Безопасность данных и информационная защита

Выполнили:

Артёменко Оксана
Бессонов Илья
Ермакова Ксения
Корнийчук Олег

ИТ-10-01

Вопросы 1-5:

1. Понятия информационной безопасности, защиты информации и защищенной системы

Автор: Ермакова Ксения
Группа: ИТ-10-01

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 Российской Федерации 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 Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации 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 России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- 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 России.

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.

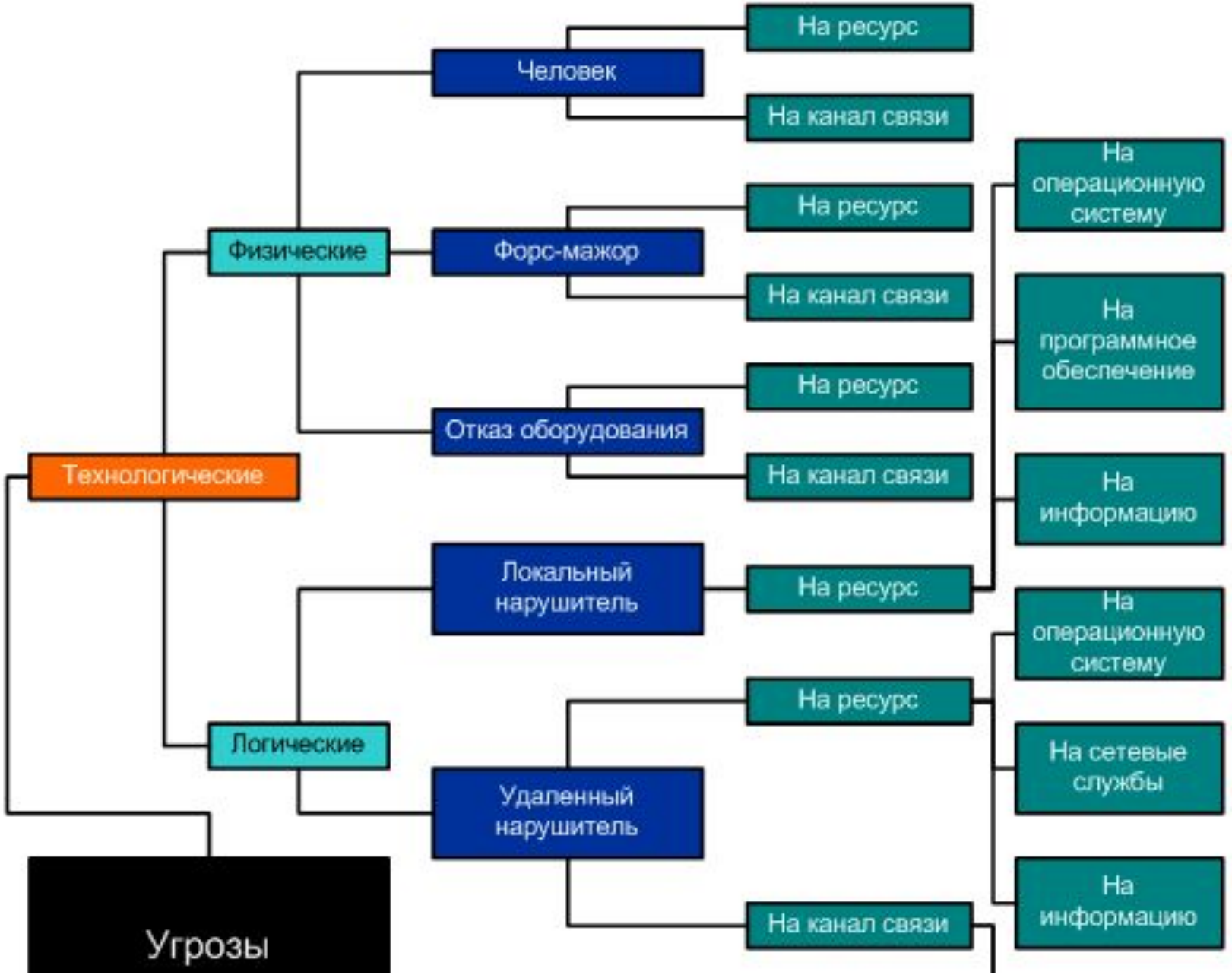
Таблица Распределение методов реализации угроз информационной безопасности по уровням

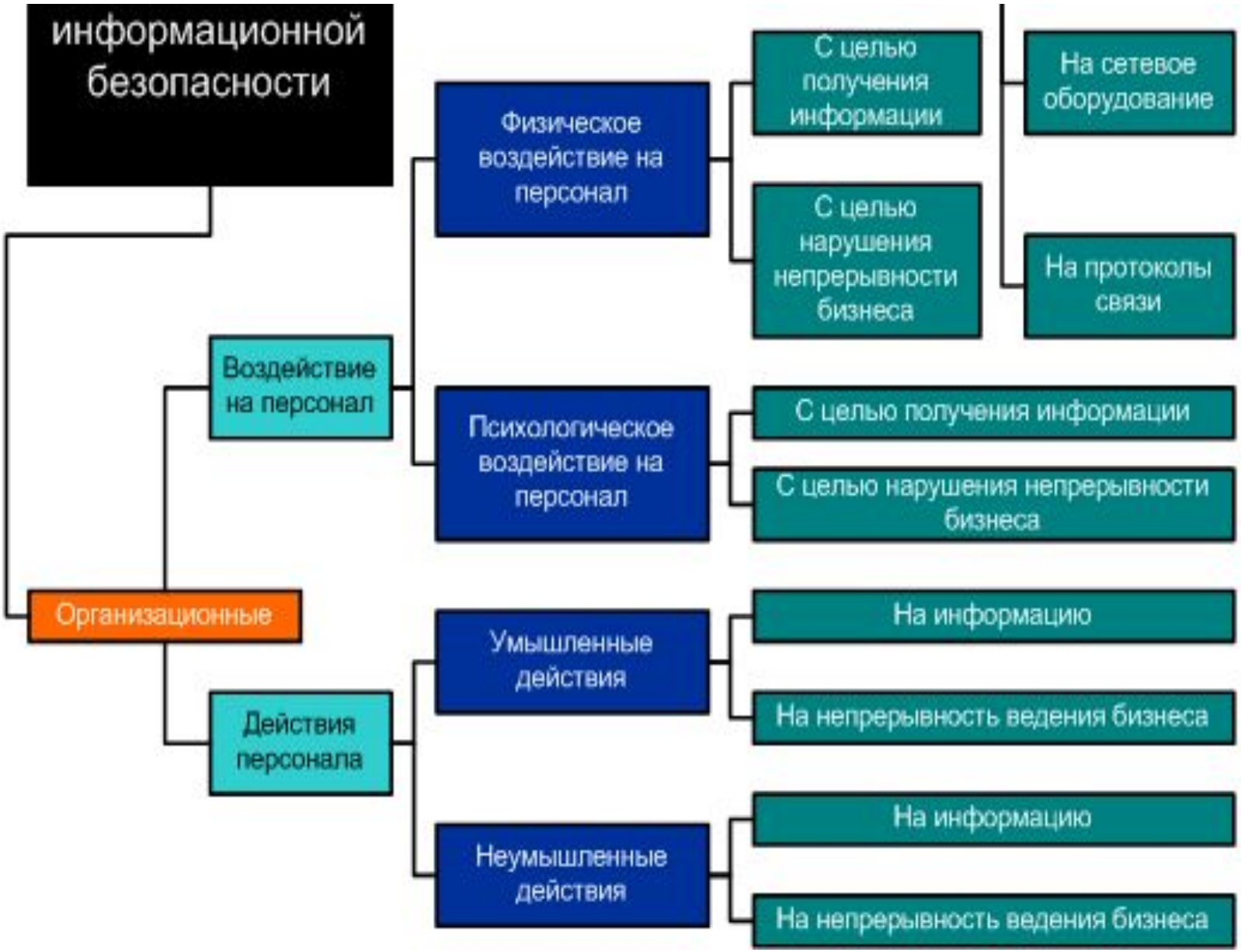
Уровень доступа к информации	Основные методы реализации угроз информационной безопасности			
	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза нарушения доступности
Носителей информации.	Определение типа и параметров носителей информации.	Хищение (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:

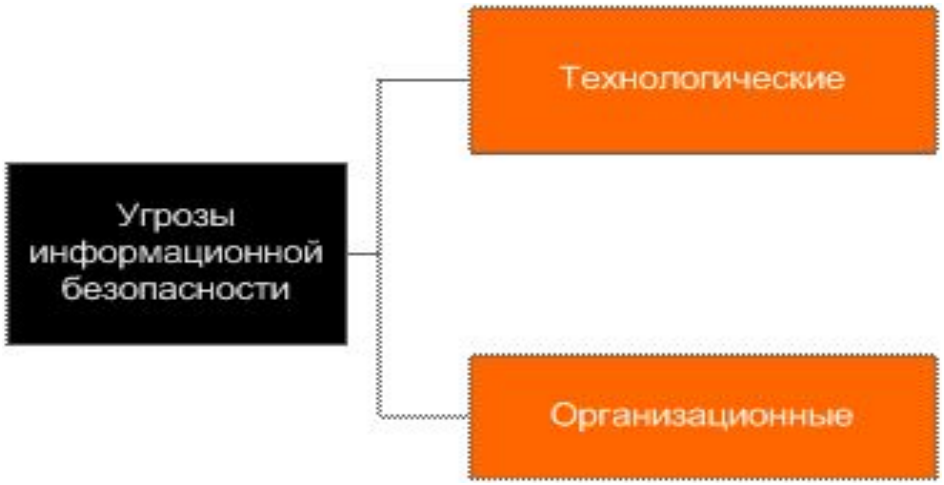
Классификация видов угроз ИБ по ряду признаков

Автор: Корнийчук Олег
Группа: ИТ-10-01

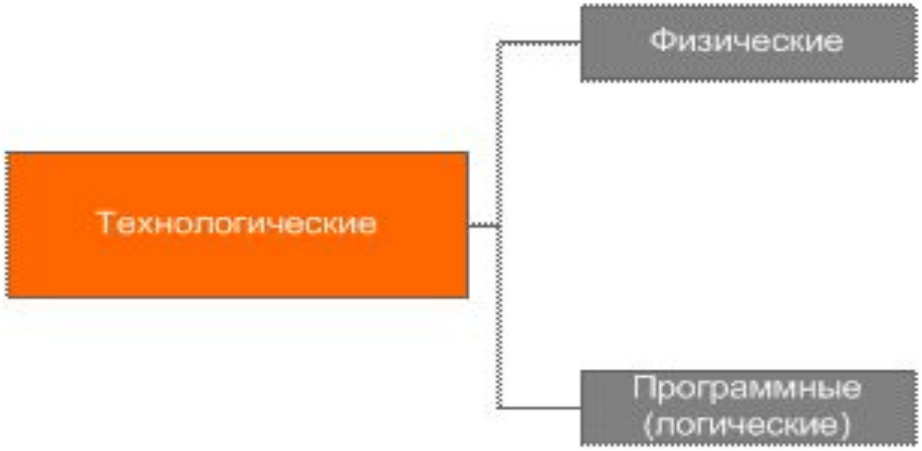

Угрозы
Технологические
Физические
Человек
На ресурс
На канал связи
Форс-мажор
На ресурс
На канал связи
Отказ оборудования
На ресурс
На канал связи
Логические
Локальный нарушитель
На ресурс
На операционную систему
На программное обеспечение
На информацию
Удаленный нарушитель
На ресурс
На операционную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

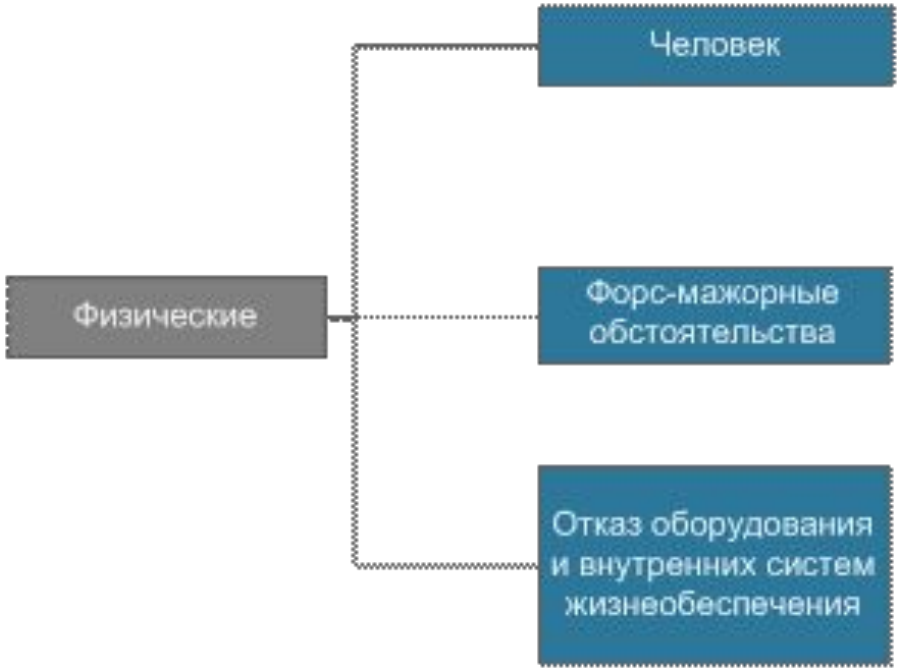
- По виду угроз информационной безопасности разделяют технологические и организационные угрозы.



