Министерство чрезвычайных ситуаций Республики Крым

УТВЕРЖДАЮ
Министр чрезвычайных ситуаций
Республики Крым
_____С. ШАХОВ
«__» _____ 2017 г.

Модели угроз безопасности информации и модели нарушителя в Министерстве чрезвычайных ситуаций Республики Крым и его подведомственных учреждениях

Симферополь 2017

Термины и определения

В настоящем документе применены следующие термины с соответствующими определениями.

Активы: информация, технические средства, программное обеспечение и документация АИТС, подлежащие защите.

Атака: 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.

Безопасность информации: состояние защищенности информации от нарушения заданных для нее **характеристик безопасности информации**.

Защита информации: деятельность, направленная на обеспечение безопасности защищаемой информации.

Защищаемая информация: информация, для которой собственником информации определены характеристики ее безопасности.

Собственником информации может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Информация конфиденциального характера (ИКХ): информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну (в том числе ПДн и коммерческая тайна).

Информационная система персональных данных: информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Канал атаки: среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) осуществляемых при проведении атаки действий.

Контролируемая зона: пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

Модель нарушителя: совокупность предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Нарушитель (субъект атаки): лицо, проводящее атаку.

Система защиты персональных данных (СЗПДн): организационно-технические меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

Среда функционирования СЗИ (СФ СЗИ): совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование СЗИ и которые способны повлиять на выполнение предъявляемых к СЗИ требований.

Средство вычислительной техники (СВТ): совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Угрозы безопасности персональных данных: совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в ИСПДн.

Характеристика безопасности объекта (в частности, информации): описание состояния защищенности объекта (в частности, информации) информации от конкретного вида угроз.

Основными характеристиками безопасности информации являются:

конфиденциальность – защищенность от несанкционированного раскрытия информации об объекте (в частности, о защищаемой информации);

целостность – защищенность от несанкционированной модификации объекта (в частности, защищаемой информации);

доступность – обеспечение своевременного санкционированного получения доступа к объекту (в частности, к защищаемой информации);

достоверность – обеспечение идентичности объекта (в частности, защищаемой информации) тому, что заявлено.

Штатное средство: техническое или программное средство из состава средств АИТС.

Сокращения

АИТС	–	автоматизированная информационно-телекоммуникационная система
АРМ		автоматизированное рабочее место
ИКХ	–	информация конфиденциального характера
ИСПДн	–	информационная система персональных данных
ЛВС	–	локальная вычислительная сеть
НСД	–	несанкционированный доступ к информации
ПДн	–	персональные данные
СВТ	–	средства вычислительной техники
СЗИ	–	средство защиты информации
СЗПДн	–	система защиты персональных данных
СФ	–	среда функционирования
А(И)С	–	автоматизированная (информационная) система Министерства чрезвычайных ситуаций Республики Крым.

1. Введение

Настоящий документ подготовлен в рамках выполнения работ по построению системы защиты конфиденциальной информации, не содержащих сведений, составляющих государственную тайну, АС.

Настоящий документ содержит модель угроз безопасности ПДн и вероятного нарушителя для АС (далее – модель угроз).

Разработка модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности КИ АИС «» и проектирования СЗ АС.

Модель угроз – документ, определяющий основные исходные условия для проверки соответствия СЗ АС заданным к ней требованиям.

При разработке модели угроз для АС использовалась нормативная база и методология ФСБ России и ФСТЭК России (Гостехкомиссии).

2. Назначение, структура и основные характеристики АС«»

2.1 Назначение АИС

Автоматизированная информационная система Министерства чрезвычайных ситуаций Республики Крым (АС) – это информационный ресурс РФ, содержащий общедоступные персональные данные.

Автоматизированная система предназначена для обработки персональных данных.

2.2 Структура АИС

Автоматизированная система функционирует на трех уровнях:

1. Информационная система специалистов – офисная автоматизация, обработка знаний (включая экспертные системы);
2. Информационные системы тактического уровня (среднее звено) – мониторинг, администрирование, контроль, принятие решений;
3. Стратегические информационные системы – формулирование целей, стратегическое планирование.

Программно-технический комплекс АС состоит из следующих функциональных составляющих:

– автоматизированные рабочие места администраторов АС;

– автоматизированные рабочие места пользователей АС.

Сеть передачи данных (каналы связи) образуют среду функционирования АС.

2.3 Основные характеристики АС

Хранимая и обрабатываемая в АС информация в соответствии с Федеральным законом РФ «», относится к информации составляющей ….

АС является многопользовательской АС с различными правами доступа пользователей к информационным ресурсам.

Информация консолидировано хранится и обрабатывается на вычислительных средствах, расположенных в физически выделенных центрах обработки данных (серверные помещения), расположенных в контролируемых зонах. По отношению к указанным центрам обработки данных реализован достаточный набор организационных и режимных мер защиты информации.

