и замыслы собственника (владельца) информации на планирование и организацию защиты своих информационных ресурсов. На уровне государства в стратегии защиты информации реализуется концепция ее защиты, создания базы и условий построения систем защиты информации на любом уровне.

ЮУрГУ

Организационно-правовой (стратегический) уровень защиты информации

Стратегический уровень не ставит перед собой цель создания системы ЗИ. На этом уровне определяются лишь условия и база формирования таких систем на любом уровне.

Условия и база для формирования на этой основе в последующем систем ЗИ должны содержать компоненты, используемые в последующем при создании систем ЗИ:

- *конкретизированные стратегические цели ЗИ;*
- *правовая база, обеспечивающая возможность решения всех вопросов, возникающих в процессе создания и функционирования систем ЗИ;*
- *система решения проблем организационного обеспечения ЗИ, создающая условия формирования систем ЗИ;*
- *финансовое и материально-техническое обеспечение ЗИ.*

ЮУрГУ

Организационно-правовой (стратегический) уровень защиты информации

Конкретизация стратегических целей защиты информации может состоять в том, чтобы были четко сформулированы цели:

- обеспечения информационной безопасности личности, общества и государства;
- надежного режимного информационного обеспечения разработки и реализации стратегических проблем управления государством;
- постановка преград на путях безвозмездного использования информационных ресурсов страны, растаскивания ее интеллектуального потенциала, объектов интеллектуальной собственности.

ЮУрГУ

Организационно-правовой (стратегический) уровень защиты информации

Содержание проблемы создания правовой базы для формирования на ее основе систем защиты информации рассмотрено нами выше, поэтому лишь кратко напомним отдельные положения. Правовая база должна позволить решать задачи защиты прав собственника на информацию и на ее защиту, установление ответственности за покушение на защищаемую информацию и на порядок ее защиты, регламентация порядка, разделение права собственности на информацию на предприятиях, имеющих различные формы собственности, особенно при выполнении предприятием государственных заказов на производство секретной продукции, и др.

ЮУрГУ

Организационно-правовой (стратегический) уровень защиты информации

Организационное обеспечение защиты информации на этом уровне может создавать условия для построения систем защиты информации разработкой типовых правил, которые можно было бы использовать в качестве основы при разработке инструкций по защите государственной и коммерческой тайны; созданием в системе государственного аппарата структур, которые проводили бы единую политику в области засекречивания-рассекречивания информации, осуществляли контрольные и экспертные функции, осуществляли подготовку специалистов в области защиты информации, и т.д.

ЮУрГУ

Организационно-правовой (стратегический) уровень защиты информации

Финансовое и материально-техническое обеспечение защиты информации должно определять источники финансирования деятельности по защите государственной тайны, организовать производство технических средств защиты информации, пригодных к применению на предприятиях различных организационно-правовых форм и форм собственности.

ЮУрГУ

Тактический уровень защиты информации

Тактический уровень защиты информации

связан с реализацией концепции и стратегии защиты информации на конкретном предприятии или в фирме. На этом уровне создаются, как правило, комплексные системы защиты информации (КСЗИ) для непосредственного выполнения функций по обеспечению безопасности информации, защиты ее от соперника, от попыток получения несанкционированного доступа к носителям защищаемой информации.

ЮУрГУ

Тактический уровень защиты информации

Можно продолжить классификацию уровней защиты информации: отдельно для государственной и отдельно для коммерческой тайны. В основу этой классификации положены отношения субординации или подчиненности.

Для системы защиты государственной тайны отношения субординации будут трехуровневыми:

- *государственный уровень (высший);*
- *отраслевой (средний);*
- *предприятие, фирма, акционерное общество и др. (низший).*

Для системы защиты коммерческой тайны отношения субординации будут двухуровневыми:

- *государство;*
- *организация.*

ЮУрГУ

СПАСИБО ЗА ВНИМАНИЕ

ЮУрГУ