Безопасность данных и информационная защита

Выполнил: Гусынин Андрей

Понятие информационной безопасности

Под информационной безопасностью понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Информационная безопасность организации — целенаправленная деятельность ее органов и должностных лиц с использованием разрешенных сил и средств по достижению состояния защищённости информационной среды организации, обеспечивающее её нормальное функционирование и динамичное развитие.

Информационная безопасность государства — состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере.

Понятие защиты информации

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Средства защиты информации, присутствующие в настоящее время условно можно разделить на несколько групп:

1. активные и пассивные технические средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при применении средств ее обработки;
2. программные и программно-технические средства, обеспечивающие разграничение доступа к информации на различных уровнях, идентификацию и аутентификацию пользователей;
3. программные и программно-технические средства, обеспечивающие защиту информации и подтверждение ее подлинности при передаче по каналам связи;
4. программно-аппаратные средства, обеспечивающие целостность программного продукта и защиту от несанкционированного его копирования;
5. программные средства, обеспечивающие защиту от воздействия программ-вирусов и других вредоносных программ;
6. физико-химические средства защиты, обеспечивающие подтверждение подлинности документов, безопасность их транспортировки и защиту от копирования.

Понятие защищенной системы

Информационной системой (или информационно-вычислительной системой) называют совокупность взаимосвязанных аппаратно-программных средств для автоматизации накопления и обработки информации. В информационную систему данные поступают от источника информации. Эти данные отправляются на хранение либо претерпевают в системе некоторую обработку и затем передаются потребителю..

Защищённая информационная система — это система, реализующая информационную модель предметной области, чаще всего — какой-либо области человеческой деятельности. Защищённая информационная система должна обеспечивать: безопасное получение (ввод или сбор), хранение, поиск, передачу и обработку (преобразование) информации

2.Понятие обеспечения ИБ, задачи обеспечения ИБ, субъект обеспечения ИБ, объект обеспечения ИБ.

Понятие «обеспечение безопасности» может быть раскрыто, с одной стороны, как средство предотвращения нанесения вреда чему-нибудь или кому-нибудь реализацией угроз, а с другой – как деятельность по предотвращению нанесения этого вреда.

Список основных целей и задач, решение которых информационная безопасность должна обеспечить (в скобках приведены английские эквиваленты):

— секретность (privacy, confidentiality, secrecy);
— целостность (data integrity);
— идентификация (identification);
— аутентификация (data origin, authentication);
— уполномочивание (authorization);
— контроль доступа (access control);
— право собственности (ownership);
— сертификация (certification); О подпись (signature);
— неотказуемость (non-repudiation);
— датирование (time stamping);
— расписка в получении (receipt); d аннулирование (annul);
— анонимность (anonymity);
— свидетельствование (witnessing);
— подтверждение (confirmation); О ратификация (validation).

Выделяются следующие виды субъектов в ИБ:

1. Граждане, в том числе иностранные, и лица без гражданства.

2. Организации:

• библиотеки;

• архивы;

• музеи;

• информационные центры и другие информационные структуры;

• информационные фонды;

• центры анализа информации;

• информационные агентства, другие органы массовой информации;

• другие организации – собственники и владельцы информационных ресурсов.

3. Органы государственной власти:

а) федеральные органы государственной власти:

– Федеральное Собрание РФ;

– Совет Федерации Федерального Собрания РФ, Государственная Дума Федерального Собрания РФ;

– Президент РФ, Администрация Президента РФ;

– Конституционный Суд РФ;

– Верховный Суд РФ;

– Высший Арбитражный Суд РФ;

– Правительство РФ;

б) федеральные министерства, ведомства, комитеты; органы государственной власти субъектов РФ:

– органы представительной власти;

– органы исполнительной власти;

– органы судебной власти; органы местного самоуправления

Основными объектами обеспечения информационной безопасности РК в общегосударственных информационных и телекоммуникационных системах являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;
- помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

3. Актуальность вопросов ИБ и защиты информации (нужно ли защищать и зачем)

Давно известно, что информация может быть настоящим сокровищем. Именно поэтому часто много усилий затрачивается как на ее охрану, так и на ее добывание. Информацию нужно защищать в тех случаях, когда есть опасения, что информация станет доступной посторонним, которые могут обратить ее во вред законному пользователю.

Информация, которая нуждается в защите, возникает в самых разных жизненных ситуациях. В таких случаях говорят, что информация содержит тайну и является защищаемой, приватной, конфиденциальной, секретной. Для наиболее типичных ситуаций введены специальные понятия: государственная тайна, военная тайна, коммерческая тайна, юридическая тайна, врачебная тайна.

И так, первая и главная причина, на которую руководитель обращает внимание, — финансовый аспект. Но она далеко не единственная. Не менее критичны следующие последствия утечек:

- ухудшение имиджа компании;
- утрата технологических секретов;
- ослабление позиций в конкурентной борьбе;
- необходимость затрат на устранение последствий утечки;
- судебные иски, поданные клиентами против компании;
- санкции контролирующих органов;
- увольнение сотрудников;
- снижение числа новых и отток существующих клиентов.

Безусловно, никто не захочет продолжать сотрудничать с банком, если любой человек «с улицы» будет иметь доступ к персональной информации по всем счетам и переводам.

