Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 5

Защита информации от несанкционированного доступа (НДС) (ЗИотНСД)

Толстой Александр Иванович

к.т.н., доцент

Кафедра «Информационная безопасность банковских систем»

Институт интеллектуальных кибернетических систем

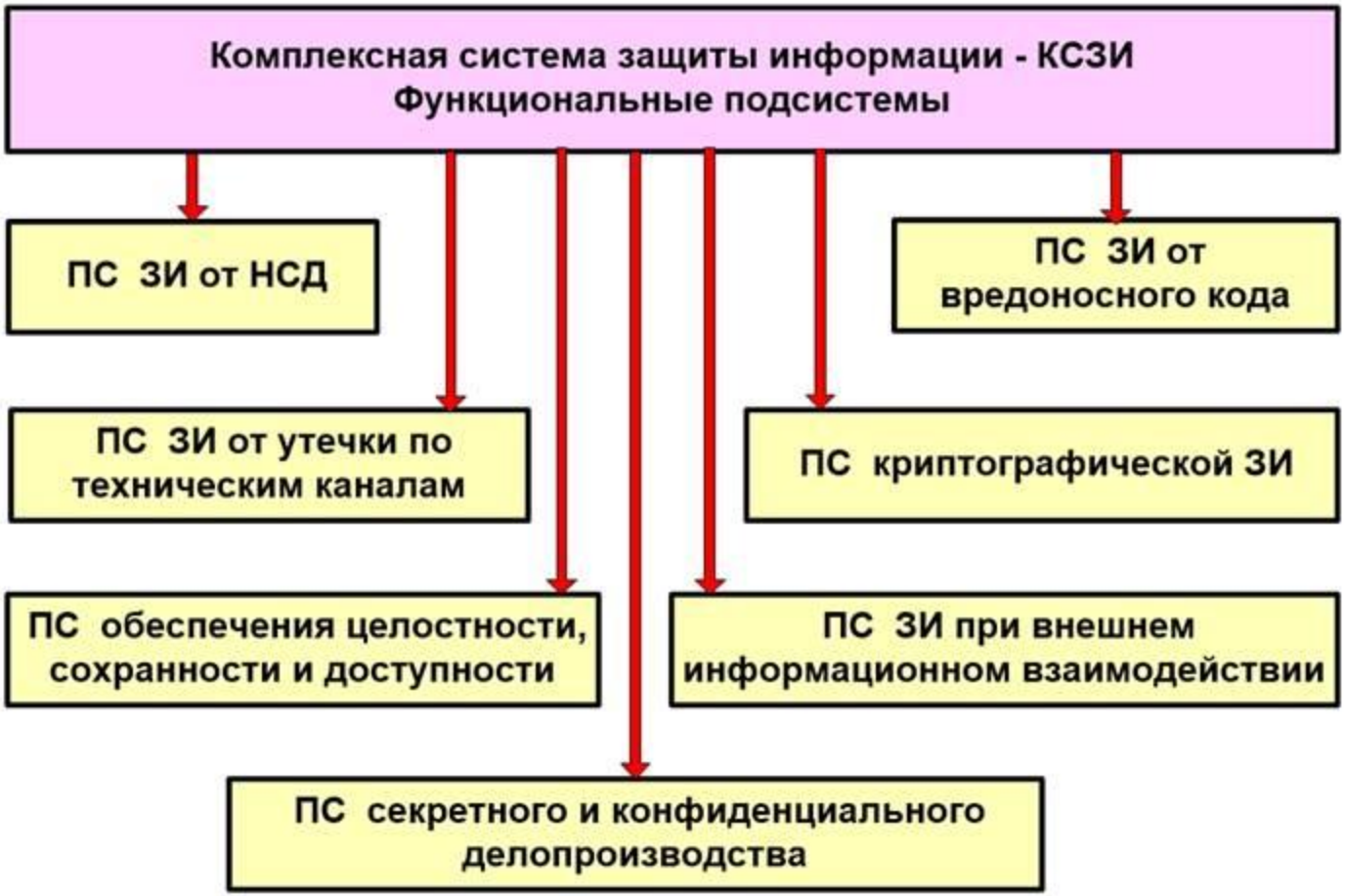
Факультет «Кибернетика и информационная безопасность»

НИЯУ МИФИ

Москва, 2017

4.1. Традиционный подход

«Комплексная система защиты информации» (КСЗИ) - **совокупность различных подсистем.**



Содержание

5.Защита информации от несанкционированного доступа (НДС) (ЗИотНСД)

Определения:

Несанкционированный доступ к информации (НСД): ***Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.***

П р и м е ч а н и е. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем

Защита от НСД: ***Предотвращение или существенное затруднение несанкционированного доступа***

ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

11 Управление доступом

Цель: Управлять доступом к информации

Необходимо:

Доступ к информации, средствам обработки информации и процессам бизнеса должен быть управляемым с учетом требований бизнеса и безопасности.

Правила управления доступом должны учитывать политику в отношении распространения и авторизации информации.

Цели защиты информации от НСД

Основной целью защиты информации является: достижение определенного уровня свойств объекта (свойств ИБ) - доступности, целостности, конфиденциальности информационных активов (ИА).

Определения:

Доступность – Свойство ИБ, состоящее в том, что ИА объекта предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

Целостность – Свойство ИБ объекта сохранять неизменность или обнаруживать факт изменения в своих ИА.

