Лекция №4

С.А. Краснов

Угрозы безопасности АС

# Угрозы безопасности АС

Лекция №4.

Тема №2: Методы и средства защиты информации от НСД.

Тема лекции: Угрозы безопасности АС.

Изучаемые вопросы:

1. Классификация угроз информационной безопасности (ИБ) автоматизированных систем (АС). Источники угроз НСД.

2. Каналы утечки информации. Классификация каналов утечки информации.

**В1.** Современная АС представляет собой сложный организационно-технический комплекс, состоящий из большого числа функциональных элементов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый из них может выйти из строя, в результате воздействия внешних или внутренних *дестабилизирующих факторов*. Дестабилизирующие факторы могут привести к возникновению *угроз безопасности АС* при наличии *уязвимых мест* в конструкции компонентов АС и в организации процессов обработки и защиты информации, неучтенных при разработке системы, а также в результате *случайных событий*, таких как стихийные бедствия, электромагнитные бури и т. п.

**Дестабилизирующими факторами** называют явления или события, которые могут появляться на каком-либо этапе жизнедеятельности АС и следствием которых могут быть несанкционированные воздействия на ресурсы системы.

**Безопасностью АС** - потенциальная способность АС выполнять заданные функции при воздействии на нее случайных или умышленных угроз.

**Воздействия на информацию в АС** могут быть (рисунок 1) *умышленными (преднамеренными)*, (например: уничтожение или считывание информации из чужих файлов; хищение носителей информации; копирование или изменение чужих программ, повреждение технических или программных средств АС и т. п.) или *случайными (непреднамеренными)*, (например: уничтожение аппаратуры или дискет с информацией пожаром, наводнением или другим стихийным бедствием; искажение данных в результате сбоев в работе аппаратуры или при передаче по каналам связи; случайное уничтожение файлов оператором, утрата носителей информации, случайная ошибка в программе и т. п.).

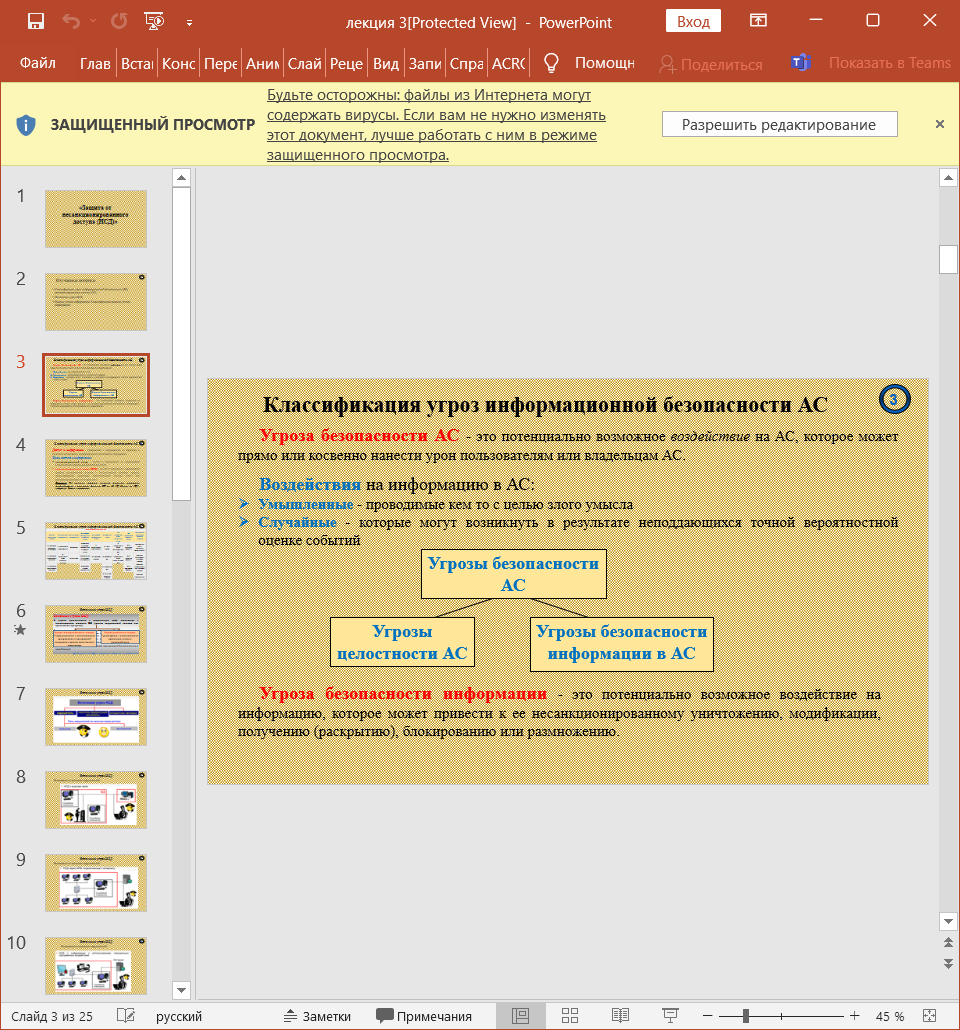


Рисунок 1

Угрозы безопасности АС разделяют на угрозы **целостности АС** и угрозы **безопасности информации в АС**. Примерами угроз целостности АС могут быть угрозы стихийных бедствий, пожаров, террористических актов, действий злоумышленника по уничтожению компонентов АС или постановке помех в каналах связи, угрозы саботажа персонала и т. п. Реализация этих угроз может привести к частичной или полной функциональной неработоспособности АС.

