

ПРОБЛЕМА БЕЗОПАСНОСТИ В СЕТЯХ



Гончаров Сергей Леонидович
Старший преподаватель



ОСНОВНЫЕ ПОНЯТИЯ БЕЗОПАСНОСТИ



Конфиденциальность

(confidentiality) — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).

Доступность

(availability) — гарантия того, что авторизованные пользователи всегда получают доступ к данным.

Целостность

(integrity) — гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.



КЛАССИФИКАЦИЯ УГРОЗ



Незаконное проникновение

- ❖ может быть реализовано через уязвимые места в системе безопасности с использованием недокументированных возможностей операционной системы.
 - Использование «чужих» паролей, полученных путем подглядывания, расшифровки файла паролей, подбора паролей или получения пароля путем анализа сетевого трафика. Важно, чтобы все пользователи сети сохраняли свои пароли в тайне, а также выбирали их так, чтобы максимально затруднить угадывание.
 - Еще один способ получения пароля — это внедрение в чужой компьютер «троянского коня». В частности, такого рода программа может считывать коды пароля, вводимого пользователем во время логического входа в систему.



Разрушение системы с помощью программ-вирусов

- ❖ Отличительной особенностью таких программ является способность «заражать» другие файлы, внедряя в них свои собственные копии.
- ❖ Чаще всего вирусы поражают исполняемые файлы.
- ❖ Когда такой исполняемый код загружается в оперативную память для выполнения, вместе с ним получает возможность исполнить свои вредительские действия вирус.
- ❖ Вирусы могут привести к повреждению или даже полной утрате информации.



Нелегальные действия легального пользователя

- этот тип угроз исходит от легальных пользователей сети, которые, используя свои полномочия, пытаются выполнять действия, выходящие за рамки их должностных обязанностей.
- ❖ Например, администратор сети имеет практически неограниченные права на доступ ко всем сетевым ресурсам.
- ❖ Однако на предприятии может быть информация, доступ к которой администратору сети запрещен.
- ❖ Нелегальные действия может попытаться предпринять и обычный пользователь сети.
- ❖ Существующая статистика говорит о том, что едва ли не половина всех попыток нарушения безопасности системы исходит от сотрудников предприятия, которые как раз и являются легальными пользователями сети.



«Подслушивание» внутри сетевого трафика

- это незаконный мониторинг сети, захват и анализ сетевых сообщений.
- ❖ Существует много доступных программных и аппаратных анализаторов трафика, которые делают эту задачу достаточно тривиальной.
- ❖ Еще более усложняется защита от этого типа угроз в сетях с глобальными связями.
- ❖ Глобальные связи, простирающиеся на десятки и тысячи километров, по своей природе являются менее защищенными, чем локальные связи.
- ❖ Такая опасность одинаково присуща всем видам территориальных каналов связи и никак не зависит от того, используются собственные, арендуемые каналы или услуги общедоступных территориальных сетей, подобных Интернету.



ВЫБОР СТРАТЕГИИ ЗАЩИТЫ ДАННЫХ

Системный подход к обеспечению безопасности





Морально-этические средства

- ❖ К морально-этическим средствам защиты можно отнести всевозможные нормы, которые сложились по мере распространения вычислительных средств в той или иной стране.
- ❖ Например, подобно тому как в борьбе против пиратского копирования программ в настоящее время в основном используются меры воспитательного плана, необходимо внедрять в сознание людей аморальность всяческих покушений на нарушение конфиденциальности, целостности и доступности чужих информационных ресурсов.



Законодательные средства защиты

- это законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации ограниченного доступа, а также вводятся меры ответственности за нарушения этих правил.
- ❖ Правовая регламентация деятельности в области защиты информации имеет целью защиту информации, составляющей государственную тайну, обеспечение прав потребителей на получение качественных продуктов, защиту конституционных прав граждан на сохранение личной тайны, борьбу с организованной преступностью.