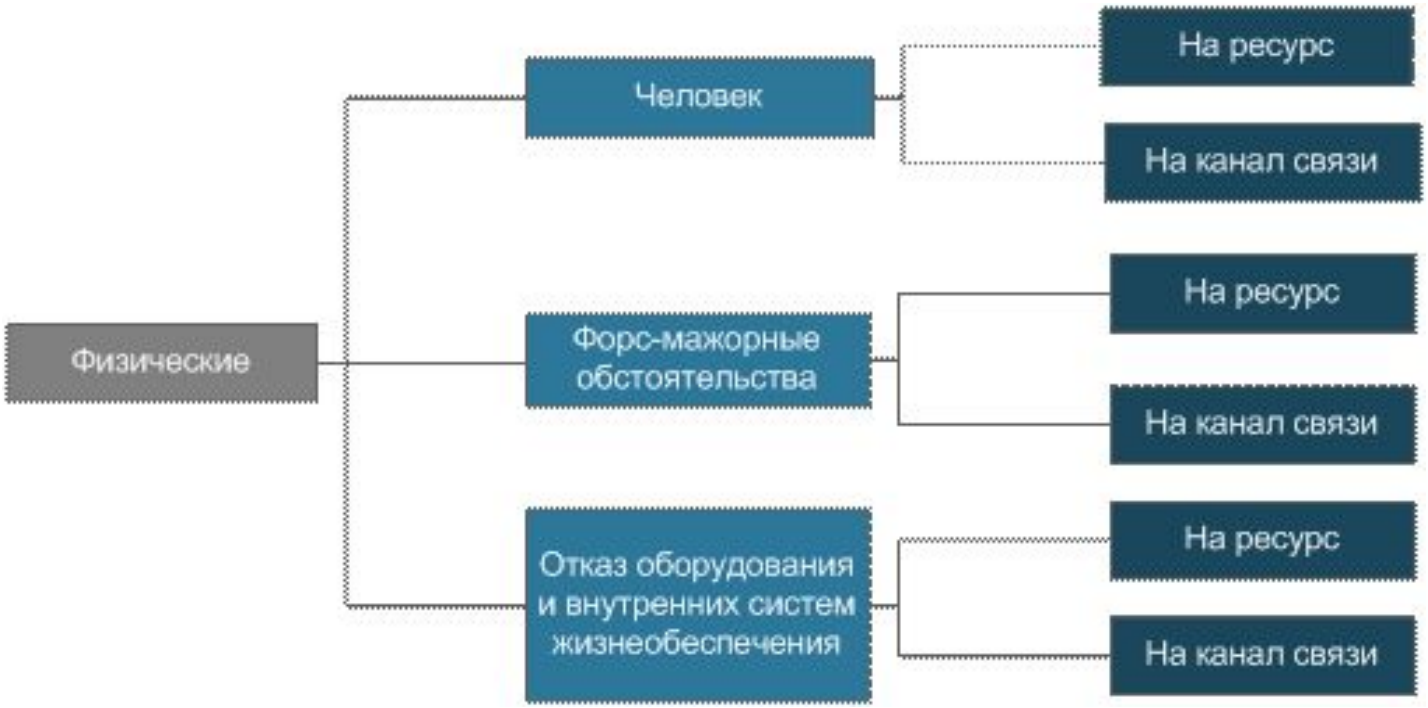
- Технологические угрозы по характеру воздействия разделяются на физические и программные (логические). Т.е. получаем такую начальную классификацию:



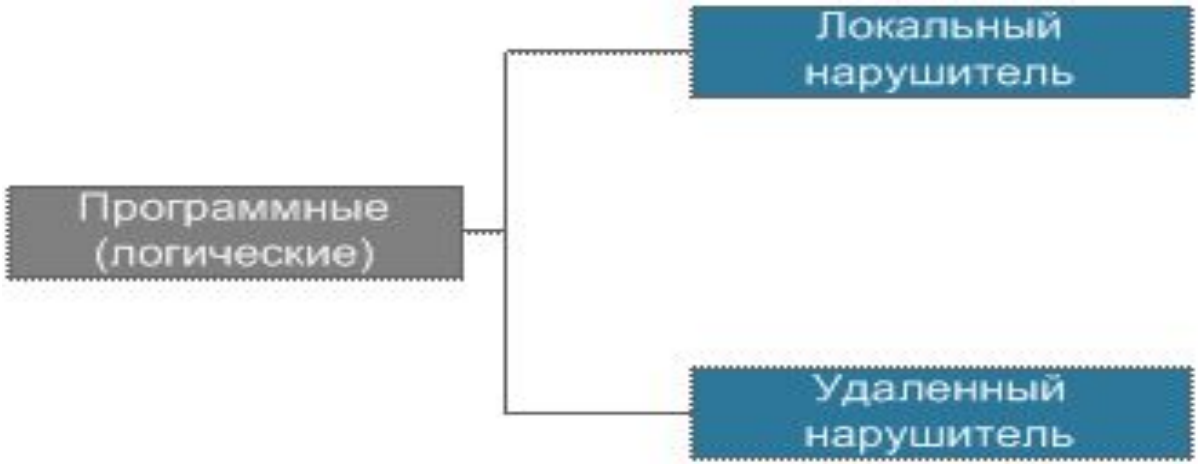
- Физические угрозы могут исходить от действий нарушителя (человека), форс-мажорных обстоятельств и отказа оборудования и внутренних систем жизнеобеспечения.



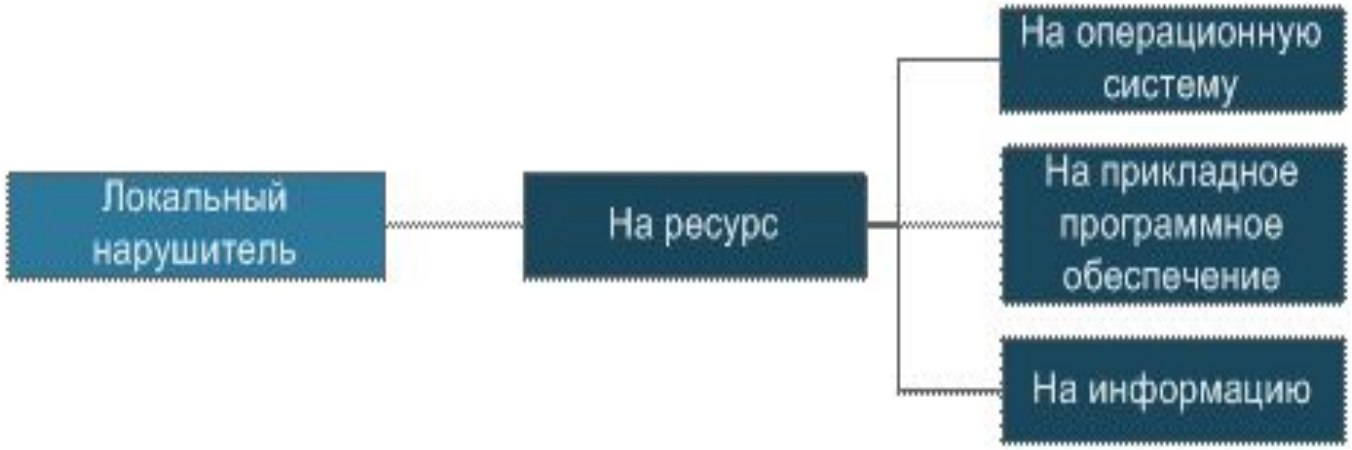
- Далее, положим, что нарушитель имеет физический доступ к помещению, в котором расположен ценный ресурс. Какие виды угроз информационной безопасности он может при этом осуществить? Чтобы реализовать угрозы при физическом доступе нарушитель может воздействовать либо непосредственно на ресурс, либо на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



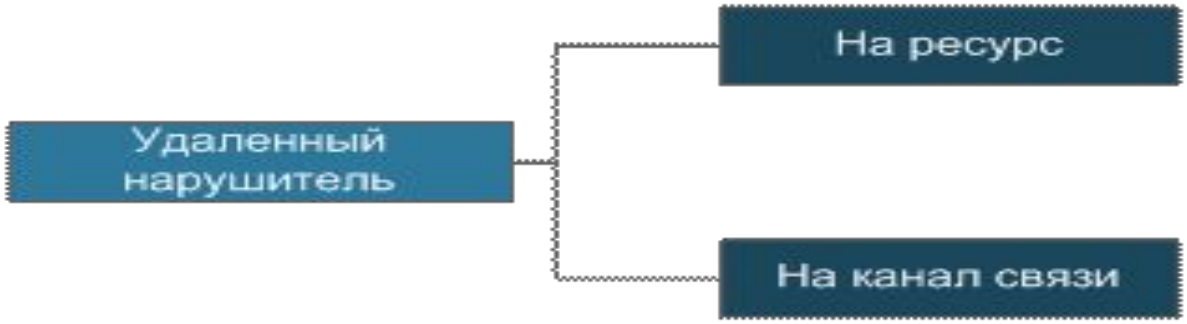
- Далее перейдем к рассмотрению программных угроз.
- Программные угрозы разделяются на угрозы, исходящие от локального нарушителя, и угрозы, исходящие от удаленного нарушителя.



- 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:

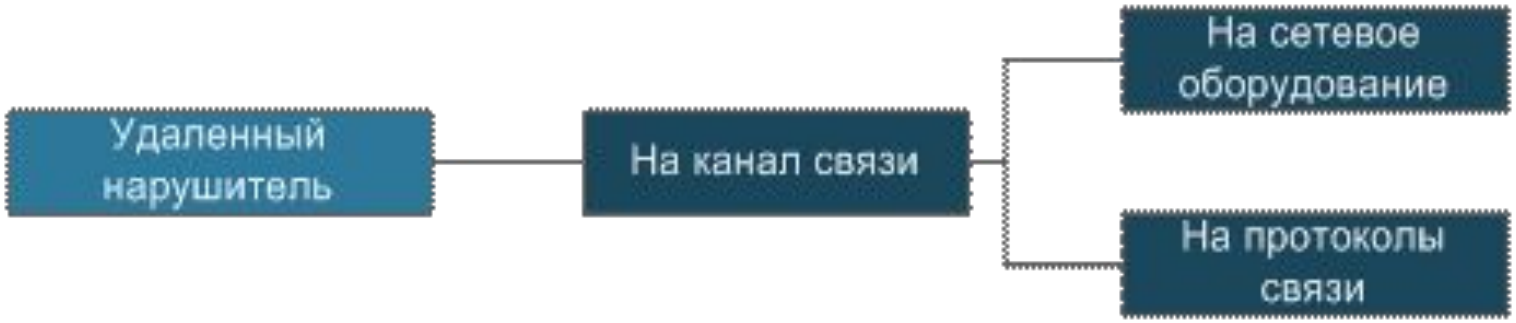


- Рассмотрим удаленные программные угрозы.
- При удаленном программном доступе нарушитель может воздействовать как на ресурс, содержащий ценную информацию, так и на каналы связи, связывающие ресурсы между собой.

