Санкт-Петербургское государственное унитарное предприятие
«Санкт-Петербургский информационно-

УТВЕРЖДАЮ	УТВЕРЖДАЮ
Председатель Комитета по информатизации и связи Санкт- Петербурга	Директор Санкт-Петербургского государственного унитарного предприятия «Санкт-Петербургский информационно-
_____ И.А. Громов	

Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга

Частная модель угроз безопасности персональных данных, обрабатываемых в КАИС КРО

на 97 листах

К Государственному Контракту № 0172200006113000042_146076
от «03»июня 2013 г

Санкт-Петербург
2013

ЛИСТ СОГЛАСОВАНИЯ

От Комитета по информатизации и связи:

Начальник отдела информационно-компьютерной безопасности Управления информационной безопасности и технической защиты информации	А.В. Лихолетов

От СПб ГУП «СПб ИАЦ»:

Начальник управления проектирования и эксплуатации систем защиты информации	В.В. Колосов

ЛИСТ СОГЛАСОВАНИЯ

Ведущий специалист-аналитик отдела проектирования систем защиты информации СПб ГУП «СПб ИАЦ»	И.Н. Рукина
Специалист-проектировщик отдела проектирования систем защиты информации СПб ГУП «СПб ИАЦ»	А.В. Болознева

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АРМ - автоматизированное рабочее место

ИСПДн - информационная система персональных данных

ИМЦ - Информационно-методический центр

КАИС КРО - Комплексная автоматизированная информационная система каталогизации ресурсов образования Санкт-Петербурга

КОИ - криптографически опасная информация

ЛВС - локальная вычислительная сеть

МЭ - межсетевой экран

НДВ - недокументированные (недекларированные) возможности

ОС - операционная система

РЦОКОиИТ - Региональный центр оценки качества образования и информационных технологий

ПДн - персональные данные

ПО - программное обеспечение

ПЭМИН - побочные электромагнитные излучения и наводки

САЗ - система анализа защищенности

СЗИ - средства защиты информации

СЗПДн - система (подсистема) защиты персональных данных

СКЗИ - средства криптографической защиты информации

СОВ - система обнаружения вторжений

СПБ ГУП «СПБ ИАЦ» - Санкт-Петербургское государственное унитарное предприятие «Санкт-Петербургский информационно-аналитический центр»

ССОП - сеть связи общего пользования

ТС - техническое средство

УБПДн - угрозы безопасности персональных данных

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Актуальная угроза безопасности персональных данных – совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

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

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность персональных данных – состояние защищенности персональных данных характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Документированные (декларированные) возможности ПО (ТС) – функциональные возможности ПО (ТС), описанные в документации на ПО (ТС).

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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

Инсталляция – установка программного продукта на компьютер. Инсталляция обычно выполняется под управлением инсталлятора – программы, которая приводит состав и структуру устанавливаемого программного изделия в соответствии с конфигурацией компьютера, а также настраивает программные параметры согласно типу имеющейся операционной системы, классам решаемых задач и режимам работы. Таким образом, инсталляция делает программный продукт пригодным для использования в данной вычислительной системе и готовым решать определенный класс задач в определенном режиме работы.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационно-телекоммуникационная сеть общего пользования – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных

действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Криптографически опасная информация (КОИ) – информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

Модель угроз – перечень возможных угроз.

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Негативные функциональные возможности – документированные и недокументированных возможности программных и аппаратных компонентов криптосредства и среды функционирования криптосредства, позволяющие:

- модифицировать или искажать алгоритм работы криптосредств в процессе их использования;
- модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием криптосредства;

– получать доступ нарушителям к хранящимся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации, а также к защищаемой информации.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Пользователь – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и(или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Средства криптографической защиты информации - средства шифрования, средства имитозащиты, средства кодирования, средства электронной цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

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

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Уровень криптографической защиты информации – совокупность требований, предъявляемых к криптосредству.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Характеристика безопасности объекта – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами по защите персональных данных:

[1] - Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

[3] - Федеральный закон от 7 мая 2013 г. №99-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием федерального закона "О ратификации Конвенции Совета Европы О защите физических лиц при автоматизированной обработке персональных данных" и федерального закона "О персональных данных";

[4] – Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

[5] - Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденный постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211;

[6] - Указ Президента Российской Федерации от 17 марта 2008 года N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

[7] - Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462);

[8] - Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 9 февраля 2005 года № 66 (зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382);

[9] - Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их

использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, № 149/6/6-622, 2008);

[10] - Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, № 149/5-144, 2008);

[11] - Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

[12] - Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России);

[13] – Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное приказом директора ФСТЭК России от 18 февраля 2013 года № 21;

[14] - Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 года № 17.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России ([11]-[14]) и ФСБ России ([8], [9]), регламентирующих порядок обеспечения безопасности ПДн.

Настоящая «Частная модель угроз безопасности ПДн, обрабатываемых в комплексной автоматизированной системе каталогизации ресурсов образования» (далее – Модель угроз КАИС КРО) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в КАИС КРО. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит данные по угрозам безопасности персональных данных, обрабатываемых в КАИС КРО, связанным:

- с использованием средств криптографической защиты информации;
- с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в КАИС КРО с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы КАИС КРО и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов КАИС КРО, разработчиков КАИС КРО и их подсистем.

Модель угроз безопасности персональных данных при их обработке в Комплексной автоматизированной информационной системе каталогизации ресурсов образования Санкт-Петербурга первоначально была разработана в 2012 году в рамках работ по модернизации системы защиты информации КАИС КРО. В этом же году на основании Модели угроз была проведена повторная классификация КАИС КРО как информационной системы персональных данных

Повторная классификация КАИС КРО как ИСПДн выполнена на основании подпункта б) пункта 12 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного

постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 (**утратило силу**, см [4]) и «Порядка проведения классификации информационных систем персональных данных», утвержденного совместным приказом ФСТЭК России, ФСБ России и Министерством информационных технологий и связи Российской Федерации от 13 февраля 2008 года №55/86/20.

В соответствии с требованиями Государственного Контракта № 0172200006113000042_146076 от «03» июня 2013 года на выполнение работ по развитию КАИС КРО в 2013 году в Модель угроз внесены дополнения, связанные с определением типа угроз безопасности персональных данных.

Определение типа угроз безопасности персональных данных актуальных для КАИС КРО выполнено в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства РФ от 1.11.2012 № 1119.

Требования к защите персональных данных при их обработке в информационных системах персональных данных [4] устанавливают четыре уровня защищенности персональных данных при их обработке в информационных системах. Необходимыми условиями определения уровня защищенности является установление типа угроз безопасности персональных данных, актуальных для информационной системы, и категории персональных данных, обрабатываемых в информационной системе.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности КАИС КРО от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- оценка вреда, который может быть причинен субъектам персональных данных[1] в случае нарушения требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- определение типа угроз безопасности персональных данных, актуальных для КАИС КРО;
- определение уровня защищенности персональных данных [4], который необходимо обеспечить при их обработке в КАИС КРО;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса КАИС КРО;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим

[1] Пункт 5 часть 1 статьи 18 Федерального закона «О персональных данных».

права доступа к такой информации;

- недопущение воздействия на технические средства КАИС КРО, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением уровня защищенности персональных данных.

В Модели угроз дано обобщённое описание КАИС КРО как объекта защиты, возможных источников УБПДн, основных классов уязвимостей КАИС КРО, возможных видов неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в КАИС КРО, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в КАИС КРО. Внесение изменений в Модель угроз КАИС КРО осуществляется также в случае внесения новых элементов в [13]. Кроме того, Модель угроз может быть пересмотрена по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений КАИС КРО, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

2. ХАРАКТЕРИСТИКА КАИС КРО КАК ИСПДН.

Комплексная автоматизированная информационная система каталогизации ресурсов образования предназначена для сбора, обработки, предоставления и распространения информации об образовательных процессах, осуществляемых образовательными учреждениями Санкт-Петербурга, на базе информационно-коммуникационных технологий с использованием иных информационных ресурсов в сфере образования.

КАИС КРО располагается по адресам дошкольных образовательных учреждений Санкт-Петербурга, общеобразовательных учреждений Санкт-Петербурга, учреждений Санкт-Петербурга начального профессионального и среднего профессионального образования, учреждений Санкт-Петербурга дополнительного образования детей, а также в Комитете по образованию, РЦОКОиИТ, ИМЦ, СПб ГУП «АТС Смольного», СПБ ГУП «СПБ ИАЦ».

КАИС КРО является государственной информационной системой, в которой обрабатываются преимущественно государственные информационные ресурсы.

В КАИС КРО аккумулируются значительные объемы информации ограниченного доступа. В первую очередь это:

- ПДн лиц, которые обучаются или обучались ранее в ОУ или ДОУ;
- ПДн лиц, являющихся родителями или опекунами обучающихся в ОУ или ДОУ,
- ПДн лиц, являющихся работниками ОУ или ДОУ.

Обработка персональных данных на объектах образования Санкт-Петербурга связана с риском нарушения тайны частной жизни граждан РФ, неприкосновенность которой гарантирует Конституция РФ.

Согласно Федеральному закону «О персональных данных» [2], при обработке персональных данных оператор в ходе обработки информации обязан предпринимать мероприятия по обеспечению безопасности ПДн.

Оператором КАИС КРО является Комитет по образованию Санкт-Петербурга.

В КАИС КРО обрабатываются персональные данные не сотрудников оператора персональных данных.

В КАИС КРО не обрабатываются специальные, биометрические и общедоступные персональные данные.

Таким образом, КАИС КРО является системой, обрабатывающей **иные категории персональных данных.**

В КАИС КРО одновременно обрабатываются персональные данные **более чем 100000 субъектов персональных данных**.

КАИС КРО является территориально-распределенной информационной системой, поскольку входящие в ее состав технические средства обработки информации размещены в пределах различных локальных составных частей, всего свыше 2000 адресов.

Контролируемой зоной КАИС КРО являются коридоры и рабочие помещения образовательных учреждений, а также серверные помещения. Границами контролируемых зон являются стены, двери, окна и межэтажные перекрытия помещений образовательных учреждений.

В качестве среды передачи данных между техническими средствами, размещенными в различных локальных составных частях используются каналы передачи данных сети «ЕМТС» и сетей связи общего пользования (ССОП), в т.ч. сети Интернет.

Взаимодействие КАИС КРО с другими государственными информационными системами осуществляется с применением средств межсетевого экранирования.

В составе КАИС КРО функционируют следующие подсистемы:

1. подсистема портал «Петербургское образование»;
2. подсистема публикации данных на портале «Петербургское образование»;
3. подсистема «Параграф»;
4. подсистема «Закрытый портал»;
5. подсистема поиска;
6. подсистема администрирования.

Подсистема портал «Петербургское образование» предназначена для предоставления пользователям КАИС КРО доступа к информации об образовательных учреждениях Санкт-Петербурга и интерактивным возможностям КАИС КРО посредством веб-интерфейса путем работы со специализированными сервисами.

Подсистема портал «Петербургское образование» имеет следующие характеристики:

1. категория обрабатываемых ПДн: **2 категория** - персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию;
2. объем обрабатываемых ПДн: **в информационной системе не обрабатываются данные более чем о 100 000 субъектах персональных данных;**
3. структура информационной системы (портал «Петербургское образование»): **локальная информационная система**, расположенная в ЦОД ГУП «АТС Смольного»;

4. режим обработки персональных данных: **многопользовательский с разграничением прав доступа пользователей;**
5. местонахождение технических средств ИСПДн: **195248, Россия, Санкт-Петербург, пр. Ириновский, д.2**;
6. эксплуатирующее подразделение: **СПб ГУП «АТС Смольного»** (администраторами средств защиты информации защищенного корпоративного узла телематических служб исполнительных органов государственной власти Санкт-Петербурга являются сотрудники Санкт-Петербургского информационно-аналитического центра);
7. вид обработки ПДн:

- хранение персональных данных пользователей;
- обезличивание персональных данных при взаимодействии с АИСУ «Параграф» и МАИС МФЦ;
- сбор персональных данных поступающих из образовательных учреждений;
- обновление, изменение персональных данных согласно поступившей информации из ОУ.

Подсистема публикация данных на портале «Петербургское образование» предназначена для решения следующих задач:

- обеспечения доступа пользователей КАИС КРО к информации об образовательных учреждениях Санкт-Петербурга, в том числе с осуществлением географической привязки к карте;
- предоставления сведений об образовательных услугах; процессах, происходящих в сфере образования;
- проведения опросов авторизованных пользователей КАИС КРО о работе образовательных учреждений Санкт-Петербурга;
- обеспечения информационной поддержки видеоконференций;
- предоставления данных в Комитет по образованию.

Подсистема «Параграф» представляет собой многофункциональный программно-технологический комплекс, ориентированный на образовательные учреждения, позволяющий автоматизировать многие элементы управленческой деятельности:

- ведение баз данных образовательных учреждений;
- автоматический выбор данных с заданными параметрами;
- подготовку в электронной и печатной форме разнообразных списков, отчетов;
- составление учебных планов;

- распределение нагрузки;
- многофакторный анализ результатов промежуточной и итоговой аттестации обучающихся.

Все локальные составные части подсистемы «Параграф» имеют в своем составе только информационные подсистемы для доступа к соответствующим локальным базам данных уровня образовательного учреждения. Системные сервисы, обеспечивающие работу локальных составных частей, обеспечиваются средствами вычислительной техники соответствующих образовательных учреждений.

