Основы информационной безопасности

Лекция 1.

Введение

Литература

Понятие информационной безопасности

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл. Термин "**информационная безопасность**" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Понятие информационной безопасности

Под **информационной безопасностью** мы будем понимать 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.

Понятие информационной безопасности

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

Понятие 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). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Понятие информационной безопасности

Из этого положения можно вывести два важных следствия:

- Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором – "да нет у нас никаких секретов, лишь бы все работало".

Понятие информационной безопасности

- Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие.
- Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Понятие информационной системы

В *самом широком смысле* **информационная система** есть совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того, чтобы своевременно обеспечивать надлежащих людей надлежащей информацией.

Понятие информационной системы

информационная система - совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

Закон Республики Беларусь от 10.11.2008 N 455-З (ред. от 04.01.2014) "Об информации, информатизации и защите информации"

Понятие информационной системы

Существуют классификации ИС по

- характеру использования информации (информационно-поисковые системы , информационно-аналитические системы , информационно-решающие системы)
- архитектуре (настольные, распределённые)
- сфере применения (экономическая, медицинская, географическая)
- масштабности (персональная, групповая, корпоративная)

Понятие информационной безопасности

Термин "**компьютерная безопасность**" (как эквивалент или заменитель ИБ) представляется нам слишком узким.

Компьютеры – только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую очередь на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на "горчичнике", прилепленном к монитору).

Понятие информационной безопасности

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы

- электро-, водо- и теплоснабжения,
- кондиционеры,
- средства коммуникаций и, конечно,
- обслуживающий персонал.

Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Понятие информационной безопасности

Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя.

Иногда таким недопустимым **ущербом** является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений.

Основные составляющие информационной безопасности

Информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только системный, комплексный подход.

Можно выделить основные составляющие информационной безопасности: обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и поддерживающей инфраструктуры.

Основные составляющие информационной безопасности

Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но, на наш взгляд, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Поясним понятия доступности, целостности и конфиденциальности.

Основные составляющие информационной безопасности

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Под **целостностью** подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Основные составляющие информационной безопасности

конфиденциальность информации - требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь;

Закон Республики Беларусь от 10.11.2008 N 455-З (ред. от 04.01.2014) "Об информации, информатизации и защите информации"

Основные составляющие информационной безопасности

доступ к информации - возможность получения информации и пользования ею;

доступ к информационной системе и (или) информационной сети - возможность использования информационной системы и (или) информационной сети;

Закон Республики Беларусь от 10.11.2008 N 455-З (ред. от 04.01.2014) "Об информации, информатизации и защите информации"

Основные составляющие информационной безопасности

Обеспечение целостности и сохранности информации, содержащейся в государственных информационных системах, осуществляется путем установления и соблюдения единых требований по защите информации от неправомерного доступа, уничтожения, модификации (изменения) и блокирования правомерного доступа к ней, в том числе при осуществлении доступа к информационным сетям.

Закон Республики Беларусь от 10.11.2008 N 455-З (ред. от 04.01.2014) "Об информации, информатизации и защите информации"

Термины и определения

подлинность электронного документа - свойство электронного документа, определяющее, что электронный документ подписан действительной электронной цифровой подписью (электронными цифровыми подписями);

подлинный электронный документ - электронный документ, целостность и подлинность которого подтверждаются с применением сертифицированного средства электронной цифровой подписи, использующего при проверке электронной цифровой подписи открытые ключи лица (лиц), подписавшего (подписавших) электронный документ;

Основные составляющие информационной безопасности

Информационные системы создаются (приобретаются) для получения определенных информационных услуг.

Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит **ущерб** всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Основные составляющие информационной безопасности

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Основные составляющие информационной безопасности

Целостность можно подразделить на **статическую** (понимаемую как неизменность информационных объектов) и **динамическую** (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Основные составляющие информационной безопасности

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит "руководством к действию". Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным.

Основные составляющие информационной безопасности

Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации.

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается у нас на серьезные трудности.

