Основы технической защиты информации

Основные понятия и модель компьютерной разведки

Варламов Олег Олегович
Доктор технических наук
Ovar@narod.ru

Актуальность проблемы обеспечения технической защиты информации (ТЗИ)

1. Противоречие: свободный обмен информацией и ограничения на ее распространение и использование.
2. Расширение сферы использования компьютеров (ЭВМ) и повышение уровня доверия к ним (критические данные).
3. Рост объемов информации на машинных носителях информации и способов доступа пользователей к информационным ресурсам.
4. Информация стала товаром, ее стали покупать и продавать
5. Много квалифицированных пользователей (с малыми доходами).
6. Увеличение угроз информации, как «обратная сторона медали».
7. Ущерб от уничтожения или разглашения информации.

Актуальность проблемы обеспечения ТЗИ будет только возрастать!

Представление информации

С точки зрения защиты информации наиболее важными являются две характеристики:

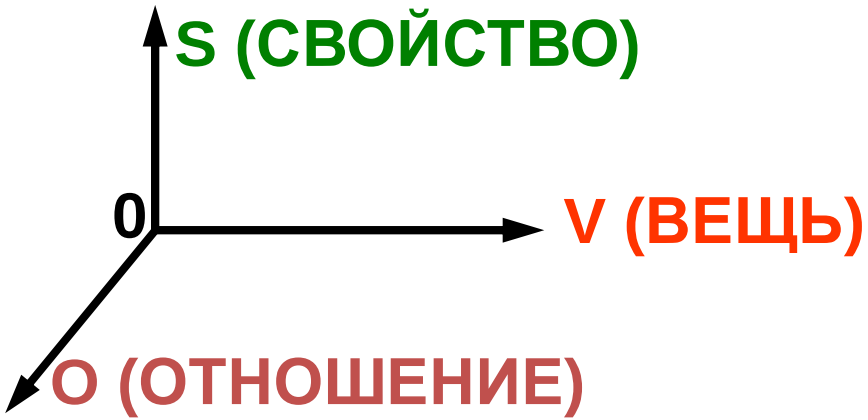
1) **Собственно смысл информации (содержание)**;
2) **Носитель информации** (или физическая среда передачи): колебания стекол, электромагнитные наводки и т.п.

Смысл (содержание)

Носитель информации

Информатизация – это материализация человеческих идеальных мыслей в виде алгоритмов и программ обработки информации.

<V,S,O> - ТРЕХМЕРНОЕ МИВАРНОЕ ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО



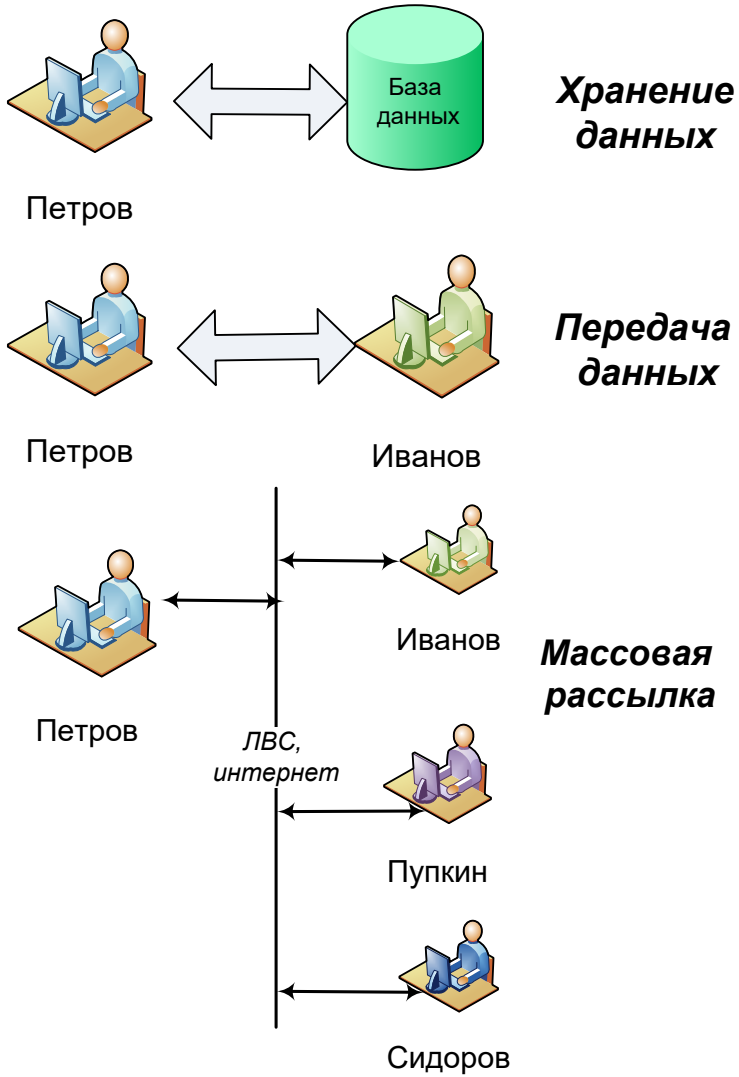
Модель универсального описания хранения и передачи информации

Базируется на понятиях:

1) отправитель информации;
2) время передачи;
3) получатель информации.