*Угрозы безопасности АС* могут быть причиной возникновения *угроз безопасности информации* в системе.

**Несанкционированное уничтожение информации** - это незаконное разрушение семантических (смысловых) связей между информационными элементами. Оно может стать результатом *физического разрушения* носителя информации (т. е. результатом нарушения целостности АС) или результатом *несанкционированных доступа к информации*.

**Несанкционированная модификация информации** - это незаконное умышленное изменение содержания информационного объекта (смысла информации).

**Несанкционированное получение (раскрытие) информации** - это получение доступа к смыслу информации, субъектами, не имеющими на это права.

Несанкционированные модификация или получение информации могут произойти только при наличии несанкционированного доступа к информации.

**Несанкционированное блокирование информации** - это нарушение функциональных возможностей АС по обработке информации, с использованием стандартных средств системы. Блокирование информации (отказ служб) не позволяет пользователям своевременно получать и обрабатывать информацию.

**Несанкционированное размножение информации** - это незаконное размножение информации без раскрытия ее содержания с целью дальнейшего использования. Несанкционированное размножение характерно для незаконного распространения программных продуктов с целью продажи или использования.

**Безопасность АС достигается** принятием мер по обеспечению конфиденциальности и целостности обрабатываемой ею информации, а также доступности и целостности компонентов и ресурсов системы.

Под **доступом к информации** понимается. Различают следующие **виды доступа** к информации.

**Доступ к информации** - ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации

**Виды доступа к информации**:

* **санкционированный доступ** – доступ к информации, не нарушающий установленные правила разграничения доступа;
* **несанкционированный доступ (НСД)** – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС).

*Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС. //РД «Защита от НСД к информации. Термины и определения»*

НСД является наиболее распространенным видом компьютерных нарушений, поэтому в дальнейшем мы будем рассматривать вопросы защиты информации от угроз безопасности информации, которые могут реализоваться при осуществлении НСД.

Надежная защита АС возможна только при полном учете всех потенциальных угроз безопасности АС.

Примерная *классификация угроз безопасности АС* по различным признакам представлена на (рисунок 2).