Пользователи осуществляют доступ к информационным ресурсам АС в объеме предоставленных полномочий с АРМ, расположенных в подразделениях ….. Указанные АРМ расположены в контролируемых зонах.

Подключения к системе АС и доступ к информационным ресурсам осуществляется установленным порядком с обязательной процедурой согласования.

3. Определение модели вероятного нарушителя

Все угрозы безопасности информации АС подразделяются на два класса:

- *непреднамеренные угрозы* (угрозы, не связанные с деятельностью человека; угрозы социально-политического характера; ошибочные действия персонала и пользователей АИТС; угрозы техногенного характера);
- *атаки*.

Непреднамеренные угрозы по своей природе не связаны со злонамеренными действиями человека по отношению к АИТС. Но эти угрозы могут не только привести к потере, искажению или компрометации информационных активов АС, но и создать условия, которые может использовать в своих целях нарушитель.

Предполагается, что защита от непреднамеренных угроз в основном регламентируется инструкциями, разработанными и утвержденными подразделениями, эксплуатирующими различные компоненты АС с учетом особенностей эксплуатации этих компонентов и действующей нормативной базы. Поэтому непреднамеренные угрозы далее детально не рассматриваются.

Как показывает мировой и отечественный опыт, *атаки* являются наиболее опасными угрозами безопасности информации, что обусловлено их тщательной подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак.

Атаки готовятся и проводятся нарушителем. При этом возможности проведения атак определяются соответствующими возможностями нарушителя.

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках разработки модели угроз и нарушителя.

Разработанная и приведенная в настоящем документе модель угроз для АС предназначена для использования при формировании требований информационной безопасности и проектных решений по СЗ АС.

Модель вероятного нарушителя включает:

- описание возможных нарушителей;
- предположения об имеющейся у нарушителя информации об объектах атак;
- предположения об имеющихся у нарушителя средствах атак;
- описание объектов и целей атак;
- описание каналов атак.

Разработка модели угроз базируется на следующих принципах:

- безопасность информации АИТС обеспечивается СЗ АС, а также используемыми в АИТС информационными технологиями. Технические и программные средства должны удовлетворять устанавливаемым в

соответствии с законодательством РФ требованиям, обеспечивающим защиту информации (в т.ч. ПДн);

- СЗ АС не предназначена для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий;
- нарушитель может действовать на различных этапах жизненного цикла программных и технических средств АИТС, включая СЗ (разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств АИТС).

На этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию программных и технических средств СЗ АС не производится обработка защищаемой ИКХ. Поэтому объектами атак могут быть только сами эти средства и документация на них.

В связи с выше изложенным, на указанных этапах жизненного цикла возможны следующие атаки:

- внесение негативных (как правило, недекларированных) функциональных возможностей, в том числе с использованием вредоносного программного обеспечения;
- внесение несанкционированных изменений в документацию на компоненты АИТС и СЗ АС.

Более сложным для анализа возможностей нарушителя является этап эксплуатации СЗ АС. Именно этот этап жизненного цикла АИТС рассмотрен далее более подробно.

Модель угроз в СЗ АС разработана на основе данных, полученных в ходе информационного обследования СЗ АС, проведенного в рамках работ по обеспечению информационной безопасности СЗ АС, в том числе обеспечению безопасности КИ при их обработке в СЗ АС.

3.1 Описание возможных нарушителей

По признаку принадлежности к СЗ АС все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование СЗ АС;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование СЗ АС.

Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Установлены следующие условия функционирования АС:

- автоматизированные рабочие места АС функционируют на контролируемых и охраняемых объектах (зданиях, помещениях);

- серверная составляющая АС, консолидирующая информационные ресурсы (в том числе ПДн), расположена в серверных помещениях, где реализуется весь необходимый и достаточный комплекс программно-технических средств и поддерживающих их организационных мер, в том числе режимных мероприятий;
- подключения к системе АС и доступ к информационным ресурсам осуществляется установленным в МЧС Республики Крым порядком с обязательной процедурой согласования;
- информационные ресурсы АС не имеют подключений к сетям общего пользования.

Учитывая указанные условия функционирования АС, предполагается, что возможные действия внешнего нарушителя приемлемо нейтрализуются и в дальнейшем анализ их действий исключается из рассмотрения в настоящей модели.

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса режимных и организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Исходя из особенностей функционирования АС, допущенные к ней физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам АИТС в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы АС (категория I);
- технический персонал АС (сотрудники эксплуатационных подразделений, осуществляющие техническое сопровождение оборудования, программного обеспечения и средств защиты информации) (категория II);
- пользователи АС (категория III);
- пользователи других АИТС, являющихся внешними по отношению к АС (категория IV);
- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы АС, но не имеющие права доступа к активам (категория V);
- обслуживающий персонал (охрана, работники инженерно–технических служб и т.д.) (категория VI);
- уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС (категория VII).

