УДК 621.391.28

Мошак Н.Н., д.т.н., Яшин А.И., д.т.н., Иванов В.И.

Модели нарушителя и угроз в автоматизированных информационных системах специального назначения на технологии «клиент-сервер»

В Доктрине информационной безопасности Российской Федерации [1] понятие «информационная безопасность» определяется как состояние защищенности национальных интересов в информационной сфере *от внутренних или внешних угроз*, включающее в себя защиту информационных ресурсов от несанкционированного доступа (НСД), а также обеспечение безопасности информационных и телекоммуникационных систем и рассматривается как одно из составляющих национальной безопасности.

Система информационной безопасности (ИБ) объекта защиты реализует требования его политики безопасности. Под политикой безопасности объекта защиты понимается формальная спецификация правил и рекомендаций, на основе которых пользователи используют, накапливают и распоряжаются информационными ресурсами и технологическими ценностями. Политика информационной безопасности в общем случае включают в себя: описание модели нарушителя и значимых угроз информационной безопасности (ИБ), определение основных приоритетов ИБ, анализ информационных рисков, требования к подсистеме ИБ объекта защиты и др.

Требования политики безопасности реализуются в подсистеме ИБ объекта защиты и обеспечиваются на основе согласованного комплекса мер и средств, в том числе: административных и организационно-технических норм и регламентов, программно-технических средств защиты, а также регулярного мониторинга ее состояния.

В статье предложены модели нарушителя и угроз информационной безопасности в автоматизированных информационных системах специального назначения (АИС СП) на технологии «клиент-сервер» с учетом специфики их структурно-функциональных характеристик. Модели нарушителя и угроз информационной безопасности служат основой разработки политики безопасности информационных и телекоммуникационных систем [2].

Краткое описание объекта защиты. Современные АИС СН строятся, как правило, на архитектуре «клиент-сервер» с применением технологии виртуальных серверов и предусматривают «закрытый» и «открытый» контуры обработки, хранения и передачи информации. В «закрытом» контуре, который может иметь различные классы защищенности («3О», «3Р» или «4Р»), обрабатывается информация с грифом «секретно», а в «открытом» контуре класса защищенности «5О» - открытая информация. При этом сертифицированными средствами однонаправленной передачи информации обеспечивается только односторонняя передача информации из «открытого» контура в «закрытый». Типовая схема организации взаимодействия контуров АИС СН приведена на рис.1.

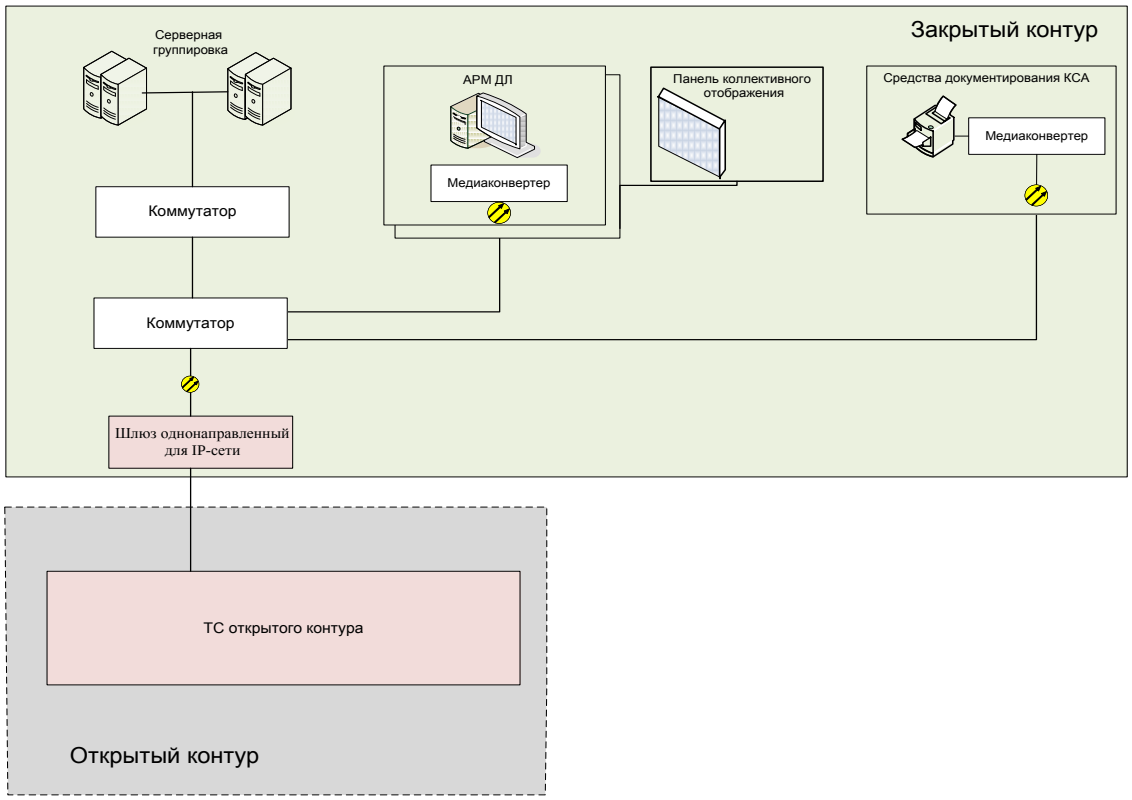

Рисунок 1. - Общая схема взаимодействия «закрытого» и «открытого» контуров АИС СН

Разграничение доступа между группами пользователей «закрытого» контура носит технологический характер и включает:

- операторы (возможность обработки информации в системе);
- администраторы (настройка и управление программно-аппаратными средствами и подсистемой защиты);
- эксплуатационно-технический персонал (установка и регламентное обслуживание ТС, доступ к информации не предъявляется).

Вешнее взаимодействие АИС СН с ведомственными системами осуществляется через «закрытый» контур с применением сертифицированных средств криптографической защиты информации (СКЗИ) с шифрованием информации гарантированной стойкости, а с другими системами – через «открытый» контур с применением сертифицированных межсетевых экранов (МЭ). В качестве базового сетевого протокола используется IP-протокол (рис. 2).