Единая БД подсистемы «Параграф» формируются на локальном сервере РЦКОИиИТ путем периодической репликации единой БД на основе предоставления реплик БД районных центров информатизации. Для передачи реплик БД в РЦКОИиИТ используются каналы передачи данных сети «ЕМТС». Отдельные локальные составные части подсистемы «Параграф» продолжают использовать для репликации БД способ доставки курьером на внешних носителях данных (флеш-устройства), до момента подключения к сети «ЕМТС».

Для работы подсистемы «Параграф» требуется, чтобы на компьютере, выполняющем роль сервера локальной составной части, был установлен и запущен сервер баз данных Firebird.

Как ИСПДн подсистема «Параграф» имеет следующие характеристики:

1. категория обрабатываемых ПДн: **категория 2** – персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию;
2. объем обрабатываемых ПДн: **в информационной системе одновременно обрабатываются персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования**;
3. по заданным оператором характеристикам безопасности ПДн: **специальная ИСПДн с заданными характеристиками безопасности** - защищенность от нарушения конфиденциальности, уничтожения, изменения, блокирования;
4. структура информационной системы: **распределенная информационная система**;
5. наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: **ИСПДн, имеющая подключения**;

6. режим обработки персональных данных в ИСПДн: многопользовательская ИСПДн;
7. разграничение прав доступа пользователей: **ИСПДн с разграничением прав доступа**;
8. местонахождение технических средств ИСПДн: **ИСПДн, все технические средства которой находятся в пределах Российской Федерации**;
9. цель создания ИСПДн (цель обработки ПДн): **обеспечение учебно-образовательного процесса**;
10. эксплуатирующее ИСПДн подразделение: **сотрудники ОУ, ДОУ**;
11. перечень ПДн, которые обрабатываются в ИСПДн: **ПДн об ученике/воспитаннике образовательного учреждения и одном либо двух родителях ученика/воспитанника, а также данные о работниках образовательного учреждения**;
12. вид обработки ПДн: **сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), уничтожение ПДн**.

Подсистема «Закрытый портал» на момент проведения обследования находилась в стадии разработки. Подсистема «Закрытый портал» предназначена для ответственных должностных лиц ИОГВ и служит для обеспечения запросов и предоставления необходимых сведений в ходе оказания государственных услуг или исполнения государственных функций. Подсистема «Закрытый портал», в частности включает автоматизированное рабочее место сотрудника администрации района Санкт-Петербурга, ответственного за социальное льготное питание учащихся ОУ.

Подсистема поиска обеспечивает автоматический выбор данных с заданными параметрами, подготовку в электронной и печатной форме разнообразных списков и отчетов. Подсистема поиска отслеживает права доступа пользователей КАИС КРО на основании поддержки аппарата разделения полномочий пользователей.

Подсистема администрирования обеспечивает выбор режима функционирования КАИС КРО, управление взаимодействием КАИС КРО с внешними системами, контроль условий эксплуатации программного обеспечения и комплекса технических средств системы. В штатном режиме подсистема администрирования функционирует круглосуточно. В сервисном режиме функционирования подсистема администрирования обеспечивает возможность обновления программного обеспечения, планового обслуживания или замены оборудования.

На основании выше представленных данных получены следующие обобщенные характеристики КАИС КРО как ИСПДн:

1. категория обрабатываемых ПДн: **категория 2** – персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию;
2. объем обрабатываемых ПДн: **в информационной системе одновременно обрабатываются персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования**;
3. по заданным оператором характеристикам безопасности ПДн: **специальная ИСПДн с заданными характеристиками безопасности** - защищенность от нарушения конфиденциальности, уничтожения, изменения, блокирования;
4. структура информационной системы: **распределенная информационная система**;
5. наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: **ИСПДн, имеющая подключения**;
6. режим обработки персональных данных в ИСПДн: **многопользовательская** ИСПДн;
7. разграничение прав доступа пользователей: **ИСПДн с разграничением прав доступа**;
8. местонахождение технических средств ИСПДн: **ИСПДн, все технические средства которой находятся в пределах Российской Федерации,** в городе Санкт-Петербург, в пределах контролируемых зон объектов информатизации КАИС КРО;
9. цель создания ИСПДн (цель обработки ПДн): **обеспечение учебно-образовательного процесса**;
10. эксплуатирующее ИСПДн подразделение: **сотрудники ОУ, ДОУ**;
11. перечень ПДн, которые обрабатываются в ИСПДн: ПДн об ученике/воспитаннике образовательного учреждения и одном либо двух родителях ученика/воспитанника, а также данные о работниках образовательного учреждения;
12. вид обработки ПДн: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), уничтожение ПДн.

По итогам повторной классификации 2012 года определено, что система защиты информации КАИС КРО должна обеспечивать нейтрализацию актуальных угроз безопасности с использованием методов и способов защиты персональных данных, предусмотренных для информационных систем персональных данных **2 класса.**

Для определения типа угроз безопасности персональных данных актуальных для КАИС КРО проведен анализ КАИС КРО как объекта защиты, рассмотрены возможные источники УБПДн, основные классы уязвимостей КАИС КРО, возможные виды неправомерных действий и деструктивные воздействия на ПДн, а также основные способы их реализации.

Значение типа угроз безопасности персональных данных, актуальных для КАИС КРО, приведено в разделе 7 настоящей Модели угроз.

3. ЭЛЕМЕНТЫ ОПИСАНИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ КАИС КРО

3.1. Исходный уровень защищенности КАИС КРО

Под уровнем исходной защищенности КАИС КРО понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик КАИС КРО. Показатели исходной защищенности КАИС КРО представлены в таблице 3.1. Показатели защищенности определены в соответствии с пунктом 2 методического документа ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Таблица 3.1 Показатели исходной защищенности КАИС КРО

№ п/п	Технические и эксплуатационные характеристики КАИС КРО	Уровень защищенности
1.	По территориальному размещению – распределенная ИСПДн, развернутая в пределах города	низкий
2.	По наличию соединения с сетями общего пользования – ИСПДн, имеющая многоточечный выход в сеть общего пользования;	низкий
3.	По встроенным (легальным) операциям с записями баз персональных данных – модификация, передача	низкий
4.	По разграничению доступа к персональным данным – к ИСПДн имеет доступ определенный перечень сотрудников	средний
5.	По наличию соединений с другими базами персональных данных иных информационных систем персональных данных – ИСПДн, в которой используется несколько баз ПДн, принадлежащих одной организации	средний
6.	По уровню обобщения (обезличивания) персональных данных – ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	средний
7.	По объему персональных данных, которые предоставляются сторонним пользователям КАИС КРО без предварительной обработки – ИСПДн предоставляющая часть ПДн	средний

Таким образом, КАИС КРО имеет **низкий уровень защищенности** (57,14% характеристик КАИС КРО соответствуют уровню «средний», 42,86% характеристик соответствуют уровню «низкий») и числовой коэффициент **Y1 = 10**.

3.2. Перечень защищаемых ресурсов КАИС КРО

Проведенное обследование показало, что в КАИС КРО обрабатываются:

1. Персональные данные, относящиеся к информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (конфиденциальная информация), и подлежащие защите согласно действующему законодательству Российской Федерации;
2. Общедоступная информация, доступ к которой не ограничивается Федеральными законами Российской Федерации, но может быть ограничен обладателем такой информации;
3. Технологическая информация, доступ к которой разрешен определенному кругу лиц из числа администраторов сети, серверов, баз данных, администраторов безопасности информации.

В КАИС КРО кроме персональных данных, а также технологической информации, раскрывающей методы и средства защиты информации, не обрабатываются другие виды информации ограниченного доступа (государственная тайна, профессиональная тайна, коммерческая тайна и др.).

Сохранение конфиденциальности, целостности и доступности технологической информации необходимо для обеспечения безопасности основного защищаемого информационного ресурса - персональных данных обучающихся и их родителей. В связи с этим, в данной модели угроз отдельно не рассматриваются угрозы безопасности технологической информации, а считается, что они соответствуют угрозам защищаемого информационного ресурса.

3.3. Перечень объектов воздействия, содержащих ресурсы КАИС КРО

В соответствии с используемой технологией обработки данных, персональные данные хранятся:

1. на сервере баз данных подсистемы портал «Петербургское образование», установленном в серверном помещении Центра хранения данных СПБ ГУП «АТС Смольного»;
2. на сервере приложений подсистемы портал «Петербургское образование», установленном в серверном помещении Центра хранения данных СПБ ГУП «АТС Смольного»;

3. на сервере резервирования подсистемы портал «Петербургское образование», установленном в серверном помещении Центра хранения данных СПБ ГУП «АТС Смольного»;
4. на сервере ВКС подсистемы портал «Петербургское образование», установленном в серверном помещении Центра хранения данных СПБ ГУП «АТС Смольного»;
5. на серверах баз данных локальных составных частей подсистемы «Параграф», установленных в образовательных учреждения Санкт-Петербурга (более 2000 учреждений);
6. на серверах баз данных районных центров информатизации образования (18 центров уровня РОНО);
7. на серверах базы данных регионального центра оценки качества образования и информационных технологий (ЦОД «Петербургское образование»);
8. на встроенных дисковых накопителях рабочих станций пользователей в виде файлов (отчетов, справок и т.п.), содержащих фрагменты БД сервера;
9. на встроенных дисковых накопителях серверов, которые содержат резервные копии баз данных.

Прикладное программное обеспечение рабочих станций пользователей, предоставляет требуемый функционал для работы с массивами персональных данных. Взаимодействие серверов и рабочих станций основано на применении протокола TCP/IP.

Основными программно-техническими средствами КАИС КРО, обрабатывающими защищаемые ресурсы, являются:

1. серверы баз данных локальных составных частей КАИС КРО;
2. прикладное программное обеспечение КАИС КРО;
3. рабочие станции пользователей с установленным прикладным обеспечением КАИС КРО;
4. коммуникационное оборудование для передачи данных.

Таким образом, объектами воздействия, обрабатывающими защищаемую информацию (обозначение «Д» в указанных ниже таблицах 6.3-6.6 и таблице 6.8, приложениях А, Б, Г), являются:

1. узлы КАИС КРО (АРМ, серверное оборудование и т.п.);
2. средства, реализующие сетевое взаимодействие в сети.

Более подробно объекты воздействия (согласно технологии обработки информации в КАИС КРО) представлены в Таблице 3.2. В графе «Важность ресурса» указывается градация объектов воздействия с точки зрения наибольшего интереса для нарушителя

(очень высокая степень опасности). Важность ресурса определяется исходя из различия объема одновременно обрабатываемых защищаемых информационных ресурсов.

Таблица 3.2 Объекты воздействия

	Наименование	**Объект воздействия**	**Особенности**	**Важность ресурса**
Д.1	АРМ	Жесткие магнитные диски (встроенные)	Может содержать защищаемые данные (в виде каких-либо отчетов, выборки и т.д.)	средняя
		Оперативная память	Защищаемые данные уничтожается сразу после отключения питания	средняя
		Кэш-память, буферы ввода-вывода		средняя
		Видеопамять		низкая
		Монитор	Память объекта предназначена только для выполнения определенных задач данного устройства	низкая
		Клавиатура		низкая
		Принтер		низкая
		Привод магнитных и оптических дисков		низкая
		Порты ввода/вывода для подключения периферийных устройств		низкая
Д.2	Сервер	Жесткие магнитные диски (встроенные)	Содержит весь массив защищаемых данных	очень высокая
		Оперативная память	Серверы работают круглосуточно, поэтому защищаемая информация не уничтожается	высокая
		Кэш-память, буферы ввода-вывода		высокая
		Видеопамять		низкая
		Монитор	Память объекта предназначена только для выполнения определенных задач данного устройства	низкая
		Привод магнитных и оптических дисков		низкая
		Порты ввода/вывода для подключения периферийных устройств		низкая
Д.3	Отчуждаемые носители информации	Флеш-накопители, оптические диски	Может содержать любые защищаемые данные (в виде каких-либо отчетов, выборки и т.д.)	средняя
		Распечатанная документация и др. материальные носители видовой информации		средняя
Д.4	Линии связи и коммутационное оборудование	Совокупность средств передачи данных – коммутаторы	Содержит защищаемые данные при информационном обмене и передаче служебной информации	средняя

В зависимости от объекта воздействия, угрозы доступа (проникновения) в программную среду КАИС КРО подразделяются на угрозы непосредственного и удаленного доступа

3.4. Безопасность системного и прикладного программного обеспечения

Важность работы по определению недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в КАИС КРО, предопределена Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119. Так Требованиями определены три типа угроз:

1. Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;
2. Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;
3. Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Основой безопасности КАИС КРО и всех ее сервисов, подсистем, приложений и автоматизированных рабочих мест является операционная система. Прежде чем разрабатывать меры защиты для приложений в сети, необходимо определить уровень защиты программного обеспечения, определяющего работу служб, на которых базируются приложения. Анализ среды функционирования прикладного программного обеспечения направлен на выявление условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным, обрабатываемым в КАИС КРО и выполнен в разделе 3.5.3 настоящей Модели угроз.

Обеспечение безопасности приложений, а также процессов, используемых для их создания, выполнения и управления данными, является камнем преткновения на текущем этапе создания системы защиты информации КАИС КРО. На ряду с обычными пользователями сегодня в КИС КРО имеет доступ большая группа разработчиков. Все приложения создаются с помощью одних и тех же средств, языков, и в любом случае при их создании присутствует человеческий фактор, так как идеальных специалистов нет, и,

следовательно, нельзя создать идеальную программу. Анализ угроз, связанных с внесением недекларированных возможностей в прикладное программное обеспечение КАИС КРО выполнении в разделе 3.4 настоящей Модели угроз.