Конфиденциальность – Свойство ИБ объекта, состоящее в том, что обработка, хранение и передача ИА осуществляются таким образом, что ИА доступны только авторизованным пользователям, объектам системы или процессам.

Авторизованный пользователь – пользователь, прошедший авторизацию.

Авторизация – предоставление прав доступа.

НСД – доступ с нарушением правил разграничения доступа.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Основные модели защиты информации от НСД

Авторизованный пользователь – пользователь, прошедший авторизацию.

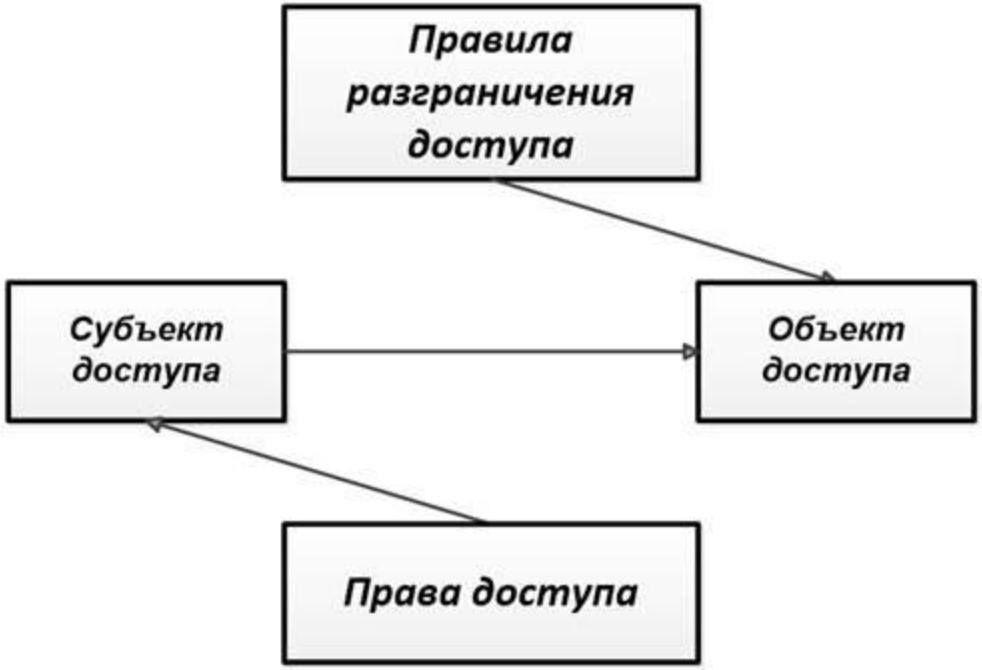
Авторизация – предоставление прав доступа.

НСД – доступ с нарушением правил разграничения доступа.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа – активная сущность (человек, объект, процесс), которая осуществляет доступ к объекту доступа и которая обладает определенными правами доступа.

Объект доступа – пассивная сущность (ИА), обладающая определенными правилами разграничения доступа



МОНИТОР обращений

Авторизованный пользователь – пользователь, прошедший авторизацию.

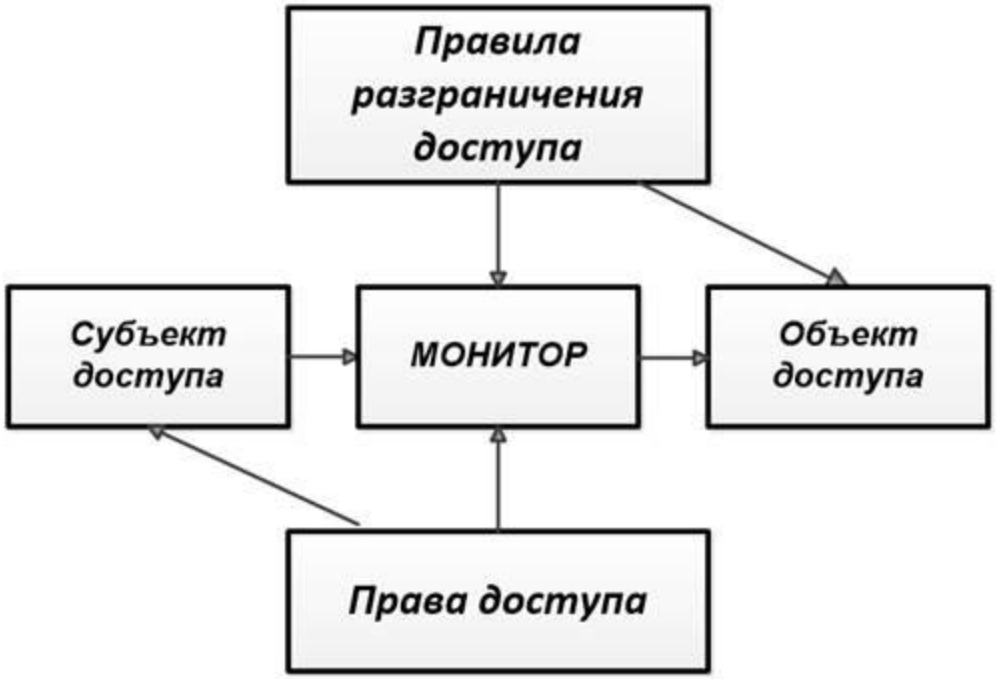
Авторизация – предоставление прав доступа.