На лиц категории I и II возложены задачи по администрированию и техническому сопровождению программно-аппаратных средств АС. Администраторы и технический персонал АС потенциально могут проводить атаки, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в АС, а также к техническим и программным средствам АС, включая средства защиты, используемые в АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в АС, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для проведения атак. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категории I и II ввиду их исключительной роли в АС должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категории I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей исключается организационными и режимными мерами.

3.2 Предположения об имеющейся у нарушителя информации об объектах атак

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- *общая информация* – информация о назначения и общих характеристиках АИТС;
- *эксплуатационная информация* – информация, полученная из эксплуатационной документации;
- *чувствительная информация* – информация, дополняющая эксплуатационную информацию об АИТС (например, сведения из проектной документации АИТС).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах АС;

- сведения об информационных ресурсах АС: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств АС;
- данные о реализованных в СЗ принципах и алгоритмах;
- исходные тексты программного обеспечения АС;
- сведения о возможных каналах атак;
- информацию о способах атак.

Предполагается, что преимущественное большинство лиц категории III и все лица категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АС, к которой они не имеют санкционированного доступа. Однако предполагается, что имеется возможность ознакомления незначительного круга лиц категории III с чувствительной информацией о АС.

Предполагается, что лица категории V владеют в той или иной части эксплуатационной и общей информацией об АС, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АС, использующих систему передачи информации.

Предполагается, что лица категории VI по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VII обладают чувствительной информацией об АС, включая информацию об уязвимостях технических и программных средств АС. Организационными мерами предполагается исключить доступ лиц категории VII к техническим и программным средствам АС в период обработки защищаемой информации.

Таким образом, наиболее информированными об АС являются лица категории III и лица категории VII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные на объектах АС конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная (аутентифицирующая) информация.

3.3 Предположения об имеющихся у нарушителя средствах атак

Предполагается, что внутренний нарушитель имеет:

- программные и аппаратные компоненты СЗИ и СФ СЗИ (штатные средства);
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Состав имеющихся у нарушителя средств, которые он может использовать для проведения атак, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах АС конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств атак в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятный нарушитель имеет все необходимые для проведения атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем (с учетом реализации на объектах функционирования АС необходимых режимных мероприятий) предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами атак обладают лица категории III и лица категории VII.

3.4 Описание объектов и целей атак

Основными объектами атак являются:

- защищаемая информация (в том числе ПДн);
- документация на СЗИ и на технические и программные компоненты СФ СЗИ;
- СЗИ (программные и аппаратные компоненты СЗИ);
- технические и программные компоненты СФ СЗИ;
- каналы связи (внутри контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами;
- помещения, в которых находятся защищаемые ресурсы АС.

Кроме этого, к объектам атак можно отнести и некоторые каналы атак. К таким каналам атак относятся:

- съемные носители информации;
- носители информации, находящиеся за пределами контролируемой зоны в связи с их ремонтом, обслуживанием или передачи для использования;
- носители информации, выведенные из употребления;
- штатные средства АС.

Дополнительно к возможным объектам атак можно отнести печатные материалы, содержащие ИКХ.

Основными информационными активами в АС являются следующие:

1. Целевая информация:

- коммерческая тайна;
- служебная информация;
- другие виды ИКХ.

2. Технологическая информация:

- защищаемая управляющая информация (конфигурационные файлы, настройки системы защиты и пр.);
- защищаемая технологическая информация средств доступа к системе управления АС (аутентификационная информация и др.);
- информационные ресурсы АС на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами АС (программное обеспечение, конфигурационные файлы, настройки системы защиты и пр.) или средств доступа к этим системам управления (аутентификационная информация и др.);
- информация о ПСЗИ, их структуре, принципах и технических решениях защиты.

3. Программное обеспечение:

- программные информационные ресурсы АС, содержащие общее и специальное программное обеспечение, резервные копии общесистемного программного обеспечения, инструментальные средства и утилиты систем управления ресурсами АС, чувствительные по отношению к случайным и несанкционированным воздействиям, программное обеспечение СЗИ.

Предполагается (с учетом реализации на объектах функционирования АС необходимых режимных мероприятий), что не являются объектами атак:

- технические каналы утечки информации;
- сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- источники и цепи электропитания;
- цепи заземления.

Целью атаки является нарушение определенных для объекта атаки характеристик безопасности или создание условий для нарушения характеристик безопасности объекта атаки.

3.5 Описание каналов атак

Возможными каналами атак являются:

– каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);

– штатные средства;

– съемные носители информации;

– носители информации, находящиеся за пределами контролируемой зоны в связи с их ремонтом, обслуживанием или передачей для использования;

– носители информации, выведенные из употребления;

– каналы связи (внутри контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами;

– канал утечки за счет электронных устройств негласного получения информации.

Предполагается (с учетом реализации на объектах функционирования АС необходимых режимных мероприятий), что не являются каналами атак:

– технические каналы утечки;

– сигнальные цепи;

– источники и цепи электропитания;

– цепи заземления;

– каналы активного воздействия на технические средства с помощью облучения.