Передача информации:
отправитель и получатель различны, а время передачи мало.

Хранение информации:
отправитель и получатель совпадают, время передачи велико.



Свойства информации для ТЗИ

- **Информация** – сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (об их свойствах, характеристиках) в некоторой предметной области, необходимые для оптимизации принимаемых решений в процессе управления этими объектами.
- **Информационные ресурсы** – отдельные документы и массивы документов, массивы документов в информационных системах.
- Важные свойства информации для обеспечения ИБ:
  - Существование в виде данных (кодированном виде);
  - Неисчерпаемость ресурса (при копировании не убывает);
  - Потенциальная полезность при монопольном владении, позволяющая получить выгоду в экономике, политике и т.д. (смысл введения ограничений на распространение, т.е. тайны).

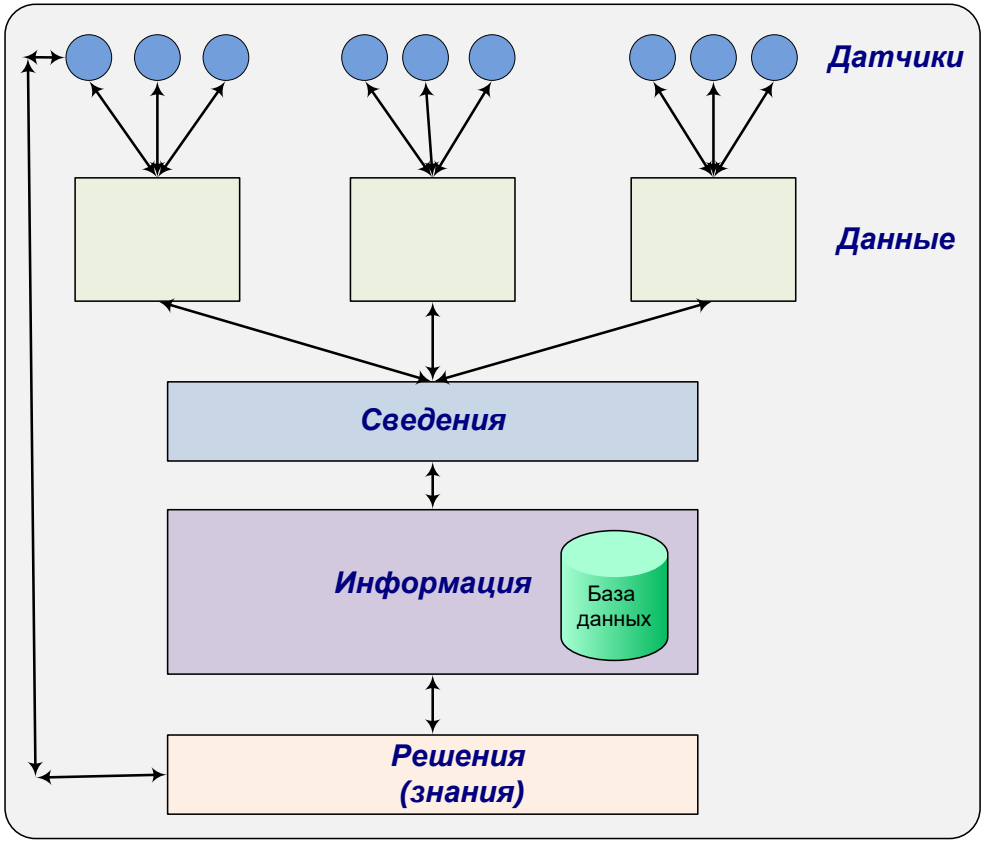
Российский государственный подход к организации работ по ТЗИ

Виды разведки

Разведка – целенаправленная деятельность по добыванию сведений в интересах информационного обеспечения руководства другого государства или конкурирующей организации.

Виды разведки: агентурная и техническая.

Техническая разведка - целенаправленная деятельность по добыванию с помощью технических систем, средств и аппаратуры сведений в интересах … конкурирующей организации, подготовки и ведения информационной борьбы.



Техническая разведка использует достижения технического прогресса и порождает его «отрицательные» последствия.