Административные меры

- это действия, предпринимаемые руководством предприятия или организации для обеспечения информационной безопасности.
- ❖ К таким мерам относятся конкретные правила работы сотрудников предприятия, например режим работы сотрудников, их должностные инструкции, строго определяющие порядок работы с конфиденциальной информацией на компьютере.
- ❖ К административным мерам также относятся правила приобретения предприятием средств безопасности.



Психологические меры

безопасности могут играть значительную роль в укреплении безопасности системы.

- ❖ Пренебрежение учетом психологических моментов в неформальных процедурах, связанных с безопасностью, может привести к нарушениям защиты.
- ❖ Время от времени пользователи должны менять пароли (обычная практика для предотвращения их подбора).
- ❖ В таких условиях злоумышленник может позвонить администратору по телефону и от имени легального пользователя попыбовать получить пароль.

Физические средства

- ❖ К *физическим* средствам защиты относятся экранирование помещений для защиты от излучения, проверка поставляемой аппаратуры на соответствие ее спецификациям и отсутствие аппаратных «жучков», средства наружного наблюдения, устройства, блокирующие физический доступ к отдельным блокам компьютера, различные замки и другое оборудование, защищающие помещения, где находятся носители информации, от незаконного проникновения и т. д. и т. п.

Технические средства

информационной безопасности реализуются программным и аппаратным обеспечением вычислительных сетей.

- ❖ Такие средства, называемые также службами сетевой безопасности, решают самые разнообразные задачи по защите системы, например контроль доступа, включающий процедуры аутентификации и авторизации, аудит, шифрование информации, антивирусную защиту, контроль сетевого трафика и много других задач.
- ❖ Технические средства безопасности могут быть либо встроены в программное (операционные системы и приложения) и аппаратное (компьютеры и коммуникационное оборудование) обеспечение сети, либо реализованы в виде отдельных продуктов, созданных специально для решения проблем безопасности.

Принципы политики безопасности





Минимальный уровень привилегий

- ❖ Одним из таких принципов является предоставление каждому сотруднику предприятия того *минимально уровня привилегий* на доступ к данным, который необходим ему для выполнения его должностных обязанностей.
- ❖ Ввести четкие ограничения для всех пользователей сети, не наделяя их излишними возможностями.



Комплексный подход

- ❖ Следующий принцип — использование *комплексного подхода* к обеспечению безопасности.
- ❖ Чтобы затруднить злоумышленнику доступ к данным, необходимо предусмотреть самые разные средства безопасности, начиная с организационно-административных запретов и кончая встроенными средствами сетевой аппаратуры.
 - административный запрет па работу в воскресные дни ставит потенциального нарушителя под визуальный контроль администратора и других пользователей,
 - физические средства защиты (закрытые помещения, блокировочные ключи) ограничивают непосредственный контакт пользователя только приписанным ему компьютером,
 - строенные средства сетевой ОС (система аутентификации и авторизации) предотвращают вход в сеть нелегальных пользователей, а для легального пользователя ограничивают возможности только разрешенными для него операциями (подсистема аудита фиксирует его действия).



Баланс надежности защиты всех уровней

- ❖ Используя многоуровневую систему защиты, важно обеспечивать *баланс надежности защиты всех уровней*.
 - Если в сети все сообщения шифруются, но ключи легкодоступны, то эффект от шифрования нулевой.
 - Если на компьютерах установлена файловая система, поддерживающая избирательный доступ на уровне отдельных файлов, но имеется возможность получить жесткий диск и установить его на другой машине, то все достоинства средств защиты файловой системы сводятся на нет.
 - Если внешний трафик сети, подключенной к Интернету, проходит через мощный брандмауэр, но пользователи имеют возможность связываться с узлами Интернета по коммутируемым линиям, используя локально установленные модемы, то деньги (как правило, немалые), потраченные на брандмауэр, можно считать выброшенными на ветер.



Максимальная защита

- ❖ Следующим универсальным принципом является использование средств, которые при отказе переходят в состояние *максимальной защиты*.
- ❖ Если, например, автоматический пропускной пункт в какое-либо помещение ломается, то он должен фиксироваться в таком положении, чтобы ни один человек не мог пройти на защищаемую территорию.
- ❖ А если в сети имеется устройство, которое анализирует весь входной трафик и отбрасывает кадры с определенным, заранее заданным обратным адресом, то при отказе оно должно полностью блокировать вход в сеть.