Основные составляющие информационной безопасности

- Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках.
- Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Основные составляющие информационной безопасности

Если вернуться к анализу интересов различных категорий субъектов информационных отношений, то почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность – какой смысл в информационной услуге, если она содержит искаженные сведения?

Основные составляющие информационной безопасности

Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими примерами.

Важность и сложность проблемы информационной безопасности

В **Доктрине информационной безопасности Российской Федерации** (здесь, подчеркнем, термин "информационная безопасность" используется в широком смысле) защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.

Важность и сложность проблемы информационной безопасности

Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (Government Computer News, июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники.

Важность и сложность проблемы информационной безопасности

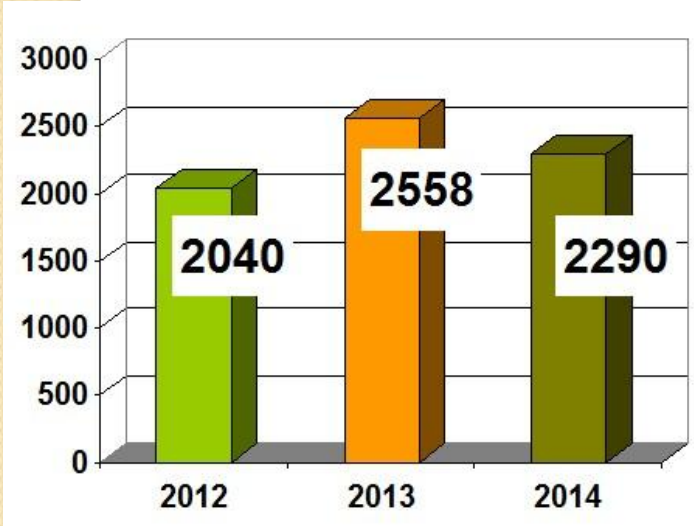
Двух тезок перепутали в банке (Республика Беларусь, 2015) и выдали им карточки друг друга. Хотя у каждого клиента там есть свой номер счета, к которому прикрепляются именные карточки.

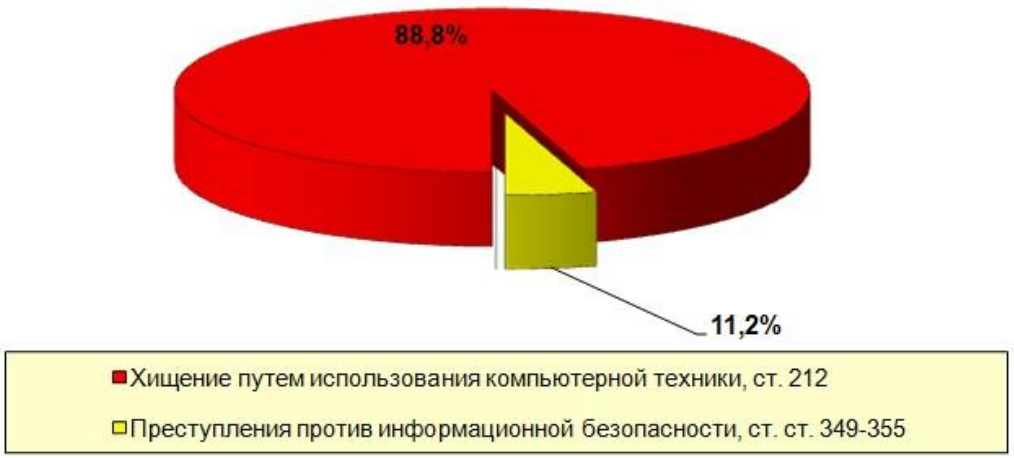
Из-за того, что в банке перепутали карточки, выданные двум тезкам, один из клиентов долгое время не мог понять, куда уходят его деньги, а милиция проверяла самые невероятные версии.