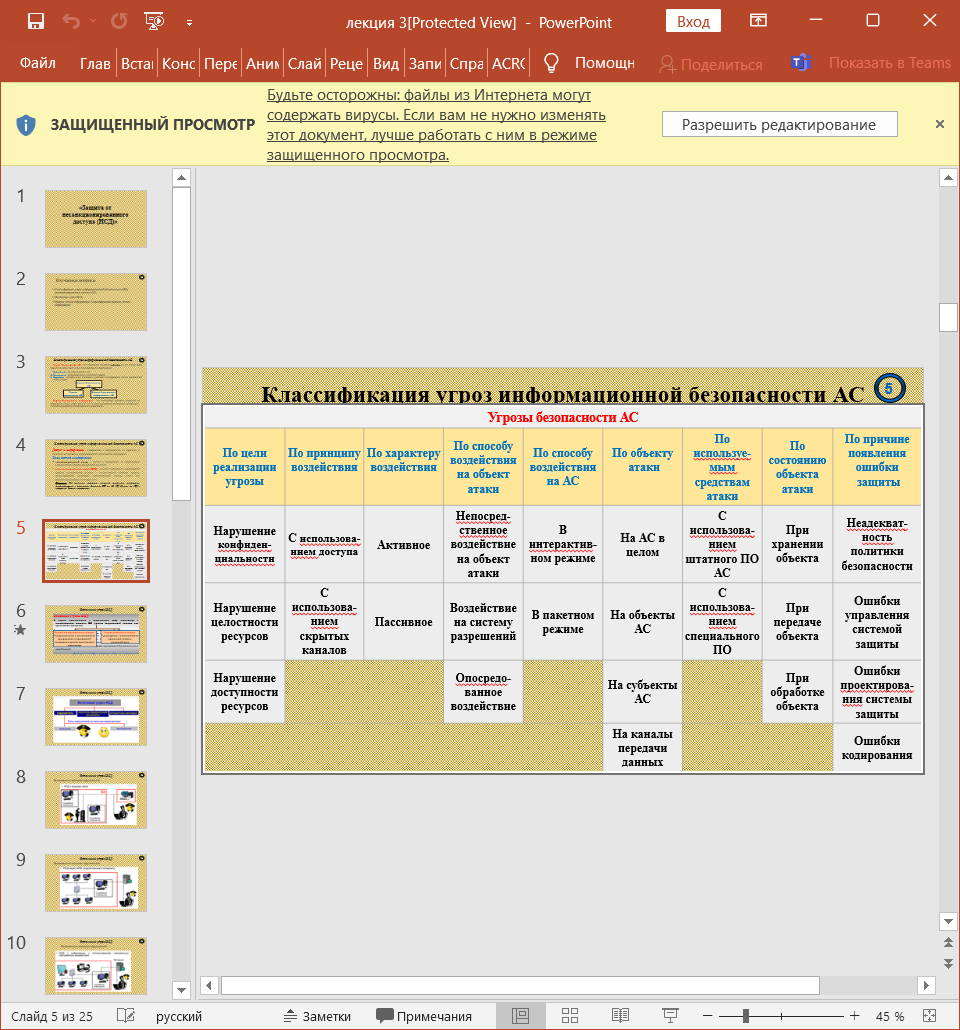


Рисунок 2

Эта классификация охватывает только *умышленные* *угрозы* безопасности АС, реализация которых может привести к нарушению безопасности информации, и как следствие, к НСД. Она не учитывает такие воздействия как стихийные бедствия, сбои и отказы оборудования и т. п.

**1.****По цели реализации угрозы**. Реализация угрозы безопасности АС может преследовать следующие цели:

1. нарушение *конфиденциальности* информации. Несанкционированное получение информации другими лицами может нанести значительный урон владельцу;
2. нарушение *целостности* информации. Ценная информация может быть утрачена или обесценена путем ее несанкционированного уничтожения или модификации;
3. нарушение (частичное или полное) *работоспособности* АС*.* Вывод из строя или некорректное изменение режимов работы компонентов АС, их модификация или подмена могут привести к получению *неверных результатов*, *отказу АС от потока информации* или *отказам при их обслуживании*. **Отказ от потока информации** означает непризнание одной из сторон факта передачи или приема сообщений.

**2. По принципу воздействия на АС:**

1. с использованием доступа субъекта системы к объекту;
2. с использованием скрытых каналов, т. е. путей передачи информации, позволяющих двум взаимодействующим процессам обмениваться информацией с нарушением принятой политики безопасности АС.

В первом случае осуществляется взаимодействие субъекта и объекта доступа, следовательно, возникает информационный поток и изменяется состояние АС. Во втором случае используются лишь побочные эффекты от взаимодействия двух субъектов АС, что не оказывает влияния на состояние системы.

**3.****По характеру воздействия на АС:**

1. **активное воздействие** это может быть доступ к определенным наборам данных, программам, вскрытие паролей и т. д.
2. **пассивное воздействие** осуществляется путем наблюдения каких-либо побочных эффектов (например, от работы программы) и их анализа. Пассивное воздействие всегда связано только с нарушением *конфиденциальности информации* в АС, так как при нем никаких действий с объектами и субъектами не производится.

**4. По способу воздействия на объект атаки** (при активном воздействии):

* непосредственное воздействие на объект атаки, например, непосредственный доступ к набору данных, программ, каналу связи и т. п.;
* воздействие на систему разрешений. При этом способе несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом;
* опосредованное воздействие (через других пользователей).

**5. По способу воздействия на АС:**

1. в интерактивном режиме, т. е. когда нарушитель непосредственно вводит команды, которые могут привести к НСД;
2. в пакетном режиме, т. е. когда действия по преодолению защиты производит программа без активного управляющего воздействия нарушителя.

**6. По объекту атаки**.

Воздействию могут подвергаться следующие компоненты АС:

* **АС в целом**, т. е. когда нарушитель пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Для этого может использоваться непосредственное проникновение на территорию и в помещения АС, могут перехватываться и подделываться пароли, осуществляться взлом или доступ к АС через сеть;
* **объекты и элементы защиты**, т. е. данные и программы в оперативной памяти или на внешних носителях, сами устройства системы (дисководы, сетевые устройства, терминалы, оперативная память, процессор), каналы передачи данных и т. д.;
* **субъекты АС,** т. е. *процессы* и *подпроцессы пользователей*. Целью таких атак является либо прямое воздействие на работу процесса - его приостановка, изменение *привилегий* или *характеристик*, либо обратное воздействие - использование нарушителем привилегий или характеристик другого процесса в своих целях;
* **каналы передачи данных**, т. е. на *пакеты* (*дейтаграммы*), передаваемые по каналу связи и на сами *каналы связи*. Воздействие на пакеты может рассматриваться как атака на объекты сети. Воздействие на каналы - род атак характерный для сети, к нему относятся: прослушивание канала и анализ трафика; подмена или модификация сообщений в каналах связи и на узлах ретрансляции; изменение топологии и характеристик сети, правил коммутации и адресации.

**7. По используемым средствам атаки:**

1. с использованием стандартного программного обеспечения;
2. с использованием специально разработанных программ.

**8. По состоянию объекта атаки.**

Объект атаки может находиться в одном из трех состояний:

1. **хранение**. При этом воздействие на объект атаки обычно осуществляется с использованием доступа;
2. **передача**. Воздействие предполагает либо доступ к фрагментам передаваемой информации (например, перехват пакетов в канале связи сети), либо прослушивание с использованием скрытых каналов;
3. **обработка**. При этом воздействию подвергается процесс пользователя.