Из года в год средний ущерб от информационной «утечки» возрастает. Признанным экспертом в области отслеживания и анализа подобных инцидентов является Ponemon Institute. По данным этой организации, в 2010 году «стоимость» одной утечки приблизилась к 3 млн фунтов стерлингов. Кстати, буквально два–три года назад она составляла 2 млн. Исходя из этого, руководитель должен принять одно из самых важных решений — о необходимости защиты данных. Кому-то этот постулат может показаться настолько очевидным, что и обсуждать здесь вроде бы нечего. Тем не менее, практика показывает, что хорошего специалиста по информационной безопасности, как и хорошего системного администратора, руководство со временем начинает воспринимать как «дармоеда»: мол, сидит, ничего не делает, да еще и прибавку к зарплате требует. Но не следует недооценивать роль IT-специалиста в компании. Ведь именно он является тем «инструментом», с помощью которого минимизируются все риски и издержки, грозящие предприятию в случае утечки конфиденциальных сведений. Итак, будем считать, что оснований для защиты информации у нас достаточно и с вопросом «Зачем?» мы разобрались.

4.Понятие нарушителей (злоумышленников) ИБ, группы внешних и внутренних нарушителей, классификация по уровню возможностей нарушителей.

Под нарушителем в общем виде можно рассматривать лицо или группу лиц, которые в результате предумышленных или непредумышленных действий обеспечивает реализацию угроз информационной безопасности.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону нарушители могут подразделяться на два типа:

- нарушители, не имеющие права доступа в контролируемую зону территории (помещения) — внешние нарушители;
- нарушители, имеющие право доступа в контролируемую зону территории (помещения) — внутренние нарушители.

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства

При рассмотрении нарушителей необходимо разделить их на группы по возможностям воздействия на его компоненты. Групп нарушителей две:

- внешние нарушители (группа О) – физические лица, не обладающие правами доступа внутрь контролируемой зоны и соответственно не имеющие возможности прямого воздействия на компоненты информации;
- внутренние нарушители (группа И) – физические лица, обладающие правами доступа внутрь контролируемой зоны и соответственно имеющие доступ к техническим средствам информации.

Классификация нарушителей по уровню возможностей

1) применяет методы социальной инженерии: манипуляцию, нейролингвистическое программирование, подкуп, шантаж;

2) применяет пассивные средства: технические средства перехвата без модификации компонентов системы, например закладки между разъемом для клавиатуры и проводом от нее;

3) использует только штатные средства и недостатки системы защиты информации (СЗИ) для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные носители информации, которые могут быть скрытно пронесены через посты безопасности;

4) применяет методы и средства активного воздействия: модификация и подключение дополнительных технических устройств, подключение к каннам связи, внедрение программных и аппаратных закладок, использование специальных инструментов и технологических программ.

5.Угрозы ИБ: понятие угрозы, классические угрозы, особенности и примеры их реализации.

Угрозы информационной безопасности

Под угрозой в национальном стандарте понимается потенциальная причина инцидента, способного нанести ущерб системе или организации.

Угроза безопасности информации — потенциально возможное воздействие на информацию, которое прямо или косвенно может нанести урон пользователям или владельцам информации (компьютерной системы).

Виды угроз информационной безопасности РК

По своей общей направленности угрозы информационной безопасности РК подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению Казахстана;
- угрозы информационному обеспечению государственной политики РК;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории РК.

В безопасности информации различают три классические угрозы безопасности информации.

- Угроза конфиденциальности состоит в нарушении установленных ограничений на доступ к информации.
- Угроза целостности — несанкционированное изменение информации.
- Угроза доступности информации осуществляется, когда несанкционированно блокируется доступ к информации (блокирование может быть постоянным или на некоторое время, достаточное, чтобы информация стала бесполезной).

Кроме перечисленных угроз выделяют еще одну угрозу, реализация которой, как правило, предшествует реализации любой из классических угроз.— преодоление защиты компьютерной системы, выявление параметров, функций и свойств ее системы безопасности.

Кроме этого классификацию угроз можно проводить по ряду других базовых признаков, например:

- по природе возникновения;
- по степени преднамеренности проявления;
- по непосредственному источнику угроз;
- по положению источника угроз;
- по степени зависимости от активности АС;
- степени воздействия на АС и т.п.

ОСНОВНЫЕ МЕТОДЫ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К основным направлениям реализации злоумышленником информационных угроз относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства системы программных или технических механизмов, нарушающих её предполагаемую структуру и функции.

При рассмотрении вопросов защиты автоматизированных систем целесообразно использовать четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой системе информации, которая поможет систематизировать как возможные угрозы, так и меры по их нейтрализации и парированию, т.е. поможет систематизировать и обобщить весь спектр методов обеспечения защиты, относящихся к информационной безопасности. Эти уровни следующие:

- уровень носителей информации;
- уровень средств взаимодействия с носителем;
- уровень представления информации;
- уровень содержания информации.

Данные уровни были введены исходя из того, что:

1. Информация для удобства манипулирования чаще всего фиксируется на некотором материальном носителе, которым может быть бумага, дискета или иной носитель;

2. Если способ представления информации таков, что она не может быть непосредственно воспринята человеком, возникает необходимость в преобразователях информации в доступный для человека способ представления.

3. Как уже было отмечено, информация может быть охарактеризована способом своего представления или тем, что еще называется языком в обиходном смысле.