Принцип единого контрольно-пропускного пункта

- весь входящий во внутреннюю сеть и выходящий во внешнюю сеть трафик должен проходить через единственный узел сети, например через межсетевой экран (firewall).
- ❖ Только это позволяет в достаточной степени контролировать трафик.
- ❖ В противном случае, когда в сети имеется множество пользовательских станций, имеющих независимый выход во внешнюю сеть, очень трудно скоординировать правила, ограничивающие права пользователей внутренней сети по доступу к серверам внешней сети и обратно — права внешних клиентов по доступу к ресурсам внутренней сети.

Принцип баланса

- ❖ *Принцип баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение.*
- ❖ Ни одна система безопасности не гарантирует защиту данных на уровне 100%, поскольку является результатом компромисса между возможными рисками и возможными затратами.
- ❖ Определяя политику безопасности, администратор должен взвесить величину ущерба, которую может понести предприятие в результате нарушения защиты данных, и соотнести ее с величиной затрат, требуемых на обеспечение безопасности этих данных.
- ❖ Так, в некоторых случаях можно отказаться от дорогостоящего межсетевого экрана в пользу стандартных средств фильтрации обычного маршрутизатора, в других же можно пойти на беспрецедентные затраты.

Главное, чтобы принятое решение было обосновано экономически.

Политика доступа к сети





Политика доступа к сетевым службам Интернета

включает следующие пункты:

- Определение списка служб Интернета, к которым пользователи внутренней сети должны иметь ограниченный доступ.
- Определение ограничений на методы доступа, например на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничения методов доступа необходимы для того, чтобы пользователи не могли обращаться к «запрещенным» службам Интернета обходными путями.
- Принятие решения о том, разрешен ли доступ внешних пользователей из Интернета во внутреннюю сеть. Если да, то кому. Часто доступ разрешают только для некоторых, абсолютно необходимых для работы предприятия служб, например электронной почты.



Политика доступа к ресурсам внутренней сети

компания может быть выражена в одном из двух принципов:

- запрещать все, что не разрешено в явной форме;
- разрешать все, что не запрещено в явной форме.

Методы обеспечения безопасности





Шифрация (Шифрование)



Шифрация (Шифрование)

- ❖ *Шифрование* — это краеугольный камень всех служб информационной безопасности, будь то система аутентификации или авторизации, средства создания защищенного канала или способ безопасного хранения данных.

Криптосистема

- ❖ Пара процедур — шифрование и дешифрирование — называется *криптосистемой*.
- ❖ В современных алгоритмах шифрования предусматривается наличие параметра — *секретного ключа*.
- ❖ Сложность алгоритма раскрытия является одной из важных характеристик криптосистемы и называется *криптостойкостью*.



Аутентификация



Аутентификация

(authentication) предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей.

- ❖ Термин «аутентификация» в переводе с латинского означает «установление подлинности».



Аутентификация

- ❖ Аутентификацию следует отличать от *идентификации*. Идентификаторы пользователей используются в системе с теми же целями, что и идентификаторы любых других объектов, файлов, процессов, структур данных, но они не связаны непосредственно с обеспечением безопасности.
- ❖ Идентификация заключается в сообщении пользователем системе своего идентификатора, в то время как аутентификация — это процедура доказательства пользователем того, что он есть тот, за кого себя выдает, в частности, доказательство того, что именно ему принадлежит введенный им идентификатор.

Аутентификация

- ❖ В процедуре аутентификации участвуют две стороны:
 - одна сторона доказывает свою аутентичность, предъявляя некоторые доказательства,
 - а другая сторона — аутентификатор — проверяет эти доказательства и принимает решение.