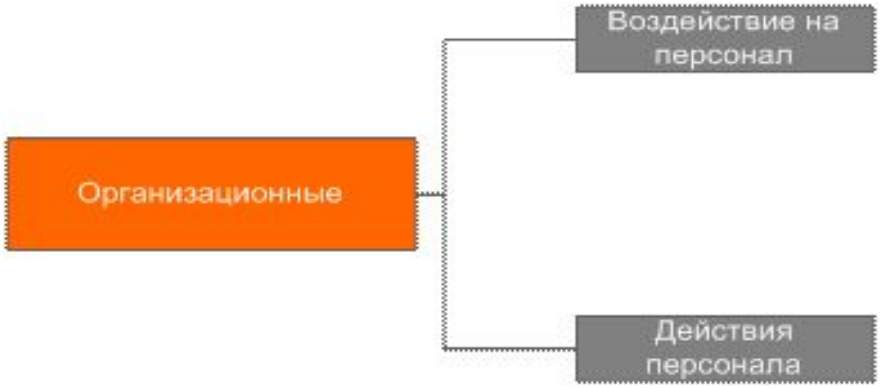


- При этом при удаленном доступе к ресурсу нарушить может воздействовать на следующие его компоненты: операционную систему, сетевые службы и ценную информацию, к которой может быть открыт удаленный

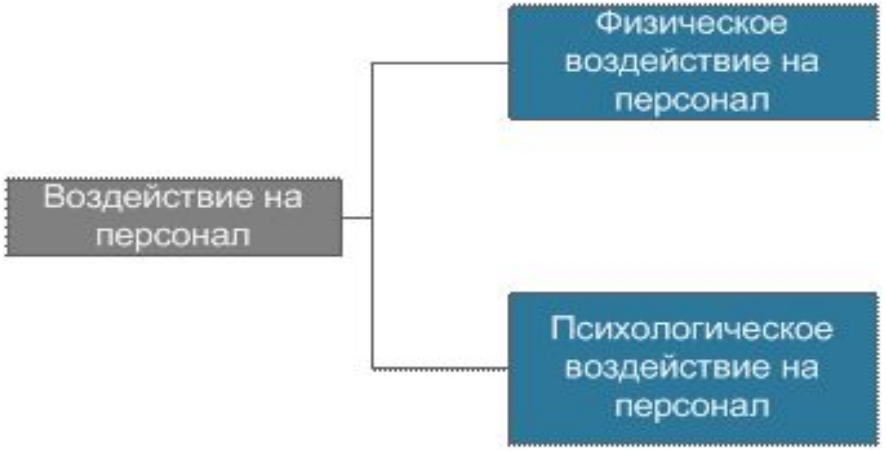
- При удаленном программном доступе к каналу связи для реализации угроз нарушитель может воздействовать непосредственно на сетевое оборудование или на протоколы передачи данных.



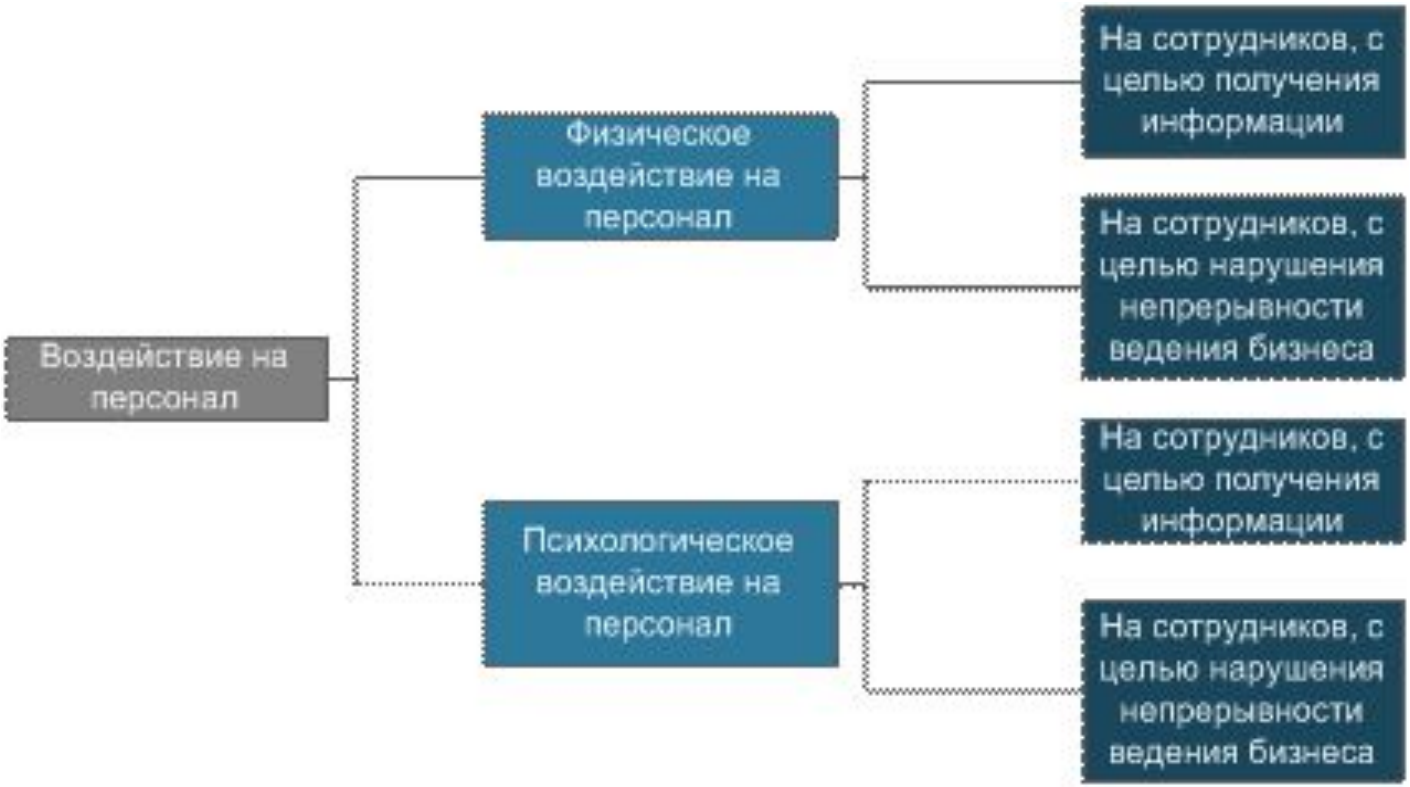
- Каким образом может быть реализована угроза информационной безопасности с помощью сотрудника организации? Злоумышленник может применить воздействие на сотрудника для получения необходимых ему сведений или сотрудник сам реализует угрозу. Организационные угрозы на информацию разделяют следующим образом:



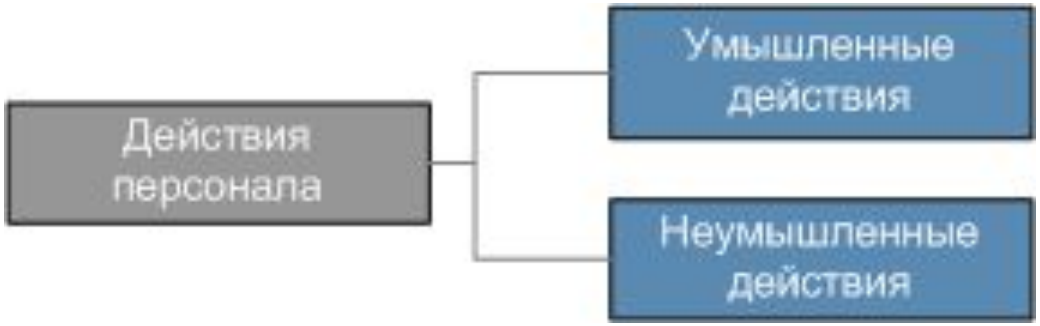
- Воздействие на персонал может быть физическим и психологическим



- 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.

Вопросы 8-13:

Уровни информационной безопасности

Автор: Артёменко Оксана
Группа: ИТ-10-01

Уровни формирования режима ИБ:

- законодательный - законы, нормативные акты, стандарты и т. д.

- административный (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами).

- процедурный (меры безопасности, ориентированные на людей).

программно-технический – электронные устройства и специальные программы защиты информации на ЭВМ.

Законодательный уровень

Группы мер:

1. **меры ограниченной направленности**, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности.

2. **направляющие и координирующие меры**, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности **(меры созидательной направленности)**.

Обзор российского законодательства в области информационной безопасности

Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

1. Конституция РФ:

Статья 24 (органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом) ;

Статья 41 (гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей);

Статья 42 (гарантирует право на знание достоверной информации о состоянии окружающей среды):

Статья 23 (гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений);

Статья 29 (гарантирует право свободно искать, получать, передавать, производить и распространять информацию любым законным способом).

2. Гражданский кодекс РФ:

Статья 139 (информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности).

3. Уголовный кодекс РФ:

Глава 28 "Преступления в сфере компьютерной информации":

- **статья 272**. Неправомерный доступ к компьютерной информации;
- **статья 273**. Создание, использование и распространение вредоносных программ для ЭВМ;
- **статья 274**. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статья 138 (предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений).

Статья 183 (предусматривает наказание за нарушение банковской и коммерческой тайны).

4. Закон «О государственной тайне»

(гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
Защита информации это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.)

5. Закон "Об информации, информатизации и защите информации«

В нем даются основные определения и намечаются направления развития законодательства в данной области. Закон выделяет цели защиты информации, ставя на первое место сохранение конфиденциальности информации. В качестве основного метода защиты информации закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию (**статья 19**).

6. Закон «О лицензировании отдельных видов деятельности»
(содержит основные определения и устанавливает перечень видов деятельности, на осуществление которых требуются лицензии).

7. Закон «Об участии в международном информационном обмене»
(В нем, как и в Законе "Об информации...", основным защитным средством являются лицензии и сертификаты).

8 . Закон «Об электронной цифровой подписи»
(развивает и конкретизирует положения закона "Об информации...". Закон содержит основные понятия и определяет сведения, которые должен содержать сертификат ключа подписи).

Основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- ориентация на созидательные, а не карательные законы;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

Административный уровень

Меры административного уровня (т.е. меры предпринимаемые руководством организации):

1. Разработка политики безопасности;

2. Проведение анализа рисков;

3. Планирование обеспечения информационной безопасности;

4. Планирование действий в чрезвычайных ситуациях;

5. Подбор механизмов и средств обеспечения информационной безопасности

Первые два этапа обычно трактуются как выработка политики безопасности и составляют так называемый административный уровень системы ОБИ предприятия.

Третий и четвертый этапы заключаются в разработке процедур безопасности. На этих этапах формируется уровень планирования системы ОБИ.

На последнем этапе практических мероприятий определяется программно-технический уровень системы ОБИ.

Политика безопасности

Основой мер административного уровня является политика безопасности.

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Разработка политики безопасности требует учета специфики конкретных организаций. Бессмысленно переносить практику режимных государственных организаций на коммерческие структуры, учебные заведения или персональные компьютерные системы. В этой области целесообразно предложить, во-первых, основные принципы разработки политики безопасности, а, во-вторых — готовые шаблоны для наиболее важных разновидностей организаций.