Взаимосвязь видов технической разведки

- Носители информации могут проявляться в совершенно неожиданных (для нормальных людей) формах.
- Например, колебания воздуха при разговоре – это не только акустические волны в воздухе, но и колебания стекол, стен, водопроводных и отопительных систем.

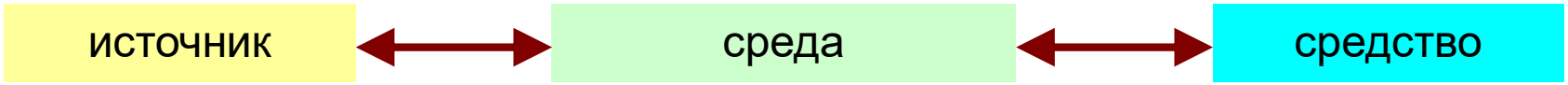
- Взаимодействуя с электроприборами, такие звуки проявляются в электрических и магнитных колебаниях.

- Существует более 30 видов технической разведки.

Канал технической разведки

Канал ТР включает:

1) **источник информации** (объект защиты);
2) **среда передачи данных** (материальный носитель информации);
3) **средство добывания информации** (приемник носителя информации).



Все каналы технической разведки описываются сочетаниями этих трех параметров.

Российский государственный подход к защите информации

- Три «классических» этапа противодействия (ПД) техническим разведкам (ТР) и технической защиты информации (ТЗИ), применяемых для обеспечения безопасности ИСПДн:
  1. Выявить угрозы.
  2. Создать систему защиты информации от этих угроз.
  3. Организовать контроль защищенности информации.

<УГРОЗЫ – ЗАЩИТА – КОНТРОЛЬ>

- Угроза – потенциально возможное событие, вызванное некоторым действием, процессом или явлением, которое может привести к нанесению ущерба чьим-либо интересам.
- Нарушение безопасности (атака) – это реализация угрозы.
  - СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ СОЗДАЕТСЯ ТОЛЬКО ОТ ВЫЯВЛЕННЫХ УГРОЗ, СОГЛАСНО РАЗРАБОТАННОЙ МОДЕЛИ УГРОЗ.

Обязательно необходимо предварительное обследование и разработка модели угроз. При появлении новых угроз системы защиты информации необходимо «модернизировать» (переделать).

Условия использования информации

- Субъекты информационных отношений:
  - Государство;
  - Организации (юридические лица);
  - Граждане (физические лица).
- Для успешного осуществления своей деятельности СУБЪЕКТЫ информационных отношений заинтересованы в обеспечении:
  1. Своевременного **доступа** к необходимой информации и АС;
  2. **Конфиденциальности** (сохранения в тайне) определенной части информации;
  3. **Достоверности** (полноты, точности, адекватности, целостности) информации и защиты от навязывания им ложной информации (т.е. от дезинформации);
  4. **Защиты** части **информации** от незаконного ее тиражирования (авторские права и т.п.);
  5. **Разграничения ответственности** за нарушения законных прав и интересов других субъектов и установленных правил обращения с информацией (доказательства для суда).

Безопасность любого ресурса АС складывается из обеспечения трех его свойств:

1. **Доступность информации** – способность обеспечивать своевременный доступ субъектов к интересующей их информации и соответствующим АС всегда, когда в обращении к ним возникает необходимость (готовность к обслуживанию);
2. **Целостность информации** – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);
3. **Конфиденциальность информации** – субъективно определяемая (назначаемая собственником) характеристика (свойство) информации, которая указывает на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (инфраструктуры) сохранять указанную информацию в тайне от субъектов, не имеющих прав на доступ к ней.

Кроме того, для защиты субъектов от «пиратства» и разграничения их ответственности необходимо обеспечивать (требования 21 века):

- **Неотказуемость** субъектов от выполненных действий;
- **Защиту от неправомерного тиражирования** информации.

Защищаемые объекты в ИБ

- В случае информационной безопасности ущерб субъектам может быть нанесен только опосредованно, через определенную информацию и ее носители.
- **Безопасность информации** - защищенность информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения или утраты (нарушения целостности) или снижения степени доступности (блокирования) информации, а также от незаконного ее тиражирования (неправомерного использования).
- Следовательно, в качестве **объектов, подлежащих защите** с целью обеспечения безопасности субъектов информационных отношений, должны рассматриваться:
  1. Информация (сведения).
  2. Любые ее носители (отдельные компоненты и АС в целом).
  3. Процессы ее обработки и передачи.