Для целей дальнейшего выбора мер по обеспечению безопасности персональных данных следует определить принципы и подходы к разработке безопасных приложений КАИС КРО, не зависимо от того, какая технология используется при написании той или иной программы, и не зависимо от типа разрабатываемого приложения.

3.5. Источники угроз безопасности персональным данным КАИС КРО

В ходе проведения обследования КАИС КРО как ИСПДн было установлено, что источниками угроз НСД в КАИС КРО являются нарушитель, программно-аппаратная закладка, носитель вредоносной программы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационной системе персональных данных. В качестве основных побудительных причин противоправных действий вероятных нарушителей безопасности информации следует рассматривать:

- получение материальной выгоды;
- моральное самоудовлетворение;
- халатность, невнимательность, спешка;
- месть;
- разведывательная деятельность.

По наличию права доступа в контролируемую зону КАИС КРО нарушители делятся на внешних и внутренних.

В качестве внешнего рассматривается нарушитель, не имеющий права легального доступа в контролируемую зону объекта информатизации, а также доступа к работе со штатными программно-техническими средствами объекта информатизации КАИС КРО. Внутренний нарушитель – это нарушитель, имеющий легальный разовый или постоянный доступ в контролируемую зону, и реализующий угрозы непосредственно в КАИС КРО. Внутренний нарушитель может иметь различные права доступа к информационным ресурсам, так и не иметь их вовсе.

Целями вероятного нарушителя, реализующего субъективные угрозы в своих интересах, являются:

1. возможность внесения изменений в текущие данные, обрабатываемые в КАИС КРО;
2. незаконное получение доступа к персональным данным, обрабатываемым в КАИС КРО для использования в своих целях;
3. нарушение возможности доступа к информационным ресурсам КАИС КРО (блокирование и/или уничтожение защищаемых информационных ресурсов).

3.5.1 Внешний нарушитель

Внешний нарушитель может быть источником угроз утечки информации по техническим каналам, а также угроз несанкционированного доступа в КАИС КРО.

По методу доступа к информационным ресурсам КАИС КРО внешних нарушителей можно разделить на две группы:

- лица, находящиеся за пределами контролируемой зоны, применяющие технические средства ведения разведки и/или закладочные устройства, размещенные в контролируемой зоне;
- лица, получившие доступ к информационным ресурсам КАИС КРО из внешних сетей телекоммуникаций, в том числе сетей связи общего пользования (сети международной ассоциации «Интернет»).

Внешний нарушитель может воздействовать на ресурс (на операционную систему, на сетевые службы, на информацию, обрабатываемую сетевыми службами) и на канал связи (на сетевое оборудование или на протоколы связи) или на персонал КАИС КРО. Воздействие на персонал может быть как физическое, так и психологическое (с целью получения информации или с целью нарушения непрерывности функционирования КАИС КРО).

Внешний нарушитель имеет следующие возможности:

1. осуществлять перехват (съем) информации с использованием технических средств регистрации и приема информации;
2. осуществлять несанкционированный доступ к каналам связи, выходящим за пределы контролируемых зон образовательных учреждений;
3. осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования;
4. осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, программных закладок;
5. осуществлять несанкционированный доступ через элементы информационной инфраструктуры КАИС КРО, которые в процессе своего жизненного цикла

(модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны;

6. осуществлять несанкционированный доступ через взаимодействующие информационные системы при их подключении к КАИС КРО;
7. перехват обрабатываемых техническими средствами ОИС персональных данных, за счет их утечки по каналам ПЭМИН с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки ПЭМИН серийной разработки.

Описание внешних нарушителей приведено в таблице 3.3.

Таблица 3.3 Классификация внешних нарушителей

Категория (вид) нарушителя, обозначение	**Квалификация**	**Техническая оснащенность**	**Степень опасности**
Лица, находящиеся за пределами контролируемой зоны и использующие технические средства ведения разведки и/или закладочные устройства – А.1.1	Высокая. Опыт получен в процессе профессиональной деятельности	Технические средства перехвата без модификации компонентов системы	Низкая
Лица, получившие доступ к информационным ресурсам КАИС КРО из внешних сетей телекоммуникаций, в том числе ССОП- А.1.2	Может быть высокой в случае профессиональной деятельности нарушителя, а также в случае сговора группы нарушителей (например с целью финансовой выгоды)	Программно-технические средства воздействия с возможностью модификации компонентов системы	Высокая

Внешними нарушителями могут быть:

1. бывшие сотрудники образовательного учреждения или организаций, осуществляющих администрирование ОИС;
2. лица, отнесенные к категории внутренних нарушителей, но осуществляющие угрозы безопасности за пределами контролируемой зоны;
3. разведывательные службы иностранных государств;
4. представители криминальных структур;
5. внешние субъекты (физические лица), стремящиеся получить доступ к информационным ресурсам в инициативном порядке.

Бывшие сотрудники могут использовать для достижения целей свои знания о технологии обработки информации в КАИС КРО, применяемых мерах по защите информации и правах доступа субъектов к защищаемым ресурсам. Полученные в

образовательном учреждении знания и опыт выделяют их в качестве наиболее опасных среди других источников внешних угроз.

В случае реализации угроз безопасности представителями разведывательных служб иностранных государств, способы реализации будут являться крайне эффективными и основываться на передовых технических решениях в совокупности с высочайшей квалификацией специалистов, однако привлечение подобных средств для добывания информации из КАИС КРО может оказаться экономически нецелесообразным.

Криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников образовательных учреждений всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания об уязвимостях программных средств, используемых в информационной системе. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными сотрудниками и криминальными структурами.

3.5.2 Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны организационно-технических мер защиты, в том числе по допуску физических лиц к персональным данным и контролю порядка проведения работ.

Внутренний нарушитель является источником угроз несанкционированного доступа к информации.

Внутренние нарушители подразделяются на категории в зависимости от способа доступа и полномочий доступа к КАИС КРО.

Внутренним нарушителем может быть лицо из следующих категорий:

1. пользователи программно-технических средств объектов информатизации КАИС КРО;
2. администраторы всех уровней иерархии объектов информатизации КАИС КРО;
3. руководители различных уровней должностной иерархии;
4. разработчики приложений КАИС КРО.

Возможности и потенциальная опасность противоправных действий внутренних нарушителей раскрыты в таблице 3.4.

Таблица 3.4. Классификация внутренних нарушителей

№ п/п	Категория нарушителя	Выполняемые функции в КАИС КРО	Возможности	Степень опасности
1.	Лицо, имеющее санкционированный доступ в КЗ, в которой размещены технические средства КАИС КРО, но не имеющее прав доступа к защищаемым ресурсам - А.2.1	Обеспечение нормального функционирования технических средств КАИС КРО	– располагает фрагментами информации, содержащими ПДн; – располагает фрагментами информации о топологии ИСПДн, об используемых коммуникационных протоколах и сервисах; – располагает именами зарегистрированных пользователей; – способен изменять конфигурацию и осуществлять несанкционированное подключение к техническим средствам ИСПДн; – способен вносить программно-аппаратные закладки.	Низкая
2.	Лицо, обеспечивающее поставку, сопровождение и ремонт технических средств КАИС КРО - А.2.2	Поставка, сопровождение и ремонт средств вычислительной техники	– обладает возможностью внесения закладок в технические средства КАИС КРО; – может располагать фрагментами информации о топологии ИСПДн и о технических средствах.	Низкая
3.	Зарегистрированный пользователь КАИС КРО, имеющий права доступа к защищаемым ресурсам с рабочего места (оператор) – А.2.3.	Чтение, поиск, ввод новых данных, извлечение данных в КАИС КРО	– располагает фрагментами информации о топологии ИСПДн, об используемых коммуникационных протоколах и сервисах; – способен изменять конфигурацию и осуществлять несанкционированное подключение к техническим средствам ИСПДн; – способен вносить программно-аппаратные закладки; – имеет учетную запись в системе; – имеет доступ к некоторому массиву ПДн.	Средняя
4.	Зарегистрированный пользователь КАИС КРО, обладающий правами администратора баз данных КАИС КРО, а	Управление учетными записями операторов, их правами доступа, техническая поддержка	– обладает информацией об алгоритмах и программах обработки данных в ИСПДн; – обладает возможностями внесения ошибок, недекларированных	Высокая

	также имеющий право на техническое обслуживание, сопровождение и модификацию компонентов закрепленного за ним объекта информатизации – А.2.4	пользователей. Доработка прикладного ПО, поддержка работоспособности основных компонентов.	возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения; – обладает информацией об уязвимостях технических и программных средств ИСПДн; – знает функциональные особенности, основные закономерности формирования массивов данных и потоков запросов к ним; – осуществляет управление доступом пользователей к ПДн.	
5.	Зарегистрированный пользователь КАИС КРО, обладающий полномочиями системного администратора/администратора безопасности КАИС КРО – А.2.5.	Настройка и управление программным обеспечением и оборудованием, включая средства защиты информации КАИС КРО; управление правилами разграничения доступа, генерация ключевых элементов, смену паролей.	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении КАИС КРО; – обладает полной информацией о КАИС КРО; – имеет доступ ко всем техническим средствам обработки информации и данным КАИС КРО, ко всем техническим и программным средствам защиты информации и протоколирования КАИС КРО; – обладает правами конфигурирования и административной настройки технических средств КАИС КРО.	Высокая
6.	Лицо, осуществляющее разработку прикладного ПО КАИС КРО – А.2.6	Разработка прикладного ПО, изменение функциональных возможностей основных компонентов КАИС КРО	– обладает возможностью внесения недекларированных возможностей, ошибок, вредоносных программ в прикладное ПО КАИС КРО на стадии его разработки; – обладает информацией об уязвимостях технических и программных средств КАИС КРО; – знает функциональные особенности, основные закономерности формирования массивов данных и потоков запросов к ним; – имеет доступ к некоторому массиву ПДн.	Высокая

Лицо из перечисленных в таблице выше категорий, в соответствии со степенью опасности (низкая – средняя – высокая), может нанести меньший или больший ущерб системе и реализовать ту или иную угрозу безопасности информации КАИС КРО.

Наибольшую вероятность реализовать угрозы безопасности информации и нанести ущерб КАИС КРО имеют пользователи с полномочиями администратора БД КАИС КРО, системного администратора / администратора безопасности, разработчика информационной системы (пользователи категории А.2.4-А.2.6).

На лиц категории А.2.4-А.2.5 возложены задачи по администрированию программно-аппаратных средств и баз данных КАИС КРО. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в КАИС КРО, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в системе, в соответствии с установленными для них административными полномочиями. Лица данной категории хорошо знакомы с основными алгоритмами, протоколами обмена данных, применяемыми в информационной системе, а также с принципами и концепциями безопасности. Предполагается, что для идентификации уязвимостей и/или реализации угроз безопасности может применяться как специализированное оборудование, так и стандартное, входящее в состав применяемых штатных средств, либо полученное из доступных источников.

Лица категории А.2.6 осуществляют разработку приложения, используя при этом одни и те же средства и языки, и в любом случае при создании прикладного ПО присутствует человеческий фактор, так как идеальных специалистов нет, и, следовательно, нельзя создать идеальную программу.

Учитывая исключительную роль лиц категорий А.2.4-А.2.6, а также их возможности по реализации угроз безопасности в КАИС КРО и сложность противодействия этим угрозам, необходимо применять:

- комплекс правовых и организационных мер, предусматривающих ответственность и правовые последствия для лиц, нарушивших требования информационной безопасности и повлекших наступление негативных последствий для субъектов персональных данных;
- комплекс организационных мер по их подбору, кадровой расстановке и контролю выполнения ими функциональных обязанностей;

– принципы и подходы к разработке безопасных приложений, не зависимо от того, какая технология используется при написании той или иной программы, и не зависимо от типа разрабатываемого приложения.

Предполагается, что лица категорий А.2.1-А.2.6 относятся к вероятным нарушителям. Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

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

В целях создания необходимых условий безопасности персональных данных предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

3.5.3 Программно-аппаратные закладки

Программно-аппаратные закладки классифицируются по методу их внедрения в компьютерную систему (Таблица 3.5).

Таблица 3.5 Классификация программно-аппаратных закладок

Тип закладки	**Среда обитания**	**Деструктивные действия**	**Вероятность нанести ущерб**
Программно-аппаратные закладки, ассоциированные с аппаратными средствами компьютера	BIOS	Внесение произвольных искажений в коды программ, находящихся в оперативной памяти компьютера	Средняя
Загрузочные закладки, ассоциированные с программами начальной загрузки	Загрузочный сектор	Перенесение фрагментов информации из одних областей оперативной или внешней памяти в другие	Средняя
Драйверные закладки	Драйверы	Искажение выводимой на внешние компьютерные устройства или в канал связи информации, полученной в результате работы других программ	Низкая
Прикладные закладки - текстовые редакторы, утилиты,	Прикладное ПО общего назначения	Изменение алгоритмов функционирования системных, прикладных и	Высокая

антивирусные мониторы и программные оболочки		служебных программ	
Исполняемые закладки - чаще всего представляют собой пакетные файлы, т. е. файлы, которые состоят из команд операционной системы, выполняемых одна за одной, как если бы их набирали на клавиатуре компьютера	Исполняемые программные модули, содержащие код закладки	Изменение алгоритмов функционирования системных, прикладных и служебных программ	Высокая
Закладки-имитаторы, интерфейс которых совпадает с интерфейсом некоторых программ, требующих ввода конфиденциальной информации (паролей, криптографических ключей, номеров кредитных карточек)	Служебные программы	Копирование информации пользователя	Высокая
Замаскированные закладки - маскируются под файловые архиваторы, дисковые дефрагментаторы	Программные средства оптимизации работы	Навязывание определенных режимов работы	Высокая

Программно-аппаратная закладка – это программа (фрагмент программы) или электронное устройство, скрытно внедряемая в защищенную систему и позволяющая нарушителю, внедрившему ее, осуществлять в дальнейшем НСД к тем или иным ресурсам защищенной системы. Целью внедрения закладки является обеспечение в нужный момент времени утечки информации, нарушения ее целостности или доступности.