НСД – доступ с нарушением правил разграничения доступа.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа – активная сущность (человек, объект, процесс), которая осуществляет доступ к объекту доступа и которая обладает определенными правами доступа.

Объект доступа – пассивная сущность (ИА), обладающая определенными правилами разграничения доступа



Дискреционная модель

$|D|$ - матрица доступа;

$O_1, \dots, O_k$ - объекты доступа, k - количество объектов;

$C_1, \dots, C_n$ - субъекты доступа, n - количество субъектов;

Права доступа:

Чт –чтение, Зп – запись, 0 – нет доступа.

$$|D| = \begin{array}{c|cccccc} & C_1 & C_2 & \dots & \dots & C_{n-1} & C_n \\ O_1 & \text{Зп / Чт} & 0 & \dots & \dots & 0 & 0 \\ O_2 & \text{Чт} & \text{Зп / Чт} & \dots & \dots & 0 & 0 \\ . & \dots & \dots & \dots & \dots & \dots & \dots \\ . & \dots & \dots & \dots & \dots & \dots & \dots \\ O_{k-1} & \text{Чт} & \text{Чт} & \dots & \dots & \text{Зп / Чт} & 0 \\ O_k & \text{Чт} & \text{Чт} & \dots & \dots & \text{Чт} & \text{Зп / Чт} \end{array}$$

Мандатная модель

Основана на правилах секретного документооборота, принятых в государственных учреждениях многих стран. Всем участникам процесса обработки защищаемой информации и документам, в которых она содержится, назначается специальная метка, получившая название уровень безопасности.

Все уровни безопасности упорядочиваются по доминированию. Контроль доступа основывается на двух правилах:

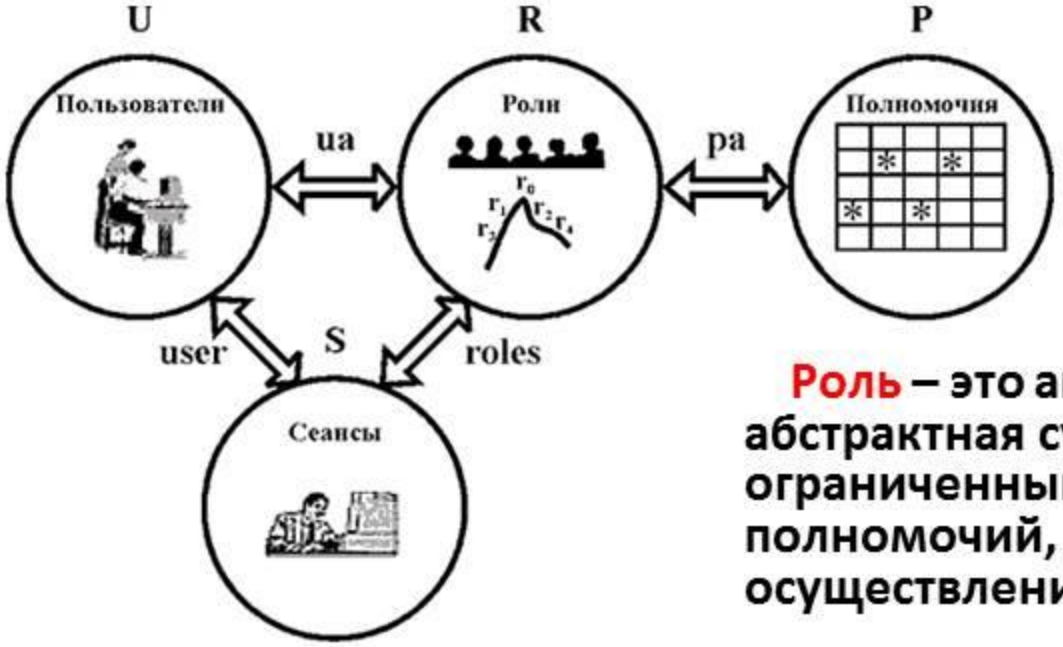
1. Субъект имеет право читать только те документы, уровень безопасности которых ниже или равен уровню субъекта.
2. Субъект имеет право заносить информацию только в документы, уровень которых выше или равен уровню субъекта.

Ролевая модель

Существенно усовершенствованная дискреционная модель.

Управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов.

В ролевой модели классическое понятие субъект замещается понятиями пользователь и роль