Аутентификация

- ❖ В качестве доказательства аутентичности используются самые разнообразные приемы:
 - аутентифицируемый может продемонстрировать знание некоего общего для обеих сторон секрета: слова (пароля) или факта (даты и места события, прозвища человека и т. п.);
 - аутентифицируемый может продемонстрировать, что он владеет неким уникальным предметом (физическим ключом), в качестве которого может выступать, например, электронная магнитная карта;
 - аутентифицируемый может доказать свою идентичность, используя собственные биохарактеристики: рисунок радужной оболочки глаза или отпечатки пальцев, которые предварительно были занесены в базу данных аутентификатора.



Авторизация доступа



Авторизация доступа

- ❖ Средства *авторизации (authorization)* контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые ему были определены администратором.
- ❖ Два класса доступа:
 - избирательный доступ;
 - мандатный доступ.



Избирательные права доступа

реализуются в операционных системах универсального назначения.

- ❖ В наиболее распространенном варианте такого подхода определенные операции над определенным ресурсом разрешаются или запрещаются пользователям или группам пользователей, явно указанным своими *идентификаторами*.



Мандатный подход

к определению прав доступа заключается в том, что вся информация делится на уровни в зависимости от степени секретности, а все пользователи сети также делятся на группы, образующие иерархию в соответствии с *уровнем допуска* к этой информации.

- ❖ Такой подход используется в известном делении информации на информацию для служебного пользования, «секретно», «совершенно секретно».

Аудит

(auditing) — фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам.

- ❖ Аудит используется для того, чтобы засекаать даже неудачные попытки «взлома» системы.



Технология защищенного канала

призвана обеспечивать безопасность передачи данных по открытой транспортной сети, например по Интернету.

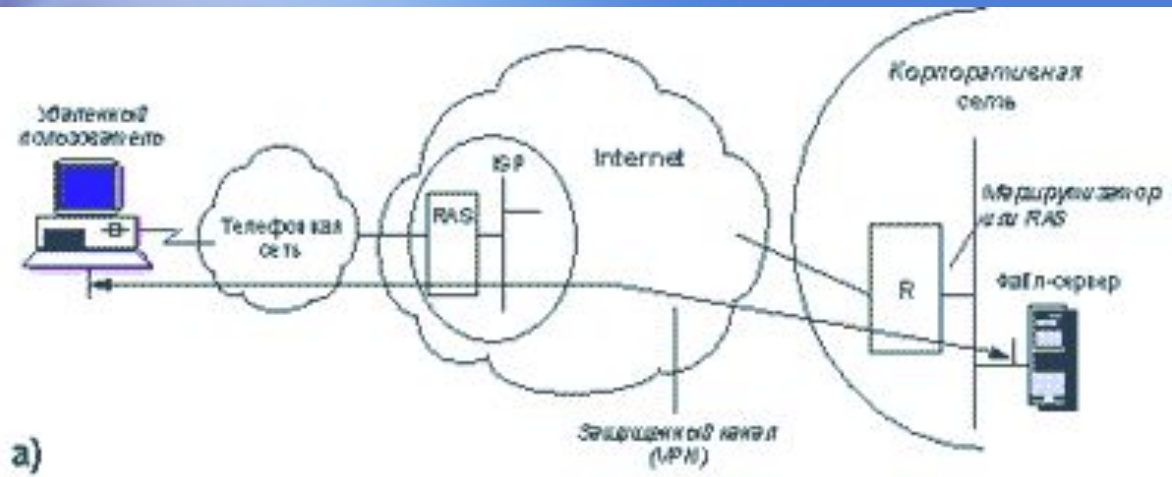


- ❖ Защищенный канал подразумевает выполнение трех основных функций:
 - взаимную аутентификацию абонентов при установлении соединения, которая может быть выполнена, например, путем обмена паролями;
 - защиту передаваемых по каналу сообщений от несанкционированного доступа, например, путем шифрования;
 - подтверждение целостности поступающих по каналу сообщений, например, путем передачи одновременно с сообщением его дайджеста.