Поскольку внедрение программно-аппаратных закладок производится нарушителем, то в дальнейшем будем считать, что возможности по осуществлению тех или иных деструктивных действий внутренним и внешним нарушителем, как источником угроз безопасности КАИС КРО, включают в себя возможности программно-аппаратных закладок.

3.5.4 Программно-математическое воздействие (вредоносная программа)

Вредоносные программы (обозначение «А» в указанной ниже таблице 6.5, приложении В) можно разделить на классы по принципу функционирования:

- загрузочные (А.3.1);
- файловые (А.3.2);
- сетевые (А.3.3);
- прочие вредоносные программы (А.3.4).

Основными действиями, выполняемыми вредоносными программами, являются:

- уничтожение информации в секторах винчестера;
- исключение возможности загрузки операционной системы;
- искажение кода загрузчика;
- форматирование логических дисков винчестера;
- закрытие доступа к COM и LPT-портам;
- замена символов при печати текстов;
- подергивания экрана;
- изменение метки диска;
- создание псевдосбойных кластеров;
- создание звуковых и (или) визуальных эффектов;
- порча файлов данных;
- перезагрузка компьютера;
- вывод на экран разнообразных сообщений;
- отключение периферийных устройств;
- изменение палитры экрана;
- заполнение экрана посторонними символами или изображениями;
- погашение экрана и перевод в режим ожидания ввода с клавиатуры;
- шифрование секторов винчестера;
- выборочное уничтожение символов, выводимых на экран при наборе с клавиатуры;
- уменьшение объема оперативной памяти;
- вызов печати содержимого экрана;
- блокирование записи на диск;
- уничтожение таблицы разбиения (Disk Partition Table);
- блокирование запуска исполняемых файлов;
- блокирование доступа к винчестеру.

По способу проникновения в КАИС КРО вредоносные программы можно разделить на:

- распространяемые при использовании отчуждаемых носителей информации (оптические компакт-диски, флеш-накопители);
- распространяемые по сети (локальной, корпоративной, глобальной).

Наличие в КАИС КРО вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную защиту.

3.6. Характеристика уязвимостей КАИС КРО

Уязвимость информационной системы персональных данных - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

В соответствии с методическим документом ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», с учетом состава КАИС КРО и источников угроз безопасности информации, уязвимости (обозначение «В» в указанных ниже таблицах 6.3-6.6, приложениях А, Б, Г) можно разделить на следующие группы:

- уязвимости программного обеспечения (В.1), которые разделяются на:
  - уязвимости системного программного обеспечения (В.1.1);
  - уязвимости прикладного программного обеспечения (В.1.2);
- уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных (В.2);
- уязвимости, вызванные недостатками организации ТЗИ от НСД (В.3);
- уязвимости применяемых средств защиты информации (В.4);
- уязвимости программно-технических средств ИС, вызванные их сбоями и отказами в работе (В.5).

3.6.1. Уязвимости программного обеспечения

Уязвимости программного обеспечения (обозначение «В.1» в указанных ниже таблицах 6.3-6.6, приложениях А, Б, Г) в КАИС КРО составляют уязвимости операционных систем (системного ПО – обозначение «В.1.1»), а также прикладного и специального ПО (обозначение «В.1.2»).

Уязвимости программного обеспечения могут быть реализованы:

- в средствах операционной системы, предназначенных для управления локальными ресурсами ИС (управление процессами, памятью, устройствами ввода/вывода и т.п.), драйверах, утилитах;
- в средствах операционной системы, предназначенных для вспомогательных функций (архивирование, дефрагментация и пр.), библиотеках процедур различного назначения;
- в сетевых средствах операционной системы.

Уязвимости в средствах операционной системы представляют собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

В прикладном и специальном ПО дополнительно появляются уязвимости, связанные с:

- функциями и процедурами, относящимся к разным прикладным программам и несовместимым между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функциями, процедурами, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду рабочих станций и серверов КАИС КРО и использования штатных функций операционной системы, выполнения НСД без обнаружения таких изменений операционной системой.

Следует иметь в виду несколько проблем обеспечения безопасности, связанных с веб-приложениями:

- внедрение SQL-кода;

– использование форм и сценариев (перевод параметров через скрытые поля, отключение сценария клиентской части и т.д.);
– элементы cookie и управление сеансом;
– общие атаки (уязвимые сценарии, переполнение буфера и т.д.).

Уязвимости используемого в КАИС КРО программного обеспечения рассмотрены с привязкой к техническим средствам КАИС КРО (таблица 3.6):

Таблица 3.6 Используемое программное обеспечение

Техническое средство	**Операционная система**	**Прикладное программное обеспечение**
АРМ пользователей и персонала КАИС КРО	MS Windows 2000 MS Windows XP MS Windows Vista MS Windows 7	MS Office 2003; MS Office 2007; WinRar 3.5-3.8; Outlook Express; IE 6-7; ABBYY Finereader 9.0 Corporate Edition RUS; Adobe Acrobat 7-9; AVP Kaspersky 6.0; АРМ «Параграф ОУ/ДОУ/Колледж»; АРМ «Закрытый портал»; АРМ КАИС КРО; Map Info 9.5; Правовые системы.
Серверы баз данных подсистемы «Параграф»	Windows Server 2003 SP2	СУБД Firebird
Сервер баз данных подсистемы портал «Петербургское образование»	Linux Ubuntu Server 11.04	VMWareESXi 4.0. СУБД MySQL v.5.5.10
Сервер приложений подсистемы портал «Петербургское образование»	Linux Ubuntu Server 11.04	VMWareESXi 4.0. FTP-сервер ProFTPD v.1.3.2. Веб-сервер Lighttpd v.1.4.26 SMTP-сервер Postfix v.2.7. POP3-сервером Dovecot v.1.2.12.
Сервер резервирования	Linux Ubuntu Server 11.04	VMWareESXi 4.0.
Сервер ВКС	Linux Ubuntu Server 11.04	VMWareESXi 4.0. ВКС «ВидеоМост»

Данные об уязвимостях разрабатываемого и распространяемого на коммерческой основе прикладного программного обеспечения собираются, обобщаются и анализируются в базе данных CVE (http://cve.mitre.org/cve/). Сводные данные об указанных уязвимостях для используемого в КАИС КРО ПО приведены в таблице 3.7. Степень критичности уязвимостей зависит от типа воздействия на приложение или

систему, наличия исправления или временного решения, представленного производителем, наличия эксплоита и возможности массовой эксплуатации уязвимости. Таким образом, для характеристики уязвимости применяется следующая градация:

1. высокая – уязвимость, которая может привести к нарушению конфиденциальности, целостности и доступности пользовательских данных или целостности и доступности вычислительных ресурсов;
2. средняя – уязвимость, которая в значительной степени смягчается такими факторами, как конфигурационные настройки по умолчанию, аудит или трудность ее применения;
3. низкая – уязвимость очень сложна для использования или ее воздействие минимально.

Таблица 3.7 Уязвимости эксплуатируемого в КАИС КРО программного обеспечения

Производитель	**Используемое ПО**	**Количество выявленных уязвимостей**	**Критичность выявленных уязвимостей**		
			Низкая	Средняя	Высокая
Microsoft	MS Windows 2003 Server	266	38	45	183
Microsoft	Windows 2000	241	28	42	171
Microsoft	MS Windows XP	198	47	30	121
Microsoft	MS Windows Vista	230	17	64	149
Microsoft	MS Windows 7	142	28	24	90
Microsoft	Office 2003	168	5	22	116
Microsoft	Office 2007	111	19	8	84
Microsoft	Office 2010	83	0	9	74
win.rar GmbH	WinRAR	12	3	4	5
Microsoft	IE 6-7;	355	88	75	192
Лаборатория Касперского	AVP Kaspersky 6.0;	9	3	3	3
Adobe	AcrobatReader	89	9	13	67
ABBYY	FineReader	В базе уязвимостей не представлено			

Среди ПО, используемого в КАИС КРО, больше всего критичных уязвимостей было обнаружено в операционных системах MS Windows.

Наиболее вероятными уязвимостями программного обеспечения в КАИС КРО являются:

- уязвимости программного обеспечения, не устраненные обновлениями разработчиков;
- заложенные в исходный код программного обеспечения недекларированные возможности по обходу механизмов аутентификации, назначения привилегий пользователям и другие функции, не предусмотренные функционалом программного обеспечения;
- уязвимости, не выявленные в случае применения защитных механизмов программного обеспечения, не прошедшего сертификацию в качестве средства защиты информации от НСД;

- уязвимости, возникающие в случаях неправильного конфигурирования программных средств, осуществляющих функции по разграничению доступа к ресурсам;
- возможность получения доступа к БД в обход специального программного обеспечения;
- возможность выделения IP адресов сетевым устройствам (хостам), несанкционированно подключаемых к ЛВС в составе КАИС КРО при использовании динамического назначения IP адресов и, как следствие, осуществление несанкционированного доступа к информации, путем подмены хоста (сервера);
- хранение в базе данных незашифрованных паролей. Если злоумышленнику удастся получить доступ в КАИС КРО, то в его руках окажется полный список паролей, которыми он может воспользоваться.

3.6.2. Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных

Основными коммутирующими устройствами, использующиеся в ЛВС локальных составных частей КАИС КРО, являются коммутаторы D-Link, LynkSys, ASUS и другие.

Взаимодействие в ЛВС ОУ на канальном уровне осуществляется по стандартным протоколам IEEE 802.3. Сегментирование пользователей на виртуальные частные сети (VLAN) не применяется. Механизмов повышения отказоустойчивости и доступности не используется. Все рабочие станции и серверы, входящие в состав КАИС КРО, подключаются непосредственно к коммутаторам доступа образовательных учреждений.

Сетевое взаимодействие всех технических средств КАИС КРО основано на протоколах TCP/IP.

TCP - базовый сетевой протокол, в настоящее время используемый в большинстве сетевых компьютерных систем. Многие производители включают поддержку этого протокола в свои программы, которые могут быть в различной степени уязвимы. Кроме того, любые сетевые службы или приложения, опирающиеся на TCP подключения, тоже подвержены нападениям, причем опасность нападения зависит, прежде всего, от продолжительности TCP сеанса.

Уязвимости протоколов сетевого взаимодействия (обозначение «В.2» в указанных ниже таблицах 6.3-6.6, приложениях А, Б, Г) связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности

служебной информации и др. Характеристика этих уязвимостей представлена в таблице 3.8.

Таблица 3.8 - Уязвимости протоколов сетевого взаимодействия

Протокол	Назначение	Характеристика уязвимости
FTP	Передача файлов по сети	Аутентификация на базе открытого теста Наличие дополнительных открытых портов
TCP	Для осуществления сетевого взаимодействия	Отсутствует механизм проверки корректности заполнения служебных заголовков пакета
IP	Для осуществления сетевого взаимодействия	Адресация узлов на базе открытого текста
UDP	Для осуществления сетевого взаимодействия	Отсутствует механизм предотвращения переполнения буфера и подтверждения доставки передаваемого пакета
DNS	Для осуществления сетевого взаимодействия	Отсутствует средство проверки аутентификации полученных данных от источника
SNMP	Для осуществления сетевого взаимодействия	Отсутствует поддержка аутентификации заголовков сообщений
ARP	Для осуществления сетевого взаимодействия	Аутентификация на основе открытого текста
RIP	Протокол обмена маршрутной информацией	Отсутствует аутентификация отправителя управляющего сообщения

3.6.3. Уязвимости, вызванные недостатками организации технической защиты информации от НСД

Проявление уязвимостей, вызванных недостатками организации технической защиты информации (ТЗИ) от НСД, возможны из-за:

1. недостаточного количества требуемых организационно-распорядительных документов в образовательных учреждениях;
2. недостаточного контроля эффективности мероприятий по защите информации в образовательных учреждениях и его структурных подразделениях;
3. незнания или игнорирования сотрудниками организационных требований при работе на объекте информатизации КАИС КРО.

Уязвимости, вызванные недостатками организации ТЗИ от НСД в КАИС КРО (обозначение «В.3» в указанных ниже таблицах 6.3-6.6, приложениях А, Б, Г) представлены в таблице 3.9.

Таблица 3.9 Уязвимости, вызванные недостатками организации ТЗИ от НСД

Группа	Уязвимость	Степень опасности

Отсутствие ОРД	1. Отсутствие Инструкции по антивирусной защите в КАИС КРО	высокая
	2. Отсутствие Руководства администратора БД КАИС КРО, Руководства пользователя КАИС КРО	высокая
	3. Отсутствие Положения об организации режима безопасности помещений, где осуществляется работа с ПДн	высокая
Несоблюдение требований по защите информации		очень высокая
Неправильная организация контроля эффективности защиты информации		высокая

3.6.4. Уязвимости СЗИ

В КАИС КРО используются программные и аппаратные средства защиты информации, их перечень представлен в таблице 3.10.