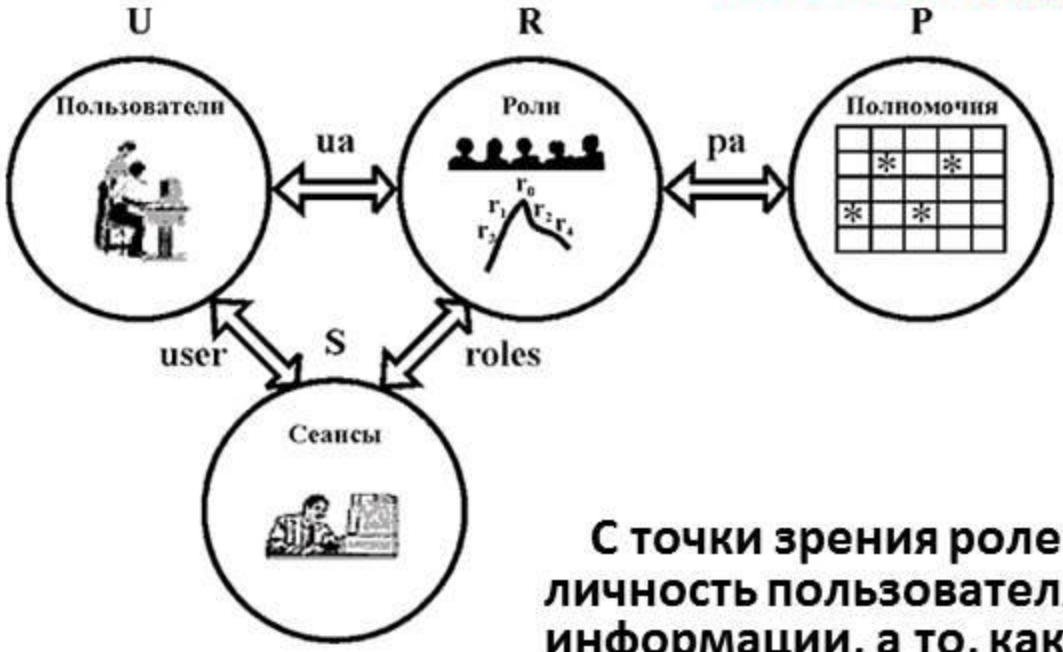


Определения:

Пользователь – это человек, работающий с системой и выполняющий определенные служебные обязанности.

Роль – это активно действующая в системе абстрактная сущность, с которой связан ограниченный, логически связанный набор полномочий, необходимых для осуществления определенной деятельности.

Ролевая модель



Это управление доступом и назначение полномочий не реальным пользователям, а абстрактным (не персонифицированным) ролям, представляющим участников определенного процесса обработки информации.

С точки зрения ролевой модели имеет значение не личность пользователя, осуществляющего доступ к информации, а то, какие полномочия ему необходимы для выполнения его служебных обязанностей.

Управление доступом осуществляется в две стадии:

1. Для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам.
2. Каждому пользователю назначается список доступных ему ролей.

Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимально необходимым для выполнения своей работы набором полномочий.

Авторизация субъектов доступа

АВТОРИЗАЦИЯ = ИДЕНТИФИКАЦИЯ + АУТЕНТИФИКАЦИ

Определения:

Авторизованный пользователь – пользователь, прошедший авторизацию.

Авторизация – предоставление прав доступа.

НСД – доступ с нарушением правил разграничения доступа.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификатор – уникальный признак субъекта или объекта доступа.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Авторизация: однофакторная, двухфакторная, многофакторная.

Идентификация (Кто ты ?): .....

Аутентификация (Чем докажешь ?): .....

Авторизация субъектов доступа

АВТОРИЗАЦИЯ = ИДЕНТИФИКАЦИЯ + АУТЕНТИФИКАЦИ

Определения:

Авторизованный пользователь – пользователь, прошедший авторизацию.

Авторизация – предоставление прав доступа.

НСД – доступ с нарушением правил разграничения доступа.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификатор – уникальный признак субъекта или объекта доступа.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Авторизация: однофакторная, двухфакторная, многофакторная.

Идентификация (Кто ты ?): ФИО, login, pin, ….

Аутентификация (Чем докажешь ?): ….

Авторизация субъектов доступа

АВТОРИЗАЦИЯ = ИДЕНТИФИКАЦИЯ + АУТЕНТИФИКАЦИ

Определения:

Авторизованный пользователь – пользователь, прошедший авторизацию.

Авторизация – предоставление прав доступа.

НСД – доступ с нарушением правил разграничения доступа.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификатор – уникальный признак субъекта или объекта доступа.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Авторизация: однофакторная, двухфакторная, многофакторная.

Идентификация (Кто ты ?): ФИО, login, pin, ….

Аутентификация (Чем докажешь ?): Фотография (паспорт), Password, отпечаток пальца, объемное изображение кисти руки, радужная оболочка глаза, сетчатка глаза, ……

Основные способы НСД

НСД – доступ с нарушением правил разграничения доступа.

К основным способам НСД относятся:

- **непосредственное обращение к объектам доступа;**
- **создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;**
- **модификация средств защиты, позволяющая осуществить НСД;**
- **внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.**

Основы защиты информации от НСД

1. Защита информации от НСД осуществляется:

- **системой разграничения доступа (СРД) субъектов доступа к объектам доступа;**
- **обеспечивающими средствами для СРД.**

2.Совокупность системы разграничения доступа и обеспечивающих средств для СРД составляет систему защиты информации от НСД:

Система ЗИ от НСД = СРД + средства СРД

Ресурсы, связанные как с СРД, так и с обеспечивающими ее средствами, включаются в объекты доступа.

Основы защиты информации от НСД

3.Основными функциями системы разграничения доступа (СРД) являются:

- **реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;**
- **реализация ПРД субъектов и их процессов к устройствам создания твердых копий;**
- **изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;**
- **управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;**
- **реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.**

Основы защиты информации от НСД

4. Обеспечивающие средства для СРД выполняют следующие функции:

- авторизацию (идентификацию и аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса;
- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Категорирование информации

1.Федеральный закон от 27.07.2006 г. № 149-83 (ред.от 06.04.2011) «Об информации, информационных технологиях и защите информации»:

Защищаемая информация подразделяется на следующие виды тайн:

1. Государственная тайна.
2. Коммерческая тайна.
3. Профессиональная тайна.
4. Служебная тайна.
5. Персональные данные.
6. Интеллектуальная собственность.