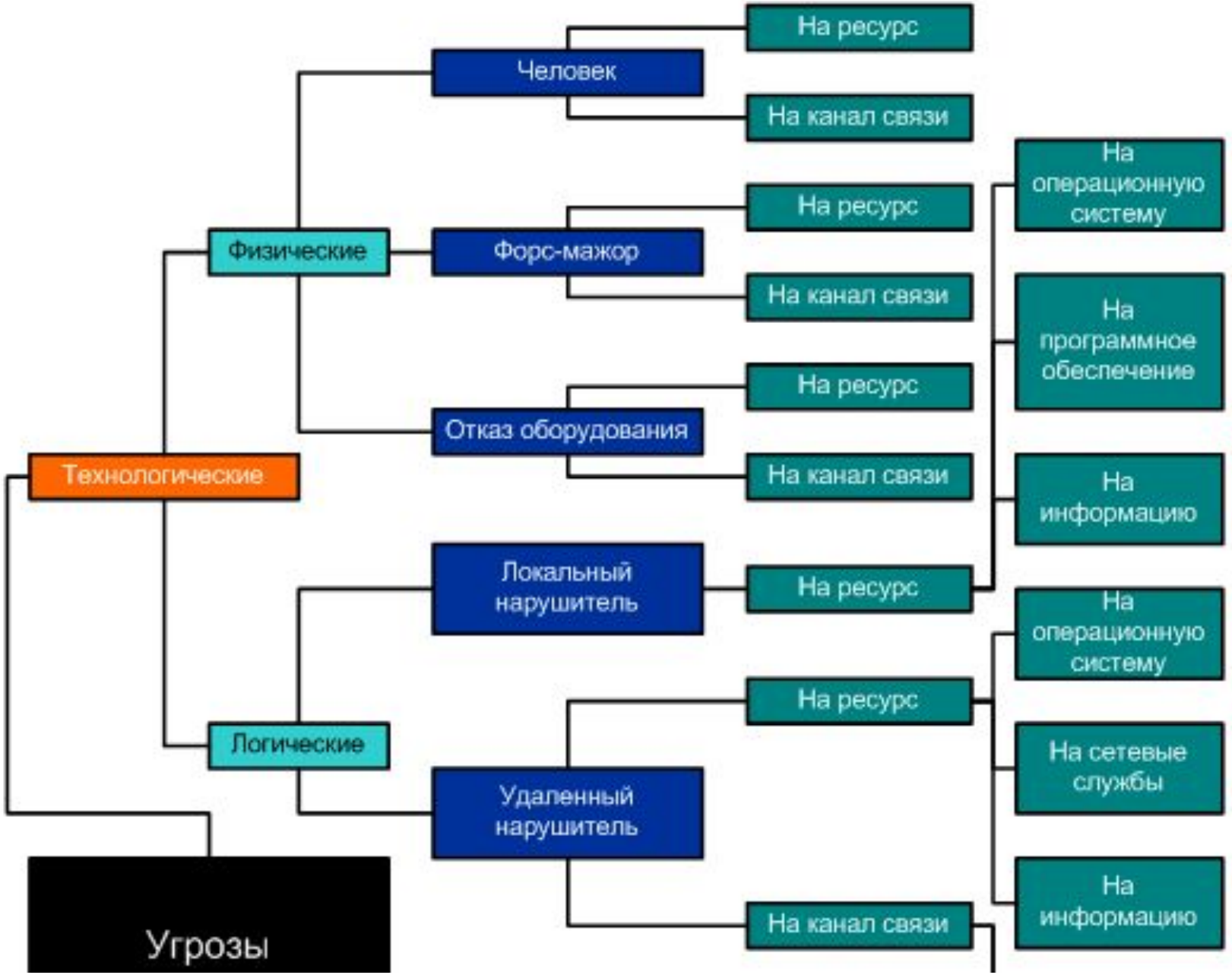
4. Человеку должен быть доступен смысл представленной информации, ее семантика.

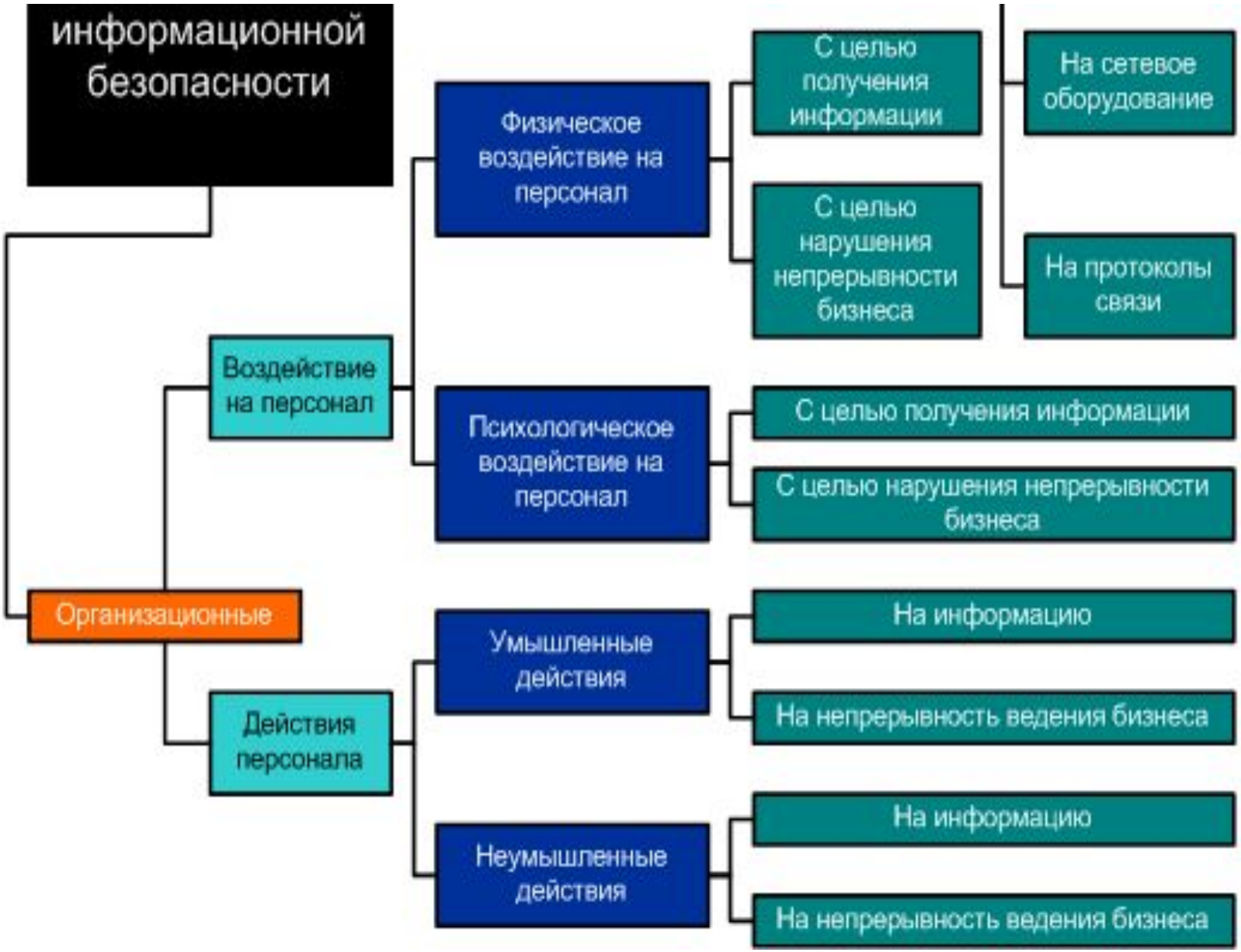
Таблица Распределение методов реализации угроз информационной безопасности по уровням

