

Угрозы конфиденциальной информации организации

Защита информации и информационная безопасность:

- [1. Угрозы информации](#)
- [2. Угрозы конфиденциальной информации.](#)
- [3. Направления защиты информации](#)
-
- **Угрозы информации**
- Под **угрозами информации**, будем понимать потенциальные или реально возможные действия по отношению к информационной сфере, приводящие к несанкционированным изменениям свойств информации (конфиденциальность, доступность, достоверность, целостность).
- По конечному проявлению можно выделить следующие угрозы информации:
- [1. Ознакомление.](#)
- [2. Модификация.](#)
- [3. Уничтожение.](#)
- [4. Блокирование.](#)

Угрозы конфиденциальной информации организации

- Конкретные реализации угроз информации называются – **сценариями угроз информации.**
- Рассмотрим соответствие свойств и угроз информации рис.3.

Угрозы конфиденциальной информации организации

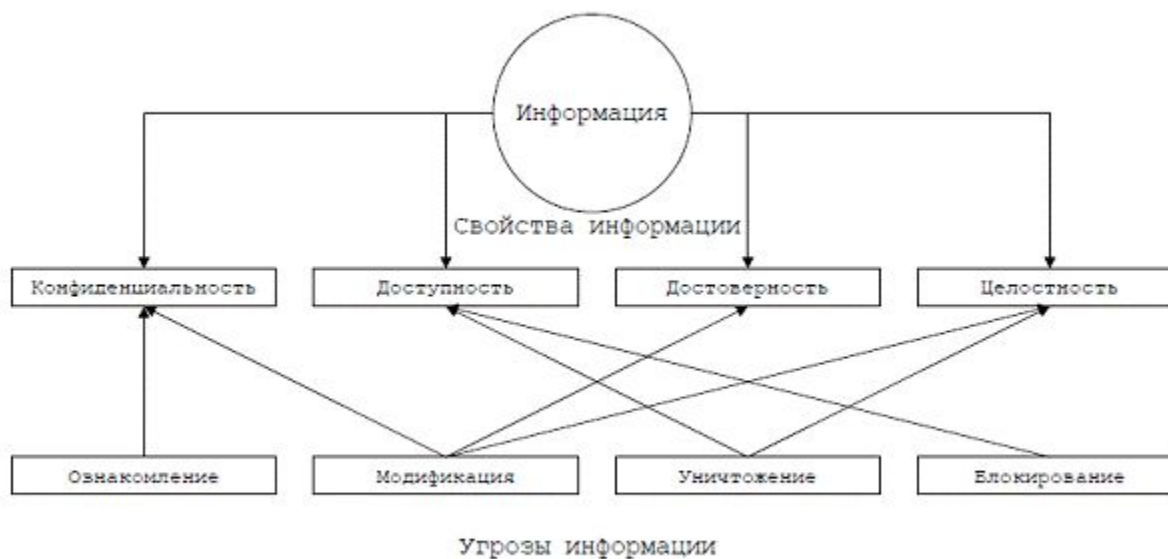


Рис. 3

Угрозы конфиденциальной информации организации

- 1. Ознакомление
- Ознакомление с конфиденциальной информацией может проходить различными путями и способами, при этом существенным, является отсутствие изменений самой информации.
- Нарушение конфиденциальности или секретности информации связано с ознакомлением с ней тех лиц, для которых она не предназначалась. Какая информация является конфиденциальной или секретной решает собственник или владелец этой информации. Они же определяют круг лиц, имеющих доступ к ней. Нарушение конфиденциальности информации может произойти путем **ознакомления** с ней лицами, не имеющими на то права и несанкционированной **модификации** грифа секретности (значимости).
- 2. Модификация
-
- - Модификация информации направлена на изменение таких свойств как **конфиденциальность, достоверность, целостность**, при этом подразумевается изменение состава и содержания сведений. Модификация информации не подразумевает ее полное уничтожение.

Угрозы конфиденциальной информации организации

- 3. Уничтожение
-
- - Уничтожение информации направлено, как правило, на целостность информации и приводит к ее полному разрушению. *Нарушение целостности информации* заключается в утере информации. При утере информации она пропадает безвозвратно и не может быть восстановлена никакими средствами. Утеря может произойти из-за разрушения или уничтожения носителя информации или его пропажи, из-за стирания информации на носителях с многократной записью, из-за пропадания питания в устройствах с энергозависимой памятью. При уничтожении информации нарушается также свойство **доступности** информации.