Таблица 3.10 Средства защиты информации КАИС КРО

Тип средства	Наименование средства
Программно-аппаратный комплекс	Межсетевой экран WatchGuard XTM 25
Программно-аппаратный комплекс	Межсетевой экран и VPN шлюз «ЗАСТАВА-Офис»
Программное средство защиты	Штатные средства операционных систем
Программное средство защиты	Штатные средства систем управления базами данных
Программное средство защиты	СЗИ НСД «DallasLock 7.7»
Программное средство защиты	Kaspersky Antivirus 6.0
Программное средство защиты	Сервис потокового антивирусного сканирования Gateway Antivirus
Программное средство защиты	Сервис предотвращения сетевых вторжений Intrusion Prevention Service

Программные средства защиты информации КАИС КРО могут иметь такие же уязвимости, как и остальное прикладное программное обеспечение КАИС КРО (п. 3.6.1. настоящего документа). В КАИС КРО используются штатные средства операционных систем и штатные средства СУБД, не сертифицированные ФСТЭК России на отсутствие в них недекларированных возможностей.

Дополнительно следует учитывать, что некорректная настройка данных программных и программно-аппаратных средств защиты может привести к появлению в системе дополнительных уязвимостей. Уязвимости аппаратных средств защиты информации неразрывно связаны с их возможными отказами и сбоями в работе.

Уязвимости СЗИ имеют обозначение «В.4» в указанных ниже таблицах 6.3-6.6, приложениях А, Б, Г.

3.6.5. Уязвимости программно-аппаратных средств КАИС КРО в результате сбоев в работе, отказов этих средств

Уязвимости программно-аппаратных средств КАИС КРО в результате сбоев в работе и отказов этих средств приведены в таблице 3.11. Степень опасности каждой уязвимости определена методом экспертного оценивания.

Таблица 3.11 Уязвимости программно-аппаратных средств КАИС КРО и степень их опасности

Уязвимость	Наименование программно-аппаратного средства	Степень опасности
В результате сбоев в работе	Серверы баз данных КАИС КРО	высокая
	Серверы приложений подсистем КАИС КРО	средняя
	Серверы резервного копирования	низкая
	Коммутационное оборудование КАИС КРО	низкая
	АРМ пользователя КАИС КРО	низкая
	АРМ администратора	средняя
	Источники бесперебойного электропитания серверного и коммутационного оборудования КАИС КРО	низкая
В результате отказов в работе	Сервер баз данных КАИС КРО	высокая
	Серверы приложений подсистем КАИС КРО	средняя
	Серверы резервного копирования	средняя
	Коммутационное оборудование КАИС КРО	низкая
	АРМ пользователя КАИС КРО	низкая
	АРМ администратора	средняя
	Источники бесперебойного электропитания серверного и коммутационного оборудования КАИС КРО	низкая

Уязвимости программно-аппаратных средств КАИС КРО в результате сбоев в работе и отказов этих средств имеют обозначение «В.5» в указанных ниже таблицах 6.3-6.6, приложениях А, Б, Г.

3.7. Перечень возможных технических каналов утечки информации

При обработке информации в информационных системах персональных данных возможно возникновение угроз безопасности персональных данных за счет реализации следующих технических каналов утечки информации:

1. визуально-оптический (визуальный обзор документов, просмотр информации с экранов дисплеев и других средств ее отображения с помощью фото и видеосъемки);
2. утечка акустической (речевой) информации;

3. утечка информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН).

Состав разглашаемых данных не зависит от типа технического канала утечки информации, по любому из них может быть реализована угроза для всего массива защищаемых данных КАИС КРО. В связи с этим, степень опасности каждого из актуальных технических каналов утечки информации считается высокой.

3.7.1. Угрозы утечки акустической (речевой) информации

Источниками угроз утечки акустической (речевой) являются физические лица, не имеющие прав легального доступа к информационным ресурсам КАИС КРО.

Лица, являющиеся зарегистрированными пользователями в качестве источников угроз утечки акустической (речевой) не рассматриваются в виду принятых организационных и контролирующих мер.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Носителем ПДн является пользователь КАИС КРО, осуществляющий голосовой ввод ПДн или акустическая система КАИС КРО воспроизводящая ПДн.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя при обработке ПДн, обусловлено наличием функций голосового ввода ПДн в информационную систему или функций воспроизведения ПДн акустическими средствами информационной системы.

Функции голосового ввода персональных данных в КАИС КРО или функций воспроизведения персональных данных акустическими средствами в КАИС КРО отсутствуют, поэтому дальнейшее рассмотрение данной угрозы представляется **нецелесообразным**.

3.7.2. Угрозы утечки видовой информации

Источниками угроз утечки видовой информации являются физические лица, не имеющие прав легального доступа к информационным ресурсам КАИС КРО.

Лица, являющиеся зарегистрированными пользователями, в качестве источника угроз утечки видовой информации не рассматриваются в виду принятых организационных и контролирующих мер.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Носителем ПДн являются:

1. технические средства КАИС КРО, создающие физические поля, в которых информация находит свое отражение в виде символов и образов;
2. распечатанные документы или иные материальные носители видовой информации.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Перехват ПДн в КАИС КРО может вестись портативной носимой аппаратурой (портативные аналоговые и цифровые фото- и видеокамеры, цифровые видеокамеры, встроенные в сотовые телефоны) – физическими лицами, при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них в условиях наличия визуального контакта, а также с применением специализированной оптической (оптикоэлектронной) аппаратуры из–за пределов контролируемой зоны при наличии прямой видимости.

Визуальное обследование АРМ пользователей и обслуживающего персонала на объектах информатизации КАИС КРО показало, что размещение устройств отображения информации не позволяет просмотр выводимой информации посторонними лицами. В рабочих помещениях не допускается бесконтрольное нахождение посторонних лиц, физический доступ к АРМ пользователей максимально затруднен и дальнейшее рассмотрение данной угрозы представляется **нецелесообразным.**

3.7.3. Угрозы утечки информации по каналам побочных электромагнитных излучения и наводок

Источниками угроз утечки информации по каналу ПЭМИ и наводок являются физические лица, не имеющие прав легального доступа к информационным ресурсам КАИС КРО.

Лица, являющиеся зарегистрированными пользователями, в качестве источников угроз утечки не рассматриваются в виду приятых организационных и контролирующих мер.

Среда распространения информативного сигнала – неоднородная за счет перехода из одной среды в другую (воздушная – материал ограждающих конструкций).

Носителем ПДн являются технические средства КАИС КРО создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами КАИС КРО.

Обработка информации, содержащей ПДн и циркулирующей в технических средствах информационной системы в виде электрических информативных сигналов, сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений, а также наводок этих излучений на токопроводящие конструкции, имеющие выход за пределы контролируемой зоны в зависимости от мощности излучений и размеров информационной системы.

Состав персональных данных, обрабатываемых в КАИС КРО, позволяет идентифицировать субъекта персональных данных и получить о нем дополнительные сведения. Разглашение этих данных может привести к негативным последствиям для субъекта персональных данных. Соответственно, рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН, избыточно, так как утечка ПДн по каналам ПЭМИН – маловероятна из-за несоответствия стоимости средств съема информации и величиной ущерба для субъекта от полученной в результате регистрации ПЭМИН информации, поэтому дальнейшее рассмотрение данной угрозы представляется **нецелесообразным.**

4. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ

К способам реализации угроз в КАИС КРО (обозначение «С» в указанных ниже таблицах 6.3-6.6, приложениях А, Б, Г) можно отнести следующие:

1. Физическое воздействие на технические средства КАИС КРО:
   - 1.1 Хищение, уничтожение, разрушение носителя защищаемых информационных ресурсов;
   - 1.2 Уничтожение, разрушение технического средства и линий связи;
   - 1.3 Нарушение электропитания технических средств;
   - 1.4 Изменение конфигурации технических средств;
   - 1.5 Несоблюдение организационных мероприятий по ЗИ.
2. Воздействие на каналы доступа, образованных с использованием штатных средств ИСПДн и обеспечивающих:
   - 2.1 Несанкционированный доступ к защищаемой информации с использованием штатных средств ИСПДн и недостатков механизмов разграничения доступа;
   - 2.2 Компрометация технологической (аутентификационной) информации с использованием штатных средств ИСПДн;
   - 2.3 Нарушение адресности и своевременности информационного обмена;
   - 2.4 Сбои и отказы программно-технических компонентов КАИС КРО.
3. Обход СЗИ:
   - 3.1 Изменение настроек программных средств СЗИ;
   - 3.2 Перехват и вскрытие паролей;
   - 3.3 Изменение состава используемого ПО и внедрение нештатного ПО.
4. Использование уязвимостей протоколов сетевого взаимодействия и каналов передачи данных:
   - 4.1 Перехват информации;
   - 4.2 Модификация передаваемых данных;
   - 4.3 Перегрузка ресурсов (отказ в обслуживании);
   - 4.4 Внедрение вредоносных программ;
   - 4.5 Удаленный несанкционированный доступ в систему.
5. Инфицирование программной среды:
   - 5.1 Передача управления на оригинальный загрузочный диск;
   - 5.2 Действия пользователя;
   - 5.3 Самостоятельная передача и запуск кода.

5. ДЕСТРУКТИВНЫЕ ВОЗДЕЙСТВИЯ НА КАИС КРО

В КАИС КРО возможны, в общем случае, следующие деструктивные воздействия (обозначение «Е» в указанных ниже таблицах 6.3-6.6, приложениях А, Б, Г):

1. Нарушение конфиденциальности информации:
   - 1.1 Утечка/ разглашение защищаемой информации;
   - 1.2 Несанкционированное копирование;
   - 1.3 Перехват информации в каналах передачи данных.
2. Нарушение целостности:
   - 2.1 Воздействие на ПО и защищаемую информацию;
   - 2.2 Воздействие на программы, данные и драйверы устройств, обеспечивающих загрузку ОС и СЗИ;
   - 2.3 Воздействие на программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) ОС;
   - 2.4 Воздействие на программы и данные прикладного и специального ПО;
   - 2.5 Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки средствами и устройствами вычислительной техники;
   - 2.6 Внедрение вредоносной программы и /или программно-аппаратной закладки;
   - 2.7 Воздействие на технологическую сетевую информацию;
   - 2.8 Воздействие на СЗИ.
3. Нарушение доступности:
   - 3.1 Нарушение и отказы функционирования средств обработки информации;
   - 3.2 Нарушение и отказы функционирования средств ввода/вывода информации;
   - 3.3 Нарушение и отказы функционирования средств хранения информации;
   - 3.4 Нарушение и отказы функционирования аппаратуры и каналов передачи данных;
   - 3.5 Нарушение и отказы функционирования СЗИ.

6. ПЕРЕЧЕНЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ КАИС КРО

По виду каналов, с помощью которых реализуется угроза безопасности персональных данных КАИС КРО выделяются 2 класса угроз:

1 Угрозы, реализуемые за счет НСД к персональным данным в КАИС КРО с использованием штатного программного обеспечения КАИС КРО или специально разрабатываемого программного обеспечения:
   - непосредственного доступа – с использованием программных и программно-аппаратных средств ввода/вывода компьютера;
   - удаленного доступа – с использованием протоколов сетевого взаимодействия.
2 Угрозы, реализуемые через каналы, возникающие за счет использования технических средств съема (добывания) информации, обрабатываемой в технических средствах КАИС КРО или вспомогательных технических средствах и системах (ВТСС) - технические каналы утечки информации.

6.1. Угрозы НСД

Угрозы НСД в КАИС КРО с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) персональных данных, и включают в себя:

- угрозы доступа (проникновения) в операционную среду с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программно-математического воздействия);
- угрозы, реализуемые при использовании протоколов межсетевого взаимодействия.

Ниже в подразделах 6.1.1 – 6.1.4 будут приведены сводные таблицы (Таблицы 6.3-6.6), по каждому типу угроз безопасности персональных данных КАИС КРО.

Используемый алгоритм описания угроз безопасности, включая правила отнесения угрозы безопасности к актуальной, определен в методическом документе ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Кроме того, в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных [4] определение типа угроз безопасности персональных данных, актуальных для информационной, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».

Для нужд настоящей Частной модели угроз безопасности персональным данным КАИС КРО экспертами разработан оригинальный подход для получения оценок уровня вреда, наносимого субъектам персональных данных, и определения типов угроз безопасности персональных данных, актуальных для КАИС КРО.

В первом столбце таблиц 6.3-6.6 приведен перечень угроз, соответствующий рассматриваемому классу.

Во втором столбце указан коэффициент реализуемости угрозы (Y), для вычисления которого используется числовой коэффициент вероятности реализации угрозы (Y2) и значение исходного уровня защищенности (Y1).

Под вероятностью реализации угрозы понимается показатель, характеризующий, насколько вероятным событием является реализация конкретной угрозы безопасности персональным данным для КАИС КРО в складывающихся условиях обстановки. Используются четыре вербальных градации этого показателя:

- **маловероятно** - отсутствуют объективные предпосылки для осуществления угрозы;
- **низкая вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности персональных данных недостаточны;
- **высокая вероятность** - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности персональных данных не приняты.

Каждой градации вероятности реализации угрозы поставлен в соответствие числовой коэффициент Y2, а именно:

0 для маловероятной угрозы;

2 для низкой вероятности угрозы;

5 для средней вероятности угрозы;

10 для высокой вероятности угрозы.

Значения частот реализации для конкретных угроз безопасности персональным данным КАИС КРО в складывающихся условиях обстановки приведены в Приложениях А, Б, В, Г настоящей Модели угроз.

