**Лекция 3**

**Анализ существующих угроз в операционных системах**

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной (СМИ); однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Итак, реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой.

Классификация информационных угроз представлены на рис.4, 5.

**Информационные угрозы**

Для государства

Для компании

(юридического лица)

Для личности

(физического лица)

Разглашение

Утечка

Информационное

оружие, кибератаки

Несанкционированный

доступ

Фальшивые сайты

Распространение секретной служебной информации (инсайдовской информации)

Фишинг (раскрытие персональных данных: логина, пароля, номера банковской карты)

Онлайновое мошенничество (поддельные письма)

Киберслежка

Кибершпионаж

Информационные противодействия

Информационная война

## рис.4. Типы информационных угроз

**Человеческие факторы**

**Информационные угрозы по факторам возникновения**

**Неумышленные**

**(случайные) угрозы**

**Умышленные**

**(преднамеренные) угрозы**

**Естественные факторы**

Пассивные угрозы

Активные угрозы

Внешние угрозы

Внутренние угрозы

**Рис.5. Классификация информационныугроз по факторам возникновения**

Информационные угрозы могут быть обусловлены:

* естественными факторами (стихийные бедствия — пожар, наводнение, ураган, молния и другие причины);
* человеческими факторами. Последние, в свою очередь, подразделяются на:

- угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные пр01раммы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий но корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно- технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

*Пассивные угрозы,* как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

*Активные угрозы* имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на *внутренние,* возникающие внутри управляемой организации, и *внешние.*

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение *промышленный шпионаж* — это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности относят:

* раскрытие конфиденциальной информации;
* компрометация информации;
* несанкционированное использование информационных ресурсов;
* ошибочное использование ресурсов; несанкционированный обмен информацией;
* отказ от информации;
* отказ от обслуживания.

Средствами реализации угрозы *раскрытия конфиденциальной информации* могут быть несанкционированный доступ к базам данных, прослушивание каналов и т.п. В любом случае получение информации, являющейся достоянием некоторого лица (группы лиц), что приводит к уменьшению и даже потере ценности информации.

Реализация угроз является следствием одного из следующих действий и событий: разглашения конфиденциальной информации, утечки конфиденциальной информации и несанкционированный доступ к защищаемой информации (106). При разглашении или утечке происходит нарушение конфиденциальности информации с ограниченным доступом