Угрозы конфиденциальной информации организации

- 4. Блокирование
-
- - Блокирование информации приводит к потере доступа к ней, т.е. к **недоступности** информации. Доступность информации заключается в том, что субъект, имеющей право на ее использование, должен иметь возможность на своевременное ее получение в удобном для него виде. При потере доступа к информации она по-прежнему существует, но воспользоваться ею нельзя. Т.е. субъект не может с ней ознакомиться, скопировать, передать другому субъекту или представить в виде удобном для использования.
- Потеря доступа может быть связана с отсутствием или неисправностью некоторого оборудования автоматизированных систем (АС), отсутствием какого-либо специалиста или недостаточной его квалификацией, отсутствием или неработоспособностью какого-то программного средства, использованием ресурсов АС для обработки посторонней информации, выходом из строя систем обеспечения АС и др. Так как информация не утеряна, то доступ к ней может быть получен после устранения причин потери доступа.

Угрозы конфиденциальной информации организации

- Перечисленные угрозы информации могут проявляться в виде комплекса последовательных и параллельных реализаций. Реализация угроз информации, связанная с нарушением свойств информации приводит к нарушению режима управления и в конечном итоге к моральным и (или) материальным потерям.
- Перечисленные выше угрозы информации могут быть классифицированы по следующим направлениям рис.4.:

Угрозы конфиденциальной информации организации



Рис. 4

Угрозы конфиденциальной информации организации

- Источники информационных угроз могут быть как **внутренними**, так и **внешними**. Чаще всего такое деление происходит по территориальному признаку и по признаку принадлежности к объекту информационной защиты рис. 5.

Угрозы конфиденциальной информации организации



Рис. 5

Угрозы конфиденциальной информации организации

- Соотношение внешних и внутренних угроз на усредненном уровне можно охарактеризовать так:
- - 82% угроз совершается собственными сотрудниками фирмы либо при их прямом или опосредованном участии;
- - 17% угроз совершается извне — внешние угрозы;
- - 1% угроз совершается случайными лицами.
- Информационные угрозы имеют векторный характер, т.е. всегда преследуют определенные **цели** и направлены на конкретные **объекты**.
- Источниками конфиденциальной информации являются люди, документы, публикации,
- технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства.
- К наиболее важным **объектам** обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:
- – **информационные ресурсы** федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных
- центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

Угрозы конфиденциальной информации организации

- – **информационно-вычислительные центры**, их информационное, техническое,
- программное и нормативное обеспечение;
- – **информационная инфраструктура** (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Угрозы конфиденциальной информации организации

- 2. Угрозы конфиденциальной информации.
-
- Для систем информационного общения существует одно общее положение, очень важное для понимания информационной безопасности в целом. Информация всегда адресна и всегда имеет владельца. Более того, адресность не произвольна, а определяется собственником информации. Если это право подчеркивается в сообщении (указывается гриф секретности), то информация становится **конфиденциальной**. Получая данную информацию, пользователь не может произвольно ею распоряжаться, она ему не принадлежит (если не было передачи права собственности). Право собственности определяется действующим в стране законодательством. В зависимости от вида собственности, конфиденциальная информация может быть отнесена к информации государственной, коммерческой, личной. Такое соотнесение делается, соподчинено, с нисходящей иерархией.
- Перечень сведений составляющих государственную тайну формирует государство в лице его институтов и учреждений. Эти сведения являются обязательной тайной для отдельных, нижестоящих по рангу, юридических и физических лиц страны.

Угрозы конфиденциальной информации организации

- Перечень сведений определяющих коммерческую тайну, формирует коммерческое предприятие. Оно же обеспечивает их сохранность и защиту. Личную тайну определяет физическое лицо. Естественно, что сохранность и защита этих сведений – его забота, хотя правовая защита за государством. Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкционированного доступа к охраняемым сведениям Рис.