Типы (модели) политики безопасности:

- дискреционная
- мандатная
- ролевая

Модель политики безопасности — формальное выражение политики безопасности.

Дискреционная (дискретная) политика безопасности

Основой дискреционной (дискретной) политики безопасности является дискреционное управление доступом (Discretionary Access Control – DAC), которое определяется двумя свойствами:

- все субъекты и объекты должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

Дискреционное управление доступом является основной реализацией разграничительной политики доступа к ресурсам при обработке конфиденциальных сведений согласно требованиям к системе защиты информации.

Данная модель характеризуется разграничением доступа между поименованными субъектами и объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Для каждой пары (субъект--объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту). Возможны, по меньшей мере, два подхода к построению дискреционного управления доступом:

- каждый объект системы имеет привязанного к нему субъекта, называемого владельцем. Именно владелец устанавливает права доступа к объекту;
- система имеет одного выделенного субъекта – суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.

Возможны и смешанные варианты построения, когда одновременно в системе присутствуют как владельцы, устанавливающие права доступа к своим объектам, так и суперпользователь, имеющий возможность изменения прав для любого объекта и/или изменения его владельца. Именно такой смешанный вариант реализован в большинстве операционных систем (UNIX или Windows семейства NT).

Достоинства

Относительно простая реализация соответствующиего разграничения доступа.

Недостатки

1. Статичность определённых в ней правил разграничения доступа. Не учитывает динамику изменений состояний компьютерной системы.
2. При использовании дискреционной политики безопасности возникает вопрос определения правил распространения прав доступа и анализа их влияния на безопасность компьютерной системы.

В общем случае при использовании данной политики безопасности перед системой защиты, которая при санкционировании доступа субъекта к объекту руководствуется некоторым набором правил, стоит алгоритмически неразрешимая задача: проверить приведут ли его действия к нарушению безопасности или нет.

В то же время имеются модели компьютерных систем, реализующих дискреционную политику безопасности (модель Take–Grant), которые предоставляют алгоритмы проверки безопасности.

Мандатная (полномочная) политика безопасности

Основу мандатной (полномочной) политики безопасности составляет мандатное управление доступом (Mandatory Access Control – MAC), которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- задана решетка уровней конфиденциальности информации;
- каждому объекту системы присвоен уровень конфиденциальности, определяющий ценность содержащейся в нем информации;
- каждому субъекту системы присвоен уровень доступа, определяющий уровень доверия к нему в компьютерной системе.

- субъект может читать объект, только если иерархическая классификация субъекта не меньше, чем иерархическая классификация объекта, и неиерархические категории субъекта включают в себя все иерархические категории объекта;
- субъект осуществляет запись в объект, только если классификационный уровень субъекта не больше, чем классификационный уровень объекта, и все иерархические категории субъекта включаются в неиерархические категории объекта.

Основная цель мандатной политики безопасности - предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т.е. противодействие возникновению в компьютерной системе неблагоприятных информационных потоков сверху вниз.

Достоинства

1. Проверки безопасности является алгоритмически разрешимой. **Е*сли начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушают ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно.***
2. Более высокая степень надёжности по сравнению с дискреционной политикой безопасности. Это связано с тем, что МБО такой системы должен отслеживать, не только правила доступа субъектов системы к объектам, но и состояния самой АС. Т.о. каналы утечки в системах данного типа не заложены в нее непосредственно, а могут появиться только при практической реализации системы.
3. Правила мандатной политики безопасности более ясны и просты для понимания разработчиками и пользователями, что также является фактором, положительно влияющим на уровень безопасности системы.

Недостатки

Реализация систем с политикой безопасности данного типа довольно сложна и требует значительных ресурсов компьютерной системы.

Ролевое управление доступом.

Ролевое разграничение доступа является развитием политики дискреционного разграничения доступа; при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

Задание ролей позволяет определить более четкие и понятные для пользователей компьютерной системы правила разграничения доступа. При этом такой подход часто используется в системах, для пользователей которых четко определен круг их должностных полномочий и обязанностей.

Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы правила разграничения доступа.

Роль является совокупностью прав доступа на объекты компьютерной системы, однако ролевое разграничение отнюдь не является частным случаем дискреционного разграничения, так как ее правила определяют порядок предоставления прав доступа субъектам компьютерной системы в зависимости от сессии его работы и от имеющихся (или отсутствующих) у него ролей в каждый момент времени, что является характерным для систем мандатного разграничения доступа. С другой стороны, правила ролевого разграничения доступа являются более гибкими, чем при мандатном подходе к разграничению.

Процедурный уровень

К процедурному уровню относятся меры безопасности, реализуемые людьми.

Группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

На этом уровне применимы важные принципы безопасности:

- непрерывность защиты в пространстве и времени;
- разделение обязанностей;
- минимизация привилегий.

В рамках **управления персоналом** в контексте информационной безопасности должно:

1. для каждой должности существовать квалификационные требования по информационной безопасности.

2. в должностные инструкции должны входить разделы, касающиеся информационной безопасности.

3. каждого работника необходимо обучить мерам обеспечения информационной безопасности теоретически и отработать выполнение этих мер практически.

Информационная безопасность ИС предприятия зависит от окружения, в котором она работает. Необходимо принимать меры для обеспечения физической защиты зданий и прилегающей территории, поддерживающей инфраструктуры и самих компьютеров.

Меры физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры.

Меры по поддержанию работоспособности:

- поддержка пользователей ИС;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Программа информационной безопасности должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима информационной безопасности преследует две главные цели:

- блокирование нарушителя и уменьшение наносимого вреда;
- недопущение повторных нарушений.

На предприятии должен быть выделен сотрудник, доступный 24 часа в сутки, отвечающий за реакцию на нарушения. Все пользователи ИС должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В случае невозможности связи с данным сотрудником, должны быть разработаны и внедрены процедуры первичной реакции на информационный инцидент.

Планирование восстановительных работ позволяет подготовиться к авариям ИС, уменьшить ущерб от них и сохранить способность к функционированию, хотя бы в минимальном объеме.

Механизмы контроля, существенные для предприятия с юридической точки зрения, включают в себя:

- Защиту данных и тайну персональной информации;
- Охрану документов организации;
- Права на интеллектуальную собственность.

Также процесс планирования таких работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;
- подготовка к реализации выбранной стратегии;
- проверка стратегии.

Программно-технический уровень

Программно-технические средства защиты располагаются на следующих рубежах:

- Защита внешнего периметра КСПД;
- Защита внутренних сетевых сервисов и информационных обменов;
- Защита серверов и рабочих станций;
- Защита системных ресурсов и локальных приложений на серверах и рабочих станциях;
- Защита выделенного сегмента руководства компании.

Сервис безопасности представляет собой совокупность механизмов, процедур и других средств управления для снижения рисков, связанных с угрозой утраты или раскрытия данных.

На программно-техническом уровне выполнение защитных функций ИС осуществляется следующими служебными сервисами обеспечения информационной безопасности:

- идентификация/аутентификация пользователей ИС (обеспечивает аутентификацию участников коммуникации и аутентификацию источника данных);
- разграничение доступа объектов и субъектов информационного обмена;
- протоколирование/аудит действий легальных пользователей;
- экранирование информационных потоков и ресурсов КСПД;
- туннелирование информационных потоков;
- шифрование информационных потоков, критической информации;

- контроль целостности;
- контроль защищенности;
- управление СОИБ.

Вопросы 14-19:

14. 1)Понятие авторизации, идентификации и аутентификации пользователей.
2)Парольная аутентификация, её достоинства и недостатки. 3) Биометрическая идентификация/аутентификация

Автор: Бессонов Илья
Группа: ИТ-10-01

Понятия авторизации, идентификации и аутентификации пользователей

1)Совокупность выполнения процедур идентификации и аутентификации принято называть процедурой ***авторизации***.

Идентификация призвана каждому пользователю (группе пользователей) сопоставить соответствующую ему разграничительную политику доступа на защищаемом объекте. Для этого пользователь должен себя идентифицировать — указать свое «имя» (идентификатор). Таким образом проверяется, относится ли регистрирующийся пользователь к пользователям, идентифицируемым системой. В соответствии с введенным идентификатором пользователю будут сопоставлены соответствующие права доступа.

Аутентификация предназначена для контроля процедуры идентификации. Для этого пользователь должен ввести секретное слово — пароль. Правильность вводимого пароля подтверждает однозначное соответствие между регистрирующимся пользователем и идентифицированным пользователем.

Парольная аутентификация, ее достоинства и недостатки

2) ***Достоинства:*** простота и привычность

***Недостатки*:** 1.возможность подобрать пароль из-за достаточно небрежного отношения большинства пользователей к формированию пароля

2.существуют и свободно доступны различные утилиты подбора паролей, в том числе, специализированные для конкретных широко распространенных программных средств

3. пароль может быть подсмотрен или перехвачен при вводе

Биометрическая идентификация /аутентификация

3)**Биометрия** представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности **отпечатков пальцев**, **сетчатки** и **роговицы** глаз, **геометрия руки и лица** и т.п. К поведенческим характеристикам относятся **динамика подписи** (ручной), стиль **работы с клавиатурой**. На стыке физиологии и поведения находятся анализ особенностей **голоса** и **распознавание речи**.

Биометрическая идентификация/аутентификация

- В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый **биометрическим шаблоном**) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).
- В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Биометрическая идентификация/аутентификация

Достоинства: пользователю гораздо удобнее предъявить себя самого, чем что-то запоминать

Недостатки: 1) биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения

2) биометрические методы не более надежны, чем база данных шаблонов

3) следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж

4) биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Биометрическая идентификация/аутентификация

Но **главная опасность** состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

15. 1) Понятие доступа к данным. и монитора безопасности.

2) Функции монитора безопасности.

3) Управление доступом, ролевое управление доступом.

Понятие доступа к данным и монитора безопасности

Вопросы представления данных тесно связаны с операциями, при помощи которых эти данные обрабатываются. К числу таких операций относятся: *выборка, изменение,включение* и *исключение* данных. В основе всех перечисленных операций лежит операция **доступа**, которую нельзя рассматривать независимо от способа представления.

В задачах поиска предполагается, что все данные хранятся в памяти с определенной идентификацией и, говоря о доступе, имеют в виду прежде всего доступ к данным (называемым ключами), однозначно идентифицирующим связанные с ними совокупности данных.

Существуют два класса методов, реализующих доступ к данным по ключу:

- методы поиска по дереву,
- методы хеширования.

Понятие доступа к данным и монитора безопасности

Методы поиска по дереву:

Определение: *Деревом называется конечное множество, состоящее из одного или более элементов, называемых узлами, таких, что:*

*1)*между узлами имеет место отношение типа "исходный-порожденный";

2)есть только один узел, не имеющий исходного. Он называется корнем;

3)все узлы за исключением корня имеют только один исходный; каждый узел может иметь несколько порожденных;

4)отношение "исходный-порожденный" действует только в одном направлении, т.е. ни один потомок некоторого узла не может стать для него предком.

Понятие доступа к данным и монитора безопасности

Методы хеширования:

Этот метод используется тогда, когда все множество ключей заранее известно и на время обработки может быть размещено в оперативной памяти. В этом случае строится специальная функция, однозначно отображающая множество ключей на множество указателей, называемая хеш-функцией (от английского "to hash" - резать, измельчать). Имея такую функцию можно вычислить адрес записи в файле по заданному ключу поиска. В общем случае ключевые данные, используемые для определения адреса записи организуются в виде таблицы, называемой хеш-таблицей. Если множество ключей заранее неизвестно или очень велико, то от идеи однозначного вычисления адреса записи по ее ключу отказываются, а хеш-функцию рассматривают просто как функцию, рассеивающую множество ключей во множество адресов.