Важность и сложность проблемы информационной безопасности

За 12 месяцев 2014 года число выявленных преступлений в сфере высоких технологий в РБ составило 2290 преступлений

http://mvd.gov.by/ru/main.aspx?guid=3311





Меры по защите информации

защита информации - комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

(в ред. Закона Республики Беларусь от 04.01.2014 N 102-З)

Меры по защите информации

Введем следующие средства:

- законодательные меры обеспечения информационной безопасности;
- административные меры (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурные меры (меры безопасности, ориентированные на людей);
- программно-технические меры.

Меры по защите информации

К правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

Меры по защите информации

К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

Меры по защите информации

К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации.

Безопасность информационных систем

Объектом нашего рассмотрения является Автоматизированная система обработки информации (АСОИ) или корпоративная (компьютерно-коммуникационная) информационная система (КИС),

Безопасность информационных систем

которая представляет собой совокупность:

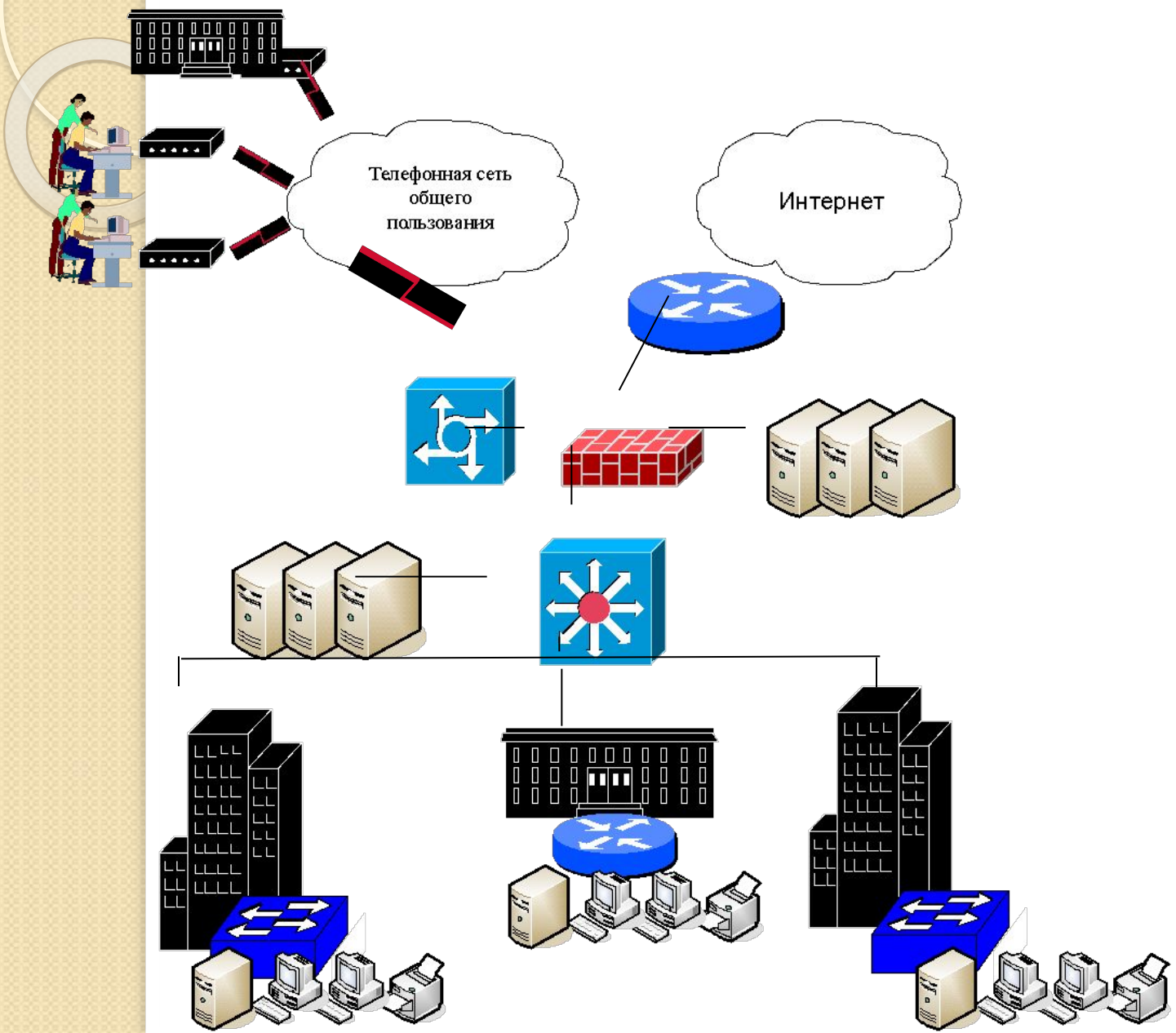
- средств вычислительной и коммуникационной техники,
- программного обеспечения,
- каналов связи,
- информации на различных носителях,
- технологий и правил,
- персонала и пользователей системы.