Коэффициент реализуемости определяется соотношением Y=(Y1+Y2)/20, где Y1 – исходный уровень защищенности КАИС КРО (рассчитан в пункте 3.1 настоящего документа и равен 10 (**низкий уровень защищенности**), Y2 – частота реализации угрозы).

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если $0 < Y \leq 0,3$, то возможность реализации угрозы признается низкой;
- если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;
- если $0,6 < Y \leq 0,8$, то возможность реализации угрозы высокая;
- если $Y>0,8$, то возможность реализации угрозы признается очень высокой.

В третьем столбце оценивается значение вреда, наносимого субъектам персональных данных. В соответствии со статьёй 2 Федерального закона РФ от 27.07.06 № 152-ФЗ «О персональных данных», оценка вреда, который может быть причинён субъектам ПДн, производится в отношении прав и свобод человека и гражданина (субъекта ПДн), в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

При оценке вреда для субъектов ПДн на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель вреда. Этот показатель имеет четыре значения:

- **отсутствие вреда** - нарушение заданных характеристик безопасности ПДн не приводит к негативным последствиям для субъектов ПДн;
- **не значительный вред** - нарушение заданных характеристик безопасности ПДн может привести к незначительным негативным последствиям для субъектов ПДн;

- **вред** - нарушение заданных характеристик безопасности ПДн может привести к негативным последствиям для субъектов ПДн;
- **значительный вред** - нарушение заданных характеристик безопасности ПДн может привести к значительным негативным последствиям для субъектов ПДн.

В следующем столбце сводных таблиц оценивается опасность каждой угрозы. Вербальный показатель опасности угрозы имеет три значения:

- **низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- **средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- **высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Для определения значения опасности угрозы экспертами проведен анализ соотношения потенциального вреда для субъектов персональных данных и значения субъективной ценности персональных данных, содержащихся в КАИС КРО. Ценность ПДн для оператора ИСПДн установлена в условных единицах. Использованы следующие градации ценности персональных данных для оператора ИСПДн:

- уровень 4 (низкая) – менее 10 у.е.[2];
- уровень 3 (не значительная) – от 10 до 100 у.е.;
- уровень 2 (средняя) – от 100 до 1000 у.е.;
- уровень 1 (высокая) – свыше 1000 у.е.

Правило определения значения опасности угрозы приведено в таблице 6.1.

Таблица 6.1 - Правила определения опасности угрозы

Вред	**Субъективная ценность**			
	Низкая	Не значительная	Средняя	Высокая
Отсутствие вреда	низкая	низкая	низкая	низкая
Не значительный вред	низкая	низкая	средняя	средняя
Вред	средняя	средняя	средняя	высокая

[2] 1 у.е. принят равным 500 рублей.

Значительный вред	высокая	высокая	высокая	высокая

Определенный экспертами уровень ценности персональных данных, содержащихся в КАИС КРО, имеет значение **уровень 1** (значительная ценность).

В последнем столбце сводных таблиц показана актуальность каждой угрозы. Выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным, осуществляется в соответствии с правилами, приведенными в таблице 6.2.

Таблица 6.2 - Правила отнесения угрозы безопасности к актуальной

Возможность реализации	**Показатель опасности угрозы**		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

6.1.1. Угрозы доступа в операционную систему

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к информации связаны с доступом:

- к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) компьютерной техники КАИС КРО, с возможность перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;
- в операционную среду, то есть среду функционирования локальной операционной системы отдельного технического средства КАИС КРО, с возможностью выполнения НСД путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;
- в среду функционирования прикладных программ (например, к системе управления базами данных);
- непосредственно к информации пользователя (к файлам, текстовой информации, полям и записям в электронных базах данных) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

Эти угрозы могут быть реализованы в случае получения физического доступа к КАИС КРО или, по крайней мере, к средствам ввода информации в КАИС КРО. Их можно объединить по условиям реализации в три группы.

Первая группа включает в себя угрозы, реализуемые в ходе загрузки операционной системы. Эти угрозы направлены на перехват паролей или идентификаторов, модификацию программного обеспечения BIOS, перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду сетевых узлов КАИС КРО. Чаще всего, такие угрозы реализуются с использованием отчуждаемых носителей информации, в условиях отсутствия запрета загрузки с внешних носителей информации, или связаны с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении.

Проведенное обследование КАИС КРО показало, что пользователям КАИС КРО образовательное учреждение не запрещена загрузка операционной среды с внешних носителей. Поэтому объективные предпосылки для осуществления угроз, реализуемых в ходе загрузки операционной системы для рабочих станций пользователей, существуют. С учетом слабой мотивации пользователей на совершение подобных действий и их не высокой технической оснащенности вероятность реализации угрозы признается низкой.

Загрузка операционной среды с внешних носителей на серверах КАИС КРО разрешена только системному администратору. В связи с тем, что доступ в серверные помещения разрешен только ограниченному числу лиц, но объективные предпосылки для реализации угрозы существуют, вероятность реализации угрозы признается низкой.

Вторая группа - угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем. Эти угрозы, как правило, направлены на выполнение непосредственно НСД к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы или какой-либо прикладной программы общего пользования, так и специально созданными для выполнения НСД программами в условиях отсутствия СЗИ от НСД и настройки операционных систем компьютерной техники КАИС КРО, например:

- программами просмотра и модификации реестра;
- специальными программами просмотра и копирования записей в базах данных;

– программами поддержки возможностей реконфигурации программной среды (настройки операционной среды и прикладного программного обеспечения в интересах нарушителя).

Третья группа включает в себя угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз - это угрозы внедрения вредоносных программ.

Проведенное обследование показало, что пользователи локальных составных частей КАИС КРО не имеют административных прав на рабочих станциях. В пилотной зоне КАИС КРО установлены средства защиты информации от НСД и запланировано дальнейшее расширение зоны действия СЗИ НСД на другие объекты информатизации КАИС КРО. Поэтому объективные предпосылки для осуществления угроз, реализуемых после загрузки операционной системы для рабочих станций пользователей, существуют, но вероятность реализации угрозы признается низкой.

Установка программного обеспечения на серверы КАИС КРО разрешена администраторам КАИС КРО и персоналу сторонних организаций, осуществляющему администрирование технических средств и баз данных КАИС КРО. В связи с тем, что права на установку программного обеспечения разрешены только ограниченному кругу лиц, но объективные предпосылки для реализации угрозы существуют (в виде внедрения нештатного ПО, ошибок разработчиков, а также недекларированных возможностей системного и прикладного ПО), вероятность реализации угрозы признается средней (т.е. принятые меры безопасности ПДн недостаточны).

Угроза доступа в операционную систему может быть представлена как совокупность источника угрозы (пункт 3.5 настоящего документа), уязвимости системы (пункт 3.6 настоящего документа), способа реализации угрозы (пункт 4 настоящего документа) и объекта воздействия (пункт 3.3 настоящего документа). Угроза будет существовать в случае, если может быть осуществлено какое-либо деструктивное воздействие на КАИС КРО (пункт 5 настоящего документа). Состав угроз по классам подробно представлен в Приложении А, перечень угроз по классам с дополнительными показателями представлен в Таблице 6.3.

Таблица 6.3 Актуальность угроз доступа в операционную систему

№	Наименование угрозы	Коэффициент реализуемости угрозы (Y)	Оценка вреда	Показатель опасности	Актуальность угрозы
1.1 Угрозы, реализуемые в ходе загрузки операционной системы					
1.	А.2.1 – Д.1 – В.1.1 – С.3.1 – Е.2.1	0. 6 – средняя	не значительный вред	средняя	актуальная
2.	А.2.1 – Д.1 – В.1.1 – С.3.1 – Е.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
3.	А.2.1 – Д.1 – В.1.1 – С.3.1 – Е.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
4.	А.2.1 – Д.1 – В.3 – С.1.4 – Е.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
5.	А.2.1 – Д.1 – В.4 – С.3.2 – Е.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
6.	А.2.1 – Д.1 – В.4 – С.3.2 – Е.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
7.	А.2.3 – Д.1 – В.1.1 – С.3.1 – Е.2.1	0. 6 – средняя	вред	высокая	актуальная
8.	А.2.3 – Д.1 – В.1.1 – С.3.1 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
9.	А.2.3 – Д.1 – В.1.1 – С.3.1 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
10.	А.2.3 – Д.1 – В.3 – С.1.4 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
11.	А.2.3 – Д.1 – В.4 – С.3.2 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
12.	А.2.3 – Д.1 – В.4 – С.3.2 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
13.	А.2.4 – Д.2 – В.1.1 – С.3.1 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
14.	А.2.4 – Д.2 – В.1.1 – С.3.1 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
15.	А.2.4 –Д.2 – В.3 – С.3.3 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
16.	А.2.4 –Д.2 – В.3 – С.3.3 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
17.	А.2.4 –Д.2 – В.3 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
18.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
19.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
20.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
21.	А.3 – Д.1 – В.1.1 – С.3.1 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
22.	А.3 – Д.1 – В.1.1 – С.3.1 – Е.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
23.	А.3 – Д.1 – В.4 – С.3.2 – Е.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
24.	А.3 – Д.1 – В.4 – С.3.2 – Е.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
25.	А.3 – Д.2 – В.1.1 – С.3.1 – Е.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
26.	А.3 – Д.2 – В.1.1 – С.3.1 – Е.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
27.	А.3 – Д.2 – В.1.1 – С.3.1 – Е.2.6	0. 6 – средняя	не значительный вред	средняя	актуальная

№	Наименование угрозы	Коэффициент реализуемости угрозы (Y)	Оценка вреда	Показатель опасности	Актуальность угрозы
28.	A.3 – Д.2 – B.4 – C.3.2 – E.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
29.	A.3 – Д.2 – B.4 – C.3.2 – E.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
1.2 Угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем					
1.	A.2.1 – Д.1 – B.1.1 – C.2.1 – E.2.1	0. 6 – средняя	не значительный вред	средняя	актуальная
2.	A.2.1 – Д.1 – B.1.1 – C.2.1 – E.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
3.	A.2.1 – Д.1 – B.1.1 – C.2.1 – E.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
4.	A.2.1 – Д.1 – B.1.1 – C.2.1 – E.2.4	0. 6 – средняя	не значительный вред	средняя	актуальная
5.	A.2.1 – Д.1 – B.1.1 – C.2.1 – E.2.5	0. 6 – средняя	не значительный вред	средняя	актуальная
6.	A.2.1 – Д.1 – B.1.1 – C.3.2 – E.2.1	0. 6 – средняя	не значительный вред	средняя	актуальная
7.	A.2.1 – Д.1 – B.1.1 – C.3.2 – E.2.5	0. 6 – средняя	не значительный вред	средняя	актуальная
8.	A.2.1 – Д.1 – B.1.2 – C.2.1 – E.2.1	0. 6 – средняя	не значительный вред	средняя	актуальная
9.	A.2.1 – Д.1 – B.1.2 – C.2.1 – E.2.4	0. 6 – средняя	не значительный вред	средняя	актуальная
10.	A.2.1 – Д.1 – B.1.2 – C.3.2 – E.2.1	0. 6 – средняя	не значительный вред	средняя	актуальная
11.	A.2.1 – Д.1 – B.1.2 – C.3.2 – E.2.5	0. 6 – средняя	не значительный вред	средняя	актуальная
12.	A.2.1 – Д.1 – B.1.2 – C.3.2 – E.2.6	0. 6 – средняя	не значительный вред	средняя	актуальная
13.	A.2.1 – Д.1 – B.4 – C.3.1 – E.1.2	0. 6 – средняя	не значительный вред	средняя	актуальная
14.	A.2.1 – Д.1 – B.4 – C.3.1 – E.2.8	0. 6 – средняя	не значительный вред	средняя	актуальная
15.	A.2.1 – Д.1 – B.4 – C.3.3 – E.2.6	0. 6 – средняя	не значительный вред	средняя	актуальная
16.	A.2.1 – Д.1 – B.4 – C.3.3 – E.2.8	0. 6 – средняя	не значительный вред	средняя	актуальная
17.	A.2.3 – Д.1 – B.4 – C.3.1 – E.2.8	0. 6 – средняя	вред	высокая	актуальная
18.	A.2.3 – Д.1 – B.3 – C.3.3 – E.2.6	0. 6 – средняя	вред	высокая	актуальная
19.	A.2.3 – Д.1 – B.3 – C.3.3 – E.2.8	0. 6 – средняя	вред	высокая	актуальная
20.	A.2.3 – Д.1 – B.4 – C.3.3 – E.2.6	0. 6 – средняя	вред	высокая	актуальная
21.	A.2.3 – Д.1 – B.4 – C.3.3 – E.2.8	0. 6 – средняя	вред	высокая	актуальная
22.	A.2.4 – Д.2 – B.1.1 – C.2.1 – E.2.3	0. 6 – средняя	вред	высокая	актуальная
23.	A.2.4 – Д.2 – B.1.1 – C.3.2 – E.2.8	0. 6 – средняя	вред	высокая	актуальная
24.	A.2.4 – Д.2 – B.4 – C.3.1 – E.2.8	0. 6 – средняя	вред	высокая	актуальная
25.	A.2.4 – Д.2 – B.4 – C.3.3 – E.2.6	0. 6 – средняя	вред	высокая	актуальная
26.	A.2.4 – Д.2 – B.4 – C.3.3 – E.2.8	0. 6 – средняя	вред	высокая	актуальная
27.	A.2.5 – Д.2 – B.1.1 – C.3.3 – E.2.1	0. 6 – средняя	вред	высокая	актуальная