Понятие доступа к данным и монитора безопасности

Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Основное назначение доверенной вычислительной базы - выполнять функции **монитора обращений**, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Реализация монитора обращений называется **ядром безопасности**. **Ядро безопасности** - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Понятие доступа к данным и монитора безопасности

Монитор обращений должен обладать **тремя качествами**:

*1)**Изолированность***. Необходимо предупредить возможность отслеживания работы монитора.

*2)**Полнота***. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

*3)**Верифицируемость***. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Функции монитора безопасности

Целевая функция монитора безопасности – фильтрация потоков с целью обеспечения безопасности (монитор обращений, который разрешает поток, принадлежащий только пользователям легального доступа. Разрешение потока в данном случае понимается как выполнение операции над объектом - получателем потока, а запрещение - как невыполнение)

Управление доступом

Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде **матрицы доступа**, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа.

Управление доступом

Фрагмент матрицы может выглядеть, так:

	Файл	Программа	Линия связи	Реляционная таблица
Пользователь 1	orw с системной консоли	e	rw с 8:00 до 18:00	
Пользователь 2				a

"o" – обозначает разрешение на передачу **прав доступа** другим пользователям,

"r" – чтение,

"w" – запись,

"e" – выполнение,

"a" – добавление информации

Тема логического управления доступом – одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты. Для систем управления реляционными базами данных объект – это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Управление доступом

Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой **произвольного (или дискреционного) управления доступом**;
- атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности – основа **принудительного (мандатного) управления доступом**.

Управление доступом

Произвольное управление доступом (называемое иногда дискреционным) - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

К сожалению, у "произвольного" подхода есть ряд недостатков. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

Управление доступом

Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, “конфиденциальный” субъект может записывать данные в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является **ролевое управление доступом** (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права

Ролям приписываются пользователи и права доступа; можно считать, что они (роли) именуют отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

16. ПОНЯТИЯ ПРОТОКОЛИРОВАНИЯ, АУДИТА, ШИФРОВАНИЯ, КОНТРОЛЯ ЦЕЛОСТНОСТИ – ФУНКЦИИ И НАЗАНАЧЕНИЕ, РОЛЬ В ОБЕСПЕЧЕНИИ ИНФОРМА- ЦИОННОЙ БЕЗОПАСНОСТИ

ПОНЯТИЕ ПРОТОКОЛИРОВАНИЯ И АУДИТА

Под **протоколированием** понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Функции *протоколирования* и *аудита*:

1)обеспечение подотчетности пользователей и администраторов;

2)обеспечение возможности реконструкции последовательности событий;

3)обнаружение попыток нарушений информационной безопасности;

4)предоставление информации для выявления и анализа проблем.

ПОНЯТИЕ ПРОТОКОЛИРОВАНИЯ И АУДИТА

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

1)дата и время события;

2)уникальный идентификатор пользователя – инициатора действия;

3)тип события;

4)результат действия (успех или неудача);

5)источник запроса (например, имя терминала);

6)имена затронутых объектов (например, открываемых или удаляемых файлов);

7)описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

Обнаружение попыток нарушений информационной безопасности – функция ***активного аудита***

ПОНЯТИЕ ПРОТОКОЛИРОВАНИЯ И АУДИТА

Задача **активного аудита** – оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

Применительно к средствам активного аудита различают **ошибки первого** и **второго рода**: пропуск атак и ложные тревоги, соответственно. Нежелательность ошибок первого рода очевидна; ошибки второго рода не менее неприятны, поскольку отвлекают администратора безопасности от действительно важных дел, косвенно способствуя пропуску атак.

Достоинства метода активного аудита – высокая производительность, малое число ошибок второго рода, обоснованность решений. Основной недостаток – неумение обнаруживать неизвестные атаки и вариации известных атак.

Основные достоинства статистического подхода – универсальность и обоснованность решений, потенциальная способность обнаруживать неизвестные атаки, то есть минимизация числа ошибок первого рода. Минусы заключаются в относительно высокой доле ошибок второго рода, плохой работе в случае, когда неправомерное поведение является типичным, когда типичное поведение плавно меняется от легального к неправомерному, а также в случаях, когда типичного поведения нет (как показывает статистика, таких пользователей примерно 5-10%).

Роль протоколирования и аудита в обеспечении ИБ

Роль протоколирования и аудита заключается в обеспечении подотчетности являющейся в первую очередь *сдерживающим средством*. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Очевидно, если есть основания подозревать какого-либо пользователя в нечестности, можно регистрировать все его действия, вплоть до каждого нажатия клавиши. При этом обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и откат некорректных изменений (если в протоколе присутствуют данные до и после модификации).

ПОНЯТИЕ ШИФРОВАНИЯ

Шифрованием называют преобразование элементов информации с помощью математической функции, после которого восстановление исходной информации становится исключительно трудным для всех, кроме лица, которому предназначается информация. Основой этого процесса является математическое значение, которое называют *ключом*, используемое функцией для однозначного сложного преобразования информации.

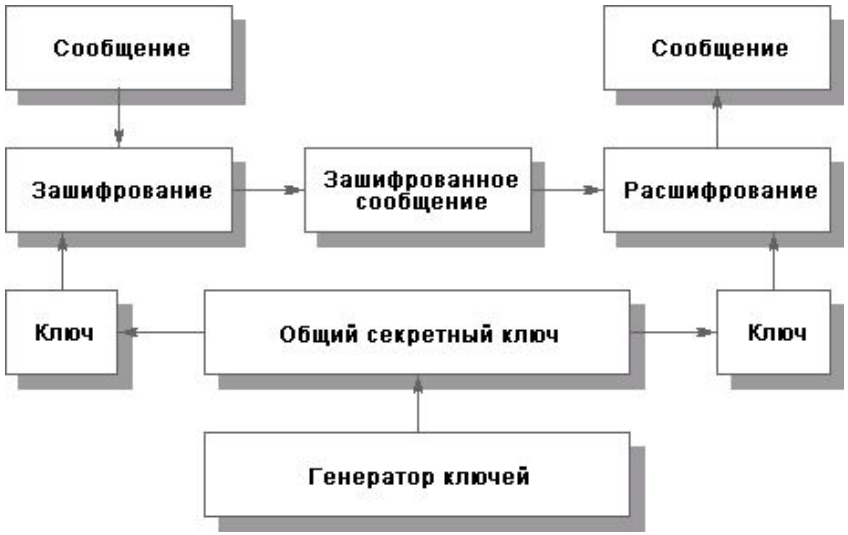
Шифрование – наиболее мощное средство обеспечения конфиденциальности. Во многих отношениях оно занимает центральное место среди программно-технических регуляторов безопасности, являясь основой реализации многих из них, и в то же время последним защитным рубежом. Например, для портативных компьютеров только шифрование позволяет обеспечить конфиденциальность данных даже в случае кражи.

В большинстве случаев и **шифрование**, и **контроль целостности** играют глубоко инфраструктурную роль, оставаясь прозрачными и для приложений, и для пользователей. Типичное место этих сервисов безопасности – на сетевом и транспортном уровнях реализации стека сетевых протоколов.

Различают два основных метода шифрования: *симметричный* и *асимметричный*.

ПОНЯТИЕ ШИФРОВАНИЯ

В симметрическом методе один и тот же ключ (хранящийся в секрете) используется и для зашифрования, и для расшифрования данных. Разработаны весьма эффективные (быстрые и надежные) методы симметричного шифрования. Существует и национальный стандарт на подобные методы – ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

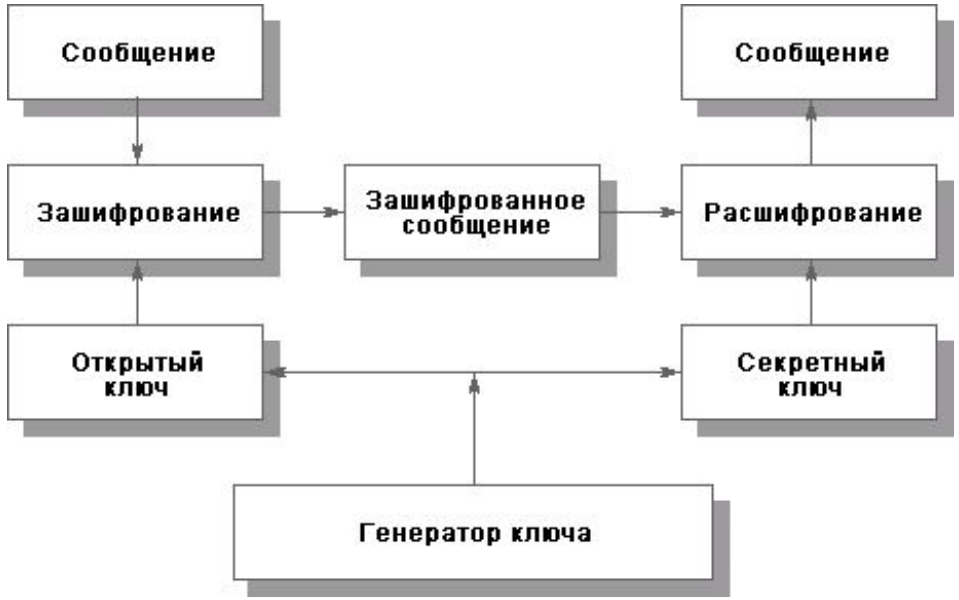


ПОНЯТИЕ ШИФРОВАНИЯ

Основным недостатком ***симметричного шифрования*** является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

ПОНЯТИЕ ШИФРОВАНИЯ

В **асимметричных методах** используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) – для расшифрования. Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.



ПОНЯТИЕ ШИФРОВАНИЯ

Существенным **недостатком** *асимметричных методов* шифрования является их низкое быстродействие, поэтому данные методы приходится сочетать с симметричными (асимметричные методы на 3 – 4 порядка медленнее). Так, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Эффективное шифрование сообщения

Расшифрование эффективно зашифрованного сообщения

ПОНЯТИЕ КОНТРОЛЯ ЦЕЛОСТНОСТИ

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказаться от совершенных действий ("неотказуемость").

Хэш-функция – это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый **дайджест**). Обозначим хэш-функцию через h, исходные данные – через T, проверяемые данные – через T'. Контроль целостности данных сводится к проверке равенства h(T') = h(T). Если оно выполнено, считается, что T' = T. Совпадение дайджестов для различных данных называется **коллизией**. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества хэшируемых данных, однако то, что h есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

ПОНЯТИЕ КОНТРОЛЯ ЦЕЛОСТНОСТИ

В современных системах контроль целостности должен распространяться не только на отдельные порции данных, аппаратные или программные компоненты. Он обязан охватывать распределенные конфигурации, защищать от несанкционированной модификации потоки данных.

В настоящее время существует достаточно решений для контроля целостности и с системной, и с сетевой направленностью (обычно контроль выполняется прозрачным для приложений образом как часть общей протокольной активности). Стандартизован программный интерфейс к этому сервису (как часть общего интерфейса службы безопасности

17. Понятие ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ. Процедуры формированиЯ цифровой подписи.

ПОНЯТИЕ ЭЦП

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе, а также обеспечивает неотказуемость подписавшегося.

Существует 2 типа процедур формирования ЭЦП:

1) На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.[8]

2) На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

ПРОЦЕДУРЫ ФОРМИРОВАНИЯ ЭЦП

Симметричные схемы имеют следующие преимущества:

1)Стойкость симметричных схем ЭЦП вытекает из стойкости используемых блочных шифров,

2)Если стойкость шифра окажется недостаточной, его легко можно будет заменить на более стойкий с минимальными изменениями в реализации.

Однако у **симметричных ЭЦП** есть и ряд недостатков:

1)Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи. Подпись может превосходить сообщение по размеру на два порядка.

2)Сгенерированные для подписи ключи могут быть использованы только один раз, так как после подписывания раскрывается половина секретного ключа.

ПРОЦЕДУРЫ ФОРМИРОВАНИЯ ЭЦП

Асимметричные схемы ЭП относятся к криптосистемам с открытым ключом. В отличие от асимметричных алгоритмов шифрования, в которых зашифрование производится с помощью открытого ключа, а расшифрование — с помощью закрытого, в схемах цифровой подписи, подпись производится с применением закрытого ключа, а проверка — с применением открытого.