Безопасность информационных систем

Корпоративная сеть организации – это территориально распределенный аппаратно-программный комплекс, который предназначен для предоставления информационных и телекоммуникационных услуг сотрудникам организации

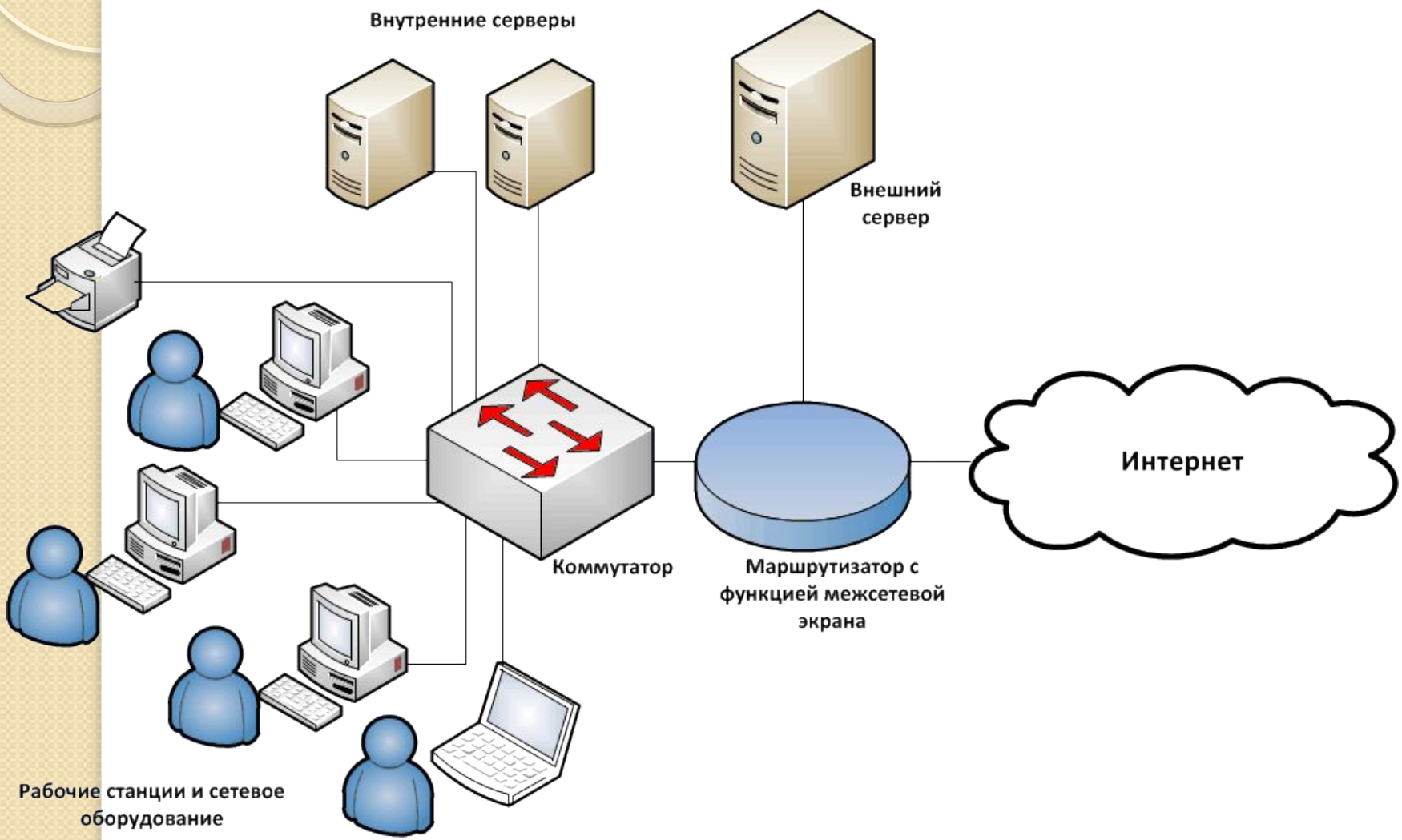
Задачей корпоративной сети является обеспечение единого информационного пространства в рамках организации