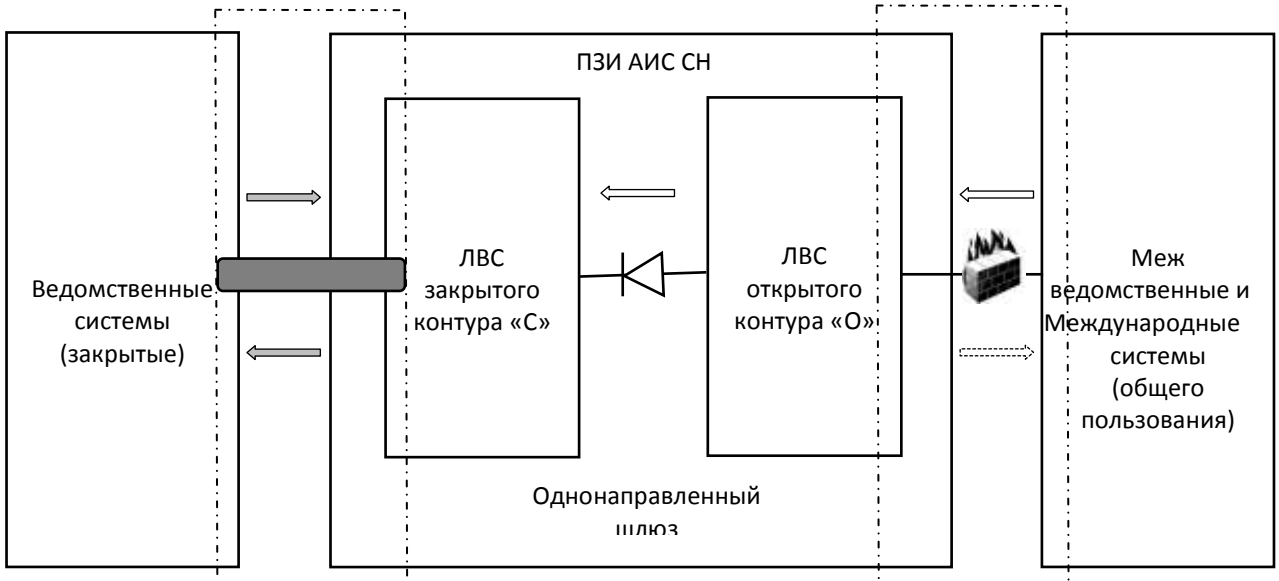

Рисунок 2. - Обобщенная схема информационных потоков в АИС СН

Подсистема защиты информации «закрытого» контура должна обеспечивать:

- сохранение информации в тайне, включая защиту информации от утечки по техническим каналам;
- защиту информации от несанкционированного доступа (далее - НСД) в соответствии с требованиями соответствующего класса защищенности с учетом актуальных угроз безопасности информации «закрытого» контура;
- идентификацию и аутентификацию;
- аудит (регистрацию событий);
- контроль целостности;
- администрирование;
- однонаправленную передачу данных;
- шифрование данных;
- антивирусную защиту.

Подсистема защиты информации «открытого» контура должна обеспечивать:

- защиту информации от НСД с учетом актуальных угроз безопасности информации «открытого» контура, отраженных в модели нарушителя;
- защиту информации, передаваемой между «открытыми» контурами объектов разного уровня по открытым каналам, включая Интернет;
- администрирование;
- антивирусную защиту;
- межсетевое экранирование.

Требования по контролю доступности, целостности и конфиденциальности информации, формируемой, обрабатываемой и передаваемой в «открытом» контуре, не предъявляются.

Модели нарушителя в «закрытом» контуре. В «закрытом» контуре модель нарушителя и угроз строится с учетом обеспечения следующей архитектуры приоритетов базовых услуг безопасности 1) конфиденциальность, 2) целостность и 3) доступность активов «закрытого» контура.

Под нарушителем понимается человек или группа лиц, имеющая своей целью нанесение целью нанесения ущерба пользователям АИС СН и (или) системе управления Пограничной службы ФСБ России в целом путем преодоления (нарушения) целевых функций, реализуемых подсистемой защиты информации «закрытого» контура АИС СН и нанесением удара на конфиденциальность, доступность и целостность «закрытого» контура.

Нарушителем может быть как физическое лицо, так и некоторый процесс, выполняющийся на вычислительных средствах «закрытого» контура. Все физические лица, имеющие доступ к ресурсам АИС СН, могут быть отнесены к следующим категориям:

- категория I - лица, не имеющие права доступа в контролируемую зону, в которой располагаются ресурсы АИС СН;
- категория II - лица, имеющие право постоянного или разового доступа в контролируемую зону, в которой располагаются ресурсы АИС СН.

Нарушители из числа лиц категории I являются внешними нарушителями, а из числа лиц категории II - внутренними нарушителями.

Предполагается, что все лица рассмотренных категорий и классов относятся к потенциальным нарушителям.

При разработке Модели нарушителя предполагается, что

- внешний нарушитель может проводить атаку только из-за пределов контролируемой зоны;
- физическое проникновение внешнего нарушителя на объект защиты с целью внедрения в «закрытый» контур АИС СН программных средств скрытого информационного воздействия (ПССИВ, например, компьютерные вирусы, программные закладки, эксплоиты и т. д.) исключено;
- осуществление атак внешним нарушителем посредством перехвата секретной информации и последующего ее анализа в каналах связи межсетевого обмена «закрытого» контура и системами Ведомственного сегмента, защищенных СКЗИ, исключено и малоэффективно с учетом степени защищенности используемых каналов связи, стоимости и времени на проведение криптоанализа и времени потери ценности перехваченной информации;
- организационными мерами исключается возможность реализации атак на закрытый контур со стороны внешнего нарушителя (в том числе, реализации каналов выноса информации) за счет использования неучтенных носителей внутренним нарушителем - пользователем «закрытого» контура АИС СН;
- организационными мерами (контроль за соблюдением правил работы с носителями, установленными ведомственными инструкциями) исключается попадание к внешнему нарушителю секретной информации из закрытого «закрытого» контура с использованием учтенных носителей пользователей;
- для реализации атак на «закрытый» контур внешний нарушитель не использует недекларированные возможности программных компонент, совместно с которыми предполагается штатное функционирование средств защиты информации;
- осуществление внешних атак на «закрытый» контур через «открытый» контур исключено ввиду организации двойного экранирования: межсетевое взаимодействие «открытого» контура с внешними системами должно осуществляться только через «демилитаризационные зоны», а с «закрытым» контуром только через однонаправленный шлюз. Межсетевое взаимодействие «закрытого» контура с внешними системами через «открытый» контур запрещено.

В модели нарушителя «закрытого» контура АИС СН предположительно должны быть учтены следующие группы потенциальных нарушителей:

- внешний нарушитель (далее - нарушитель группы Н1), не являющийся пользователями «закрытого» контура - субъект, имеющий доступ на контролируемую территорию АИС СН, но не имеющие доступа к работе со штатными средствами «закрытого» контура. К этой группе нарушителей относится администратор ЛВС «открытого» контура. Нарушитель данной группы осуществляет атаки, используя возможности по доступу к информации, передаваемой по соответствующим протоколам информационного обмена, с целью внедрения в «закрытый» «закрытый» контур АИС СН. Администратор ЛВС «открытого» контура имеет возможность производить разграничение доступа к секретной информации, используя штатные средства защиты, не имея фактического доступа к преобразованной информации на сервере, а также производить ее архивирование. Администратор ЛВС как лицо, обладающее максимальными полномочиями по администрированию сетевой операционной системы «открытого» контура, имеет максимальные возможности для внесения «программ-закладок» через однонаправленный шлюз в «закрытый» контур;
- внешний нарушитель (далее - нарушитель группы Н2), являющийся пользователем ЦСКМЗП (11 Центр ФСБ России), осуществляющий атаки с удаленных рабочих мест. Нарушитель данной группы осуществляет атаки, используя возможности по доступу к информации, передаваемой по соответствующим протоколам

информационного обмена, с целью внедрения в «закрытый» «закрытый» контур АИС СН;

- внутренний нарушитель не являющийся пользователем «закрытого» контура АСЗИ АИС СН и не имеющий доступа к информации и работе со штатными средствами (далее - нарушитель группы Н3). К данной группе относятся:

  а) сотрудники пограничных органов ФСБ России, имеющие санкционированный доступ в помещения, в которых размещается оборудование компонентов АИС СН;

  б) эксплуатационно-технический персонал «закрытого» контура (работники инженерно-технических служб и т. д.);

  в) уполномоченный персонал разработчиков АИС СН, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АИС СН под контролем пользователей.