ПРОЦЕДУРЫ ФОРМИРОВАНИЯ ЭЦП

При использовании асимметричных методов шифрования (и, в частности, электронной цифровой подписи) необходимо иметь гарантию подлинности пары (имя пользователя, открытый ключ пользователя). Для решения этой задачи в спецификациях X.509 вводятся понятия **цифрового сертификата** и **удостоверяющего центра**.

Удостоверяющий центр – это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов, имеющих следующую структуру: ***1)****порядковый номер сертификата;* ***2)****идентификатор алгоритма электронной подписи;* ***3)****имя удостоверяющего центра;* ***4)****срок годности;* ***5)****имя владельца сертификата (имя пользователя, которому принадлежит сертификат);* ***6)****открытые ключи владельца сертификата (ключей может быть несколько);* ***7)****идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;* ***8)*** *электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).*

.

ПРОЦЕДУРЫ ФОРМИРОВАНИЯ ЭЦП

Цифровые сертификаты обладают следующими свойствами:

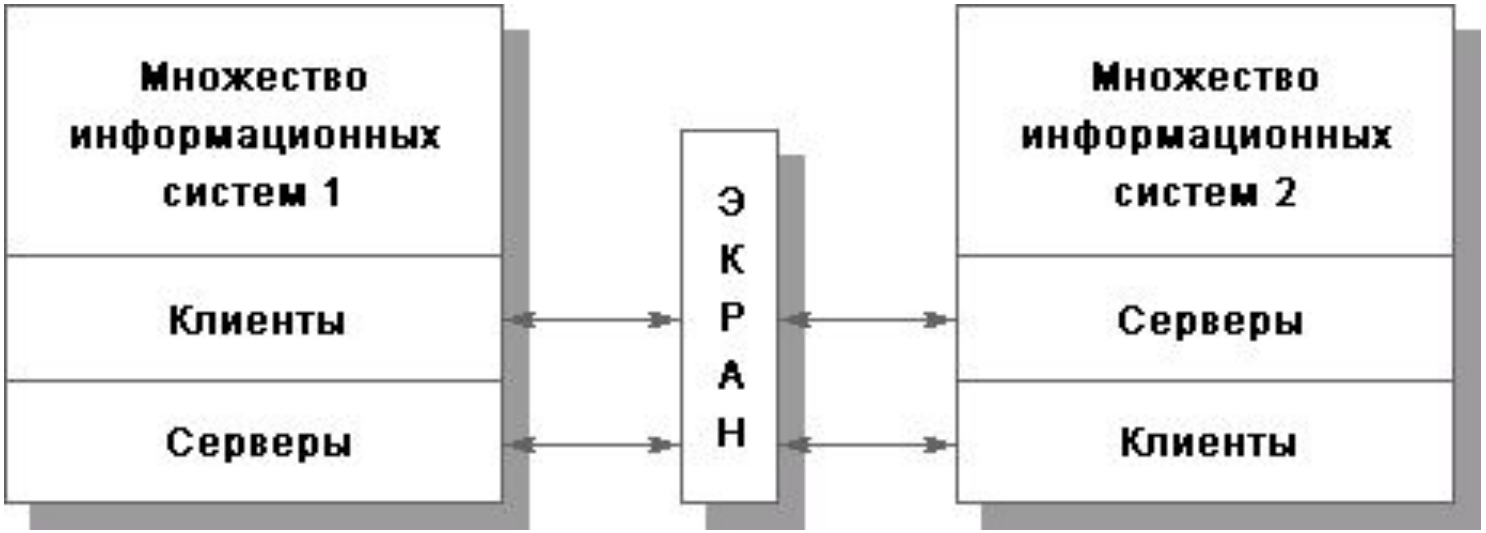
1)любой пользователь, знающий открытый ключ удостоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;

2)никто, кроме удостоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата

18. Понятие экранирования, межсетевые экраны и анализ защищенности – функции и назначение, роль в обеспечении информационной безопасности.

ЭКРАНИРОВАНИЕ

Формальная постановка задачи **экранирования**, состоит в следующем. Пусть имеется два множества информационных систем. **Экран** – это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем. Контроль потоков состоит в их **фильтрации**, возможно, с выполнением некоторых преобразований.



ЭКРАНИРОВАНИЕ

На следующем уровне детализации **экран** (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю

ЭКРАНИРОВАНИЕ

Помимо функций **разграничения доступа**, экраны осуществляют **протоколирование обмена информацией**.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как ***защита*** *внутренней области от потенциально враждебной внешней*. Так, межсетевые экраны (МЭ) (предложенный автором перевод английского термина firewall) чаще всего устанавливают для защиты корпоративной сети организации, имеющей выход в Internet (см. следующий раздел).

Экранирование помогает поддерживать *доступность* сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима **конфиденциальности** в ИС организации.

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Межсетевой экран – комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Межсетевой экран – идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отдавать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на доступность.

На *межсетевой экран* целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

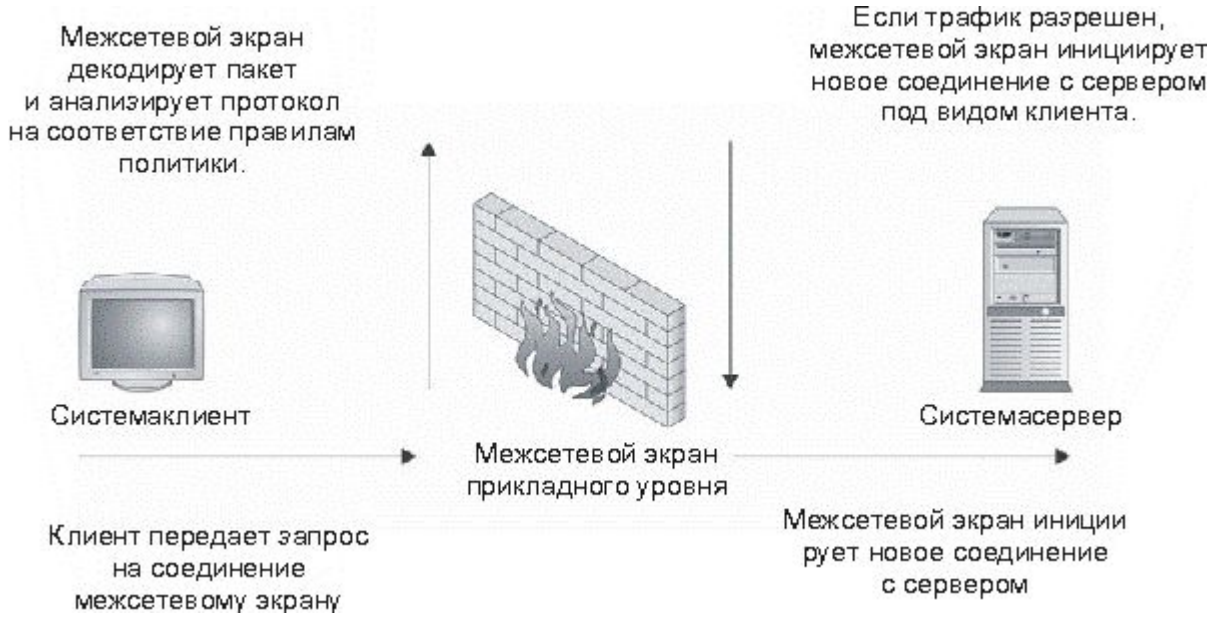
МЕЖСЕТЕВЫЕ ЭКРАНЫ

Существуют два основных типа межсетевых экранов: **межсетевые экраны прикладного уровня** и **межсетевые экраны с пакетной фильтрацией**. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика.

Межсетевые экраны прикладного уровня, или **прокси-экраны**, представляют собой программные пакеты, базирующиеся на операционных системах общего назначения или на аппаратной платформе межсетевых экранов. Межсетевой экран обладает несколькими интерфейсами, по одному на каждую из сетей, к которым он подключен. Набор правил политики определяет, каким образом трафик передается из одной сети в другую. Если в правиле отсутствует явное разрешение на пропуск трафика, межсетевой экран отклоняет или аннулирует пакеты.

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Правила политики безопасности усиливаются посредством использования модулей доступа. В межсетевом экране прикладного уровня каждому разрешаемому протоколу должен соответствовать свой собственный модуль доступа. Лучшими модулями доступа считаются те, которые построены специально для разрешаемого протокола. Например, модуль доступа FTP предназначен для протокола FTP и может определять, соответствует ли проходящий трафик этому протоколу и разрешен ли этот трафик правилами политики безопасности.



МЕЖСЕТЕВЫЕ ЭКРАНЫ

Межсетевые экраны с пакетной фильтрацией могут также быть программными пакетами, базирующимися на операционных системах общего назначения либо на аппаратных платформах межсетевых экранов. Межсетевой экран имеет несколько интерфейсов, по одному на каждую из сетей, к которым подключен экран. Аналогично межсетевым экранам прикладного уровня, доставка трафика из одной сети в другую определяется набором правил политики. Если правило не разрешает явным образом определенный трафик, то соответствующие пакеты будут отклонены или аннулированы межсетевым экраном.

Правила политики усиливаются посредством использования фильтров пакетов. Фильтры изучают пакеты и определяют, является ли трафик разрешенным, согласно правилам политики и состоянию протокола (проверка с учетом состояния).

Если протокол приложения функционирует через TCP, определить состояние относительно просто, так как TCP сам по себе поддерживает состояния. Это означает, что когда протокол находится в определенном состоянии, разрешена передача только определенных пакетов.

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Рассмотрим в качестве примера последовательность установки соединения. Первый ожидаемый пакет - пакет SYN. Межсетевой экран обнаруживает этот пакет и переводит соединение в состояние SYN. В данном состоянии ожидается один из двух пакетов - либо SYN ACK (опознавание пакета и разрешение соединения) или пакет RST (сброс соединения по причине отказа в соединении получателем). Если в данном соединении появятся другие пакеты, межсетевой экран аннулирует или отклонит их, так как они не подходят для данного состояния соединения, даже если соединение разрешено набором правил.

Если протоколом соединения является UDP, межсетевой экран с пакетной фильтрацией не может использовать присущее протоколу состояние, вместо чего отслеживает состояние трафика UDP. Как правило, межсетевой экран принимает внешний пакет UDP и ожидает входящий пакет от получателя, соответствующий исходному пакету по адресу и порту, в течение определенного времени. Если пакет принимается в течение этого отрезка времени, его передача разрешается. В противном случае межсетевой экран определяет, что трафик UDP не является ответом на запрос, и аннулирует его.

МЕЖСЕТЕВЫЕ ЭКРАНЫ

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на межсетевом экране (см. рис. 10.2), а направляются непосредственно к конечной системе. При поступлении пакетов межсетевой экран выясняет, разрешен ли данный пакет и состояние соединения правилами политики. Если это так, пакет передается по своему маршруту. В противном случае пакет отклоняется или аннулируется.

МЕЖСЕТЕВЫЕ ЭКРАНЫ

МЭ на сеансовом уровне (также известные как *stateful*) — отслеживающие сеансы между приложениями, не пропускающие пакеты нарушающих спецификации TCP/IP, часто используемых в злонамеренных операциях — сканировании ресурсов, взломах через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных.

МЭ на сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;

Гибридные межсетевые экраны:

Производители межсетевых экранов прикладного уровня в определенный момент пришли к выводу, что необходимо разработать метод поддержки протоколов, для которых не существует определенных модулей доступа. Вследствие этого увидела свет технология модуля доступа Generic Services Proxy (GSP). GSP разработана для поддержки модулями доступа прикладного уровня других протоколов, необходимых системе безопасности и при работе сетевых администраторов. В действительности GSP обеспечивает работу межсетевых экранов прикладного уровня в качестве экранов с пакетной фильтрацией.