**9. По причине появления используемой ошибки защиты**.

Ошибка может быть обусловлена одной из следующих причин:

* *неадекватность политики безопасности реальной АС*. Это означает, что разработанная для данной АС политика безопасности дает возможность выполнения несанкционированных действий;
* *ошибки административного управления СЗИ*, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной АС;
* ошибки в алгоритмах программ защиты, в связях между ними и т. п., которые возникают на *этапе проектирования программы* и с помощью которых можно использовать их способом, не описанным в документации к ней (в спецификациях);
* ошибки реализации алгоритмов программ защиты (ошибки кодирования), связей между ними и т. п., которые возникают на *этапе реализации или отладки* и могут также служить источником недокументированных свойств.

Изложенная классификация показывает сложность определения возможных угроз информации в АС и способов их реализации.

1. **Источники угроз НСД**

В соответствии с РД «Защита от НСД к информации. Термины и определения» основными угрозами являются (рисунок 3).

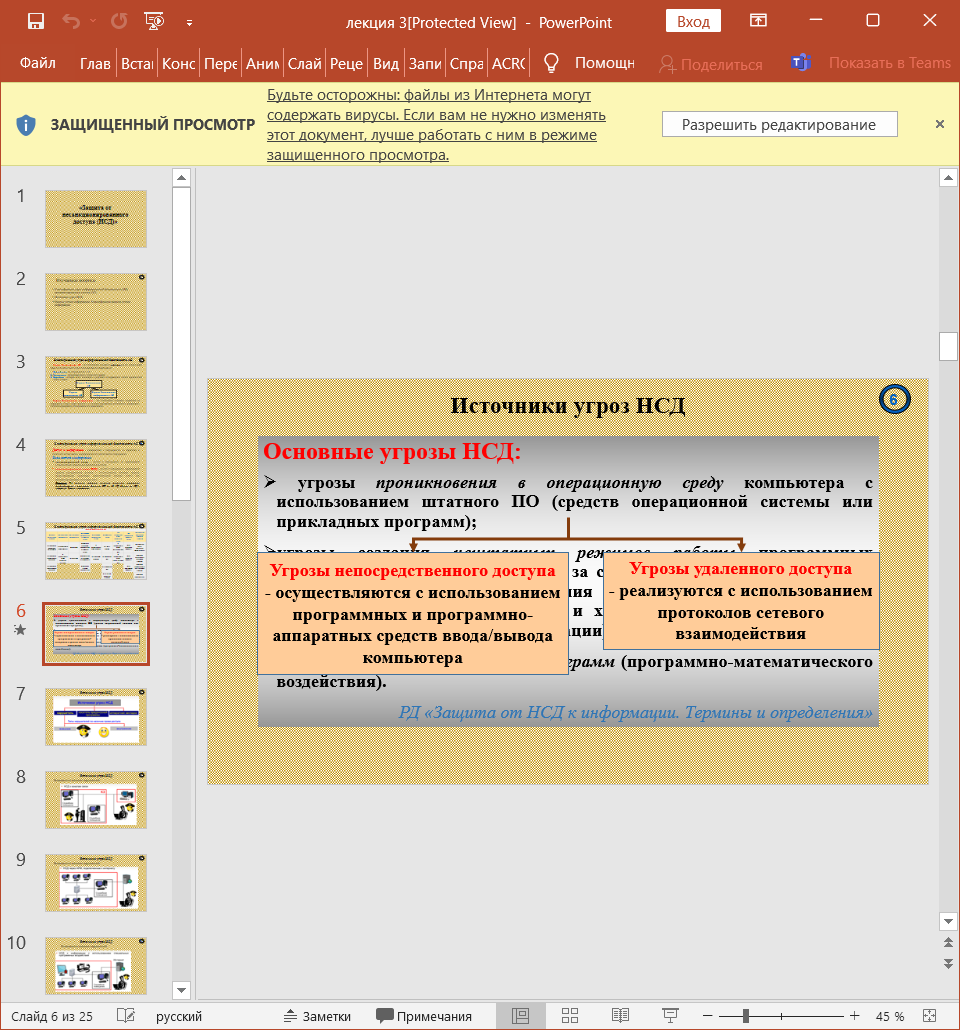


Рисунок 3

Источники угроз НСД представлены на (рисунок 4).

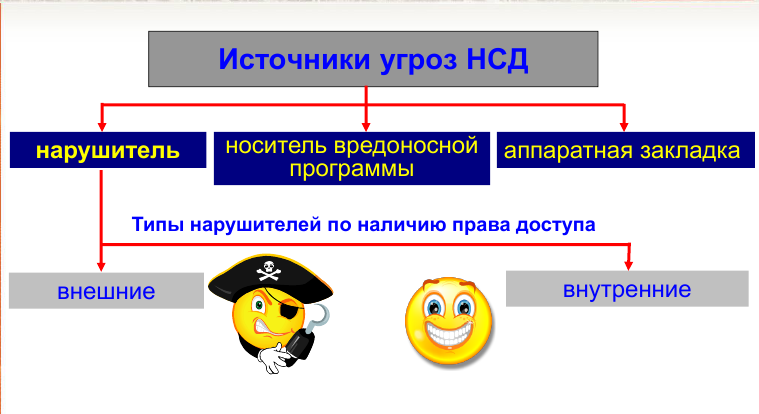


Рисунок 4

**Внешние нарушители:**

1. Разведслужбы государств
2. Криминальные структуры
3. Конкуренты
4. Недобросовестные партнеры
5. Внешние субъекты (физические лица).