- внутренний нарушитель, являющийся пользователем других систем ФСБ России, но не являющийся пользователем «закрытого» контура АИС СН и не имеющий доступа к работе со штатными средствами АИС СН, но пытающийся нарушить конфиденциальность обрабатываемой в закрытом «закрытом» контуре АИС СН информации (далее именуемый - нарушитель Н4).
- внутренний нарушитель (далее - нарушитель группы Н5), являющийся легальным пользователем «закрытого» контура, имеющий доступ к работе со штатными средствами «закрытого» контура и возможность обработки информации в системе, но пытающиеся получить доступ к объектам защиты «закрытого» контура в нарушение предоставленных им полномочий. К данной группе нарушителей относятся операторы «закрытого» контура;
- внутренний нарушитель (далее - нарушитель группы Н6), являющийся привилегированным легальным пользователем «закрытого» контура, имеющий доступ к работе со штатными средствами «закрытого» контура, но пытающиеся получить доступ к объектам защиты «закрытого» контура в нарушение предоставленных им полномочий. К данной группе нарушителей относятся

  а) администратор СУБД (Н6а) отвечает за управление и конфигурирование СУБД, обеспечение непрерывного сервиса СУБД. Выполняет процедуры подготовки резервного копирования. Является экспертом в области администрирования применяемой СУБД. Владеет информацией о физической структуре СУБД, ее компонентах, концепциях и стратегиях применения. Имеет все возможности по настройке параметров СУБД, включая возможности добавления и удаления пользователей, присвоения привилегий пользователям, любые изменения данных, хранящихся в СУБД, а также хранимых процедур СУБД. Может произвести действия, нарушающие безопасность СУБД и обрабатываемых данных «закрытого» контура.

  б) администратор БД (Н6б) занимается разграничением прав доступа к объектам БД, управляет созданием, модификацией и удалением объектов. Администратор БД владеет информацией о логической структуре данных, имеет представление о хранимой информации, привилегиях доступа пользователей к данным. Может произвести действия, нарушающие безопасность обрабатываемых данных АСЗИ.

  в) администратор ОС (Н6в) занимается управлением и конфигурированием ОС. Отвечает за обеспечение непрерывных сервисов, необходимых для успешной работы СУБД и клиентов системы. Администратор ОС является экспертом в области администрирования применяемой ОС, других системных программных средств, а также в особенностях реализации СУБД в данной ОС. Владеет информацией об особенностях конфигурации, параметров настройки и организации функционирования БД в данной ОС. Имеет все возможности по

настройке параметров ОС, включая возможности добавления и удаления пользователей, присвоения привилегий пользователям, удаление журнала аудита ОС. Может произвести действия, нарушающие безопасность ОС, СУБД и обрабатываемых данных в «закрытом» контуре.

г) администратор аппаратной платформы (АП) (Н6г) занимается управлением и конфигурированием аппаратной платформы. Отвечает за обеспечение непрерывных сервисов, необходимых для успешной работы ОС и поддерживаемых ею приложений. Администратор АП является экспертом в области используемой аппаратной платформы, владеет информацией об используемых физических устройствах, аппаратной конфигурации системы. Не имея непосредственного доступа к информации БД, обеспечивает функционирование СУБД и прикладного ПО.

д) администратор ПСЗИ «закрытого» контура (Н6д) имеет полномочия по предоставлению прав пользователям и управлению регистрационными журналами ПСЗИ. Обеспечивает настройку систем защиты от НСД, систем криптографической защиты информации. Предоставляет полномочия и списки доступа в системах защиты от НСД.

При разработке мероприятий по защите информации в «закрытом» контуре АИС СН необходимо также предусмотреть возможные несанкционированные действия разработчиков АИС СН на этапах ее разработки, внедрения и сопровождения. Возможными направлениями несанкционированных действий внутреннего нарушителя являются:

- доступ к защищаемой информации с целью нарушения ее конфиденциальности (хищение, ознакомление с информацией);
- доступ к информации с целью нарушения ее целостности (модификация информации);
- доступ к программно-техническим средствам с целью постоянного или временного нарушения доступности информации;
- использование ЭУНПИ в режимных помещениях и других ТС.

Внутренний нарушитель также может проводить атаку из-за пределов контролируемой зоны. Предполагается, что доступ к защищаемой информации внутренний нарушитель может получить путем:

- преодоления (обхода) системы разграничения доступа;
- использования специальных программных средств или не декларированных возможностей легально используемого ПО;
- перехвата акустической информации;
- визуального съема информации, выводимой на средства отображения;
- перехвата из-за пределов контролируемой зоны и анализа сигналов (в том числе, побочных), сопровождающих функционирование программно-технических средств ЛВС «закрытого» контура, а также передаваемых в сетях связи.

Кроме того, внутренний нарушитель может также предпринимать действия, приводящие к недоступности защищаемой информации для легального пользователя или к ее искажению (в том числе навязыванию ложной информации).

Внутренний нарушитель может предпринимать указанные действия на всех этапах жизненного цикла АИС СН и ее компонентов (установка и наладка технических средств, разработка и настройка ПО, эксплуатация, модернизация, вывод из эксплуатации или ремонт программно-технических средств), а также на всех технологических этапах обработки информации и во всех режимах функционирования программно-технических средств «закрытого» контура АИС СН.

При рассмотрении возможных действий внутреннего нарушителя считаются выполненными следующие ограничения и предположения:

- все зарегистрированные пользователи «закрытого» контура имеют не ниже 3 формы допуска;
- работа по подбору кадров и специальные мероприятия исключают возможность сговора между внутренним и внешним нарушителями, создания коалиций нарушителей, то есть объединения (сговора) и целенаправленных действий двух и более пользователей по преодолению ПСЗИ «закрытого» контура;
- организационно-техническими и режимными мерами исключен несанкционированный доступ в выделенные помещения, к программно-техническим средствам «закрытого» контура, структурированной кабельной системе, к системам электропитания и заземления, а также пронос фото-, видео устройств, сотовых телефонов и иных не разрешенных к применению ТС и ЭУНПИ;
- внутренний нарушитель скрывает свои несанкционированные действия от других сотрудников;
- нарушения могут быть следствием непреднамеренных ошибок пользователей, администраторов, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности внутренний нарушитель может использовать любое имеющееся в его распоряжении средство съема и перехвата информации, воздействия на информацию и технические средства «закрытого» контура только из-за пределов контролируемой зоны;
- в «закрытом» контуре предпринимаются меры по обеспечению контролируемой зоны, исключающие бесконтрольное пребывание и действия лиц и/или транспортных средств (пропускной режим, средства инженерно-технической защиты), пронос фото-, видео устройств, сотовых телефонов и иных не разрешенных к применению ТС и ЭУНПИ.
- захват объекта противником считается исключенным.