Безопасность – это защищенность от опасностей

- Полностью устранить все возможные опасности (угрозы) нельзя
- Безопасность – это защищенность от возможного ущерба, наносимого при реализации угроз. **Субъектами нанесения ущерба являются люди**
- Ущерб может быть:
  - материальным,
  - моральным,
  - физическим.
- Наноситься ущерб может:
  - прямо
  - косвенно.
- Автоматизированная система (АС) – это организационно-техническая система:
  - Технические средства обработки и передачи данных (СВТ и связь);
  - Методы и алгоритмы обработки данных в виде программного обеспечения;
  - Информация на различных носителях;
  - Обслуживающий персонал;
  - Пользователи системы.
- Обработка информации в АС – любая совокупность операций (создание, хранение, передача, преобразование и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

Виды мер и основные принципы обеспечения ТЗИ

- Правовые (законодательные, нормативные правовые акты, регламентирующие правила обращения с информацией … устанавливающие ответственность за нарушения. Являются сдерживающим фактором для потенциальных нарушителей);
- Морально-этические (нормы поведения, бывают оформлены в виде правил или предписаний – устав, кодекс и т.п.);
- Технологические (использование избыточности и направлены на уменьшение вероятности ошибок и нарушений, например, двойной ввод информации, несколько разрешений от разных лиц и т.п.);
- Организационные (административные и процедурные, регламентируют процессы функционирования АС, использования ее ресурсов, деятельность персонала и пользователей);
- Физические (создание физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей, охрана, наблюдение, связь и сигнализация);
- Технические (аппаратные и программные, основаны на использовании различных устройств и программ, входящих в состав АС и выполняющих функции защиты).

Правовые основы обеспечения ИБ

- В Конституции РФ определено, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Ограничения этого права могут устанавливаться законом только в целях охраны личной, семейной, профессиональной, коммерческой и гос.тайны, а также нравственности.
- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» подразделят информацию на категории:
  - Свободного доступа (общедоступная, т.е. информация, доступ к которой не ограничен);
  - Ограниченного доступа, которая подразделяется на:
    - Государственную тайну;
    - Конфиденциальная (коммерческая, служебная, личная, семейная и иные тайны, персональные данные).
- **Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Государственная система защиты информации

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России, ранее Гостехкомиссия России) – является федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам (ПД ТР) и технической защиты информации (ТЗИ).
- ФСБ, МВД, Минобороны, ФСО, СВР и их структурные подразделения по защите информации.
- Структурные и межотраслевые подразделения по технической защите информации органов государственной власти.
- Управления ФСТЭК России по федеральным округам.
- Головная научно-исследовательская организация в РФ по ТЗИ (ФГУП ГНИИИ ПТЗИ ФСТЭК России).
- Головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские организации по ТЗИ органов гос. власти.
- Предприятия, проводящие работы с использованием гос. тайны, их подразделения по ТЗИ.
- Предприятия, проводящие работы в области ТЗИ.
- Высшие учебные заведения, институты повышения квалификации и учебные центры дополнительного образования в области ТЗИ.

Лицензирование, сертификация и аттестация

- Лицензирование – разрешение на определенный вид деятельности.
- Сертификация – процедура подтверждения соответствия, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация удостоверяет в письменной форме (сертификат), что продукция соответствует установленным требованиям.
- Аттестация - комплексная проверка защищаемого объекта информатизации в реальных условиях эксплуатации. По результатам аттестации выдается «Аттестат соответствия», подтверждающий, что объект удовлетворяет требованиям стандартов или иных нормативно-технических документов по безопасности информации.
- «Заочно» или «типично» провести аттестацию нельзя, что увеличивает сроки и стоимость, но «делегирует» риски и «снимает» ответственность.

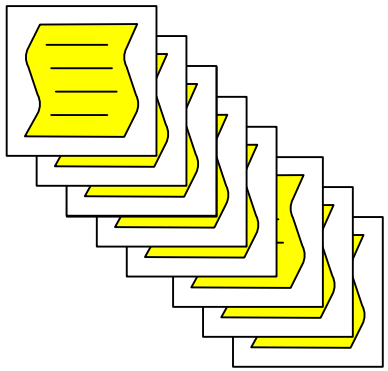
Системы сертификации средств защиты информации

Фрагмент описания требований по «АС 1 Г»

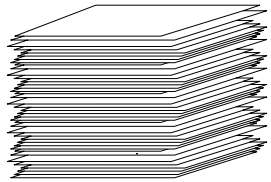
АС. Защита от НСД к информации. Классификация АС и требования по защите информации.

Для «1Г»:

Подсистема управления доступом



- Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
- Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
- Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.
- ...



Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты

- Идентификация (именование и опознание), аутентификация (подтверждение подлинности) пользователей системы.
- Разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям.
- Регистрация и оперативное оповещение о событиях, происходящих в системе.
- Криптографическое закрытие (шифрование) хранимых и передаваемых по каналам связи данных.
- Контроль целостности и аутентичности (подлинности и авторства) данных.
- Резервирование и резервное копирование.
- Фильтрация трафика и трансляция адресов.
- Обнаружение вторжений (атак).
- Выявление и нейтрализация действий компьютерных вирусов.
- Затирание остаточной информации на носителях.
- Выявление уязвимостей (слабых мест) системы.
- Маскировка и создание ложных объектов.
- Страхование рисков.

Эти механизмы могут комбинироваться (варьироваться) и должны системно использоваться в комплексе с другими мерами защиты.

Модель технической компьютерной разведки

Техническая компьютерная разведка (ТКР) – это добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и характеристик пользователей.

Источники информации для ТКР:

1) данные, сведения и информация, обрабатываемые, в том числе передаваемые и хранимые, в компьютерных системах и сетях;
2) характеристики программных, аппаратных и программно-аппаратных комплексов;
3) характеристики пользователей компьютерных систем и сетей.

Виды ТКР

По принципам построения программно-аппаратных комплексов, каналам распространения информации и функциональному назначению выделяют **девять видов** ТКР (угроз):

1. **СЕМАНТИЧЕСКУЮ;**
2. **АЛГОРИТМИЧЕСКУЮ;**
3. **ВИРУСНУЮ;**
4. **РАЗГРАНИЧИТЕЛЬНУЮ;**
5. **СЕТЕВУЮ;**
6. **ПОТОКОВУЮ;**
7. **АППАРАТНУЮ;**
8. **ФОРМАТНУЮ;**
9. **ПОЛЬЗОВАТЕЛЬСКУЮ.**

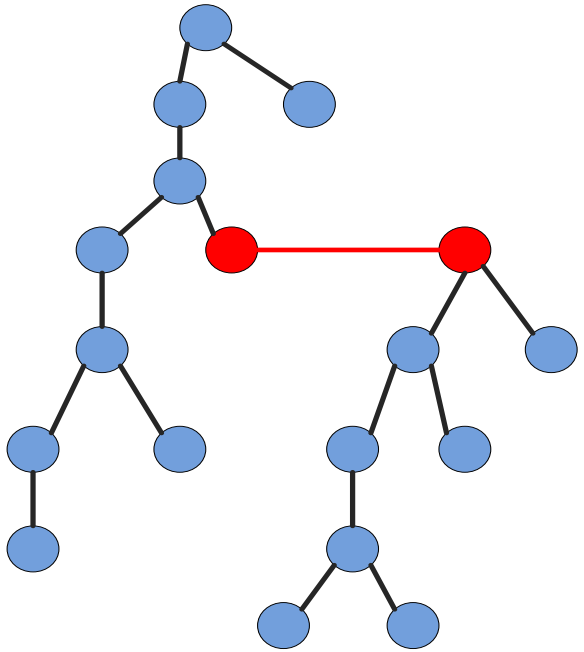
Семантическая ТКР

Обеспечивает добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов.

Семантическая разведка занимается анализом фактографической информации и представляет собой угрозу для ПДн. В Руководящих документах ФСТЭК России способы защиты от нее не указаны, тем не менее защиту от нее необходимо предусмотреть.

Алгоритмическая ТКР

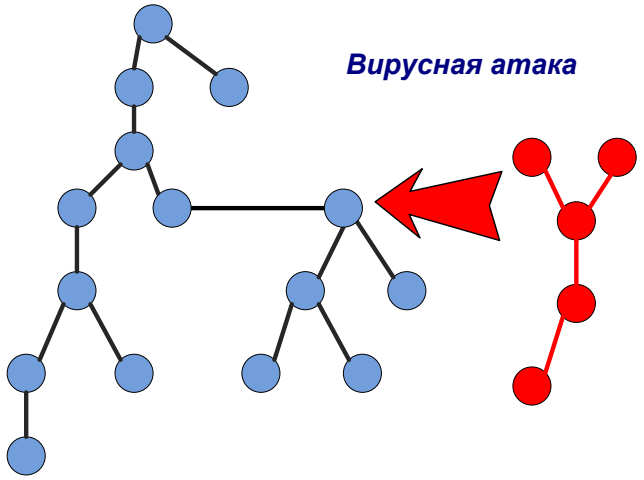
Использует программно-аппаратные закладки и недекларированные возможности для добывания данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей (создают алгоритмы работы программ и оборудования).