3.6 Основные способы атак

При определении основных способов атак учитывался принцип защиты на всех этапах жизненного цикла АС и ее компонентов, условия функционирования АС, а также предположения о возможных нарушителях, сформулированные в подразделах 3.1 – 3.3.

Возможны следующие атаки:

1) атаки, основанные на использовании СЗИ с уязвимостями и недокументированными (недекларированными) возможностями, внесенными на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию программных и технических средств АС;

2) перехват разглашаемых сведений о защищаемой информации, о АС и ее компонентах, включая СЗИ и СФ СЗИ;

3) атаки, основанные на документированных и недокументированных (недекларированных) возможностях оборудования (в том числе за счет модификации IP-трафика при несанкционированном подключении к каналу связи в пределах контролируемой зоны);

4) хищение производственных отходов (распечаток, записей, списанных носителей и т.п.);

5) восстановление (в том числе и фрагментарное) защищаемой информации и информации о АИТС путем анализа выведенных из

употребления и ставших после этого доступными нарушителю съемных носителей информации;

6) 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 АС;

7) негласное (скрытое) временное изъятие или хищение съемных носителей защищаемой информации, аутентифицирующей или ключевой информации;

8) негласная (скрытая) модификация защищаемой информации, хранящейся на носителях информации (в том числе на съемных носителях информации);

9) визуальный просмотр защищаемой информации, отображаемой на средствах отображения (экранах мониторов);

10) ознакомление с распечатанными документами, содержащими защищаемую информацию;

11) перехват защищаемой информации из каналов связи в пределах контролируемой зоны, незащищенных от НСД к информации организационно-техническими мерами;

12) целенаправленное искажение защищаемой информации в каналах связи в пределах контролируемой зоны, незащищенных от НСД к информации организационно-техническими мерами;

13) навязывание ложной (специально сформированной нарушителем) информации через каналы связи в пределах контролируемой зоны, не защищенные от НСД к информации организационно-техническими мерами;

14) перенаправление потоков данных путем воздействия через каналы связи в пределах контролируемой зоны, незащищенные от НСД к информации организационно-техническими мерами;

15) целенаправленное искажение команд управления, передаваемых по каналам связи в пределах контролируемой зоны, не защищенным от НСД к информации организационно-техническими мерами;

16) нарушение связи за счет преднамеренной загрузки трафика ложными сообщениями, приводящее к исчерпанию пропускной способности каналов связи;

17) доступ к оставленным без присмотра функционирующим штатным средствам;

18) несанкционированное изменение конфигурации технических средств;

19) подбор аутентифицирующей информации пользователей;

20) модификация ведущихся в электронном виде регистрационных протоколов (журналов регистрации);

21) модификация технических средств;

22) модификация программных средств с использованием штатных средств, включая нелегальное внедрение и использование неучтенных программ;

23) модификация программных средств АС с использованием вредоносных программ, размещенных на съемных носителях информации;

24) модификация программных средств с использованием внедренных в ЕК АСУ ТР компьютерных вирусов;

25) вызывание сбоев технических средств АС;

26) внесение неисправностей в технические средства АС;

27) утечка, модификация, блокирование или уничтожение защищаемой информации с использованием штатных средств;

28) утечка, модификация, блокирование или уничтожение защищаемой информации с использованием вредоносных программ, размещенных на съемных носителях информации;

29) блокирование или уничтожение технических, программных и программно-технических компонентов АС;

30) несанкционированный доступ к защищаемой информации в процессе ремонтных и регламентных работ;

31) методы социальной инженерии для получения сведений об АС, способствующих созданию благоприятных условий для применения других методов;

32) несанкционированный доступ к защищаемой информации за счет внедренных в технические средства специальных закладочных устройств, предназначенные для бесконтрольного съема информации.

4. Модель угроз безопасности информации

К основным угрозам безопасности информации АС относятся следующие:

Угроза 1

1. Аннотация угрозы – осуществление несанкционированного доступа (ознакомления) с целевой информацией при ее обработке и хранении в АС.

2. Возможные источники угрозы – пользователи АС.

3. Способ реализации угрозы – осуществление доступа к целевой информации с использованием штатных средств, предоставляемых АС.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к целевой информации, связанные с возможностью предоставления доступа к целевой информации неуполномоченным на это лицам.

5. Вид активов, потенциально подверженных угрозе – целевая информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение служебной информации и персональных данных, используемых в АС.

Угроза 2

1. Аннотация угрозы – осуществление несанкционированного копирования (хищения) информации, содержащей конфиденциальные сведения (в том числе баз данных АС).

2. Возможные источники угрозы – пользователи АС.

3. Способ реализации угрозы – осуществление действий с использованием штатных средств (предоставляемых АС), направленных на копирование (выгрузку) информации из баз данных АС.

4. Используемые уязвимости – недостатки механизмов безопасного взаимодействия АРМ пользователей с серверами АС.