Их возможности представлены(рисунки 5-9)



Рисунок 5



Рисунок 6

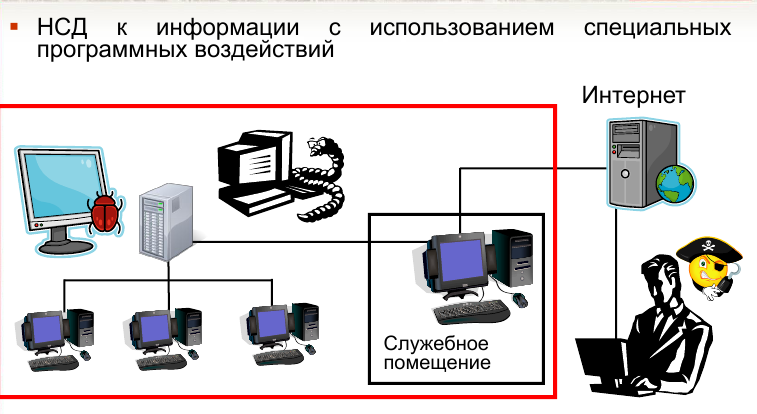


Рисунок 7

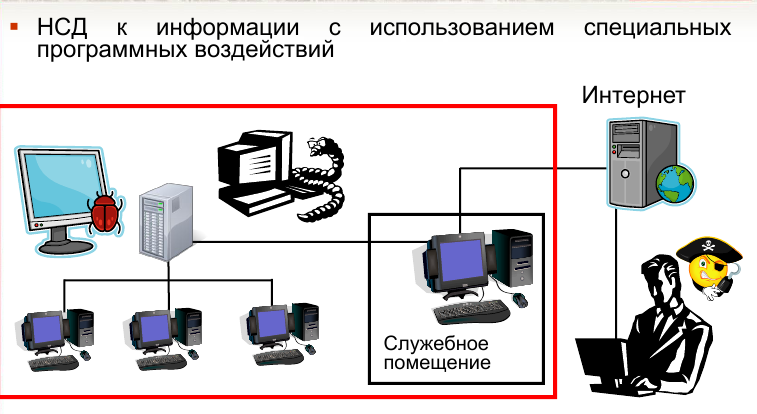


Рисунок 8



Рисунок 9

Внутренние нарушители: 8 категорий (рисунки 10-17).

1 категория внутренних нарушителей:

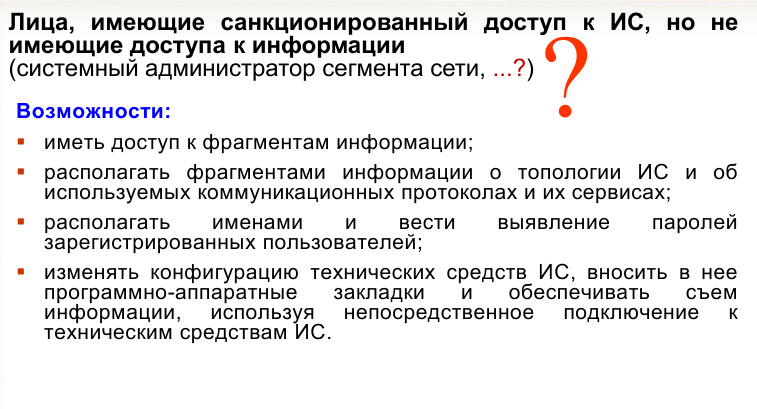


Рисунок 10

2 категория внутренних нарушителей:

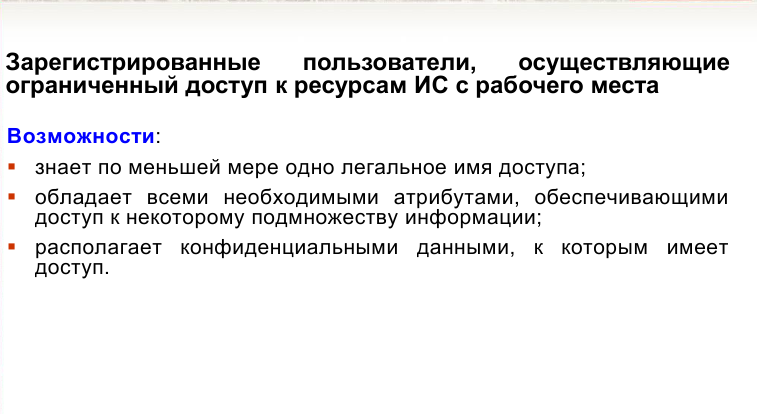


Рисунок 11

3 категория внутренних нарушителей:

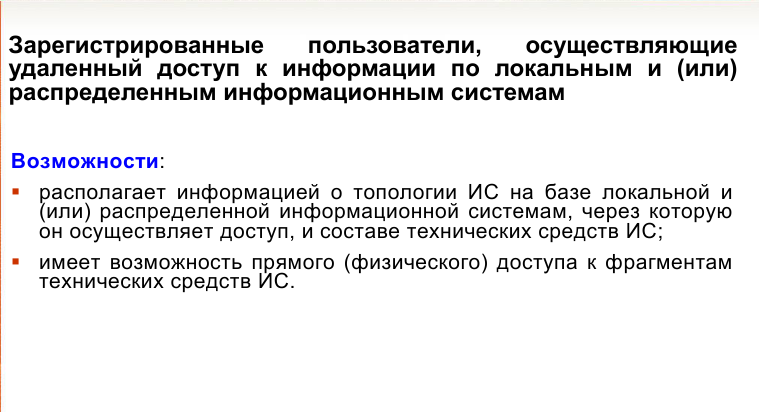


Рисунок 12

4 категория внутренних нарушителей:

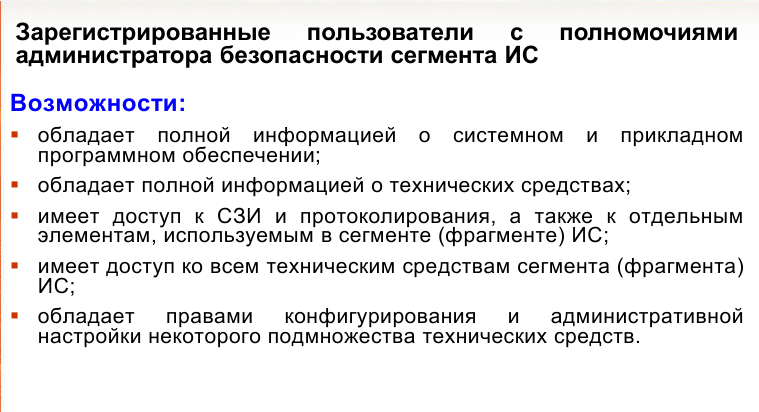


Рисунок 13

5 категория внутренних нарушителей:

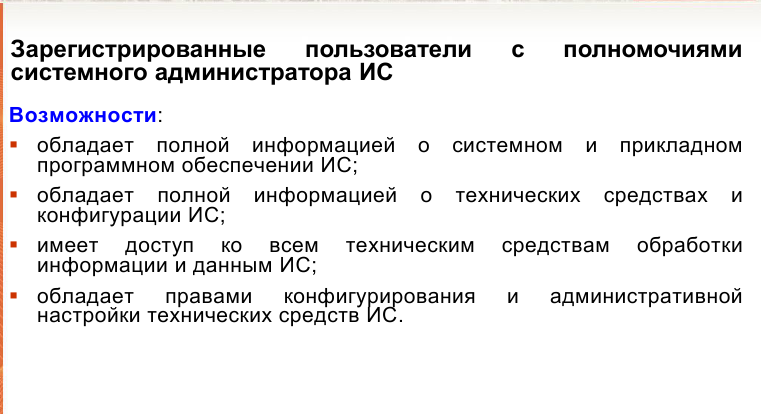


Рисунок 14

6 категория внутренних нарушителе:

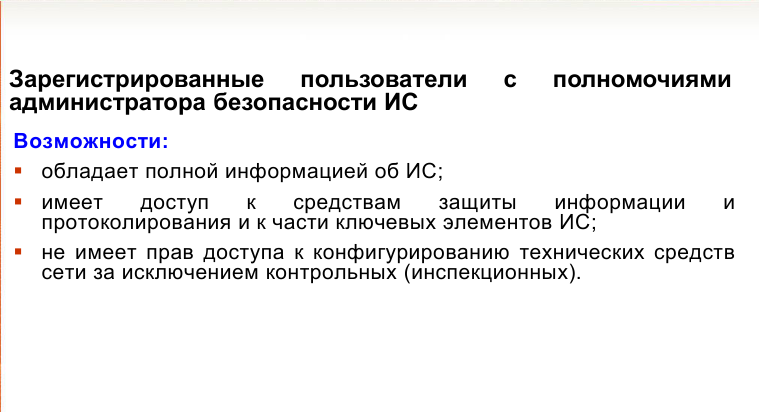


Рисунок 15

7 категория внутренних нарушителей:

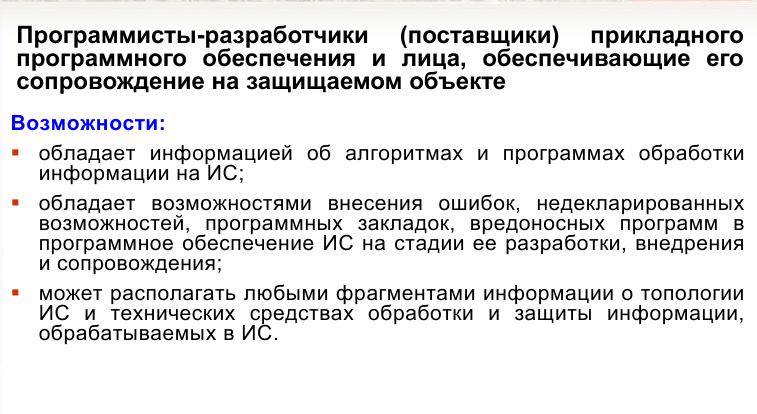


Рисунок 16

8 категория внутренних нарушителей:

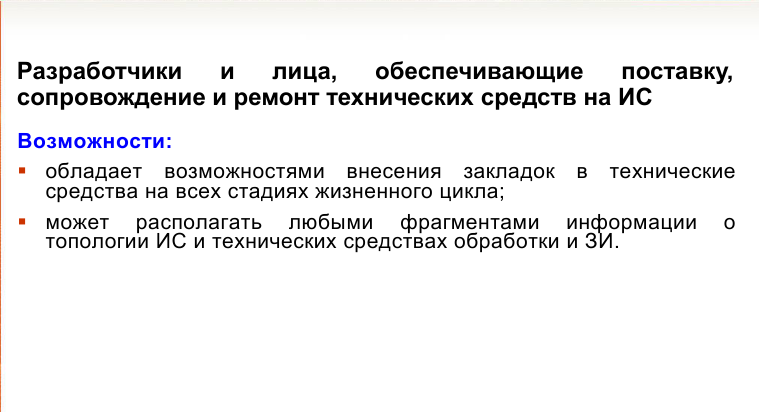


Рисунок 17

В общем случае возможные способы НСД к информации АС представлены на (рисунок 18).

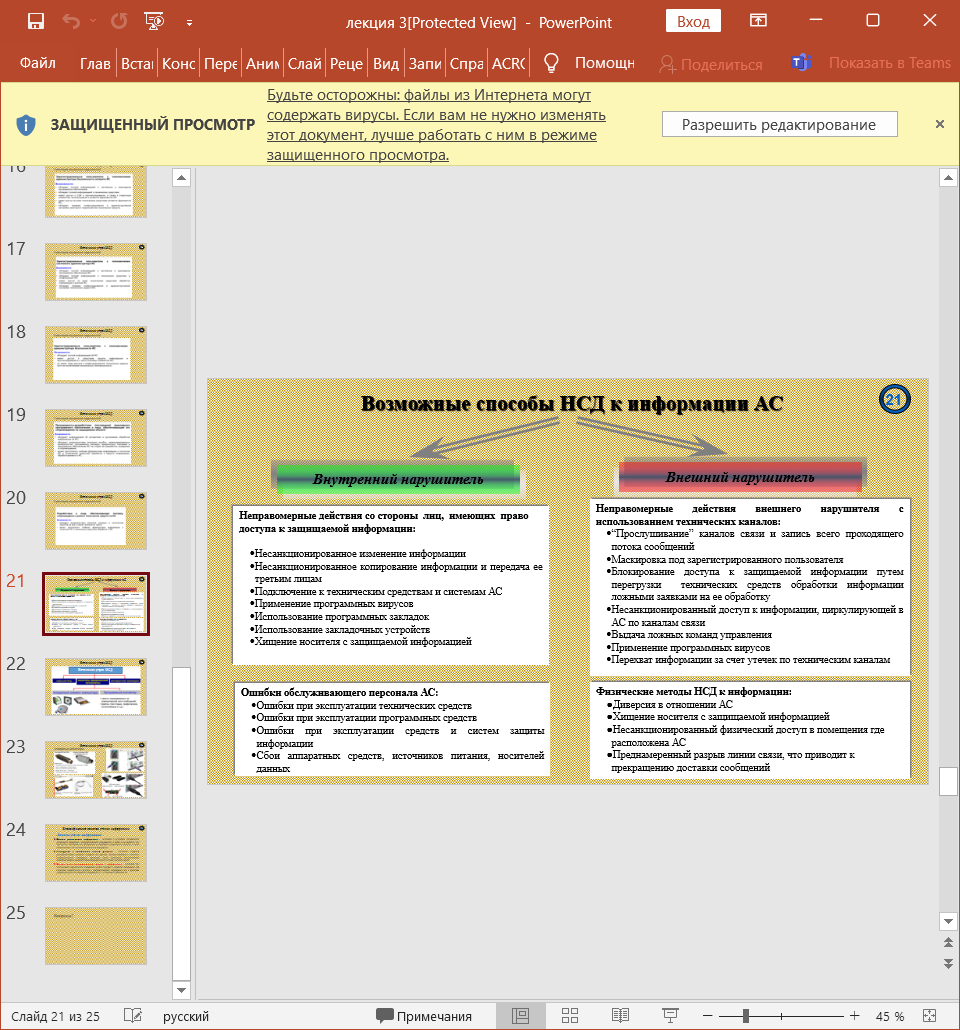


Рисунок 18

Носители вредоносной программы (рисунки 19-20)