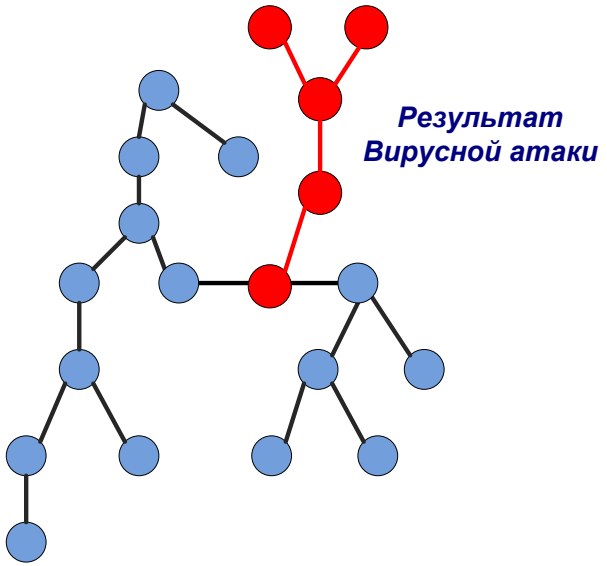
Представляет собой угрозу для любого программного обеспечения на уровне программных закладок и недекларируемых возможностей. Основным средством защиты ПДн от нее является сертификация («НДВ») и проверка на соответствие требованиям РД "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Для ИСПДн необходимо пройти НДВ по 4 уровню контроля (может измениться). Для аппаратуры – «спецпроверки».

Вирусная ТКР

Обеспечивает добывание данных путем внедрения и применения вредоносных программ («вирусов») в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами.



Вирусная разведка представляет собой угрозу для программного обеспечения, но для противодействия ей существуют специализированные средства, работающие независимо от программного обеспечения прикладного уровня.
В Руководящих документах ФСТЭК есть требования к подсистеме антивирусной защиты ИСПДн.



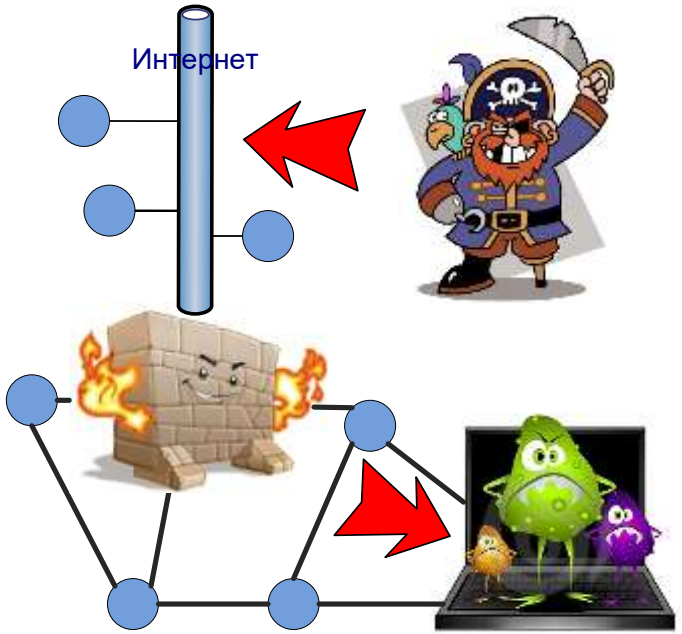
Разграничительная ТКР

Обеспечивает добывание информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе **несанкционированного доступа (НСД)** к информации, а также реализацию несанкционированного доступа при физическом доступе к компьютерам или машинным носителям информации (МНИ)

Важная угроза для ИСПДн. Защита от нее подробно описана в Руководящих документах ФСТЭК России.
Для защиты от нее необходимо использовать средства противодействия разграничительной разведке и не допущения несанкционированного доступа к конфиденциальной информации.
Для подтверждения эффективности работы используемых программных средств служит сертификация по требованиям РД Гостехкомиссии на "СВТ не менее 5 уровня".

Сетевая ТКР

Обеспечивает добывание данных из компьютерных сетей, путем зондирования сети, инвентаризации и анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации, используя выявленные уязвимости систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскирование своих действий.