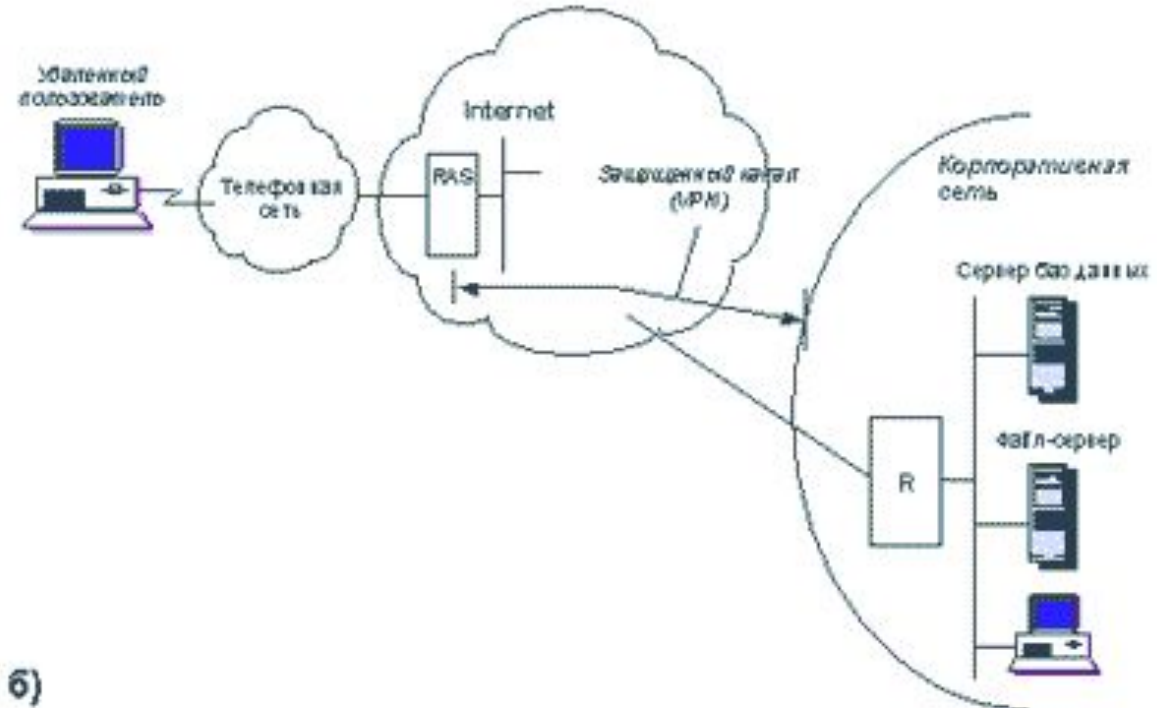


Технология защищенного канала

- ❖ Совокупность защищенных каналов, созданных предприятием в публичной сети для объединения своих филиалов, часто называют *виртуальной частной сетью* (Virtual Private Network, VPN).




а)



б)

Два способа
образования
защищенного
канала

- 
- ❖ Существует два способа образования VPN:
 - с помощью специального программного обеспечения конечных узлов;
 - с помощью специального программного обеспечения шлюзов, стоящих на границе между частной и публичной сетями.



МЕЖСЕТЕВЫЕ ЭКРАНЫ



Межсетевые экраны

- ❖ Межсетевые экраны (firewall, брандмауэр) делают возможной фильтрацию входящего и исходящего трафика, идущего через вашу систему.
- ❖ Межсетевой экран использует один или более наборов «правил» для проверки сетевых пакетов при их входе или выходе через сетевое соединение, он или позволяет прохождение трафика или блокирует его.
- ❖ Правила межсетевого экрана могут проверять одну или более характеристик пакетов, включая но не ограничиваясь типом протокола, адресом хоста источника или назначения и портом источника или назначения.
- ❖ Межсетевые экраны могут серьезно повысить уровень безопасности хоста или сети.

Межсетевые экраны

- ❖ Они могут быть использованы для выполнения одной или более нижеперечисленных задач:
 - Для защиты и изоляции приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети интернет.
 - Для ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети интернет.
 - Для поддержки преобразования сетевых адресов (network address translation, NAT), что дает возможность задействовать во внутренней сети приватные IP адреса и совместно использовать одно подключение к сети Интернет (либо через один выделенный IP адрес, либо через адрес из пула автоматически присваиваемых публичных адресов).