Предполагается, что внешний нарушитель:

- обладает общими знаниями по порядку эксплуатации ПЗИ «закрытого» контура (нарушители Н2);
- знает характерные особенности функционирования (технологию использования и структуру) «закрытого» контура АИС СН (нарушители Н2);

Внешний нарушитель может осуществлять атаки:

- на технические средства «закрытого» контура АИС СН;
- на каналы связи, выходящие за пределы контролируемой зоны объектов АИС СН, используемые для передачи информации ограниченного доступа, с целью перехвата данной информации и последующего ее анализа, уничтожения, модификации, блокирования доступа к ней, а также реализации попыток преодоления ПСЗИ «закрытого» контура, навязывания ложной информации и нарушения работоспособности «закрытого» контура АИС СН в целом и ее отдельных компонент;
- посредством перехвата побочных электромагнитных излучений и наводок вне контролируемой зоны объектов, на которых располагаются технические средства «закрытого» контура АИС СН, и их последующего анализа;
- посредством перехвата сигналов, циркулирующих в сети питания и шине заземления (при возможности контактного подключения к ним за пределами контролируемой зоны);
- на помещения «закрытого» контура АИС СН, в которых циркулирует секретная акустическая информация.

Внешний нарушитель может эффективно использовать всю имеющуюся у него информацию при подготовке и проведении атак.

Предполагается, что внутренний нарушитель, являющийся пользователем «закрытого» контура АИС СН (нарушители Н4, Н5 и Н6):

- является специалистом средней квалификации, не обладающим знаниями по разработке и тестированию (отладке) программного обеспечения (Н4, Н5);
- является специалистом высшей квалификации, обладающим знаниями по разработке и тестированию (отладке) программного обеспечения (Н6);
- является экспертом в области администрирования применяемой СУБД. Обладает возможностями по управлению и конфигурированию СУБД. Владеет информацией о физической структуре СУБД, ее компонентах, концепциях и стратегиях применения. Имеет все возможности по настройке параметров СУБД, включая возможности добавления и удаления пользователей, присвоения привилегий пользователям, любые изменения данных, хранящихся в СУБД, а также хранимых процедур СУБД (Н6а).
- обладает возможностями по разграничению прав доступа к объектам БД, управляет созданием, модификацией и удалением объектов, владеет информацией о логической структуре данных, имеет представление о хранимой информации, привилегиях доступа пользователей к данным (Н6б).
- является экспертом в области администрирования применяемой ОС, других системных программных средств, а также в особенностях реализации СУБД в данной ОС, владеет информацией об особенностях конфигурации, параметров настройки и организации функционирования БД в данной ОС. Обладает возможностями по управлению и конфигурированию ОС. Имеет все возможности по настройке параметров ОС, включая возможности добавления и удаления пользователей, присвоения привилегий пользователям, удаление журнала аудита ОС (Н6в).
- является экспертом в области используемой аппаратной платформы, владеет информацией об используемых физических устройствах, аппаратной конфигурации системы. Обладает возможностями по управлению и конфигурированию аппаратной платформы ЛВС «закрытого» контура, а также максимальными полномочиями по администрированию сетевой операционной системы. Имеет максимальные возможности для внедрения «программ-закладок» (скрытых программных воздействий) в программное обеспечение ТС «закрытого» контура не имея непосредственного доступа к информации БД, обеспечивает функционирование СУБД и прикладного ПО «закрытого» контура.
- имеет возможность по предоставлению и изменению полномочий и списков доступа в системах защиты от НСД и управлению регистрационными журналами СЗИ «закрытого» контура. Обладает максимальными правами по настройке систем защиты от НСД (Н6д).
- имеет данные об организации работы, структуре и используемых технических, программных и программно-технических средствах «закрытого» контура АИС СН (Н5, Н6);
- обладает знаниями по порядку эксплуатации ПСЗИ (Н5, Н6);
- знает характерные особенности функционирования (технологию использования и структуру) «закрытого» контура АИС СН (только для нарушителя Н5, Н6);
- имеет сведения об информационных ресурсах «закрытого» контура АИС СН: порядок и правила создания, хранения и передачи информации, структуре и свойствах информационных потоков (только для нарушителя Н5, Н6);
- располагает данными о реализованных в «закрытом» контуре АИС СН средствах защиты информации, включая описания используемых в шифровальных

(криптографических) средствах криптографических алгоритмов и протоколов, описанием используемых криптографических алгоритмов (только для нарушителя Н5, Н6);

- может иметь данные об уязвимостях «закрытого» контура АИС СН, использующих недокументированные (не декларированные) возможности технических, программных и программно-технических средств «закрытого» контура АИС СН (только для нарушителя Н5, Н6);
- обладает возможностями по несанкционированным действиям с использованием штатных средств «закрытого» контура АИС СН (Н4, Н5, Н6);
- имеет физический доступ к техническим средствам и линиям связи в пределах выделенных ему полномочий, осуществляет легальный доступ к программно-аппаратным средствам и информации со своего рабочего места в соответствии с установленными для него полномочиями, но может пытаться получить доступ к ресурсам «закрытого» контура АИС СН, выходящий за пределы его полномочий (Н4, Н5, Н6);
- имеет сведения о возможных для «закрытого» контура АИС СН каналах атак (только для нарушителя Н5, Н6);
- знает информацию о способах (методах) атак на «закрытый» контур АИС СН (только для нарушителя Н5, Н6).

Предполагается, что внутренний нарушитель, не являющийся пользователем «закрытого» контура АИС СН (Н3), может получить физический доступ к техническим средствам, линиям связи, системам электропитания и заземления «закрытого» контура АИС СН при выполнении им обязанностей по регламентному обслуживанию данных средств. Возможности внутреннего нарушителя Н3 существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- исключение несанкционированного допуска физических лиц в контролируемую зону и к программно-техническим средствам;
- контроль порядка проведения работ.

Внутренний нарушитель этого типа может осуществлять:

- непреднамеренные (ошибочные) действия при выполнении работ по техническому обслуживанию средств «закрытого» контура АИС СН;
- попытки НСД к объектам доступа «закрытого» контура АИС СН с использованием штатных программно-технических средств «закрытого» контура АИС СН без нарушения их целостности.

Возможность сговора внутренних нарушителей Н3 и Н4, с персоналом организаций-разработчиков подсистем АИС СН, а также с внешним нарушителем должна быть исключена применением режимных мер.