Категорирование информации

1.Федеральный закон от 27.07.2006 г. № 149-83 (ред.от 06.04.2011) «Об информации, информационных технологиях и защите информации»:

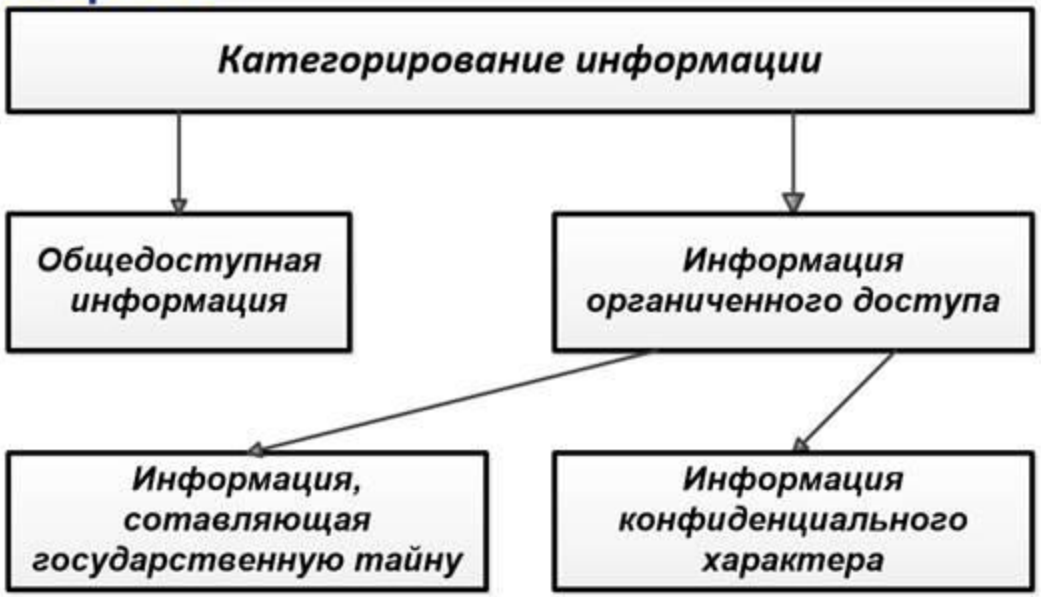
Защищаемая информация подразделяется на следующие виды тайн:

3. Профессиональная тайна:

- врачебная тайна;
- нотариальная тайна;
- адвокатская тайна;
- тайна связи;
- тайна усыновления;
- тайна страхования;
- тайна исповеди;
- банковская тайна.

Категорирование информации

1.Федеральный закон от 27.07.2006 г. № 149-83 (ред.от 06.04.2011) «Об информации, информационных технологиях и защите информации»:

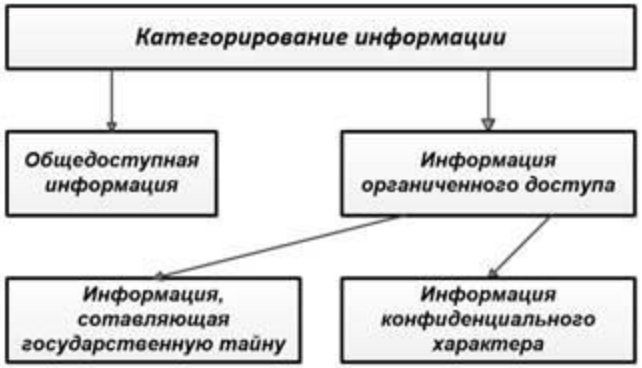


2.Закон РФ от 21.07.1993 г. № 5485-1 (ред.от 08.11.2011) «О государственной тайне»

3.Указ Президента РФ от 06.03.1997 г. № 188 (ред.от 23.09.2009) «Об утверждении Перечня сведений конфиденциального характера»

Категорирование информации

2.Закон РФ от 21.07.1993 г.
№ 5485-1 (ред.от 08.11.2011)
«О государственной тайне»:



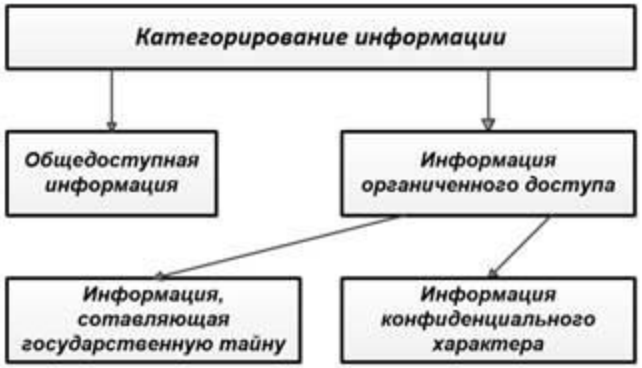
Государственная тайна — это защищаемые государством сведения в области его:

- Военной деятельности,
- Внешнеполитической деятельности,
- Экономической деятельности,
- Разведывательной деятельности,
- Контрразведывательной и оперативно-
- розыскной деятельности,
- Противодействия терроризму.