№	Наименование угрозы	Коэффициент реализуемости угрозы (Y)	Оценка вреда	Показатель опасности	Актуальность угрозы
28.	А.2.5 – Д.2 – В.1.1 – С.3.3 – Е.2.5	0. 6 – средняя	вред	высокая	актуальная
29.	А.2.5 – Д.2 – В.1.1 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
30.	А.2.5 – Д.2 – В.1.2 – С.3.3 – Е.2.1	0. 6 – средняя	вред	высокая	актуальная
31.	А.2.5 – Д.2 – В.1.2 – С.3.3 – Е.2.5	0. 6 – средняя	вред	высокая	актуальная
32.	А.2.5 – Д.2 – В.1.2 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
33.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
34.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
35.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.4	0. 6 – средняя	вред	высокая	актуальная
36.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
37.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.8	0. 6 – средняя	вред	высокая	актуальная
38.	А.2.5 – Д.2 – В.4 – С.3.1 – Е.2.8	0. 6 – средняя	вред	высокая	актуальная
39.	А.2.5 – Д.2 – В.4 – С.3.3 – Е.2.8	0. 6 – средняя	вред	высокая	актуальная
1.3 Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ					
1.	А.2.1 – Д.1 – В.3 – С.3.3 – Е.2.1	0. 6 – средняя	не значительный вред	средняя	актуальная
2.	А.2.1 – Д.1 – В.3 – С.3.3 – Е.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
3.	А.2.1 – Д.1 – В.3 – С.3.3 – Е.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
4.	А.2.1 – Д.1 – В.3 – С.3.3 – Е.2.4	0. 6 – средняя	не значительный вред	средняя	актуальная
5.	А.2.1 – Д.1 – В.3 – С.3.3 – Е.2.6	0. 6 – средняя	не значительный вред	средняя	актуальная
6.	А.2.1 – Д.1 – В.4 – С.3.3 – Е.2.1	0. 6 – средняя	не значительный вред	средняя	актуальная
7.	А.2.1 – Д.1 – В.4 – С.3.3 – Е.2.2	0. 6 – средняя	не значительный вред	средняя	актуальная
8.	А.2.1 – Д.1 – В.4 – С.3.3 – Е.2.3	0. 6 – средняя	не значительный вред	средняя	актуальная
9.	А.2.1 – Д.1 – В.4 – С.3.3 – Е.2.4	0. 6 – средняя	не значительный вред	средняя	актуальная
10.	А.2.1 – Д.1 – В.4 – С.3.3 – Е.2.6	0. 6 – средняя	не значительный вред	средняя	актуальная
11.	А.2.3 – Д.1 – В.3 – С.3.3 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
12.	А.2.3 – Д.1 – В.3 – С.3.3 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
13.	А.2.3 – Д.1 – В.3 – С.3.3 – Е.2.4	0. 6 – средняя	вред	высокая	актуальная
14.	А.2.3 – Д.1 – В.3 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
15.	А.2.3 – Д.1 – В.4 – С.3.3 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
16.	А.2.3 – Д.1 – В.4 – С.3.3 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная

№	Наименование угрозы	Коэффициент реализуемости угрозы (Y)	Оценка вреда	Показатель опасности	Актуальность угрозы
17.	А.2.3 – Д.1 – В.4 – С.3.3 – Е.2.4	0. 6 – средняя	вред	высокая	актуальная
18.	А.2.3 – Д.1 – В.4 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
19.	А.2.4 – Д.2 – В.3 – С.3.3 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
20.	А.2.4 – Д.2 – В.3 – С.3.3 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
21.	А.2.4 – Д.2 – В.3 – С.3.3 – Е.2.4	0. 6 – средняя	вред	высокая	актуальная
22.	А.2.4 – Д.2 – В.3 – С.3.3 – Е.2.5	0. 6 – средняя	вред	высокая	актуальная
23.	А.2.4 – Д.2 – В.3 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
24.	А.2.4 – Д.2 – В.4 – С.3.3 – Е.2.2	0. 6 – средняя	вред	высокая	актуальная
25.	А.2.4 – Д.2 – В.4 – С.3.3 – Е.2.3	0. 6 – средняя	вред	высокая	актуальная
26.	А.2.4 – Д.2 – В.4 – С.3.3 – Е.2.4	0. 6 – средняя	вред	высокая	актуальная
27.	А.2.4 – Д.2 – В.4 – С.3.3 – Е.2.5	0. 6 – средняя	вред	высокая	актуальная
28.	А.2.4 – Д.2 – В.4 – С.3.3 – Е.2.6	0. 6 – средняя	вред	высокая	актуальная
29.	А.2.5 – Д.2 – В.1.2 – С.2.2 – Е.2.1	0. 75 – высокая	вред	высокая	актуальная
30.	А.2.5 – Д.2 – В.1.2 – С.2.2– Е.2.4	0. 75 – высокая	вред	высокая	актуальная
31.	А.2.5 – Д.2 – В.1.2 – С.2.2 – Е.2.5	0. 75 – высокая	вред	высокая	актуальная
32.	А.2.5 – Д.2 – В.1.2 – С.2.2 – Е.2.6	0. 75 – высокая	вред	высокая	актуальная
33.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.2	0. 75 – высокая	вред	высокая	актуальная
34.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.3	0. 75 – высокая	вред	высокая	актуальная
35.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.4	1.00 – очень высокая	вред	высокая	актуальная
36.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.5	0. 75 – высокая	вред	высокая	актуальная
37.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.6	1.00 – очень высокая	вред	высокая	актуальная
38.	А.2.5 – Д.2 – В.3 – С.3.3 – Е.2.8	0. 75 – высокая	вред	высокая	актуальная

Таким образом, выявлено 29 угроз, реализуемых в результате загрузки операционной системы, все из них признаны актуальными для КАИС КРО. При этом угроз, связанных с наличием недекларированных (недокументированных) возможностей в системном ПО – 13.

Угроз, реализуемых после загрузки операционной системы независимо от того, какая прикладная программа запускается пользователем – 39 актуальных угроз. Угроз, связанных с наличием недекларированных (недокументированных) возможностей в системном ПО – 9. Угроз, связанных с наличием недекларированных (недокументированных) возможностей в прикладном ПО – 8.

Угроз, реализуемых в зависимости от того, какая прикладная программа запускается пользователем – 38 актуальных угроз. При этом угроз, связанных с наличием недекларированных (недокументированных) возможностей в прикладном ПО – 4.

Реализация актуальных угроз доступа в операционную систему может привести к нарушению заданных оператором характеристик безопасности информационного ресурса КАИС КРО, что в свою очередь может стать причиной нанесения ущерба субъектам персональных данных.

6.1.2. Угрозы создания нештатных режимов работы программных и программно-аппаратных средств

Ремонт технических средств (системные блоки, серверное и коммуникационное оборудование) при гарантийных случаях производится организациями-поставщиками, при негарантийных случаях осуществляется по договору обслуживания со сторонней организацией (сервисным центром). Над развитием КАИС КРО трудится большая группа разработчиков.

Помещения, в которых размещены технические средства КАИС КРО, оборудованы охранной и пожарной сигнализацией. Доступ в серверные помещения, в которых размещены основные серверные и коммуникационные технические средства, разрешен только лицам из числа администраторов. Тем не менее, объективные предпосылки для реализации угроз существуют в виде недостаточного контроля эффективности мероприятий по защите информации в структурных подразделениях и недостатков технологии разработки прикладного ПО. Вероятность реализации угрозы признается средней в отношении серверного и коммуникационного оборудования (как элементов высокой степени опасности).

Угроза создания нештатных режимов работы программных и программно-аппаратных средств может быть представлена как совокупность: источник угрозы (пункт 3.5 настоящего документа), уязвимости системы (п. 3.6), способа реализации угрозы (п. 4) и объекта воздействия (п. 3.3). Угроза будет существовать в случае, если может быть осуществлено какое-либо деструктивное воздействие на КАИС КРО (п. 5). Состав угроз подробно представлен в Приложении Б, перечень угроз с дополнительными показателями представлен в Таблице 6.4.

Таблица 6.4. Актуальность угроз создания нештатных режимов работы программных и программно-аппаратных средств КАИС КРО

№	Наименование угрозы	Коэффициент реализуемости угрозы (Y)	Оценка вреда	Показатель опасности	Актуальность угрозы
Угрозы, реализуемые путем физического доступа к элементам ИСПДн					
1.	А.2.1 – Д.1 – В.3 – С.1.1 – Е.1.1	0.6 – средняя	не значительный вред	средняя	актуальная
2.	А.2.1 – Д.1 – В.3 – С.1.1 – Е.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
3.	А.2.1 – Д.1 – В.3 – С.1.4 – Е.2.6	0.6 – средняя	не значительный вред	средняя	актуальная
4.	А.2.1 – Д.3 – В.3 – С.1.1 – Е.1.1	0.6 – средняя	не значительный вред	средняя	актуальная
5.	А.2.1 – Д.3 – В.3 – С.1.1 – Е.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
6.	А.2.2 – Д.1 – В.3 – С.1.1 – Е.1.1	0.6 – средняя	не значительный вред	средняя	актуальная
7.	А.2.2 – Д.1 – В.3 – С.1.1 – Е.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
8.	А.2.2 – Д.1 – В.3 – С.1.4 – Е.2.6	0.6 – средняя	не значительный вред	средняя	актуальная
9.	А.2.2 – Д.2 – В.3 – С.1.1 – Е.1.1	0.6 – средняя	не значительный вред	средняя	актуальная
10.	А.2.2 – Д.2 – В.3 – С.1.1 – Е.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
11.	А.2.2 – Д.2 – В.3 – С.1.4 – Е.2.6	0.6 – средняя	не значительный вред	средняя	актуальная
12.	А.2.2 – Д.4 – В.3 – С.1.4 – Е.2.6	0.6 – средняя	не значительный вред	средняя	актуальная
13.	А.2.3 – Д.1 – В.3 – С.1.1 – Е.1.2	0.75 – высокая	вред	высокая	актуальная
14.	А.2.3 – Д.1 – В.3 – С.1.4 – Е.2.6	0.75 – высокая	вред	высокая	актуальная
15.	А.2.3 – Д.1 – В.3 – С.1.4 – Е.2.8	0.6 – средняя	вред	высокая	актуальная
16.	А.2.4 – Д.2 – В.3 – С.1.1 – Е.1.2	0.6 – средняя	вред	высокая	актуальная
Угрозы преднамеренных действий внутренних нарушителей (лиц, допущенных к защищаемой информации)					
17.	А.2.3 – Д.1 – В.3 – С.1.5 – Е.1.1	0.6 – средняя	вред	высокая	актуальная
18.	А.2.3 – Д.1 – В.3 – С.1.5 – Е.1.2	0.6 – средняя	вред	высокая	актуальная
19.	А.2.3 – Д.1 – В.3 – С.1.5 – Е.2.1	0.6 – средняя	вред	высокая	актуальная
20.	А.2.3 – Д.2 – В.3 – С.1.5 – Е.1.2	0.6 – средняя	вред	высокая	актуальная
21.	А.2.3 – Д.3 – В.3 – С.1.5 – Е.1.2	0.6 – средняя	вред	высокая	актуальная
22.	А.2.4 – Д.2 – В.3 – С.1.5 – Е.1.1	0.6 – средняя	вред	высокая	актуальная
23.	А.2.4 – Д.2 – В.3 – С.1.5 – Е.1.2	0.6 – средняя	вред	высокая	актуальная
24.	А.2.4 – Д.2 – В.3 – С.1.5 – Е.2.1	0.6 – средняя	вред	высокая	актуальная
25.	А.2.4 – Д.2 – В.3 – С.1.5 – Е.2.6	0.6 – средняя	вред	высокая	актуальная
26.	А.2.5 – Д.2 – В.3 – С.1.5 – Е.1.1	0.6 – средняя	вред	высокая	актуальная
27.	А.2.5 – Д.2 – В.3 – С.1.5 – Е.1.2	0.6 – средняя	вред	высокая	актуальная
28.	А.2.5 – Д.2 – В.3 – С.1.5 – Е.2.1	0.6 – средняя	вред	высокая	актуальная
29.	А.2.5 – Д.2 – В.3 – С.1.5 – Е.2.2	0.6 – средняя	вред	высокая	актуальная

№	Наименование угрозы	Коэффициент реализуемости угрозы (Y)	Оценка вреда	Показатель опасности	Актуальность угрозы
30.	A.2.5 – Д.2 – В.3 – С.1.5 – Е.2.3	0.6 – средняя	вред	высокая	актуальная
31.	A.2.5 – Д.2 – В.3 – С.1.5 – Е.2.4	0.6 – средняя	вред	высокая	актуальная
32.	A.2.5 – Д.2 – В.3 – С.1.5 – Е.2.6	0.6 – средняя	вред	высокая	актуальная
33.	A.2.5 – Д.2 – В.3 – С.1.5 – Е.2.8	0.6 – средняя	вред	высокая	актуальная
34.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.1.1	0.6 – средняя	вред	высокая	актуальная
35.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.1.2	0.6 – средняя	вред	высокая	актуальная
36.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.2.1	0.6 – средняя	вред	высокая	актуальная
37.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.2.2	0.6 – средняя	вред	высокая	актуальная
38.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.2.4	0.75 – высокая	вред	высокая	актуальная
39.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.2.6	0.6 – средняя	вред	высокая	актуальная
40.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.2.8	0.6 – средняя	вред	высокая	актуальная
41.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.3.1	0.75 – высокая	вред	высокая	актуальная
42.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.3.2	0.75 – высокая	вред	высокая	актуальная
43.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.3.3	0.75 – высокая	вред	высокая	актуальная
44.	A.2.6 – Д.2 – В.3 – С.1.5 – Е.3.5	0.75 – высокая	вред	высокая	актуальная

Таким образом, выявлены 44 актуальных угрозы создания нештатных режимов работы программных и программно-аппаратных средств КАИС КРО. Из них, связанных с возможностью внесения недекларированных возможностей в процессе разработки прикладного программного обеспечения – 11.