Сеть организации



- Зона подключения к сетям общего пользования - Интернет;
- Зона подключения абонентов по коммутируемым линиям связи;
- Зона расположения внешних серверов;
- Зона расположения внутренних корпоративных серверов ;
- Зона расположения локальной сети

Безопасность информационных систем



Уровни информационной инфраструктуры

- уровень персонала
- уровень приложений
- уровень СУБД
- уровень ОС
- уровень сети

Уровень сети

Каналы связи

- оптические
- витая пара
- медь
- радиоволны

Технологии канального уровня

- Ethernet/FastEthernet/Gigabit Ethernet
- ATM
- ADSL
- IEEE 802.11

Уровень сети

Сетевые устройства

- коммутаторы
- маршрутизаторы
- специализированные устройства
- компьютеры

Протоколы

- Стек OSI
- Стек TCP/IP
- Стек IPX/SPX
- Стек NetBIOS/SMB

Другие уровни

Уровень ОС

- Windows
- Unix
- NetWare

Уровень СУБД

- MS SQL
- Oracle

Уровень приложений

- Web
- E-mail

Уровень пользователей

- Администраторы
- Пользователи

Актуальность проблемы защиты информации в корпоративных сетях

- Современные уровни и темпы развития средств информационной безопасности значительно отстают от уровней и темпов развития информационных технологий.
- Высокие темпы роста парка персональных компьютеров, применяемых в разнообразных сферах человеческой деятельности.
- Резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных.
- Значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютерных сетей.
- Многочисленные уязвимости в программных и сетевых платформах.

Безопасность информационных систем

- Бурное развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.
- Современные методы накопления, обработки и передачи информации способствовали появлению угроз, связанных с возможностью *потери*, *искажения* и *раскрытия* данных, адресованных или принадлежащих конечным пользователям.
- Низкая квалификация конечных пользователей в вопросах потенциальных угроз при работе в локальных сетях и глобальной сети Интернет.

Стек протоколов TCP\IP

Transmission Control Protocol/Internet Protocol (TCP/IP) - это промышленный стандарт стека протоколов, разработанный для глобальных сетей.

Лидирующая роль стека TCP/IP объясняется следующими его свойствами:

- Это наиболее завершенный стандартный и в то же время популярный стек сетевых протоколов, имеющий многолетнюю историю.
- Почти все большие сети передают основную часть своего трафика с помощью протокола TCP/IP.
- Это метод получения доступа к сети Internet.
- Этот стек служит основой для создания intranet- корпоративной сети, использующей транспортные услуги Internet и гипертекстовую технологию WWW, разработанную в Internet.
- Все современные операционные системы поддерживают стек TCP/IP.
- Это гибкая технология для соединения разнородных систем как на уровне транспортных подсистем, так и на уровне прикладных сервисов.
- Это устойчивая масштабируемая межплатформенная среда для приложений клиент-сервер.