Принципы работы межсетевых экранов

- ❖ Существует два основных способа создания наборов правил межсетевого экрана: «включающий» и «исключающий».
- ❖ Исключающий межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил.
- ❖ Включающий межсетевой экран действует прямо противоположным образом. Он пропускает только трафик, соответствующий правилам и блокирует все остальное.
- ❖ Включающий межсетевой экран обеспечивает гораздо большую степень контроля исходящего трафика.



Принципы работы межсетевых экранов

- ❖ Поэтому включающий межсетевой экран является лучшим выбором для систем, предоставляющих сервисы в сети Интернет.
- ❖ Он также контролирует тип трафика, порождаемого вне и направляющегося в вашу частную сеть.
- ❖ Трафик, не попавший в правила, блокируется, а в файл протокола вносятся соответствующие записи.
- ❖ Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика.



Принципы работы межсетевых экранов

- ❖ Безопасность может быть дополнительно повышена с использованием «межсетевого экрана с сохранением состояния».
- ❖ Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений.
- ❖ Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (Denial of Service, отказ в обслуживании), если множество новых соединений открывается очень быстро.
- ❖ Большинство межсетевых экранов позволяют комбинировать поведение с сохранением состояния и без сохранения состояния, что позволяет создавать оптимальную конфигурацию для каждой конкретной системы.



ПРАВОВАЯ РЕГЛАМЕНТАЦИЯ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ



Правовая регламентация

деятельности в области защиты информации имеет целью защиту информации, составляющей государственную тайну, обеспечение прав потребителей на получение качественных продуктов, защиту конституционных прав граждан на сохранение личной тайны, борьбу с организованной преступностью.



Регламентация может выражаться в следующей форме:

- ❖ обязательное лицензирование некоторых видов деятельности;
- ❖ необходимость иметь разрешение на некоторые виды деятельности;
- ❖ требование сертификации некоторых видов продуктов.

Основные документы

- ❖ *Лицензия* является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока.
- ❖ *Разрешение* выдается на некоторые виды разовых работ, независимо имеется ли у данной организации лицензия. Например, организация которая имеет лицензию на разработку шифровальных средств, должна получить разрешение на их экспорт.
- ❖ *Сертификат* - официальный документ, удостоверяющий, что продукт прошел тестирование и соответствует требованиям нормативных документов.



Виды деятельности, требующие лицензии:

- ❖ В области шифровальных средств:
 - разработка;
 - производство;
 - монтаж, наладка и установка;
 - ремонт и сервисное обслуживание;
 - реализация;
 - предоставление услуг по шифрованию;
 - предоставление консультационных услуг;
 - эксплуатация.
- ❖ Те же виды деятельности, относящиеся к **системам, использующим шифровальные средства и предназначенным для телекоммуникаций**. Лицензии должны получать все предприятия и организации, независимо от их ведомственной принадлежности и прав собственности.



Виды деятельности, на которые выдаются разрешения

- ❖ экспорт и импорт шифровальных средств, предназначенных для использования при обработке, хранении и передаче информации по каналам связи;
- ❖ экспорт и импорт закрытых (с помощью шифровальных средств) систем и комплексов телекоммуникаций;
- ❖ экспорт услуг в области шифрования;
- ❖ открытие учебных специальностей, курсов для организаций, имеющих лицензию на работу по подготовке кадров;



Виды деятельности, на которые не нужны лицензии и разрешения

- ❖ эксплуатация шифровальных средств физическими лицами и негосударственными организациями для защиты информации, не составляющей государственную тайну, во внутренних сетях без выхода в сети общего пользования или для связи с зарубежными партнерами;
- ❖ выявление электронных устройств перехвата информации в помещениях и устройствах негосударственных предприятий, если это не связано с обработкой информации, составляющей государственную тайну;
- ❖ издательская, рекламная и выставочная деятельность.



***Спасибо за
внимание!***