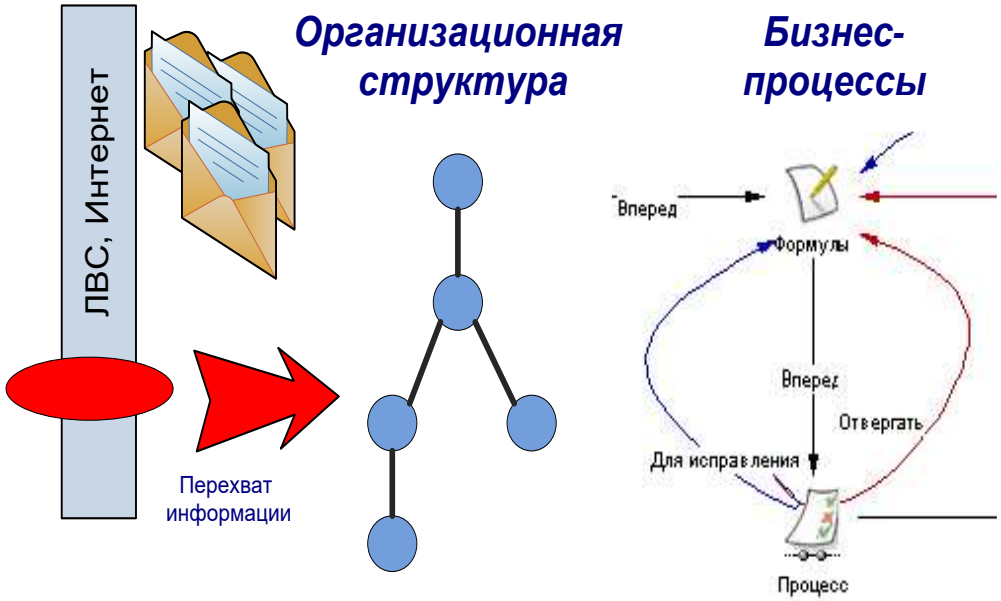


Представляет собой большую угрозу для ПДн. Средства защиты должны располагаться на сетевом уровне взаимодействия, где разработаны специальные аппаратные, программные и программно-аппаратные средства, прежде всего межсетевые экраны (МЭ), которые обязательно должны пройти сертификацию по «МЭ».

Кроме того, согласно руководящих документов ФСТЭК России, необходимо создавать подсистему обнаружения вторжений, требования к которой разработаны в ФСБ.

Потоковая ТКР

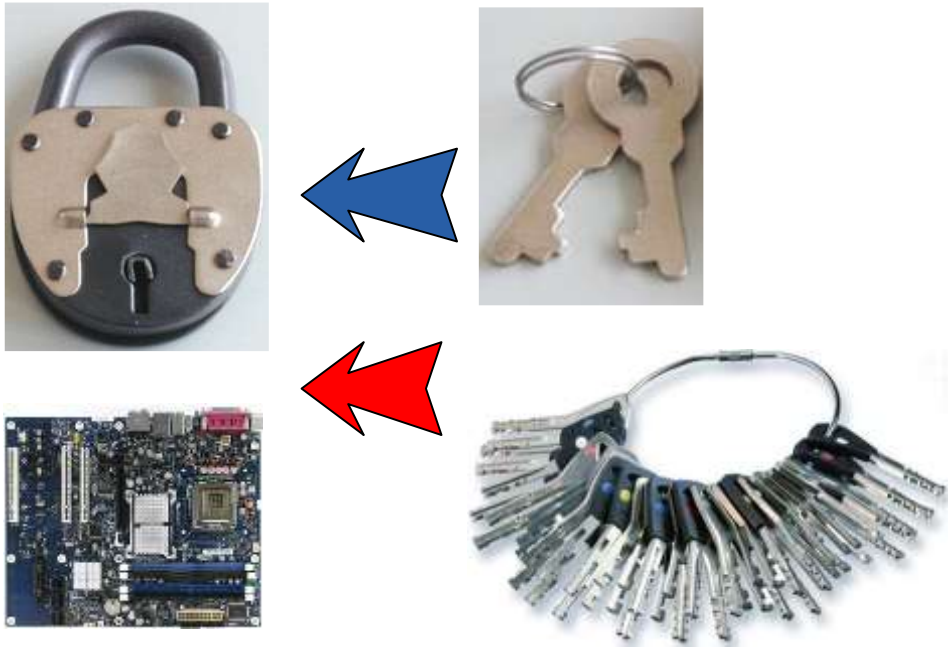
Обеспечивает добывание информации и данных путем перехвата, обработки и анализа сетевого трафика (без доступа к текстам сообщений), а также выявления структур компьютерных сетей и их технических параметров.
Позволяет выявлять организационную структуры, правила принятия решений, бизнес-процессы, направления деятельности и планы развития.



Опосредованно угрожает безопасности ПДн и может выявлять дополнительную информацию о субъектах ПДн или организациях.
Отсутствуют явно сформулированные требования руководящих документов Гостехкомиссии (ФСТЭК России) по защите от потоковой ТКР.
При реализации защиты от этого вида ТКР должны применяться специальные программно–аппаратные комплексы.