Уровень доступа к информации	Основные методы реализации угроз информационной безопасности			
	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза нарушения доступности
Носителей информации.	Определение типа и параметров носителей информации.	Хищение (копирование) носителей информации; перехват ПЭМИН.	Уничтожение машинных носителей информации.	Выведение из строя машинных носителей информации.
Средств взаимодействия с носителем.	Получение информации о программно-аппаратной среде; получение детальной информации о функциях, выполняемых системой; получение данных о применяемых системах защиты.	Несанкционированный доступ к ресурсам системы; совершение пользователем несанкционированных действий; несанкционированное копирование программного обеспечения; перехват данных, передаваемых по каналам связи.	Внесение пользователем несанкционированных изменений в программы и данные; установка и использование нештатного программного обеспечения; заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонент системы; обход механизмов защиты.
Представления информации.	Определение способа представления информации.	Визуальное наблюдение; раскрытие представления информации (дешифрование).	Внесение искажения в представление данных; уничтожение данных.	Искажение соответствия синтаксических и семантических конструкций языка.
Содержания информации.	Определение содержания данных на качественном уровне.	Раскрытие содержания информации.	Внедрение дезинформации.	Запрет на использование информации.

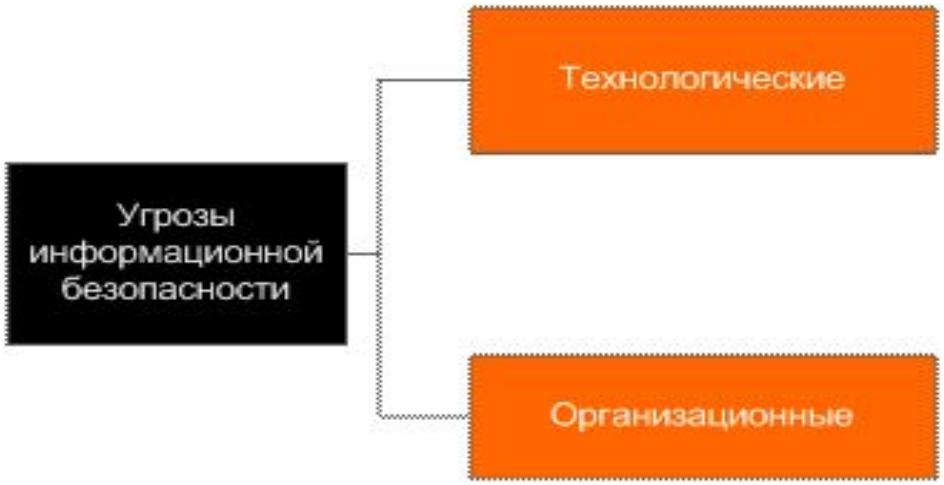
Вопрос 6, 7:

- Классификация видов угроз ИБ по ряду признаков

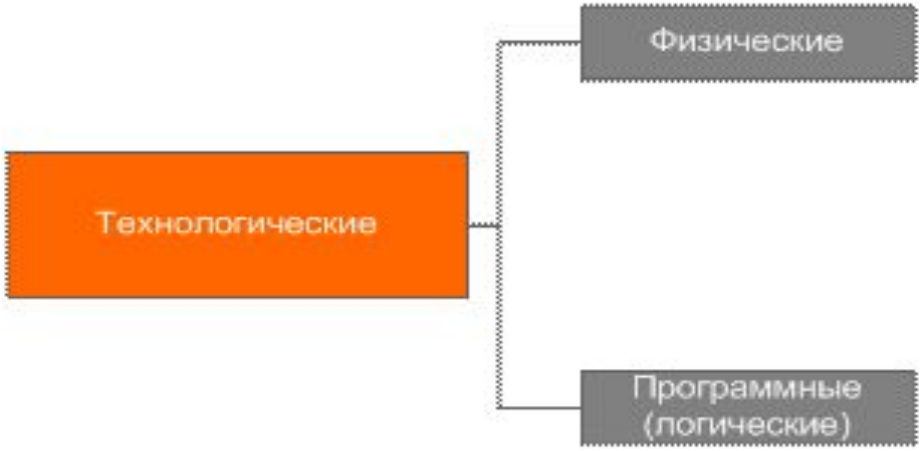

Угрозы
Технологические
Физические
Человек
На ресурс
На канал связи
Форс-мажор
На ресурс
На канал связи
Отказ оборудования
На ресурс
На канал связи
Логические
Локальный нарушитель
На ресурс
На операционную систему
На программное обеспечение
На информацию
Удаленный нарушитель
На ресурс
На операционную систему
На сетевые службы
На канал связи
На информацию