АНАЛИЗ ЗАЩИЩЕННОСТИ

Сервис **анализа защищенности** предназначен для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить (и устранить) пробелы в защите раньше, чем их сможет использовать злоумышленник. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а "оперативные" бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Системы анализа защищенности (называемые также **сканерами защищенности**) основаны на накоплении и использовании знаний. В данном случае имеются в виду знания о пробелах в защите: о том, как их искать, насколько они серьезны и как их устранять.

Соответственно, ядром таких систем является **база уязвимых мест**, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.

АНАЛИЗ ЗАЩИЩЕННОСТИ

В принципе, могут выявляться бреши самой разной природы: наличие вредоносного ПО (в частности, вирусов), слабые пароли пользователей, неудачно сконфигурированные операционные системы, небезопасные сетевые сервисы, неустановленные заплаты, уязвимости в приложениях и т.д. Однако наиболее эффективными являются **сетевые сканеры** (очевидно, в силу доминирования семейства протоколов TCP/IP), а также антивирусные средства.

Антивирусную защиту мы причисляем к средствам анализа защищенности, не считая ее отдельным сервисом безопасности. Сканеры могут выявлять уязвимые места как путем пассивного анализа, то есть изучения конфигурационных файлов, задействованных портов и т.п., так и путем имитации действий атакующего. Некоторые найденные уязвимые места могут устраняться автоматически (например, лечение зараженных файлов), о других сообщается администратору.

Системы анализа защищенности снабжены **автообнаружением** компонентов анализируемой ИС и графическим интерфейсом (помогающим, в частности, эффективно работать с протоколом сканирования).

АНАЛИЗ ЗАЩИЩЕННОСТИ

Контроль, обеспечиваемый системами анализа защищенности, носит реактивный, запаздывающий характер, он не защищает от новых атак, однако следует помнить, что оборона должна быть эшелонированной, и в качестве одного из рубежей контроль защищенности вполне адекватен. Подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные бреши в защите годами остаются неустраненными.

19. Обеспечение высокой доступности, туннелированные и управление – функции и назначение, роль в обеспечении информационной безопасности.

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

Доступность системы в общем случае достигается за счет применения трех групп мер, направленных на повышение:

1)БЕЗОТКАЗНОСТИ (под этим понимается минимизация вероятности возникновения какого-либо отказа);

2)ОТКАЗОУСТОЙЧИВОСТИ(способности к нейтрализации отказов, "живучести", то есть способности сохранять требуемую эффективность, несмотря на отказы отдельных компонентов);

3)ОБСЛУЖИВАЕМОСТИ (под обслуживаемостью понимается минимизация времени простоя отказавших компонентов, а также отрицательного влияния ремонтных работ на эффективность информационных сервисов, то есть быстрое и безопасное восстановление после отказов).

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

ОБЕСПЕЧЕНИЕ БЕЗОТКАЗНОСТИ:

1)Проактивное управление, базирующееся на постоянном сборе и анализе информации о функционировании ИС. Для реализации этого процесса целесообразно применять программное обеспечение, построенное в архитектуре менеджер-агент и ориентированное на поддержку распределенных разнородных конфигураций. В качестве претендентов на эту роль можно указать семейства продуктов Solstice (Solstice Enterprise Manager и ассоциированные продукты) компании SunSoft и OpenView компании Hewlett-Packard. Одним из важных достоинств этих решений является возможность дублирования центра управления.(информация, которая собирается в центре управления, не должна ограничиваться чисто компьютерными параметрами. Не менее важны параметры окружающей среды, такие как качество электропитания, температура и влажность в серверной комнате. Например, выход из строя кондиционера, если не предпринять немедленных мер, может повести к серьезным авариям вычислительной техники.)

2)Системы управления допускают **задание программируемых реакций** на определенные события, такие как выход отслеживаемого параметра за допустимые пределы. Данная возможность автоматизации анализа регистрационной информации должна использоваться максимально широко. (По результатам анализа может быть принято решение об оптимизации ИС, об установке дополнительного оборудования или о ремонте компонентов, работающих неустойчиво.)

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

3)Централизованное резервное копирование, в том числе для клиентским рабочих мест, проводимое в соответствии с утвержденным расписанием, повышает доступность данных. Перечисленные интегрирующие окружения позволяют единообразно осуществлять копирование с автоматическим учетом специфики обслуживаемых сервисов (например, СУБД) без необходимости приостанавливать последние, но с сохранением целостности информации.

4)Балансировка загрузки, ее равномерное распределение по наличным ресурсам, является еще одним важным инструментом повышения безотказности. Избегать пиковых нагрузок — значит продлить срок службы оборудования и уменьшить вероятность проявления программных ошибок.

5)Консультационная служба является средством повышения безотказности работы пользователей, а также обслуживающего персонала.

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

ОБЕСПЕЧЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ:

Основным средством повышения "живучести" является внесение избыточности в конфигурацию аппаратных и программных средств, поддерживающей инфраструктуры и персонала, **резервирование** технических средств и **тиражирование** информационных ресурсов (программ и данных).

Меры по обеспечению отказоустойчивости можно разделить на **локальные** и **распределенные**. **Локальные меры** направлены на достижение "живучести" отдельных компьютерных систем или их аппаратных и программных компонентов (в первую очередь с целью нейтрализации внутренних отказов ИС). Типичные примеры подобных мер – использование кластерных конфигураций в качестве платформы критичных серверов или "горячее" резервирование активного сетевого оборудования с автоматическим переключением на резерв. Если в число рассматриваемых рисков входят серьезные аварии поддерживающей инфраструктуры, приводящие к выходу из строя производственной площадки организации, следует предусмотреть **распределенные меры** обеспечения живучести, такие как создание или аренда резервного вычислительного центра. При этом, помимо дублирования и/или тиражирования ресурсов, необходимо предусмотреть средства автоматического или быстрого ручного переконфигурирования компонентов ИС, чтобы обеспечить переключение с основной площадки на резервную.

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

Выделяют следующие классы тиражирования (резервирования):

Симметричное/асимметричное. Тиражирование называется симметричным, если все серверы, предоставляющие данный сервис, могут изменять принадлежащую им информацию и передавать изменения другим серверам. В противном случае тиражирование называется асимметричным.

Синхронное/асинхронное. Тиражирование называется синхронным, если изменение передается всем экземплярам сервиса в рамках одной распределенной транзакции. В противном случае тиражирование называется асинхронным.

Осуществляемое средствами сервиса, хранящего информацию/**внешними средствами**.

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

Асимметричное тиражирование теоретически проще симметричного, поэтому целесообразно выбрать асимметрию.

Труднее всего выбрать между **синхронным** и **асинхронным тиражированием**. **Синхронное** идейно проще, но его реализация может быть тяжеловесной и сложной, хотя это внутренняя сложность сервиса, невидимая для приложений. **Асинхронное тиражирование** устойчивее к отказам в сети, оно меньше влияет на работу основного сервиса.

Чем надежнее связь между серверами, вовлеченными в процесс тиражирования, чем меньше время, отводимое на переключение с основного сервера на резервный, чем жестче требования к актуальности информации, тем более предпочтительным оказывается **синхронное тиражирование**.

С другой стороны, недостатки **асинхронного тиражирования** могут компенсироваться процедурными и программными мерами, направленными на контроль целостности информации в распределенной ИС. Сервисы, входящие в состав ИС, в состоянии обеспечить ведение и хранение журналов транзакций, с помощью которых можно выявлять операции, утерянные при переключении на резервный сервер. Даже в условиях неустойчивой связи с удаленными филиалами организации подобная проверка в фоновом режиме займет не более нескольких часов, поэтому **асинхронное тиражирование** может использоваться практически в любой ИС.

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

Асинхронное тиражирование может производиться на сервер, работающий в режиме "горячего" резерва, возможно, даже обслуживающего часть пользовательских запросов, или на сервер, работающий в режиме "теплого" резерва, когда изменения периодически "накатываются", но сам резервный сервер запросов не обслуживает.

Достоинство "теплого" резервирования в том, что его можно реализовать, оказывая меньшее влияние на основной сервер. Это влияние вообще может быть сведено к нулю, если асинхронное тиражирование осуществляется путем передачи инкрементальных копий с основного сервера (резервное копирование необходимо выполнять в любом случае).

Основной недостаток "теплого" резерва состоит в длительном времени включения, что может быть неприемлемо для "тяжелых" серверов, таких как кластерная конфигурация сервера СУБД. Здесь необходимо проводить измерения в условиях, близких к реальным.

Второй недостаток "теплого" резерва вытекает из опасности малых изменений. Может оказаться, что в самый нужный момент срочный перевод резерва в штатный режим невозможен.

Учитывая приведенные соображения, следует в первую очередь рассматривать возможность **"горячего" резервирования**, либо тщательно контролировать использование **"теплого" резерва** и регулярно (не реже одного раза в неделю) проводить пробные переключения резерва в "горячий" режим.

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

ОБЕСПЕЧЕНИЕ ОБСЛУЖИВАЕМОСТИ:

Меры по обеспечению **обслуживаемости** направлены на снижение сроков диагностирования и устранения отказов и их последствий.

Для обеспечения обслуживаемости рекомендуется соблюдать следующие архитектурные принципы:

1)ориентация на построение информационной системы из унифицированных компонентов с целью упрощения замены отказавших частей;

2)ориентация на решения **модульной** структуры с возможностью **автоматического обнаружения** отказов, **динамического переконфигурирования** аппаратных и программных средств и **замены** отказавших **компонентов в "горячем" режиме**.

Динамическое переконфигурирование преследует две основные цели:
изоляция отказавших компонентов;
сохранение работоспособности сервисов.

Изолированные компоненты образуют зону поражения реализованной угрозы. Чем меньше соответствующая зона риска, тем выше обслуживаемость сервисов. Так, при отказах блоков питания, вентиляторов и/или дисков в современных серверах зона риска ограничивается отказавшим компонентом; при отказах процессорных модулей весь сервер может потребовать перезагрузки (что способно вызвать дальнейшее расширение зоны риска)

ОБЕСПЕЧЕНИЕ ВЫСОКОЙ ДОСТУПНОСТИ

Возможность программирования реакции на отказ также повышает **обслуживаемость систем**. Каждая организация может выбрать свою стратегию реагирования на отказы тех или иных аппаратных и программных компонентов и автоматизировать эту реакцию.

Возможность удаленного выполнения административных действий – важное направление повышения **обслуживаемости**, поскольку при этом ускоряется начало восстановительных мероприятий, а в идеале все работы (обычно связанные с обслуживанием программных компонентов) выполняются в удаленном режиме, без перемещения квалифицированного персонала, то есть с высоким качеством и в кратчайшие сроки.

Существенный аспект повышения обслуживаемости – организация консультационной службы для пользователей (**обслуживаемость пользователей**), внедрение программных систем для работы этой службы, обеспечение достаточной пропускной способности каналов связи с пользователями, в том числе в режиме пиковых нагрузок.

ТУННЕЛИРОВАНИЕ

Туннелирование следует рассматривать как самостоятельный сервис безопасности. Его суть состоит в том, чтобы "упаковать" передаваемую порцию данных, вместе со служебными полями, в новый "конверт". В качестве синонимов термина "туннелирование" могут использоваться "конвертование" и "обертывание".