5. Вид активов, потенциально подверженных угрозе – целевая информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение персональных данных и коммерческой тайны, используемых в АС.

Угроза 3

1. Аннотация угрозы – осуществление необнаруженной несанкционированной модификации (подмены) целевой информации (прежде всего, персональных данных и коммерческой тайны).

2. Возможные источники угрозы – пользователи АС.

3. Способ реализации угрозы – осуществление необнаруженной модификации (подмены) целевой информации с использованием штатных средств, предоставляемых АС.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к целевой информации и механизмов аудита, связанные с возможностью необнаруженной модификации (подмены) целевой информации неуполномоченными на это лицами.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе персональные данные и коммерческая тайна).

6. Нарушаемые характеристики безопасности активов – целостность; достоверность.

7. Возможные последствия реализации угрозы – навязывание должностным лицам модифицированной (ложной) информации; передача по запросам модифицированной (ложной) информации и нарушение режимов функционирования АС.

Угроза 4

1. Аннотация угрозы – осуществление необнаруженного несанкционированного блокирования (нарушения доступности) целевой информации.

2. Возможные источники угрозы – пользователи АС; пользователи других АИТС, являющихся внешними по отношению к АС.

3. Способ реализации угрозы – осуществление необнаруженного блокирования доступности целевой информации с использованием штатных средств АС, предоставляемых АС, а также с использованием специализированных инструментальных средств.

4. Используемые уязвимости – недостатки механизмов безопасного администрирования сервисов, предоставляемых АС а также механизмов аудита, связанные с возможностью бесконтрольного несанкционированного блокирования доступности целевой информации.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе служебная информация и персональные данные).

6. Нарушаемые характеристики безопасности активов – доступность.

7. Возможные последствия реализации угрозы – непредставление целевой информации заинтересованным лицам в отведенные временные интервалы; нарушение штатного режима функционирования АС.

Угроза 5

1. Аннотация угрозы – перехват защищаемой информации в каналах связи (каналах передачи данных) с использованием специально разработанных технических средств и программного обеспечения (специализированных программно-технических средств).

2. Возможные источники угрозы – пользователи АС; пользователи других АИТС, являющихся внешними по отношению к АС; уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – перехват целевой и технологической информации с использованием специально разработанных технических средств и программного обеспечения, не входящих в состав АС.

4. Используемые уязвимости – недостатки механизмов защиты передаваемой информации, связанные с возможностью ее перехвата из каналов связи и последующего с ней ознакомления.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе персональные данные и коммерческая информация); технологическая информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение персональных данных и коммерческой информации, используемых в АС; несанкционированное ознакомление с принципами функционирования механизмов защиты в АС, создание предпосылок к подготовке и проведению атак на информационные ресурсы АС.

Угроза 6

1. Аннотация угрозы – внедрение в АС компьютерных вирусов.

2. Возможные источники угрозы – пользователи АС; уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – внедрение компьютерных вирусов при взаимодействии с внешними системами (выгрузка баз данных, файловый обмен и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах пользователей АС.

4. Используемые уязвимости – недостатки механизмов защиты информационных ресурсов АС от компьютерных вирусов.

5. Вид активов, потенциально подверженных угрозе – программное обеспечение.

6. Нарушаемые характеристики безопасности активов – целостность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирование АС; реализация различного рода негативных

информационных воздействий на целевую, технологическую информацию и программное обеспечение АС.

Угроза 7

1. Аннотация угрозы – осуществление необнаруженных несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.) на программно-аппаратные элементы АС.

2. Источники угрозы – пользователи АС; пользователи других АИТС, являющихся внешними по отношению к АС.

3. Способ (метод) реализации угрозы – несанкционированные информационные воздействия (направленные на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.) с использованием специализированного программно-аппаратного обеспечения.

4. Используемые уязвимости – недостатки механизмов защиты программно-аппаратных элементов АС от несанкционированных внешних воздействий.

5. Вид активов, потенциально подверженных угрозе – технологическая информация; программное обеспечение.

6. Нарушаемые характеристики безопасности активов – конфиденциальность, целостность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования АС; снижение уровня защищенности АС; подготовка к последующим воздействиям и осуществление несанкционированного доступа к защищаемым информационным ресурсам ЕК АСУ ТР.

Угроза 8

1. Аннотация угрозы – осуществление несанкционированного доступа к информационным активам, основанное на использовании СЗИ, телекоммуникационного оборудования с уязвимостями и недокументированными (недекларированными) возможностями, внесенными на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств ЕК АСУ ТР.

2. Возможные источники угрозы – пользователи АС, уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – использование необнаруженных уязвимостей и недокументированных (недекларированных) возможностей СЗИ, телекоммуникационного оборудования.

4. Используемые уязвимости – наличие недокументированных (недекларированных) возможностей, внесенных на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств АС.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе персональные данные и коммерческая тайна), технологическая информация, программное обеспечение.