информационной безопасности
Организационные
Воздействие на персонал
Физическое воздействие на персонал
С целью получения информации
На сетевое оборудование
С целью нарушения непрерывности бизнеса
На протоколы связи
Психологическое воздействие на персонал
С целью получения информации
С целью нарушения непрерывности бизнеса
Действия персонала
Умышленные действия
На информацию
На непрерывность ведения бизнеса
Неумышленные действия
На информацию
На непрерывность ведения бизнеса

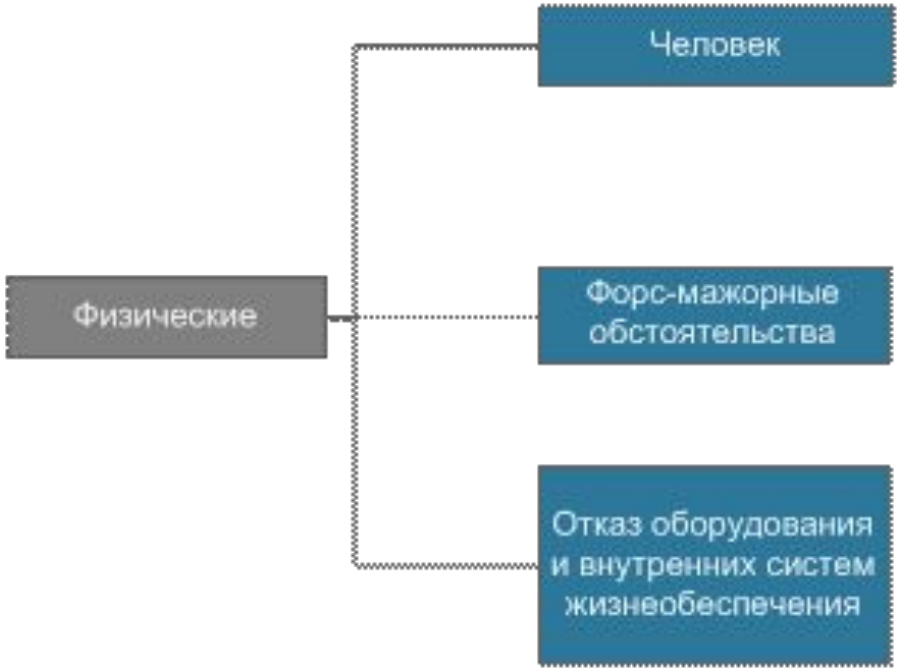
- По виду угроз информационной безопасности разделяют технологические и организационные угрозы.



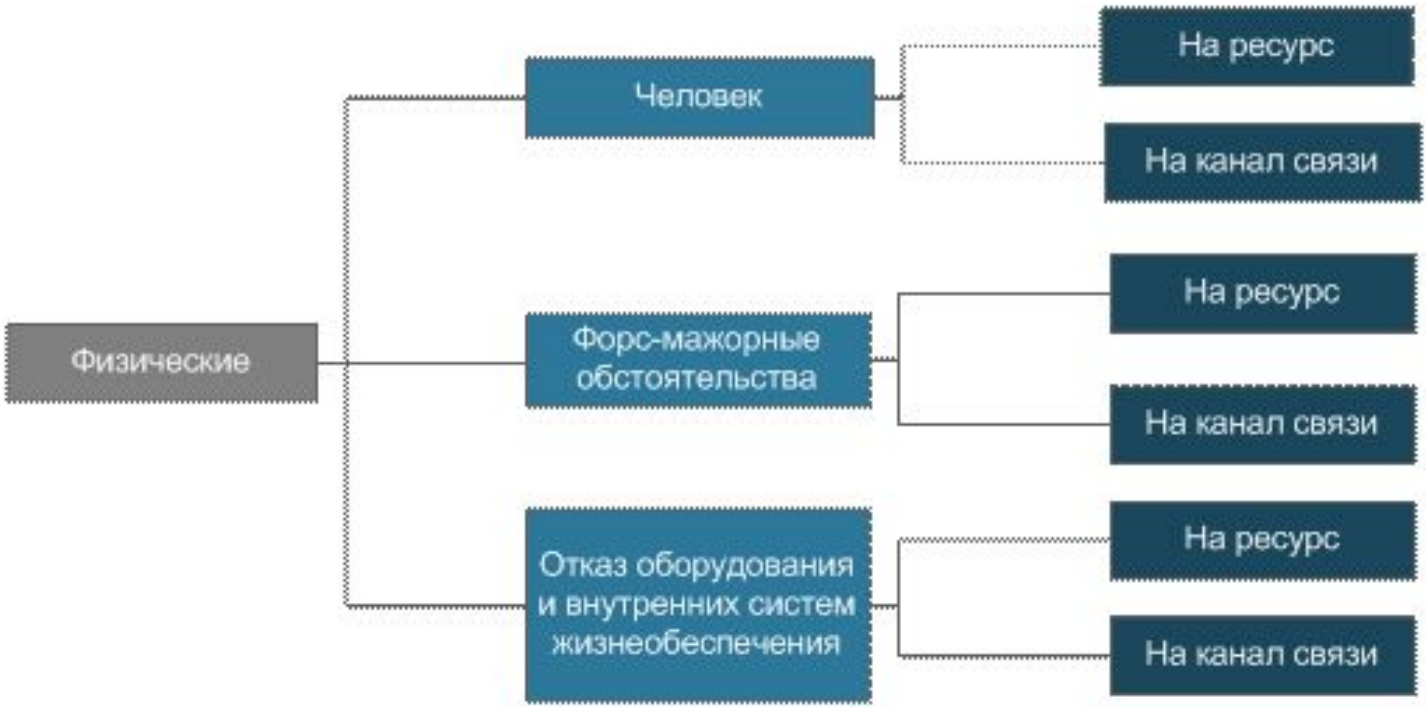
- Технологические угрозы по характеру воздействия разделяются на физические и программные (логические). Т.е. получаем такую начальную классификацию:



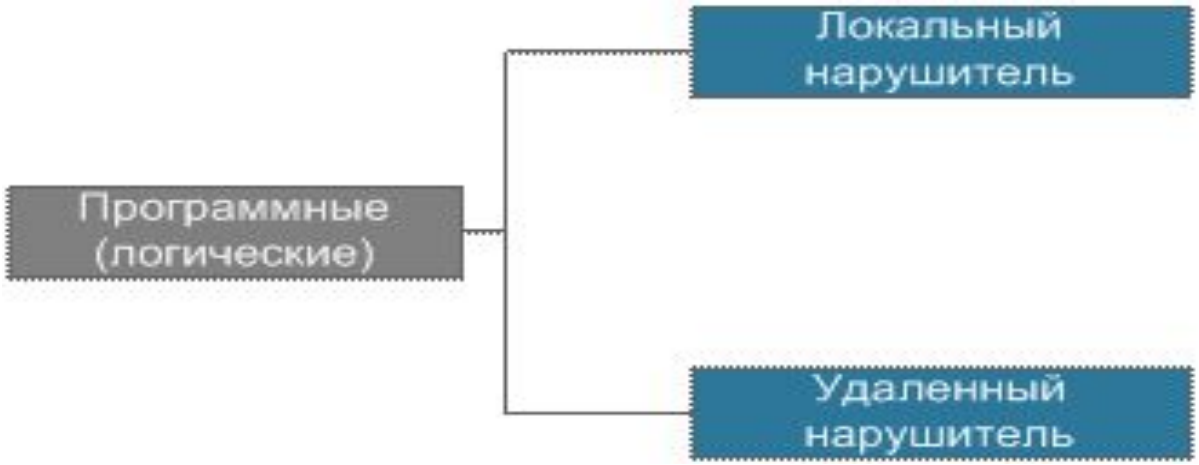
- Физические угрозы могут исходить от действий нарушителя (человека), форс-мажорных обстоятельств и отказа оборудования и внутренних систем жизнеобеспечения.



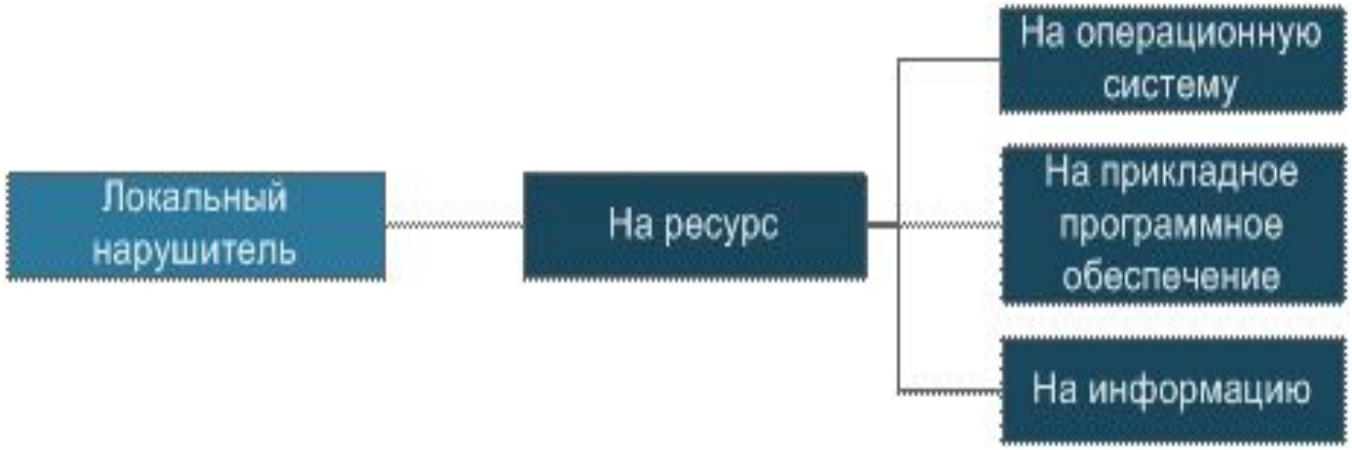
- Далее, положим, что нарушитель имеет физический доступ к помещению, в котором расположен ценный ресурс. Какие виды угроз информационной безопасности он может при этом осуществить? Чтобы реализовать угрозы при физическом доступе нарушитель может воздействовать либо непосредственно на ресурс, либо на канал связи. Таким образом, получим:



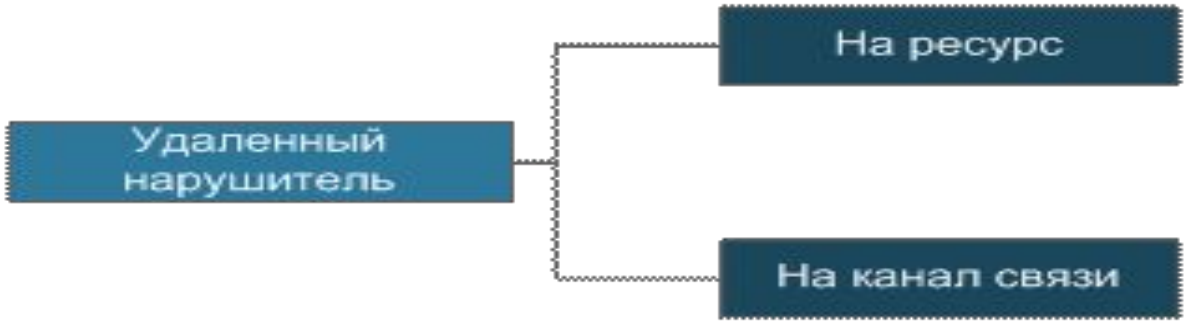
- Далее перейдем к рассмотрению программных угроз.
- Программные угрозы разделяются на угрозы, исходящие от локального нарушителя, и угрозы, исходящие от удаленного нарушителя.