Туннелирование может применяться для нескольких целей:

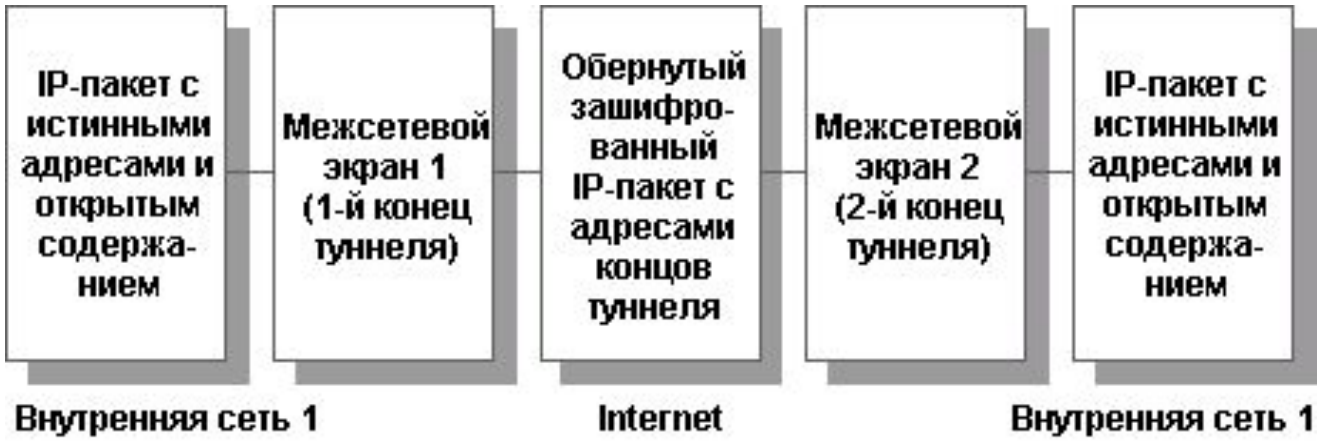
1)передачи через сеть пакетов, принадлежащих протоколу, который в данной сети не поддерживается (например, передача пакетов IPv6 через старые сети, поддерживающие только IPv4);

2)обеспечения слабой формы конфиденциальности (в первую очередь конфиденциальности трафика) за счет сокрытия истинных адресов и другой служебной информации;

3)обеспечения конфиденциальности и целостности передаваемых данных при использовании вместе с криптографическими сервисами.

ТУННЕЛИРОВАНИЕ

Комбинация **туннелирования** и **шифрования** (наряду с необходимой криптографической инфраструктурой) на выделенных шлюзах и экранирования на маршрутизаторах поставщиков сетевых услуг (для разделения пространств "своих" и "чужих" сетевых адресов в духе виртуальных локальных сетей) позволяет реализовать такое важное в современных условиях защитное средство, как виртуальные частные сети. Подобные сети, наложенные обычно поверх Internet, существенно дешевле и гораздо безопаснее, чем собственные сети организации, построенные на выделенных каналах.



Концами туннелей, помимо корпоративных межсетевых экранов, могут быть мобильные компьютеры сотрудников.

УПРАВЛЕНИЕ

Управление – интегрирующая оболочка информационных сервисов и сервисов безопасности (в том числе средств обеспечения высокой доступности), обеспечивающую их нормальное, согласованное функционирование под контролем администратора ИС.

Управление подразделяется на:
1) мониторинг компонентов;
2) контроль (то есть выдачу и реализацию управляющих воздействий);
3) координацию работы компонентов системы.

Системы управления *должны*:
1)позволять администраторам планировать, организовывать, контролировать и 2)учитывать использование информационных сервисов;
3)давать возможность отвечать на изменение требований;
4)обеспечивать предсказуемое поведение информационных сервисов;
5)обеспечивать защиту информации.

УПРАВЛЕНИЕ

Пять функциональных областей **управления**:

1) управление конфигурацией (установка параметров для нормального функционирования, запуск и остановка компонентов, сбор информации о текущем состоянии системы, прием извещений о существенных изменениях в условиях функционирования, изменение конфигурации системы);

2) управление отказами (выявление отказов, их изоляция и восстановление работоспособности системы);

3) управление производительностью (сбор и анализ статистической информации, определение производительности системы в штатных и нештатных условиях, изменение режима работы системы);

4) управление безопасностью (реализация политики безопасности путем создания, удаления и изменения сервисов и механизмов безопасности, распространения соответствующей информации и реагирования на инциденты);

5) управление учетной информацией (т.е. взимание платы за пользование ресурсами).

УПРАВЛЕНИЕ

Системы управления распределенными ИС строятся в архитектуре **менеджер/агент**. Агент (как программная модель управляемого объекта) выполняет управляющие действия и порождает (при возникновении определенных событий) извещения от его имени. В свою очередь, менеджер выдает агентам команды на управляющие воздействия и получает извещения.

Иерархия взаимодействующих менеджеров и агентов может иметь несколько уровней. При этом элементы промежуточных уровней играют двоякую роль: по отношению к вышестоящим элементам они являются агентами, а к нижестоящим – менеджерами. **Многоуровневая архитектура** менеджер/агент – ключ к распределенному, масштабируемому управлению большими системами.

Обязательным элементом при любом числе архитектурных уровней является **управляющая консоль**.

УПРАВЛЕНИЕ

К числу концептуально важных можно отнести понятие **"проактивного"**, то есть **упреждающего управления**. Упреждающее управление основано на предсказании поведения системы на основе текущих данных и ранее накопленной информации. Простейший пример подобного управления – выдача сигнала о возможных проблемах с диском после серии программно-нейтрализуемых ошибок чтения/записи. В более сложном случае определенный характер рабочей нагрузки и действий пользователей может предшествовать резкому замедлению работы системы; адекватным управляющим воздействием могло бы стать понижение приоритетов некоторых заданий и извещение администратора о приближении кризиса.

Системы управления должны уметь эволюционировать, причем разные её компоненты могут делать это с разной скоростью. Никакая жесткая, монолитная система такого не выдержит.
Единственный выход – наличие **каркаса**, с которого можно снимать старое и "навешивать" новое, не теряя эффективности управления.

УПРАВЛЕНИЕ

Каркас как самостоятельный продукт необходим для достижения по крайней мере следующих целей:

1)сглаживание разнородности управляемых информационных систем,

2(предоставление унифицированных программных интерфейсов для быстрой разработки управляющих приложений;

3)создание инфраструктуры управления, обеспечивающей наличие таких свойств, как поддержка распределенных конфигураций, масштабируемость, информационная безопасность и т.д.;

4)предоставление функционально полезных универсальных сервисов, таких как планирование заданий, генерация отчетов и т.п.

Вопросы 20-22:

20.Понятие атаки на систему информационной безопасности. Классификация основных видов атак (локальные атаки, удаленные атаки, атаки на каналы передачи данных).

Автор: Корнийчук Олег
Группа: ИТ-10-01

20.Понятие атаки на систему информационной безопасности. Классификация основных видов атак (локальные атаки, удаленные атаки, атаки на каналы передачи данных).

- Атака - любое действие, нарушающее безопасность информационной системы. Более формально можно сказать, что атака - это действие или последовательность связанных между собой действий, использующих уязвимости данной информационной системы и приводящих к нарушению политики безопасности.
- Локальные атаки (источником данного вида атак являются пользователи и/или программы локальной системы);
- Удаленные атаки (источником атаки выступают удаленные пользователи, сервисы или приложения)

- Классификация сетевых атак
- В общем случае существует информационный поток от отправителя (файл, пользователь, компьютер) к получателю (файл, пользователь, компьютер):

- Все атаки можно разделить на два класса: пассивные и активные.

- I. Пассивная атака
- Пассивной называется такая атака, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

- II. Активная атака
- Активной называется такая атака, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают следующие типы активных атак:
- Отказ в обслуживании - DoS-атака (Denial of Service)
- Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. Противник может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной атаки является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных клиентов. Классическим примером такой атаки в сетях TCP/IP является SYN-атака, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения. В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.

- Модификация потока данных - атака "man in the middle"
- Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

- Создание ложного потока (фальсификация)
- Фальсификация (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого.

- Повторное использование
- Повторное использование означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая replay-атака. На самом деле replay-атаки являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов атаки для получения несанкционированного доступа, его часто рассматривают как отдельный тип атаки.

- Перечисленные атаки могут существовать в любых типах сетей, а не только в сетях, использующих в качестве транспорта протоколы TCP/IP, и на любом уровне модели OSI. Но в сетях, построенных на основе TCP/IP, атаки встречаются чаще всего, потому что, во-первых, Internet стал самой распространенной сетью, а во-вторых, при разработке протоколов TCP/IP требования безопасности никак не учитывались.

21. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.

- **Вирус** - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управление
- В настоящее время известно более 70000 компьютерных вирусов, их можно классифицировать по следующим признакам:

- **В зависимости от среды** обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.
- **По способу заражения** вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

- **По степени воздействия** вирусы можно разделить на следующие виды:
- неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
- опасные вирусы, которые могут привести к различным нарушениям в работе компьютера
- очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.
- **По особенностям алгоритма** вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии, распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

- **Методы борьбы с вирусами**
- Способы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса; способы обнаружения и удаления неизвестного вируса.
- Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов.
- Следует также обратить внимание на несколько терминов, применяемых при обсуждении антивирусных программ:

- **“Ложное срабатывание”** (False positive) — детектирование вируса в незараженном объекте (файле, секторе или системной памяти). Обратный термин — “False negative”, т.е. недетектирование вируса в зараженном объекте.
- **“Сканирование по запросу”** (“on-demand”) — поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания (system scheduler).
- **“Сканирование на-лету”** (“real-time”, “on-the-fly”) — постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т.п.). В этом режиме антивирус постоянно активен, он присутствует в памяти “резидентно” и проверяет объекты без запроса пользователя.

- **Классификация Антивирусов**
- **Сканеры**
- Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые “маски”. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.
- К достоинствам сканеров всех типов относится их универсальность, к недостаткам — размеры антивирусных баз, которые сканерам приходится “таскать за собой”, и относительно небольшую скорость поиска вирусов.

- **CRC-сканеры**
- Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.
- CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту “слабость” CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них.

- **Блокировщики**
- Антивирусные блокировщики — это резидентные программы, перехватывающие “вирусо-опасные” ситуации и сообщающие об этом пользователю. К “вирусо-опасным” относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения.
- К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно “выползает неизвестно откуда”. К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний.

- **Иммунизаторы**
- Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса. Первые обычно записываются в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у таких иммунизаторов всего один, но он летален: абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время.
- Второй тип иммунизации защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные (пример — печально известная строка “MsDos”, предохраняющая от ископаемого вируса “Jerusalem”). Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске вирус натыкается на нее и считает, что система уже заражена.
- Такой тип иммунизации не может быть универсальним, поскольку нельзя иммунизировать файлы от всех известных вирусов: одни вирусы считают уже зараженными файлы, если время создания файла содержит метку 62 секунды, а другие — 60 секунд. Однако несмотря на это, подобные иммунизаторы в качестве полумеры могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

22. Понятие системы информационной безопасности, ее цели состав.

- Система информационной безопасности - это функционирующая как единое целое совокупность организаций, используемых этими организациями в своей деятельности средств, проводимых ими в рамках своей деятельности мероприятий, и применяемых ими при проведении мероприятий методов, устремленная на ликвидацию внутренних и внешних угроз жизненно важным интересам субъекта безопасности, создание, поддержание и развитие состояния защищенности его информационной среды.

- Цели : централизация управления и контроль над всеми службами и системами информационной безопасности, гибкое распределение уровней доступа и управления,
- минимизация рисков для объекта в целом и всех подразделений,
- возможность дистанционного мониторинга и управления средствами и системами интегрированной системы безопасности,
- регистрация всех событий и инцидентов в реальном времени, осуществление анализа и обеспечение комплексного аудита действий автоматики и персонала во внештатных ситуациях, анализ данных с целью предотвращения внештатных ситуаций,
- обеспечение взаимодействия в режиме реального времени за счет программирования логических связей между подсистемами,
- стандартизация, унификация и оптимизация информационно-управляющих ресурсов обеспечения безопасности всех связанных служб и подразделений.

- Состав: системы разграничения доступа к информации,
- системы аутентификации и авторизации,
- средства криптографической защиты информации,
- системы межсетевого экранирования,
- системы контроля электронной почты и web-трафика,
- системы резервного копирования и аварийного восстановления,
- системы сегментирования ЛВС (Локальная вычислительная сеть),
- системы антивирусной защиты информации,
- системы мониторинга и обнаружения/предотвращения вторжений,
- системы управления техническими средствами информационной безопасности.