6. Нарушаемые характеристики безопасности активов – конфиденциальность, целостность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение защищаемой информации; нарушение режимов функционирования АС.

Угроза 9

1. Аннотация угрозы – осуществление несанкционированного доступа к защищаемой информации, основанное на восстановлении (в том числе фрагментарном) остаточной информации путем анализа выведенных из употребления, сданных в ремонт, на обслуживание, переданных для использования другим пользователям или для использования за пределами АС носителей информации.

2. Возможные источники угрозы – пользователи АС, уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – восстановление остаточной информации на носителях защищаемой информации с использованием специализированных инструментальных средств.

4. Используемые уязвимости – недостатки механизмов гарантированного уничтожения защищаемой информации, связанные с возможностью ее последующего несанкционированного восстановления.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе персональные данные и коммерческая тайна), технологическая информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение защищаемой информации.

Угроза 10

1. Аннотация угрозы – целенаправленное искажение, навязывание ложной (специально сформированной нарушителем) защищаемой информации в каналах связи (каналах передачи данных), с использованием специально разработанных технических средств и программного обеспечения (специализированных программно-технических средств).

2. Возможные источники угрозы – пользователи АС; пользователи других АИТС, являющихся внешними по отношению к АС; персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – осуществление целенаправленного искажения, навязывание ложной (специально сформированной нарушителем) защищаемой информации с использованием специально разработанных технических средств и программного обеспечения (специализированных программно-технических средств), не входящих в состав АС.

4. Используемые уязвимости – недостатки механизмов защиты информации, передаваемой по каналам связи, связанные с возможностью ее искажения и навязывания ложной информации.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе персональные данные и коммерческая тайна); технологическая информация.

6. Нарушаемые характеристики безопасности активов – целостность, достоверность.

7. Возможные последствия реализации угрозы – навязывание должностным лицам искаженной, ложной (специально сформированной нарушителем) информации; нарушение режимов функционирования АС.

Угроза 11

1. Аннотация угрозы – целенаправленное блокирование защищаемой информации в каналах связи (каналах передачи данных), с использованием специально разработанных технических средств и программного обеспечения (специализированных программно-технических средств).

2. Возможные источники угрозы – пользователи АС; пользователи других АИТС, являющихся внешними по отношению к АС; уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – осуществление целенаправленного блокирования защищаемой информации с использованием специально разработанных технических средств и программного обеспечения (специализированных программно-технических средств), не входящих в состав АС.

4. Используемые уязвимости – недостатки механизмов защиты передаваемой информации, связанные с возможностью ее блокирования в каналах связи.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе персональные данные и коммерческая тайна); технологическая информация.

6. Нарушаемые характеристики безопасности активов – доступность.

7. Возможные последствия реализации угрозы – непредставление целевой информации заинтересованным лицам в отведенные временные интервалы; нарушение штатного режима функционирования АС; срыв выполнения поставленных задач.

Угроза 12

1. Аннотация угрозы – внедрение в АС вредоносного программного обеспечения.

2. Возможные источники угрозы – пользователи АС; уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – внедрение вредоносного программного обеспечения при взаимодействии с внешними системами (выгрузка баз данных, файловый обмен и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах пользователей и администраторов АС.

4. Используемые уязвимости – недостатки механизмов защиты информационных ресурсов АС от вредоносного программного обеспечения.

5. Вид активов, потенциально подверженных угрозе – целевая информация; технологическая информация; программное обеспечение.

6. Нарушаемые характеристики безопасности активов – конфиденциальность; целостность; доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение коммерческой тайны и персональных данных; создание предпосылок к подготовке и проведению атак на информационные ресурсы АС; нарушение режимов функционирование АС; реализация различного рода негативных воздействий на целевую, технологическую информацию и программное обеспечение АС.

Угроза 13

1. Аннотация угрозы – перехват разглашаемых сведений о защищаемой информации, о АС и ее компонентах, включая СЗИ и СФ СЗИ.

2. Возможные источники угрозы – сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы АС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно–технических служб и т.д.); уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – осуществление перехвата разглашаемых сведений о защищаемой информации, о АС и ее компонентах, включая СЗИ и СФ СЗИ путем прямого прослушивания, а также с использованием специализированных инструментальных средств.

4. Используемые уязвимости – недостатки реализации необходимых организационно-режимных мероприятий на объектах АС, связанные с возможностью перехвата разглашаемой защищаемой информации.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе персональные данные и коммерческая тайна); аутентификационная информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение защищаемой информации; создание предпосылок к подготовке и проведению атак на информационные ресурсы АС.

Угроза 14

1. Аннотация угрозы – хищение производственных отходов (распечаток, записей, списанных носителей) с целью последующего анализа и несанкционированного ознакомления с целевой и технологической информацией.

2. Возможные источники угрозы – сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы АС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно–технических служб и т.д.); уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – осуществление прямого хищения производственных отходов (распечаток, записей, списанных носителей).