- Рассмотрим программные локальные угрозы на ценный информационный ресурс. При локальном доступе на программном уровне нарушить может осуществить угрозу только на ресурс, при этом на ресурсе располагаются следующие компоненты: операционная система, прикладное программное обеспечение, а также сама ценная информация, хранящаяся и обрабатываемая на ресурсе. Нарушение функционирования, целостности или конфиденциальности любого из этих элементов может привести к потере ценной информации. Получим:

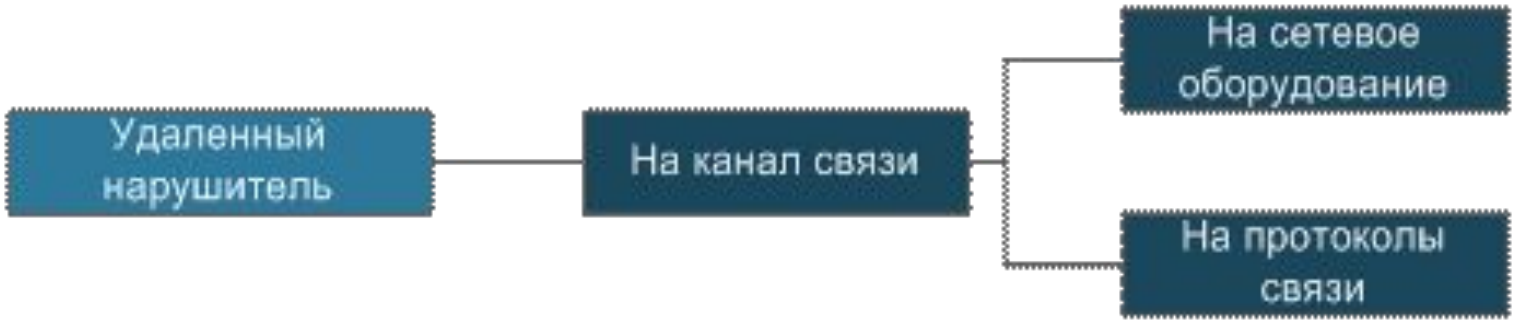


- Рассмотрим удаленные программные угрозы.
- При удаленном программном доступе нарушитель может воздействовать как на ресурс, содержащий ценную информацию, так и на каналы связи, связывающие ресурсы между собой.

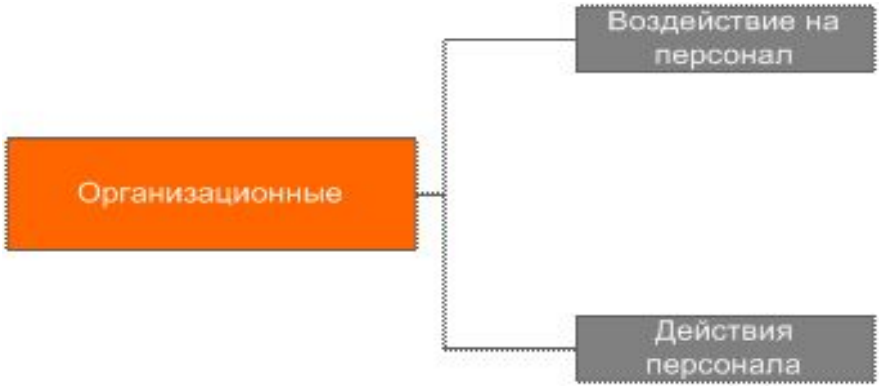


- При этом при удаленном доступе к ресурсу нарушить может воздействовать на следующие его компоненты: операционную систему, сетевые службы и ценную информацию, к которой может быть открыт удаленный

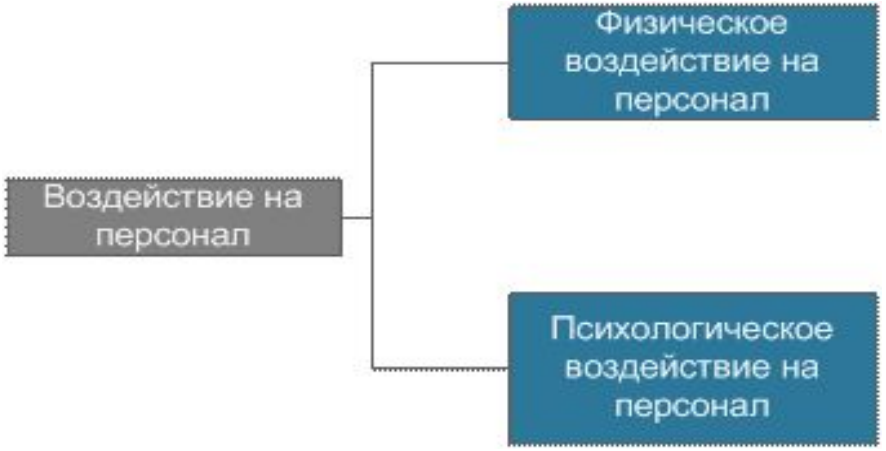
- При удаленном программном доступе к каналу связи для реализации угроз нарушитель может воздействовать непосредственно на сетевое оборудование или на протоколы передачи данных.