Описание каналов атак. Каналами атак являются:

- каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);
- штатные средства АИС СН;
- съемные носители информации;
- носители информации, выведенные из употребления;
- штатные программно-аппаратные средства АИС СН;
- информационные и управляющие интерфейсы СВТ;

- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;
- каналы связи вне контролируемой зоны, не защищенные от НСД к информации организационно-техническими мерами;
- каналы, образуемые в результате применения активных радиотехнических методов (АРТМ) (из-за пределов контролируемой зоны);
- каналы распространения побочных электромагнитных излучений и наводок, сопровождающих функционирование технических средств АИС СН (за пределами контролируемой зоны);
- выходящие за пределы контролируемой зоны цепи инженерно-технических систем (пожаротушения, сигнализации и т.д.), цепи электропитания, цепи заземления, инженерно-технические коммуникации (отопления, водоснабжения и т.д.);
- каналы утечки за счет ЭУНПИ.

Описание объектов и целей атак. К объектам атак (объектам защиты) «закрытого» контура относятся:

- информация, обрабатываемая, передаваемая и хранимая с использованием ТС «закрытого» контура;
- аппаратно-программное обеспечение «закрытого» контура.

Основными целями атак являются:

- нарушение конфиденциальности защищаемой информации (конфиденциальность - защищенность от несанкционированного раскрытия информации об объекте атаки);
- нарушение целостности защищаемой информации (целостность - защищенность от несанкционированной модификации объекта атаки);
- нарушение достоверности защищаемой информации (достоверность - идентичность объекта атаки тому, что заявлено);
- нарушение доступности защищаемой информации (доступность - обеспечение своевременного санкционированного получения доступа к объекту атаки);
- нарушение подконтрольности защищаемой информации. (подконтрольность - обеспечение того, что действия субъекта по отношению к объекту атаки могут быть прослежены уникально по отношению к субъекту).

Предположения об имеющихся у нарушителя средствах атак. Нарушитель может использовать следующие средства атак:

- *штатные средства «закрытого» контура АИС СН;*
- *доступные в свободной продаже технические, программные и программно-технические средства;*
- *специально разработанные технические, программные и программно-технические средства;*
- *средства перехвата и обработки информации в каналах связи, проходящих вне контролируемой зоны, кабельных системах и коммутационном оборудовании, расположенных в пределах контролируемой зоны.*

Внешний нарушитель может осуществлять атаки:

- на технические средства АИС СН (нарушители Н1, Н2);
- на каналы связи, выходящие за пределы контролируемой зоны объектов, на которых располагаются технические средства «закрытого» контура АСЗИ АИС СН, посредством перехвата секретной информации, последующего ее анализа, уничтожения, модификации, блокирования информации, реализации попыток преодоления системы защиты информации, доступа, навязывания ложной информации и нарушения работоспособности «закрытого» контура АСЗИ АИС СН в целом и ее отдельных компонент (нарушители Н1).

Внешний нарушитель может эффективно использовать всю имеющуюся у него информацию при подготовке и проведении атак.

Внутренний нарушитель Н3, может получить физический доступ к техническим средствам, линиям связи, системам электропитания и заземления при выполнении им обязанностей по регламентному обслуживанию данных средств.

Внутренний нарушитель Н3, может использовать для доступа к защищаемой информации доступные в свободной продаже аппаратные средства и программное обеспечение.

Для реализации доступа к информации, обрабатываемой в «закрытом» контуре АИС СН, внутренний нарушитель, не являющийся пользователем «закрытого» контура АИС СН, может располагать:

- компьютером, не имеющим доступа к сети Интернет;
- средствами разработки и отладки программного обеспечения;
- общедоступными компьютерными вирусами.

Возможности внутреннего нарушителя, не являющегося пользователем «закрытого» контура АИС СН, существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- исключение несанкционированного допуска физических лиц в контролируемую зону и к программно-техническим средствам;
- контроль порядка проведения работ.

Внутренний нарушитель Н3 может осуществлять:

- непреднамеренные (ошибочные) действия при выполнении работ по техническому обслуживанию средств «закрытого» контура АИС СН;
- попытки НСД к объектам доступа «закрытого» контура АИС СН с использованием штатных программно-технических средств «закрытого» контура АИС СН без нарушения их целостности;
- попытки НСД к акустической и визуальной информации «закрытого» контура АИС СН.
- Внутренний нарушитель Н4 и Н5:
- может использовать для доступа к защищаемой информации штатные средства «закрытого» контура АИС СН, ССЦ, ТЦОД ПВДНП и других ведомственных систем;
- обладает возможностями по несанкционированным действиям с использованием штатных средств «закрытого» контура АИС СН, ССЦ, ФЦОД ПВДНП;
- имеет физический доступ к техническим средствам и линиям связи в пределах выделенных ему полномочий, осуществляет легальный доступ к программно-аппаратным средствам и информации со своего рабочего места в соответствии с установленными для него полномочиями, но может пытаться получить доступ к ресурсам «закрытого» контура АИС СН, выходящий за пределы его полномочий.

Описание способов реализации атак закрытого контура (ЗР)

Нарушитель может использовать следующие основные способы атак на закрытый «закрытый» контур АИС СН:

- атаки, основанные на использовании уязвимостей и недокументированных (недекларированных) возможностей средств защиты, внесенных в процессе разработки этих средств (Н1, Н2, Н3, Н4, Н5, Н6);

- атаки, основанные на использовании уязвимостей и недокументированных (недекларированных) возможностей средств защиты, внесенных при транспортировке этих средств (Н1, Н2, Н3, Н4, Н5, Н6);
- атаки, основанные на использовании уязвимостей и недокументированных (недекларированных) возможностей, внесенных при создании и наладке системы защиты (Н1, Н3, Н4, Н5, Н6);
- считывание или восстановление информации (в том числе и фрагментарное) по остаточным следам на носителях защищаемой информации, сданных в ремонт, на обслуживание, переданных для использования другими пользователями или для использования за пределами «закрытого» контура АИС СН (Н3, Н4, Н5, Н6);
- негласное (скрытое) временное изъятие съемных носителей защищаемой информации, аутентифицирующей или ключевой информации (Н3, Н4, Н5, Н6);
- негласная (скрытая) модификация защищаемой информации, хранящейся на съемных носителях информации (Н4, Н5, Н6);
- визуальный просмотр защищаемой информации на экране монитора (Н3, Н4, Н5, Н6);
- ознакомление с распечатанной защищаемой информацией (Н3, Н4, Н5, Н6);
- вывод информации на неучтенные носители (в том числе, вывод на печать), а также с нарушением требований руководящих и нормативных документов, регламентирующих порядок обращения с информацией соответствующей категории доступа (Н4, Н5, Н6);
- доступ к оставленным без присмотра функционирующим штатным средствам «закрытого» контура АИС СН (Н3, Н4, Н5, Н6);
- несанкционированное изменение конфигурации технических средств «закрытого» контура АИС СН (Н6г);
- подбор аутентифицирующей информации пользователей (Н1, Н2, Н5, Н6);
- несанкционированный доступ к защищаемой информации с использованием штатных средств «закрытого» контура АИС СН (Н4, Н5, Н6);
- модификация ведущихся в электронном виде регистрационных протоколов (журналов регистрации) (Н6);
- модификация технических средств «закрытого» контура АИС СН (Н6г);
- модификация программных средств «закрытого» контура АИС СН (Н6);
- вызывание сбоев технических средств «закрытого» контура АИС СН (Н3, Н4, Н5, Н6);
- внесение неисправностей в технические средства «закрытого» контура АИС СН (Н3, Н4, Н5, Н6);
- блокирование или уничтожение информации, технических, программных и программно-технических компонентов «закрытого» контура АИС СН (Н2, Н3, Н4, Н5, Н6);
- несанкционированный доступ к защищаемой информации в процессе ремонтных и регламентных работ (Н3);
- атаки, основанные на использовании уязвимостей и недокументированных (не декларируемых) возможностей технических, программных и программно-технических средств «закрытого» контура АИС СН, взаимодействующих со средствами защиты и способных повлиять на их функционирование (Н2, Н3, Н4, Н5, Н6).