Категорирование информации

3.Указ Президента РФ от 06.03.1997 г. № 188 (ред.от 23.09.2009) «Об утверждении Перечня сведений конфиденциального характера»:

Информация конфиденциального характера:



- Сведения о фактах, событиях и обстоятельствах частной жизни, позволяющие идентифицировать его личную жизнь (персональные данные).
  - Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты.
- Служебные сведения (служебная тайна).
  - Сведения, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.).
- Сведения, связанные с коммерческой деятельностью (коммерческая тайна).
- Сведения о существе изобретений, полезной модели или промышленного образца.

Физический доступ - доступ к объекту доступа, включая доступ в помещение, в котором расположен объект доступа, позволяющий физически воздействовать на него.

Логический доступ - доступ к ресурсу доступа, в том числе удаленный, реализуемый с использованием вычислительных сетей, каналов и (или) линий связи, позволяющий, в том числе без физического доступа, воздействовать на ресурс доступа, используя его функциональные возможности.

Объект доступа - часть организации, представляющая собой автоматизированную систему (АС), используемую для обработки, передачи и (или) хранения информации в рамках выполнения и (или) обеспечения выполнения основных бизнес процессов организации.

Ресурс доступа - часть объекта доступа.

Субъект доступа – сотрудник организации, осуществляющий физический и (или) логический доступ, или программный сервис, осуществляющий логический доступ.

Легальный субъект доступа - субъект доступа, наделенный полномочиями на осуществление физического и (или) логического доступа.

Пример АС – автоматизированная система управления технологическим процессом (АСУ ТП) критически важного объекта (КВО).

Субъект доступа - сотрудник организации, осуществляющий физический и (или) логический доступ, или программный сервис, осуществляющий логический доступ.

Субъекты доступа разделяются на следующие категории:

пользователи АС организации - субъекты доступа, осуществляющие доступ к объектам и (или) ресурсам доступа с целью использования услуг, предоставляемых АС в рамках реализации основных бизнес процессов организации;

эксплуатационный персонал АС - субъекты доступа, которые решают задачи обеспечения эксплуатации и администрирования объектов и (или) ресурсов доступа, для которых необходимо осуществление логического доступа;

технический персонал АС - субъекты доступа, решающие задачи, связанные с обеспечением эксплуатации объектов доступа, для выполнения которых не требуется осуществление логического доступа;

вспомогательный персонал организации - субъекты доступа, выполняющие хозяйственную деятельность и осуществляющие физический доступ к объектам доступа без цели их непосредственного использования;

программные сервисы - процессы выполнения программ в АС, осуществляющие логический доступ к ресурсам доступа.

Физический доступ - доступ к объекту доступа, включая доступ в помещение, в котором расположен объект доступа, позволяющий физически воздействовать на него.

Логический доступ - доступ к ресурсу доступа, в том числе удаленный, реализуемый с использованием вычислительных сетей, каналов и (или) линий связи, позволяющий, в том числе без физического доступа, воздействовать на ресурс доступа, используя его функциональные возможности.

Ресурс доступа - часть объекта доступа (АС), представляющая собой одну или совокупность следующих составляющих:

программная составляющая - *установленное в АС программное обеспечение (ПО), в том числе встроенное, системное, ПО серверов приложений, и прикладное ПО, используемое для обработки, передачи и (или) хранения информации в рамках выполнения и (или) обеспечения выполнения основных бизнес процессов организации;*

информационная составляющая - *информация, обрабатываемая, хранящаяся и (или) передаваемая с использованием средств АС, и установленного на них программного обеспечения.*

Аутентификационные данные (АД) - данные в любой форме и на любом носителе, известные или принадлежащие легальному субъекту доступа - легальному владельцу АД, или данные, которыми обладает легальный субъект доступа, используемые для выполнения процедуры аутентификации при осуществлении субъектом доступа логического доступа.

Фактор аутентификации - тип АД, используемых субъектом доступа для осуществления доступа:

- пароль легального субъекта доступа;
- данные, хранимые на персональных технических устройствах аутентификации (например, токенах, смарт-картах, носителях, которыми обладает легальный субъект доступа);
- биометрические данные физического лица - легального субъекта доступа.

Однофакторная аутентификация - аутентификация, для осуществления которой используется один фактор аутентификации.

Многофакторная аутентификация - аутентификация, для осуществления которой используется два и более различных факторов аутентификации.

Персональный временный пароль - АД, позволяющие единственному субъекту доступа осуществлять логический доступ в течение его рабочего дня или осуществить однократный логический доступ.

Компрометация АД - событие, связанное с возникновением возможности использования АД субъектом доступа, не являющимся легальным владельцем указанных АД.

Требования к обеспечению ИБ при физическом доступе:

Самостоятельный доступ в помещения, в которых располагаются объекты доступа (далее - помещения), предоставляется только сотрудникам организации в соответствии с перечнем субъектов доступа.

Перечень субъектов доступа формируется для отдельных помещений или для группы помещений. Доступ в помещения лиц, не включенных в указанный перечень, возможен совместно с субъектами доступа, включенными в указанный перечень и несущими ответственность за соответствие действий, выполняемых сопровождаемыми ими лицами, заявленным целям их доступа в помещение.