Угрозы конфиденциальной информации организации

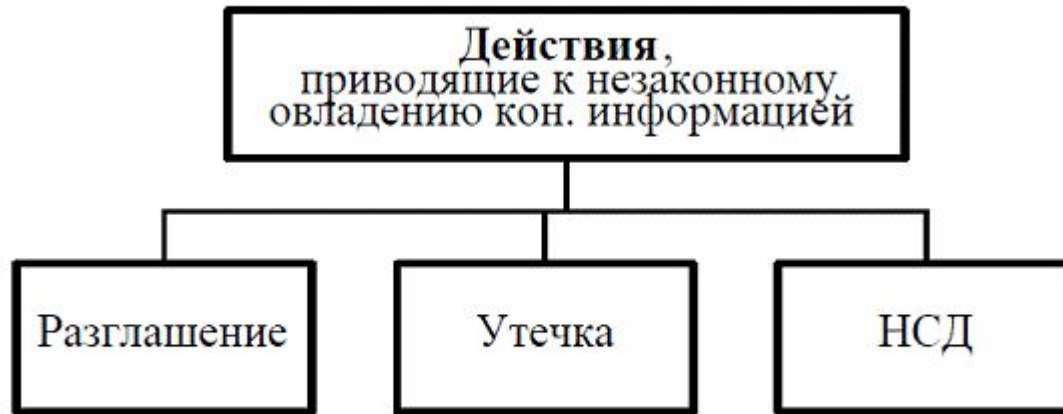


Рис. 7

Угрозы конфиденциальной информации организации

- **1. Разглашение — это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.**
- Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с конфиденциальной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации.
- К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами средствами передачи официальной информации (почта, телефон, телеграф и др.).
- Неформальные коммуникации включают личное общение, выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газеты, интервью, радио, телевидение и др.).
- Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Тут важно отметить, что субъектом в этом процессе выступает источник (владелец) охраняемых секретов.

Угрозы конфиденциальной информации организации

- Следует отметить информационные особенности этого действия. Информация содержательная, осмысленная, упорядоченная, аргументированная, объемная и доводится зачастую в реальном масштабе времени. Часто имеется возможность диалога. Информация ориентирована в определенной тематической области и документирована. Для получения интересующей злоумышленника информации последний затрачивает практически минимальные усилия и использует простые легальные технические средства.
- **2. Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она доверена по техническим каналам утечки информации.**
- Утечка информации осуществляется по различным техническим каналам. Известно, что информация вообще переносится или передается либо энергией, либо веществом. Это либо акустическая (звук), либо электромагнитное излучение, либо лист бумаги и др.
- С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации световые лучи, звуковые волны, электромагнитные волны, материалы и вещества.

Угрозы конфиденциальной информации организации

- Соответственно этому классифицируются и каналы утечки информации на визуальнооптические, акустические, электромагнитные и материально-вещественные. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям.
- Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.
-
-
- **3. Несанкционированный доступ - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.**
- Для реализации этих действий злоумышленнику приходится проникать на объект защиты, используя различные технические средства. С развитием компьютерных технологий стал доступен дистанционный несанкционированный доступ к охраняемой информации или, иначе говоря - компьютерный взлом.

Угрозы конфиденциальной информации организации

- **С учетом изложенного остается рассмотреть вопрос, какие условия способствуют неправомерному овладению конфиденциальной информацией:**
 - – Разглашение (излишняя болтливость сотрудников) - 32%
 - – Несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок - 24%
 - – Отсутствие на фирме надлежащего контроля и жестких условий обеспечения информационной безопасности - 14%;
 - – Традиционный обмен производственным опытом - 12%;
 - – Бесконтрольное использование информационных систем - 10%;
 - – Наличие предпосылок возникновения среди сотрудников конфликтов - 8%;

Угрозы конфиденциальной информации организации

- **3. Направления защиты информации**
- С учетом сложившейся практики обеспечения информационной безопасности выделяют
- следующие **направления защиты информации:**
- **1. Правовая защита** - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- **2. Организационная защита** - это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Угрозы конфиденциальной информации организации

- 3. **Инженерно-техническая защита** - это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.
- Для реализации защиты информации создается система безопасности.
- Под **Системой безопасности** будем понимать организационную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятий, государства от внутренних и внешних угроз.
- В рамках системы безопасности присутствует система защиты информации.
- **Система защиты информации (СЗИ)** – это организованная совокупность специальных органов средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.