4. Используемые уязвимости – недостатки организационно-технических мер, обеспечивающих гарантированное уничтожение производственных отходов в АС, связанные с возможностью их несанкционированного хищения и последующего использования для проведения аналитических исследований.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в т.ч. персональные данные и коммерческая тайна); технологическая информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение защищаемой

информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы АС.

Угроза 15

1. Аннотация угрозы – осуществление несанкционированного визуального просмотра защищаемой информации, отображаемой на средствах отображения (экранах мониторов), а также несанкционированное ознакомление с распечатываемыми документами, содержащими защищаемую информацию.

2. Возможные источники угрозы – сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы АС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно–технических служб и т.д.); уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – осуществление несанкционированного визуального просмотра защищаемой информации, отображаемой на средствах отображения (экранах мониторов), несанкционированного ознакомления с распечатываемыми документами, содержащими защищаемую информацию.

4. Используемые уязвимости – недостатки реализации необходимых организационно-режимных мероприятий на объектах АС, связанные с возможностью несанкционированного визуального просмотра защищаемой информации на средствах отображения (экранах мониторов), а так же несанкционированного ознакомления с распечатываемыми документами, содержащими защищаемую информацию.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе персональные данные и коммерческая тайна); технологическая информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы АС.

Угроза 16

1. Аннотация угрозы – преднамеренное осуществление сбоев, внесение неисправностей, уничтожение технических и программно-технических компонентов АС.

2. Возможные источники угрозы – пользователи АС; уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – осуществление сбоев, внесение неисправностей, уничтожение технических и программно-технических компонентов АС путем непосредственного физического воздействия.

4. Используемые уязвимости – недостатки механизмов физической защиты компонентов АС, связанные с возможностью осуществления сбоев, внесения неисправностей, уничтожения технических, и программно-технических компонентов АС.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в т.ч. персональные данные и коммерческая тайна), технологическая информация, программное обеспечение.

6. Нарушаемые характеристики безопасности активов – доступность, целостность.

7. Возможные последствия реализации угрозы – непредоставление целевой информации заинтересованным лицам в отведенные временные интервалы; нарушение штатного режима функционирования АС; срыв выполнения поставленных задач.

Угроза 17

1. Аннотация угрозы – осуществление несанкционированного доступа к защищаемой информации в процессе ремонтных и регламентных работ.

2. Возможные источники угрозы – уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – осуществление несанкционированного доступа к защищаемой информации в процессе ремонтных и регламентных работ.

4. Используемые уязвимости – доступ лиц, имеющих право на техническое обслуживание, к техническим и программным средствам АС в момент обработки с использованием этих средств защищаемой информации.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в т.ч. персональные данные и коммерческая тайна), технологическая информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы АС; нарушение режимов функционирование АС.

Угроза 18

1. Аннотация угрозы – осуществление несанкционированного доступа к оставленным без присмотра функционирующим штатным средствам.

2. Возможные источники угрозы – сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются активы АС, но не имеющие права доступа к активам; обслуживающий персонал (охрана, работники инженерно–технических служб и т.д.); уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС.

3. Способ реализации угрозы – осуществление несанкционированного доступа к оставленным без присмотра функционирующим штатным средствам.

4. Используемые уязвимости – недостатки реализации необходимых организационно-режимных мероприятий на объектах АС, связанные с возможностью несанкционированного доступа к оставленным без присмотра функционирующим штатным средствам.

5. Вид активов, потенциально подверженных угрозе – целевая информация (в том числе служебная информация и персональные данные); технологическая информация.

6. Нарушаемые характеристики безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы АС.

5. Определение класса информационной системы

Исходя из приведенной модели угроз, в АС требуется обеспечить конфиденциальность, целостность и доступность КИ.

Учитывая, что в АС обрабатывается и хранится КИ …..(описывается режим обработки КИ и другие особенности, определяется класс защищенности)

Подробный анализ возможности реализации в АС требований защиты КИ с соответствующим обоснованием исключений (относительно требований к АС класса 1Г) приведен в таблице 1.

Таблица 1 – Обоснование реализации в АС требований безопасности КИ

№ п/п	Требование безопасности КИ	Действие над требованием	Обоснование исключения или добавления требования
1.	Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации	исключено	**Реализован адекватный набор организационных мероприятий.** ПДн консолидировано хранятся на серверах, расположенных в контролируемых помещениях. Количество администраторов АС ограничено. Администраторы руководствуются организационно-распорядительной документацией, в которой четко прописаны правила перемещения КИ на носители информации. Пользователи АС получают доступ к КИ в объеме установленных для них полномочий.
2.	Должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее используемую для хранения защищаемых данных (файлов)	исключено	**Отсутствуют соответствующие угрозы.** В числе вероятных нарушителей отсутствуют нарушители, располагающие необходимыми возможностями по доступу к информационным ресурсам АС, средствами и знаниями, а также достаточной мотивацией для совершения действий, направленных на восстановление однократно очищенной (в соответствии с требованиями ко 2 классу ИСПДн) из оперативной памяти и внешних накопителей информации.
3.	Должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления	исключено	**Отсутствуют соответствующие угрозы.** АС является АСс клиент-серверной архитектурой построения. Информационные ресурсы хранятся и обрабатываются исключительно на серверах АС с