Перечисленные способы реализации атак нарушителями могут использоваться в различных сочетаниях, направленных на достижение конкретной цели.

Модель нарушителей в «закрытом» контуре приведена на рисунке 3.

Рисунок 3.- Модель нарушителей в «закрытом» контуре.

Модели угроз «закрытого» контура. Под угрозами безопасности информационных и программных активов АИС СН понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение активов, а также иных несанкционированных действий при их обработке в АИС СН.

Угрозы безопасности информации реализуются действиями нарушителя, которые могут предприниматься им с целью проведения атак на компоненты АИС СН. При этом атаки определены, если определены объект, цель, канал и способ нападения, а также средства нападения.

Под уровнем угрозы понимается вероятность ее осуществления. Оценка уязвимостей предполагает определение вероятности успешного осуществления угроз безопасности. Успешное осуществление угрозы означает нанесение ущерба активам «закрытого» контура. Наличие уязвимостей в «закрытом» контуре обусловлено слабостями защиты. Таким образом, вероятность нанесения ущерба определяется вероятностью осуществления угрозы и величиной уязвимости. Величина риска определяется на основе стоимости актива, уровня угрозы и величины уязвимости. С увеличением стоимости актива, уровня угрозы и величины уязвимости возрастает и величина риска. На основе оценки величины рисков определяются требования безопасности.

Угрозы безопасности информации для «закрытого» контура вытекают из модели нарушителя «закрытого» контура и технологии обработки секретной информации в «закрытом» контуре.

Общее описание угроз информационное безопасности. Все угрозы для защищаемой в «закрытом» контуре АИС СН информации подразделяются на два класса:

- угрозы, не являющиеся атаками;
- атаки.

Под атакой понимается целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого.

Существуют угрозы, которые не являются атаками, но которые могут не только привести к потере, искажению или компрометации защищаемой информации, но и создать условия, которые может использовать в своих целях нарушитель.

К таким угрозам относятся:

- угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и т.д.);
- угрозы социально–политического характера: забастовки, саботаж, локальные конфликты, сопровождаемые нападением на объект, в котором размещаются ресурсы «закрытого» контура АИС СН, и т.д.;
- ошибочные действия и (или) нарушения требований эксплуатационной и другой документации персоналом и пользователями «закрытого» контура АИС СН, к которым, в частности, относятся:

а. непредумышленное искажение или удаление программных компонентов;

б. внедрение и использование неучтенных программ;

в. игнорирование организационных ограничений (установленных правил) при работе с ресурсами «закрытого» контура АИС СН, включая средства защиты информации, в частности:

д. нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);

е. предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требованиям;

ж. настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;

и. несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

к. угрозы техногенного характера, основными из которых являются:

л. аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т. д.);

м. неисправности, сбои аппаратных компонентов средств «закрытого» контура АИС СН, нестабильность параметров системы электропитания, заземления и т. д.;

н. помехи и наводки, приводящие к сбоям в работе аппаратных компонентов средств «закрытого» контура АИС СН.

Основными целями атак в «закрытом» контуре являются:

- нарушение конфиденциальности защищаемой информации (конфиденциальность - защищенность от несанкционированного раскрытия информации об объекте атаки);
- нарушение целостности защищаемой информации (целостность - защищенность от несанкционированной модификации объекта атаки);

- нарушение достоверности защищаемой информации (достоверность - идентичность объекта атаки тому, что заявлено);
- нарушение доступности защищаемой информации (доступность - обеспечение своевременного санкционированного получения доступа к объекту атаки).

Основные угрозы нарушения **конфиденциальности** в «закрытом» контуре:

- ознакомление с секретными данными, хранимыми или обрабатываемыми в базах данных «закрытого» контура, лиц, не допущенных к данным сведениям;
- НСД к АРМ пользователя и нелегальное использование нарушителем прав легального пользователя;
- несанкционированный доступ к информации, выводимой на устройства отображения;
- действия вредоносных программ и вирусов;
- компрометация ключевой информации подсистемы криптографической защиты информации «закрытого» контура;
- нарушение регламента выполнения работ;
- ошибки администрирования;
- создание неучтенных, незаконных копий информационных массивов;
- хищение носителей секретной информации (магнитных дисков, лент, запоминающих устройств и целых ПЭВМ;
- перехват административных паролей серверов и сетевого оборудования с помощью прослушивания сети;
- перехват побочных электромагнитных излучений и наводок АРМ пользователей на вспомогательные технические средства и системы (ВТСС), непосредственно не участвующие в обработке секретной информации, но размещаемые совместно с АРМ пользователей;
- перехват сигналов акустоэлектрических преобразований АРМ пользователей «закрытого» контура и ВТСС, размещаемых в выделенных помещениях ВП;
- перехват обрабатываемой на АРМ пользователей «закрытого» контура секретной информации по цепям электропитания и системе заземления методом ВЧ-навязывания;
- перехват секретной информации из защищаемых помещений «закрытого» контура и установленных ТС за счет ЭУНПИ;
- перехват секретной акустической речевой информации по ТКУИ, в том числе при использовании активных радиотехнических методов.
- несанкционированный доступ к ТС «закрытого» контура внутренних нарушителей, не являющихся пользователями «закрытого» контура;
- внедрение аппаратных или программных «закладок» и «вирусов» с целью регистрации и передачи защищаемой секретной информации или дезорганизации функционирования «закрытого» контура;
- перехват секретной информации за счет использования ЭУНПИ;
- перехват обрабатываемой секретной информации по цепям электропитания и системе заземления, в том числе методом ВЧ- навязывания;
- перехват секретной информации за счет использования ЭУНПИ;
- перехват IP-соединений и работа от имени администратора или пользователя «закрытого» контура;
- генерация фальшивых управляющих ICMP-пакетов для изменения параметров маршрутизации;
- использование слабых мест в сетевых службах для взлома сетевых ресурсов «закрытого» контура;
- использование слабых мест системы доменных имен DNS для формирования ложных таблиц хостов «закрытого» контура;

- использование протокола SNMP управления ЛВС «закрытого» контура для получения сведений о сетевом оборудовании и возможного перехвата и подмены управляющих сетевых сообщений;
- удаленные атаки на средства защиты от НСД и средства криптографической защиты информации с целью нарушения их работы;
- неквалифицированные или неправомерные действия администраторов систем защиты информации, приводящие к нарушению работы этих систем и др.;

Нарушение **конфиденциальности** может привести к несанкционированному предоставлению привилегий пользователям СУБД и ОС, что может повлечь доступ и искажение информации в «закрытом» контуре и служебной информации файлов аудита СУБД и ОС «закрытого» контура, а так же к разглашению или утечке секретной информации из «закрытого» контура. Нарушитель, поразив конфиденциальность компонент «закрытого» контура (например, перехватив административные пароли) может исказить какой либо конфигурационный файл и тем самым осуществить атаку на целостность и доступность системы.