Помещения, в которых располагаются объекты доступа, могут быть оборудованы следующими средствами защиты: механическими замками, кодовыми замками, Системной охранной сигнализации, Системой контроля и управления доступом (СКУД), телевизионной системой наблюдения (система физической защиты).

Номенклатура используемых СЗ определяется характером объекта доступа (оборудованием, располагаемое в помещении).

Требования к обеспечению ИБ при логическом доступе:

Учетная запись - логический объект (информация), существующий в пределах одного или нескольких ресурсов доступа и представляющий субъекта доступа в его (их) пределах.

Выделяются следующие типы учетных записей, используемых для организации логического доступа:

пользовательская учетная запись - запись, используемая пользователями для осуществления логического доступа;

операторская учетная запись - запись, используемая эксплуатационным персоналом для осуществления логического доступа без предоставления всех прав доступа (неограниченных прав доступа), в том числе без предоставления права изменения электронных журналов выполненных операций и права изменения настроек технических средств ведения электронных журналов выполненных операций, в том числе учетная запись администратора АС, у которого отсутствуют неограниченные права доступа, и администратора ИБ АС, у которого отсутствуют неограниченные права доступа;

административная учетная запись - запись, используемая эксплуатационным персоналом для осуществления доступа с предоставлением всех прав доступа (неограниченных прав доступа) в пределах ресурса доступа, к которому предоставляется логический доступ, в том числе с предоставлением возможности изменения электронных журналов выполненных операций и изменения настроек технических средств ведения электронных журналов выполненных операций;

техническая учетная запись - запись, в том числе встроенная, используемая программными сервисами.

Требования к обеспечению ИБ при логическом доступе:

Логический доступ пользователей и эксплуатационного персонала осуществляется с использованием уникальных учетных записей, за исключением случаев необходимости осуществления непрерывного логического доступа (например, посменная работа).

Выделяются следующие категории паролей, используемые для организации логического доступа:

пользовательские пароли – для пользователей с использованием пользовательской учетной записи;

операторские пароли – для эксплуатационного персонала с использованием операторской учетной записи;

административные пароли – для эксплуатационного персонала с использованием административной учетной записи;

технические пароли - при необходимости, для организации логического доступа программных сервисов с использованием технической учетной записи.

Структура паролей должна соответствовать следующим требованиям:

Определенная длина пароля (например, длина пользовательского и операторского пароля должна быть не менее шести символов; длина технического и административного паролей должна быть не менее восьми символов);

в числе символов пароля обязательно должны присутствовать буквы (в верхнем и нижнем регистрах) и цифры;

пароль не должен включать в себя легко вычисляемые сочетания символов (например, имена, фамилии, наименования ЛВС), а также общепринятые сокращения (например, СВТ, ЛВС, USER, SYSOP).

Требования к обеспечению ИБ при логическом доступе:

Логический доступ - доступ к ресурсу доступа, в том числе удаленный, реализуемый с использованием вычислительных сетей, каналов и (или) линий связи, позволяющий, в том числе без физического доступа, воздействовать на ресурс доступа, используя его функциональные возможности.

Логический доступ пользователей и эксплуатационного персонала осуществляется с использованием уникальных учетных записей, за исключением случаев необходимости осуществления непрерывного логического доступа (например, посменная работа).

Контроль за осуществлением логического доступа к ресурсам доступа, которые относятся к отдельной категории объектов и (или) ресурсов доступа, реализуется с использованием технических средств или, при отсутствии возможности использования технических средств, организационными мерами.

Положение Банка России П-410:

3.Требования к обеспечению ИБ при логическом доступе

Логический доступ пользователей и эксплуатационного персонала к ресурсам доступа, включенным в КоБ ВБИ или КоБ СИ, должен осуществляться с использованием мер защиты, реализующих однофакторную аутентификацию.

Логический доступ пользователей и эксплуатационного персонала к ресурсам доступа, включенным в КоБ ИОД или КоБ УОС, должен осуществляться с использованием мер защиты, реализующих многофакторную аутентификацию.

Пользователи не должны осуществлять логический доступ к ресурсам доступа, включенным в контур безопасности системно-технической инфраструктуры.

Контроль за осуществлением логического доступа эксплуатационным персоналом к ресурсам доступа, которые относятся к отдельной категории объектов и (или) ресурсов доступа, реализуется с использованием технических средств или, при отсутствии возможности использования технических средств, организационными мерами.

8.Обзор программно-аппаратных средств ЗИ от НСД

Лидеры рынка РФ разработок ПА средств ЗИ от НСД:

1. ***Группа компаний «Информзащита» (холдинг):***

- **«Код безопасности»** (разработчик СЗИ Secret Net, ЭЗ «Соболь», «Континент», СКЗИ М-506А-ХР, «КОД БЕЗОПАСНОСТИ: ИНВЕНТАРИЗАЦИЯ», HONEYPOT MANAGER, ПАК «РОСОМАХА» и др.),
- **НИП «Информзащита»** (системный интегратор),
- **Учебный центр «Информзащита»,**
- **«Национальный аттестационный центр» (НАЦ),**
- **Компания «ТрастВерс»** (разработчик системы «КУБ»).