Рисунок 19

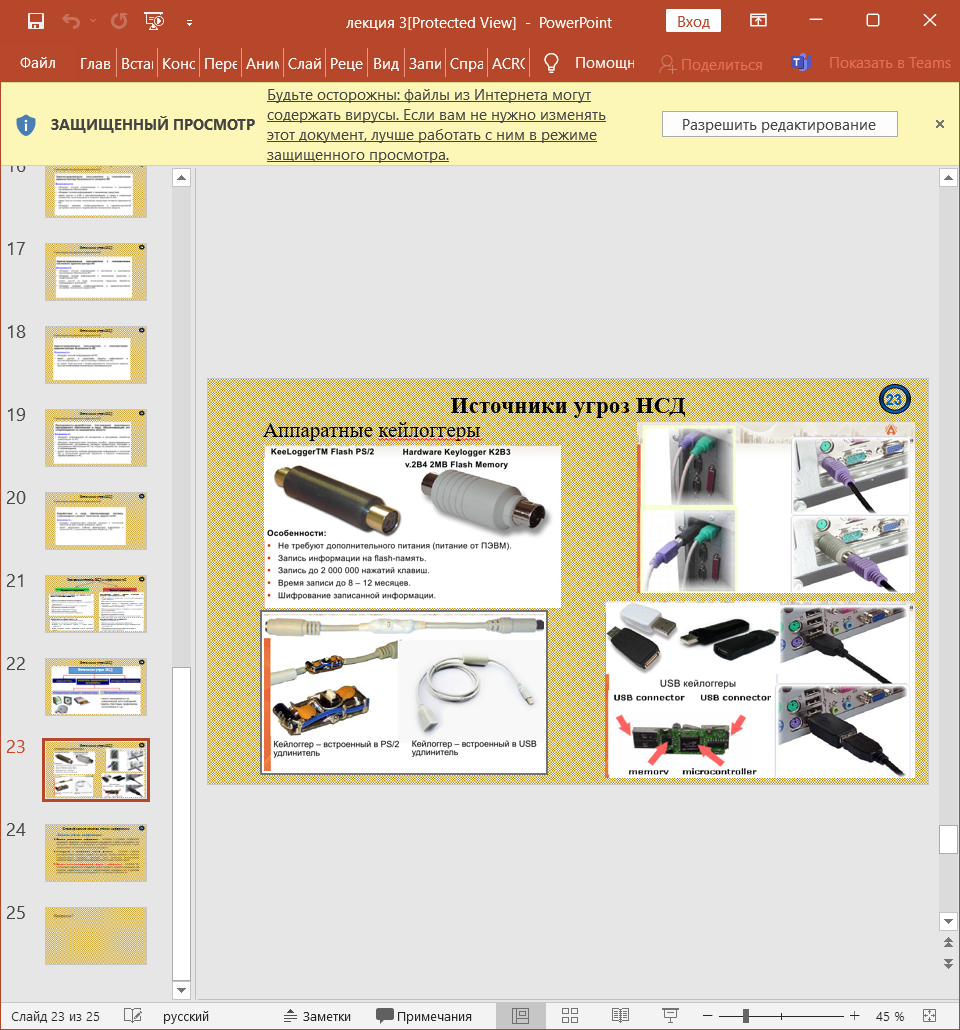


Рисунок 20

1. **Классификация каналов утечки информации**
2. **Каналы разглашения информации** - возникают в результате неправильной организации обращения с конфиденциальной информацией, а также из-за халатного или преступного отношения лиц, допущенных к информации ограниченного доступа, к своим обязанностям по обеспечению безопасности информации.
3. **Агентурные и технические каналы разведки** - специально создаются разведывательными органами государств или другими, заинтересованными в получении конфиденциальной информации субъектами, путем организации дополнительных нештатных каналов взаимодействия информационной системы с внешней средой.
4. **Каналы несанкционированного доступа к информации** - возникают при использовании нарушителем стандартных средств передачи и обработки информации для получения семантического доступа к конфиденциальной информации или к функциям управления процессом обработки информации, т. е. к объектам и субъектам АС.

*Каналы разглашения информации*

Например, разглашение информации ограниченного доступа может произойти при ее попадании в средства массовой информации, при ведении персоналом АС секретных переговоров вне помещений, специально установленных для этих целей, при отправке в ремонт магнитных носителей информации без специальной процедуры уничтожения остаточных данных, при передаче секретной информации в незашифрованном виде по открытым каналам связи, при записи секретного файла в незащищенную область памяти жесткого магнитного диска сетевого сервера и т.п. В результате возникновения таких ситуаций информация может стать доступна лицам, не имеющим на это права, в том числе и противнику.

*Агентурные и технические каналы разведки*

При этом могут использоваться различные технические средства ведения разведки, проникновение шпионов на территорию объектов АС или агентурная вербовка персонала АС.

***Каналы несанкционированного доступа к информации***

Выявления всех потенциально возможных каналов НСД к информации в АС сложная задача. С целью систематизации этого процесса необходимо рассмотреть все возможные информационные и функциональные связи между объектами и субъектами доступа на информационном уровне.

**Причинами** появления каналов НСД могут быть:

* умышленные или случайные действия пользователей АС, нарушающие правила разграничения доступа к информации;
* некорректные действия обслуживающего персонала АС, имеющего права на выполнение определенных функций в системе (программистов, системных программистов, администраторов, операторов и технического персонала);
* умышленные действия нарушителей, пытающихся обойти систему защиты информации АС с помощью вхождения в штатные каналы связи АС;
* неправильно выбранная и настроенная система защиты информации;
* ненадежность работы технического и программного обеспечения АС;
* ошибки при выборе, организации и проведении политики безопасности и так далее.

Вопросы?