Основные угрозы нарушения **целостности** программ и данных «закрытого» контура:

- несанкционированное изменение БД прикладных задач «закрытого» контура;
- несанкционированное изменение компонентов ОС и СУБД, а также программного обеспечения приложений «закрытого» контура;
- несанкционированное изменение операционной среды АРМ пользователей «закрытого» контура;
- несанкционированные действия нарушителя от имени легального пользователя «закрытого» контура, носящие деструктивный характер или приводящие к искажению информации;
- изменения конфигурации и режимов функционирования серверов «закрытого» контура;
- внесение несанкционированных изменений в настройки коммуникационного оборудования «закрытого» контура.
- сбои оборудования;
- физическое воздействия;
- преднамеренные действия легальных пользователей по нарушению функционирования системы или преодолению механизмов защиты «закрытого» контура;
- ошибки в системном и программном обеспечении;
- вирусные воздействия.

Нарушение **целостности** данных, а также программных компонентов, находящихся как на сервере, так и на рабочих станциях «закрытого» контура может привести к некорректному функционированию ПО и преодолению системы защиты. Нарушитель, поразив целостность компонент «закрытого» контура, может заблокировать ее нормальное функционирование и тем самым осуществить атаку на доступность системы.

Средства поддержания целостности разделяются на две группы: средства контроля целостности и средства восстановления целостности после её нарушения. С помощью этих средств решаются следующие основные задачи:

- обеспечение целостности программ и обрабатываемых данных;
- обеспечение целостности сообщений при передаче информации по каналам связи;
- обеспечение целостности архивной информации;
- обеспечение целостности системы защиты.

Основные угрозы нарушения **доступности** активов «закрытого» контура:

- удаленные атаки на сетевые сервисы с целью нарушения их работы (перехват паролей и трафика, атаки типа «отказ в обслуживании» (Denial of Service), использование возможных уязвимостей сервисов);
- локальные атаки на систему защиты ОС внутренним легальным пользователем «закрытого» контура (подбор паролей, использование возможных уязвимостей файловой системы, настроек сервисов и драйверов) с целью нарушения работы серверов приложений «закрытого» контура;
- неквалифицированные или неправомерные действия администраторов ОС и СУБД «закрытого» контура, приводящие к нарушению работы прикладных задач;
- изменения конфигурации ОС АРМ пользователей ЛВС «закрытого» контура (файлов CONFIG.SYS и AUTOEXEC.BAT, файлов ядра ОС и др.);
- удаление (модификации) исполняемых файлов прикладного и системного программного обеспечения;
- внесение компьютерных вирусов;
- внедрение программ, осуществляющих некорректные действия в АСИ, из-за имеющихся в них ошибок или специальных программных «закладок»;
- внесение модификаций в ПО системы управления ЛВС «закрытого» контура, приводящих к дезорганизации функционирования АРМ пользователей «закрытого» контура;
- вывод из строя или изменение конфигурации сетевого оборудования «закрытого» контура, приводящее к потери доступа к сетевым ресурсам;
- проявление ошибок программно-аппаратных средств «закрытого» контура;
- некомпетентное использование и настройка средств защиты;
- случайный ввод ошибочных данных;
- искажение регистрационных данных;
- действия вредоносных программ;
- неправомерное включение, выключение оборудования или изменение режимов работы устройств и программ;
- повреждение или утрата регистрационной, конфигурационной или иной информации, влияющей на функционирование сервисов безопасности «закрытого» контура.

Нарушения **доступности** информационных, программных и аппаратных ресурсов может привести к дезорганизации процесса обработки информации (несанкционированный останов СУБД, ОС, уничтожение данных и так далее).

В настоящем документе предполагается, что защита от угроз, не являющихся атаками, в основном регламентируется инструкциями, разработанными и утвержденными подразделениями, эксплуатирующими различные компоненты «закрытого» контура АИС СН с учетом особенностей эксплуатации этих компонентов и действующей нормативной базы.

Кроме этого, большинству угроз, не являющихся атаками, можно сопоставить атаки, и защита от такого рода угроз должна обеспечиваться средствами защиты информации, входящими в подсистему информационной безопасности «закрытого» контура АИС СН и разрабатываемыми в основном с целью противодействия атакам.

Модель нарушителя в «открытом» «открытом» контуре. В «открытом» контуре модель нарушителя, как правило, строится с учетом обеспечения только базовой услуги безопасности - **целостность** активов «открытого» контура. Базовые услуги безопасности доступность и конфиденциальность в Модели нарушителя «открытого» контура не рассматриваются.

При разработке Модели нарушителя предполагается, что

- внешний нарушитель может проводить атаку только из-за пределов контролируемой зоны;
- для внешнего нарушителя объектом интересов является только информация межсетевого взаимодействия «открытого» контура АИС СН с «открытыми» контурами ведомственных и других систем. Открытая информация, циркулирующая в «открытом» контуре, не является объектом интересов внешнего нарушителя;
- атаки внешнего нарушителя на «закрытый» «закрытый» контур АИС СН со стороны открытого контура невозможны;
- атаки на целостность и доступность ресурсов «открытого» контура АИС СН со стороны внутренних нарушителей (легальных пользователей, эксплуатационно-технического персонала, а также группы нарушителей Н4) не критична с учетом ценности обрабатываемой открытой информации и влияния на функционирование АИС СН в целом.

В модели нарушителя «открытого» контура АИС СН, с учетом выше приведенных предположений, должны быть учтены только следующие группы потенциальных нарушителей:

- внешние нарушители (группа Н2);
- внешние нарушители (группа Н7) - субъекты, не имеющий доступа на контролируемую территорию объектов размещения ТС «открытого» контура АИС СН - пользователи взаимодействующих ведомственных систем, а также пользователи сети Интернет.