СЗИ Secret Net предназначено для решения следующих типовых задач (программное средство):

- **ЗИ на рабочих станциях и серверах в соответствии с требованиями регулирующих органов**
- **Контроль утечек и каналов распространения защищаемой информации**

Электронный замок «Соболь» предназначен для решения следующих типовых задач (программно-аппаратное средство):

- ***Защита компьютеров от НСД и обеспечение доверенной загрузки***
- ***Создание доверенной программной среды для повышения класса защиты СКЗИ***

8.Обзор программно-аппаратных средств ЗИ от НСД

Возможности СЗИ Secret Net :

- **Гибкое разграничение доступа пользователей к информации и ресурсам защищаемой автоматизированной системы.**
- **Централизованное иерархическое управление упрощает применение СЗИ в больших системах и в организациях с большим количеством филиалов.**
- **Защита важных бизнес-данных от утечек через внешние устройства, сетевые интерфейсы, устройства печати и др.**
- **Контроль функционирования системы за счет подготовки широкого спектра наглядных отчетов о состоянии Secret Net и о зафиксированных событиях.**
- **Контроль подключения устройств к терминальному серверу с тонких клиентов, а также к виртуальной машине.**
- **Высокая масштабируемость (эффективная защита как отдельных рабочих станций, так и вычислительных инфраструктур).**

Возможности Электронного замка «Соболь»:

- **Идентификация и аутентификация пользователей обеспечивается до загрузки ОС при помощи ключей iButton, iKey2032, eToken, Rutoken и др.**
- **Регистрация попыток доступа в системном журнале, записи которого хранятся в специальной энергонезависимой памяти.**
- **Контроль целостности (неизменности) аппаратной конфигурации компьютера, файлов ОС и реестра Windows, прикладных программ.**
- **Доверенная загрузка: запрет загрузки ОС с внешних носителей, что гарантирует загрузку штатной доверенной операционной системы.**
- **Наличие сертифицированного аппаратного датчика случайных чисел (может быть использован в СКЗИ для генерации надежных ключей шифрования).**
- **Наличие дополнительного модуль сторожевого таймера блокирует доступ к компьютеру при обнаружении попытки отключения электронного замка «Соболь».**

8.Обзор программно-аппаратных средств ЗИ от НСД

Лидеры рынка РФ разработок ПА средств ЗИ от НСД:

2.ОКБ САПР: разработчик и вендор Семейства СЗИ НСД АККОРД:

- **Аккорд-АМДЗ**
- **ПАК Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE)**
- **ПАК Аккорд-Win32 К и ПАК Аккорд-Win64 К**
- **ПАК СЗИ НСД Аккорд-Х**
- **ПАК Аккорд-Х К**
- **ПАК Аккорд-XL**
- **Аккорд-В.**
- **Аккорд-У**
- **Аккорд-РАУ**
- **Коммутатор SATA-устройств**
- **Устройство блокировки USB-портов**
- **Считыватели биометрических данных**
- **СУЦУ**
- **Средства интеграции с системой видеомониторинга**
- **СЗИ НСД «ИНАФ»**

2.ОКБ САПР: Аккорд-АМДЗ

Аппаратный модуль доверенной загрузки (АМДЗ) для IBM-совместимых ПК – серверов и рабочих станций локальной сети, обеспечивающий защиту устройств и информационных ресурсов от несанкционированного доступа.

«Доверенная загрузка» – это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя.

Аккорд-АМДЗ может быть реализован на различных контроллерах, но его базовая функциональность всегда остается одинаковой.

2.ОКБ САПР: ПАК Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE)

Программно-аппаратные комплексы средств ЗИ (ПАК СЗИ) Аккорд-Win32 и Аккорд-Win64 предназначены для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам.

Возможности:

- Защита от несанкционированного доступа к ПЭВМ;
- Идентификация/ аутентификация пользователей до загрузки ОС.
- Аппаратный контроль целостности системных файлов и критичных разделов реестра;
- Доверенная загрузка ОС;
- Контроль целостности программ и данных, их защита от несанкционированных модификаций;
- Создание индивидуальной для каждого пользователя изолированной рабочей программной среды;
- Запрет запуска неразрешенных программ;
- Разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа;
- Разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа;
- Автоматическое ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса;
- Усиленная аутентификация терминальных станций с помощью контроллера Аккорд или ПСКЗИ ШИПКА;
- Контроль доступа к USB устройствам;
- ……..

2.ОКБ САПР:

ПАК СЗИ НСД Аккорд-Х - предназначен для разграничения доступа пользователей к рабочим станциям под управлением ОС семейства Linux.

Аккорд-В - предназначен для защиты инфраструктуры виртуализации VMware vSphere 4.1, VMware vSphere 4.0 и VMware Infrastructure 3.5.

Аккорд-У - это ПАК, совмещающий функции АМДЗ с функциями криптографической защиты данных.

Аккорд-РАУ («подсистема распределенного аудита и управления») - это ПО для автоматизации управления защитой информации в АС. Она объединяет АРМ администратора безопасности информации и пользовательские терминалы, оснащенные СЗИ семейства "АККОРД".

Устройство блокировки USB-портов - предназначено для блокировки 2-х портов USB, поддерживает стандарты USB 1.1 и USB 2.0.

Считыватели биометрических данных - поддержка биометрической аутентификации в ПАК «Аккорд-Win32» по сосудистому руслу ладони и отпечатку пальца.

Благодарю за внимание!

Толстой Александр Иванович