Аппаратная ТКР

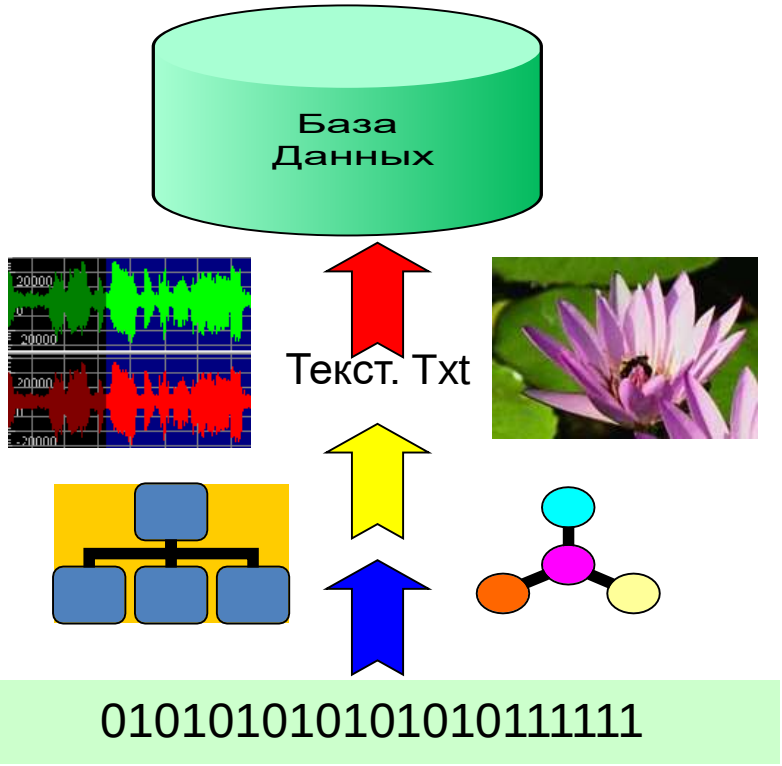
Обеспечивает добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими типами ТКР.



Аппаратная разведка направлена на получение информации об аппаратуре, т.е. о "железе", и непосредственно для ПДн не представляет угрозы.
Может играть вспомогательную роль для других видов ТКР (сетевой, вирусной и т.п.).
Требований в Руководящих документах ФСТЭК России нет.
Необходимость защиты определяет Оператор ПДн.

Форматная ТКР

Обеспечивает добывание информации и сведений путем "вертикальной" обработки, фильтрации, декодирования и других преобразований форматов представления, передачи и хранения добытых данных в сведения, а затем в информацию для последующего ее представления Заказчику или для семантической ТКР.

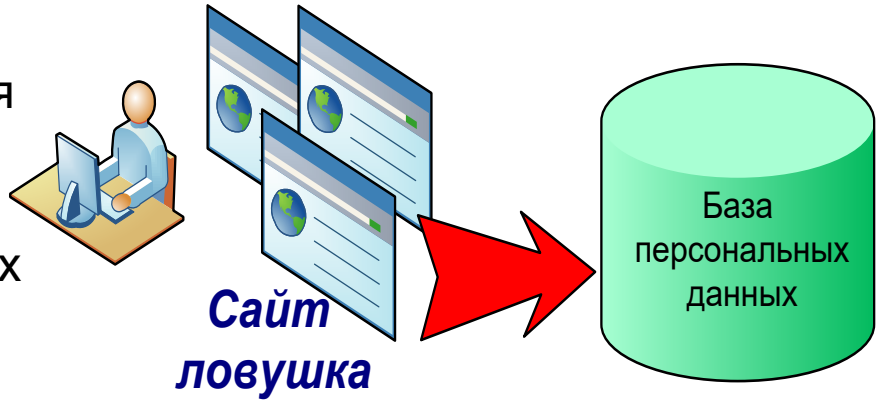


Представляет опосредованную угрозу для ИСПДн.
Однако специальных явно сформулированных требований по противодействию в Руководящих документах ФСТЭК России (за исключением криптографии) пока нет.

Оператор ПДн может использовать криптографические средства защиты информации, вплоть до российских сертифицированных СКЗИ.

Пользовательская ТКР

Обеспечивает добывание информации о пользователях, их деятельности и интересах (ПДн) на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной информационной инфраструктуре (приманке).



Непосредственно угрожает безопасности ПДн, но требований к ней в Руководящих документах ФСТЭК России нет.
Следовательно, Оператор сам вправе определить, как защищать ПДн и информацию ограниченного доступа.
Например, можно применять методы «избыточного трафика», «разбиения на несколько пользователей», использовать защищенные вычислительные устройства и т.п.

Вопросы

Спасибо за внимание!
Ваши вопросы?

дтн Варламов Олег Олегович
OVar@narod.ru
Тлф. +7(926) 276-76-45