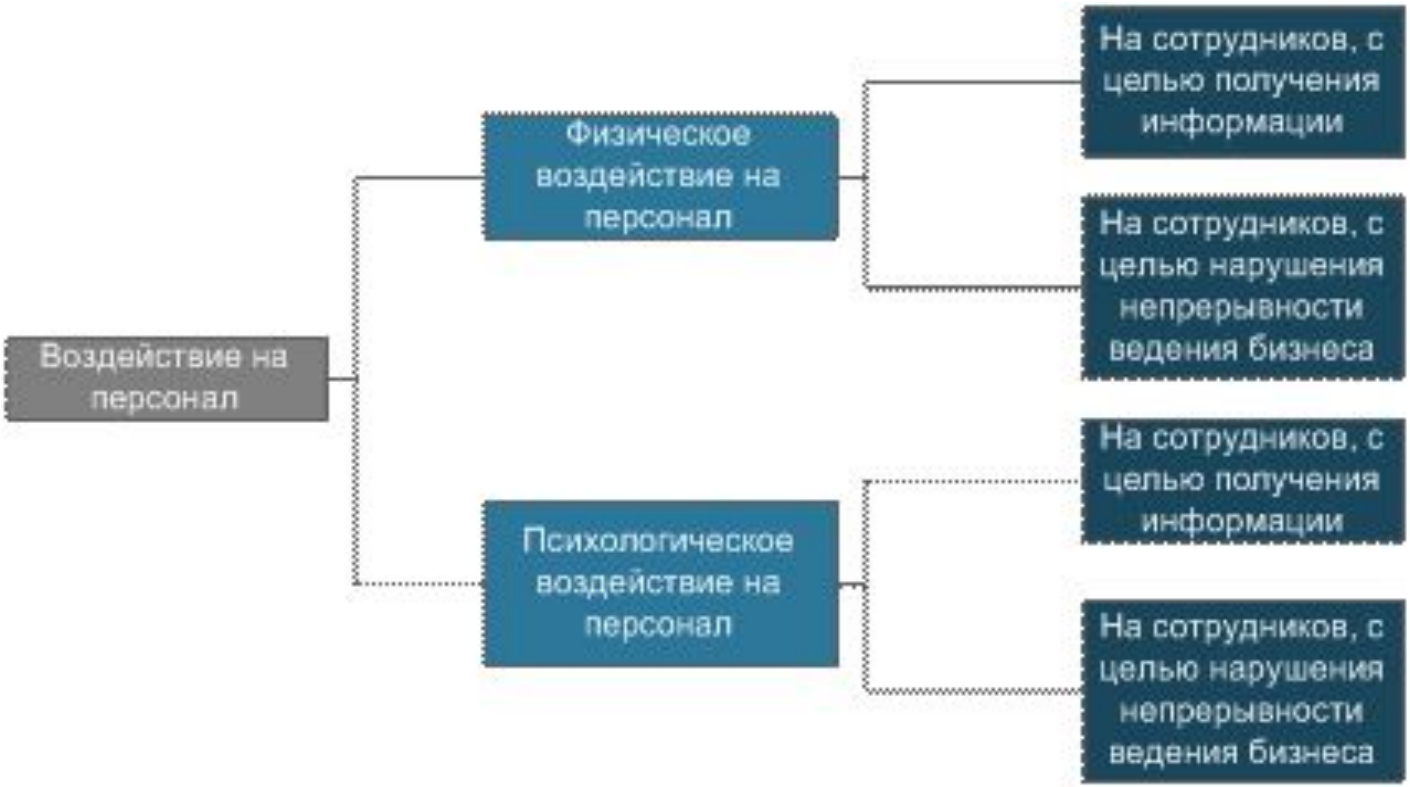
- Каким образом может быть реализована угроза информационной безопасности с помощью сотрудника организации? Злоумышленник может применить воздействие на сотрудника для получения необходимых ему сведений или сотрудник сам реализует угрозу. Организационные угрозы на информацию разделяют следующим образом:



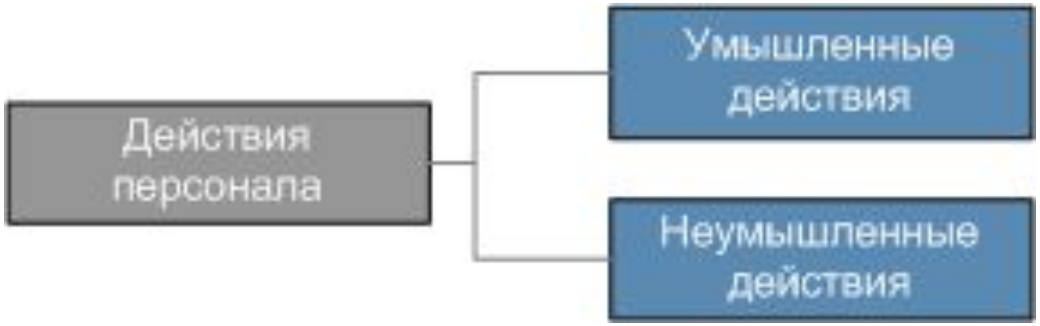
- Воздействие на персонал может быть физическим и психологическим



- Воздействие на персонал (физическое и психологическое) может быть реализовано с целью получения ценной информации или с целью нарушения непрерывности ведения бизнеса.



- А действия персонала - умышленными или неумышленными.



- При этом и умышленные и неумышленные действия могут угрожать как информации, так и непрерывности ведения бизнеса.