№ п/п	Требование безопасности КИ	Действие над требованием	Обоснование исключения или добавления требования
	доступом. Маркировка должна отражать уровень конфиденциальности объекта		централизованным администрированием и ведением ресурсов. Угрозы, связанные с возможностью несанкционированного (в т.ч. ошибочного) использования информационных ресурсов (без их дополнительного маркирования) незначительны и в существующих условиях функционирования АС нереализуемы.
4.	Должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации	исключено	**Отсутствуют соответствующие угрозы.** АС является АСс клиент-серверной архитектурой построения. Информационные ресурсы хранятся и обрабатываются исключительно на серверах АС с централизованным администрированием и ведением ресурсов. Угрозы, связанные с возможностью несанкционированного использования (хищения) однократно учтенных носителей информации со стороны предполагаемого нарушителя незначительны и в существующих условиях функционирования АС нереализуемы.
5.	Регистрация выдачи (приема) носителей информации в журнале (карточке)	исключено	**Отсутствуют соответствующие угрозы.** Количество администраторов и используемых ими учитываемых носителей информации ограничено. Пользователи АС не осуществляют выгрузку КИ напрямую из АС на носители информации. Угрозы, связанные с несанкционированным использованием (хищением) учтенных носителей информации со стороны предполагаемого нарушителя незначительны и в существующих условиях

№ п/п	Требование безопасности КИ	Действие над требованием	Обоснование исключения или добавления требования
			функционирования АС нереализуемы.
6.	Реализация в АС мер специальной защиты информации, направленных на предотвращение утечки КИ по техническим каналам	исключено	**Отсутствуют соответствующие угрозы.** Ввиду наличия необходимых организационных и режимных мер защиты КИ, связанных с ограничением доступа в помещения и на объекты функционирования АС, а также физического выделения серверного сегмента АС в отдельные центры обработки данных, угрозы связанные с возможностью несанкционированного доступа к КИ с использованием технических каналов утечки со стороны предполагаемого нарушителя незначительны и в существующих условиях функционирования АС нереализуемы.
7.	Должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются дата и время изменения полномочий, идентификатор субъекта доступа (администратора), осуществившего изменения	добавлено	**Возможна реализация существующих угроз.** Учитывая зависимость уровня защищенности АС от предоставляемого пользователям объема полномочий, необходимо предотвращать угрозы, связанные с попытками (со стороны пользователей АС и пользователей внешних систем) расширения предоставленного объема полномочий с использованием штатных и специализированных инструментальных средств и последующего несанкционированного доступа к КИ.
8.	Должна осуществляться сигнализация попыток нарушения защиты	добавлено	**Возможна реализация существующих угроз.** Учитывая наличие большого числа пользователей АС и пользователей внешних систем,

№ п/п	Требование безопасности КИ	Действие над требованием	Обоснование исключения или добавления требования
			функционирующих удаленно от консолидированных информационных ресурсов, необходимо предотвращать угрозы, связанные с попытками (со стороны пользователей АС и пользователей внешних систем) осуществления несанкционированных информационных воздействий на защищаемые информационные ресурсы АС с использованием штатных и специализированных инструментальных средств.
9.	Должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы средств защиты информации в составе СЗПДн	добавлено	**Возможна реализация существующих угроз.** Учитывая масштабность функционального наполнения АС, характер хранимых и обрабатываемых КИ, большое количество пользователей и предоставляемых системой сервисов, необходимо наличие администратора (службы) защиты информации, ответственного за ведение, нормальное функционирование и контроль работы средств защиты информации в составе АС

6. Выводы

Учитывая, что АС является АС с многопользовательской архитектурой и консолидированным хранением и обработкой КИ и коммерческой тайны в физически выделенных центрах обработки данных с реализацией необходимого объема организационных и режимных мер защиты, то о возможностях нарушителя можно сделать следующие выводы.

1. Атаки внешнего нарушителя, направленные на каналы связи посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации, реализация попыток преодоления системы защиты КИ, с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам нейтрализуются организационными и режимными мероприятиями, а также условиями функционирования АС.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса режимных и организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в АС лиц категории I и II в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица категорий III-VII относятся к вероятным нарушителям. Среди лиц категорий III-VII наиболее опасными вероятными нарушителями являются лица категории III (пользователи АС) и лица категории VII (уполномоченный персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС).

Представленная модель угроз с описанием вероятного нарушителя для АС должна использоваться при формировании обоснованных требований безопасности КИ (профиля защиты АС) и проектировании СЗКИ АС.