Предположения об имеющейся у нарушителя информации

Предположения об имеющейся у внешнего нарушителя информации. Предполагается, что внешний нарушитель:

- обладает общими знаниями по порядку эксплуатации ПСЗИ «открытого» контура АИС СН (нарушители Н2);
- знает характерные особенности функционирования (технологию использования и структуру) «открытого» контура АИС СН (нарушители Н2);

Внешний нарушитель может осуществлять атаки:

- на технические средства внешнего взаимодействия «открытого» контура АИС СН;
- на каналы связи, выходящие за пределы контролируемой зоны объектов АИС СН, используемые для передачи информации ограниченного доступа, с целью перехвата данной информации и последующего ее анализа, уничтожения, модификации, блокирования доступа к ней, а также реализации попыток преодоления ПСЗИ «открытого» контура АИС СН, навязывания ложной информации и нарушения работоспособности «открытого» контура АИС СН в целом и ее отдельных компонент.

Внешний нарушитель может эффективно использовать всю имеющуюся у него информацию при подготовке и проведении атак.

Описание каналов атак

Каналами атак являются:

- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;
- каналы связи вне контролируемой зоны, не защищенные от НСД к информации организационно-техническими мерами.

Описание объектов и целей атак

К объектам атак (объектам защиты) «открытого» контура АИС СН относятся:

- информация межсетевого взаимодействия с системами Межведомственного и Международного сегментов, обрабатываемая, передаваемая и хранимая с использованием ТС «открытого» контура АИС СН;
- аппаратно-программное обеспечение внешней защиты «открытого» контура АИС СН.

К защищаемой информации относятся:

- информация, используемая при идентификации и аутентификации пользователей при организации межсетевого взаимодействия с системами Межведомственного и Международного сегментов;
- ключевая информация межсетевого обмена.

Защищаемые программные и технические средства:

- межсетевые экраны внешнего взаимодействия;
- внешние сервера аутентификации;
- сетевые коммутаторы, маршрутизаторы;
- каналы связи межсетевого взаимодействия «открытого» контура АИС СН;
- ПО средств внешней защиты информации.

Основными целями атак являются:

- нарушение целостности защищаемой информации в каналах связи общего пользования в процессе межсетевого взаимодействия «открытого» контура АИС СН с системами Межведомственного и Международного сегментов;
- нарушение доступности защищаемой информации;
- нарушение конфиденциальности защищаемой информации;

Предположения об имеющихся у нарушителя средствах атак. Нарушитель может использовать следующие средства атак:

- штатные средства «открытого» контура АИС СН;
- доступные в свободной продаже технические, программные и программно-технические средства;
- специально разработанные технические, программные и программно-технические средства;
- средства перехвата и обработки информации в каналах связи, проходящих вне контролируемой зоны, кабельных системах и коммутационном оборудовании, расположенных в пределах контролируемой зоны.

Внешний нарушитель может осуществлять атаки:

- на технические средства внешней защиты «открытого» контура АИС СН (нарушители Н2, Н7);
- на каналы связи, выходящие за пределы контролируемой зоны объектов, на которых располагаются технические средства «открытого» контура АИС СН (нарушители Н2, Н7).

Возможности внешнего нарушителя (Н4, Н7) существенно зависят от степени защищенности используемых каналов связи (применение криптографических средств защиты, межсетевых экранов, средств обнаружения компьютерных атак и др.).

С учетом особенностей функционирования «открытого» контура и применения средств защиты для противодействия указанным атакам можно предположить, что нарушители (Н4, Н7) относятся к нарушителю, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки. Данный нарушитель является специалистом средней квалификации и для реализации атак не использует недекларированные возможности программных компонент, совместно с которыми предполагается штатное функционирование средств защиты информации

«открытого» контура, располагает только доступными в свободной продаже исходными текстами программного обеспечения средств защиты и т. п.

Возможными направлениями действий внешнего нарушителя (Н4, Н7) являются:

- доступ к информации «открытого» контура с целью нарушения ее целостности (модификация информации, в том числе навязывание ложной информации);
- доступ к каналам управления телекоммуникационного и мультипротокольного оборудования межсетевого взаимодействия «открытого» контура с целью постоянного или временного нарушения доступности информации.

Внешний нарушитель (Н4, Н7) может проводить атаку только из-за пределов контролируемой зоны.

Нарушитель (Н4, Н7) может использовать следующие основные способы атак на открытый контур «О:

- перехват разглашаемых сведений об аутентифицирующей или ключевой информации «открытого» контура и ее компонентах, включая средства и систему защиты;
- перехват ключевой информации межсетевого обмена;
- нарушение связи между контуром «О» и системами Межведомственных и Международных сегментов за счет преднамеренной загрузки трафика ложными сообщениями, приводящей к исчерпанию пропускной способности каналов связи, не защищенных от НСД к информации организационно-техническими мерами.

Модель нарушителя «открытого» контура приведена на рисунке 4.

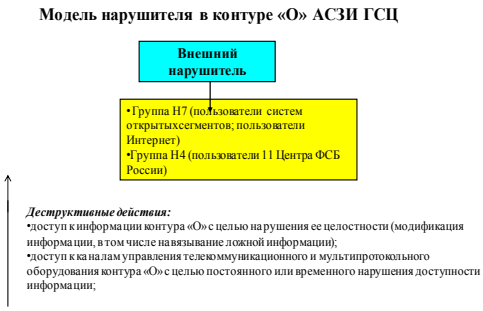

Рисунок 4. - Модель нарушителя «открытого» контура

Модели угроз в «открытом» контуре. Угрозы нарушения целостности и/или доступности информации «открытого» контура:

- удаленные атаки на сетевые сервисы «открытого» контура с целью нарушения их работы (перехват паролей и трафика, атаки типа «отказ в обслуживании», использование уязвимостей сервисов);
- повреждение каналов связи;
- действия, приводящие к частичному или полному отказу сетевого оборудования и средств сетевого управления «открытого» контура;
- неправомерная модификация передаваемых данных, технической и служебной информации.

Угрозы нарушения конфиденциальности информации «открытого» контура:

- незаконное подключение к линиям связи с целью модификации передаваемых сообщений, подмены законного пользователя, перехвата всего потока данных с целью его дальнейшего анализа (включая получение аутентифицирующей и ключевой информации для его последующего неправомерного использования) и т.п.;

- незаконное подключение к сетевому оборудованию с целью изменения настроек и анализа проходящего потока данных и служебного трафика;
- воздействие на внешнее сетевое оборудование «открытого» контура, приводящее к его некорректному функционированию (неправильной фильтрации, адресации информации и т.п.);
- использование уязвимостей интерфейсов и протоколов взаимодействия оборудования «открытого» контура.

Выводы

1. Угрозы безопасности информации в АИС СП должны определяться по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей АИС СП, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).
2. В моделях нарушителей АИС СП в обязательном порядке должны быть учтены привилегированные легальные пользователи с правами администраторов компонент АИС СП.
3. При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

Литература

1. Доктрина информационной безопасности Российской Федерации // Новая газета. – 15 сентября 2000.

2. Мошак Н.Н., Тимофеев Е.А. Особенности построения политики информационной безопасности в инфокоммуникационной сети // «Электросвязь», №9, 2005.