6.1.3. Угрозы программно-математического воздействия

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в КАИС КРО, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации КАИС КРО посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями КАИС КРО.

В КАИС КРО в качестве системы антивирусной защиты используется Kaspersky Antivirus 6.0. Объективные предпосылки для реализации угроз программно-математического воздействия существуют в виде игнорирования организационных ограничений (установленных правил) при работе на технических средствах КАИС КРО и возможности подключения пользователями отчуждаемых носителей.

Вероятность реализации угрозы ПМВ признается низкой в части воздействия на серверное оборудование (как элемента высокой степени опасности).

Для описания угрозы программно-математического воздействия достаточно класса вредоносной программы и способа инфицирования. Угроза будет существовать в случае, если несанкционированный доступ будет успешно осуществлен. Состав угроз программно-математического воздействия подробно представлен в Приложении В, перечень угроз с дополнительными показателями представлен в Таблице 6.5.

Таблица 6.5 Угрозы программно-математического воздействия

№	Наименование угрозы	Коэффициент реализуемости угрозы (Y)	Оценка вреда	Показатель опасности	Актуальность угрозы
1.	A.3.1 – C.5.1 – E.2.2	0.6 – средняя	не значительный вред	средняя	актуальная
2.	A.3.1 – C.5.1 – E.2.6	0.6 – средняя	не значительный вред	средняя	актуальная
3.	A.3.2 – C.5.2 – E.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
4.	A.3.2 – C.5.2 – E.2.1	0.6 – средняя	не значительный вред	средняя	актуальная
5.	A.3.2 – C.5.2 – E.2.2	0.6 – средняя	не значительный вред	средняя	актуальная
6.	A.3.2 – C.5.2 – E.2.3	0.6 – средняя	не значительный вред	средняя	актуальная
7.	A.3.2 – C.5.2 – E.2.4	0.6 – средняя	не значительный вред	средняя	актуальная
8.	A.3.2 – C.5.2 – E.2.5	0.6 – средняя	не значительный вред	средняя	актуальная
9.	A.3.2 – C.5.2 – E.2.6	0.6 – средняя	не значительный вред	средняя	актуальная
10.	A.3.3 – C.5.3 – E.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
11.	A.3.3 – C.5.3 – E.2.1	0.6 – средняя	не значительный вред	средняя	актуальная
12.	A.3.3 – C.5.3 – E.2.3	0.6 – средняя	не значительный вред	средняя	актуальная
13.	A.3.3 – C.5.3 – E.2.5	0.6 – средняя	не значительный вред	средняя	актуальная
14.	A.3.3 – C.5.3 – E.2.4	0.6 – средняя	не значительный вред	средняя	актуальная
15.	A.3.3 – C.5.3 – E.2.6	0.6 – средняя	не значительный вред	средняя	актуальная
16.	A.3.4 – C.5.2 – E.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
17.	A.3.4 – C.5.2 – E.1.3	0.6 – средняя	не значительный вред	средняя	актуальная
18.	A.3.4 – C.5.2 – E.2.7	0.6 – средняя	не значительный вред	средняя	актуальная
19.	A.3.4 – C.5.2 – E.2.1	0.6 – средняя	не значительный вред	средняя	актуальная
20.	A.3.4 – C.5.2 – E.2.3	0.6 – средняя	не значительный вред	средняя	актуальная
21.	A.3.4 – C.5.2 – E.2.5	0.6 – средняя	не значительный вред	средняя	актуальная
22.	A.3.4 – C.5.2 – E.2.4	0.6 – средняя	не значительный вред	средняя	актуальная
23.	A.3.4 – C.5.2 – E.2.6	0.6 – средняя	не значительный вред	средняя	актуальная

Таким образом, выявлено 23 актуальных для КАИС КРО угрозы программно-математического воздействия.

6.1.4. Угрозы при межсетевом взаимодействии

Угрозы безопасности путем использования протоколов межсетевого взаимодействия в КАИС КРО реализуются исходя из:

- топологии КАИС КРО (разграничение информационных потоков КАИС КРО и других информационных систем осуществляется без учета требований РД по информационной безопасности);
- наличия многоточечного подключения ЛВС локальных составных частей КАИС КРО к сетям общего пользования и (или) сетям международного информационного обмена.

Подключение ЛВС образовательных учреждений к сетям общего пользования и (или) сетям международного информационного обмена представляет собой наибольшую опасность при реализации угроз безопасности.

Угрозы безопасности ПДн различаются по нескольким основным признакам:

- характер угрозы (активная, пассивная);
- цель реализации угрозы (нарушение определенных характеристик безопасности);
- условие начала реализации угрозы (условное, безусловное);
- наличие обратной связи с ИСПДн;
- расположение нарушителя относительно ИСПДн;
- уровень, на котором реализуется угроза (по эталонной модели взаимодействия открытых систем ISO/OSI);
- соотношение количества нарушителей и элементов ИСПДн, относительно которых реализуется угроза.

Исходя из признаков, можно выделить наиболее часто реализуемые в настоящее время угрозы безопасности при межсетевом взаимодействии:

- анализ сетевого трафика;
- сканирование сети;
- угроза выявления пароля;
- подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением прав доступа;
- внедрение ложного объекта сети;
- отказ в обслуживании;

– удаленный запуск приложений.

В целях защиты информационных ресурсов образовательных учреждений со стороны сетей связи общего пользования, в ЛВС образовательных учреждений применяются:

– сертифицированное ФСБ России средство криптографической защиты информации – «Застава», осуществляющее функции межсетевого экранирования между ЕМТС и ЛВС образовательных учреждений;
– сертифицированный ФСТЭК России межсетевой экран WatchGuard XTM 25, осуществляющий функции межсетевого экранирования со стороны каналов передачи данных интернет-провайдера;
– сервис предотвращения сетевых вторжений Intrusion Prevention Service, установленный на ПАК WatchGuard XTM 25.

ПАК «Застава» (сертификат ФСТЭК №1586 от 31.03.2008 по 3 классу для МЭ) установлен как элемент выполнения обязательных технических требований для подключения ОИГВ к ЕМТС и не может быть отнесен к СрЗИ, входящим в состав системы защиты информации КАИС КРО.

На момент проведения обследования ПАК WatchGuard XTM 25 был установлен только в пилотной зоне КАИС КРО.

Таким образом, существуют объективные предпосылки для реализации угроз безопасности с использованием протоколов межсетевого взаимодействия в виде:

– отсутствие межсетевого экранирования на границах КАИС КРО;
– отсутствие средств обнаружения атак и поиска уязвимостей;
– игнорирование организационных ограничений (установленных правил) при работе на средствах вычислительной техники.

Угроза безопасности информации, реализуемая с использованием протоколов межсетевого взаимодействия, может быть представлена как совокупность источника угрозы (пункт 3.5 настоящего документа), уязвимости системы (пункт 3.6 настоящего документа), способа реализации угрозы (пункт 4 настоящего документа) и объекта воздействия (пункт 3.3 настоящего документа). Угроза будет существовать в случае, если может быть осуществлено какое-либо деструктивное воздействие на КАИС КРО (пункт 5 настоящего документа). Состав угроз подробно представлен в Приложении Г, перечень угроз с дополнительными показателями представлен в Таблице 6.6.

Таблица 6.6 - Актуальность угроз безопасности информации, реализуемых путем использования протоколов межсетевого взаимодействия

№	Наименование угрозы	Коэффициент реализуемости угрозы (Y)	Оценка вреда	Показатель опасности	Актуальность угрозы
1.	A.2.1 – Д.1 – B.2 – C.4.1 – E.1.3	0.6 – средняя	не значительный вред	средняя	актуальная
2.	A.2.1 – Д.1 – B.2 – C.4.2 – E.2.1	0.6 – средняя	не значительный вред	средняя	актуальная
3.	A.2.1 – Д.1 – B.2 – C.4.2 – E.2.7	0.6 – средняя	отсутствие вреда	низкая	не актуальная
4.	A.2.1 – Д.1 – B.2 – C.4.2 – E.3.1	0.6 – средняя	не значительный вред	средняя	актуальная
5.	A.2.1 – Д.1 – B.2 – C.4.2 – E.3.2	0.6 – средняя	не значительный вред	средняя	актуальная
6.	A.2.1 – Д.1 – B.2 – C.4.3 – E.3.1	0.6 – средняя	не значительный вред	средняя	актуальная
7.	A.2.1 – Д.1 – B.2 – C.4.3 – E.3.2	0.6 – средняя	не значительный вред	средняя	актуальная
8.	A.2.1 – Д.1 – B.2 – C.4.4 – E.2.1	0.6 – средняя	не значительный вред	средняя	актуальная
9.	A.2.1 – Д.1 – B.2 – C.4.4 – E.2.3	0.6 – средняя	не значительный вред	средняя	актуальная
10.	A.2.1 – Д.1 – B.2 – C.4.5 – E.1.1	0.6 – средняя	не значительный вред	средняя	актуальная
11.	A.2.1 – Д.1 – B.2 – C.4.5 – E.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
12.	A.1.2 – Д.4 – B.2 – C.4.2 – E.2.7	0.6 – средняя	отсутствие вреда	низкая	не актуальная
13.	A.1.2 – Д.4 – B.2 – C.4.2 – E.3.1	0.6 – средняя	не значительный вред	средняя	актуальная
14.	A.1.2 – Д.4 – B.2 – C.4.3 – E.2.7	0.6 – средняя	отсутствие вреда	низкая	не актуальная
15.	A.1.2 – Д.4 – B.2 – C.4.3 – E.3.1	0.6 – средняя	не значительный вред	средняя	актуальная
16.	A.1.2 – Д.4 – B.2 – C.4.3 – E.3.3	0.6 – средняя	не значительный вред	средняя	актуальная
17.	A.1.2 – Д.4 – B.2 – C.4.4 – E.1.3	0.6 – средняя	не значительный вред	средняя	актуальная
18.	A.1.2 – Д.4 – B.2 – C.4.4 – E.2.7	0.6 – средняя	не значительный вред	средняя	актуальная
19.	A.1.2 – Д.4 – B.2 – C.4.4 – E.3.1	0.6 – средняя	не значительный вред	средняя	актуальная
20.	A.1.2 – Д.4 – B.2 – C.4.4 – E.3.3	0.6 – средняя	не значительный вред	средняя	актуальная
21.	A.1.2 – Д.2 – B.2 – C.4.5 – E.1.2	0.6 – средняя	не значительный вред	средняя	актуальная
22.	A.1.2 – Д.2 – B.2 – C.4.5 – E.1.3	0.6 – средняя	не значительный вред	средняя	актуальная
23.	A.1.2 – Д.2 – B.2 – C.4.5 – E.2.7	0.6 – средняя	не значительный вред	средняя	актуальная
24.	A.1.2 – Д.2 – B.2 – C.4.5 – E.3.1	0.6 – средняя	не значительный вред	средняя	неактуальная
25.	A.1.2 – Д.2 – B.2 – C.4.5 – E.3.3	0.6 – средняя	не значительный вред	средняя	неактуальная
26.	A.1.2 – Д.2 – B.2 – C.4.5 – E.3.4	0.6 – средняя	не значительный вред	средняя	неактуальная

Таким образом, выявлено 26 угроз, реализуемых при межсетевом взаимодействии, из которых 23 (88,5 %) являются актуальными для КАИС КРО.

Реализация актуальных угроз реализуемых при межсетевом взаимодействии может привести к нарушению заданных оператором характеристик безопасности информационного ресурса КАИС КРО, что в свою очередь может стать причиной нанесения ущерба субъектам персональных данных.

7. РЕЗУЛЬТАТЫ АНАЛИЗА УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕКОМЕНДАЦИИ ПО ПРИСВОЕНИЮ КЛАССА

Обобщенные данные по выявленным угрозам представлены в таблице 7.1.

Таблица 7.1 Угрозы безопасности персональных данных

	Выявлено угроз		В том числе, связанных с наличием недокументированных возможностей в системном ПО	В том числе, связанных с наличием недокументированных возможностей в прикладном ПО
	всего	из них актуальных		
Угрозы доступа в ОС	106	106	22	12
Угрозы создания нештатных режимов работы программных и программно-аппаратных средств	44	44	-	11
Угрозы программно-математического воздействия	23	23	-	-
Угрозы, реализуемые при межсетевом взаимодействии	26	23 (88,5%)	-	-
Итого	199	196 (98,5%)	22	23

Анализ угроз безопасности информации, обрабатываемой в КАИС КРО, показал, что основными причинами возникновения актуальных угроз являются следующие факторы, а именно:

- преднамеренные или случайные действия пользователей и обслуживающего персонала;
- применение недостаточно эффективных технических средств защиты информации;
- низкий уровень исходной защищенности КАИС КРО, обусловленный наличием многоточечного выхода в сеть общего пользования и большим объемом персональных данных, передаваемых по незащищенным каналам связи;
- недоработки организационных мер по противодействию угрозам безопасности.

Выявленные актуальные угрозы КАИС КРО можно описать в следующих основных качествах:

- как доступ в ИСПДн пользователя, не идентифицированного средством защиты;
- как способ обхода средства защиты информации (СЗИ) от НСД;
- как возможность некорректной реализации разграничительной политики доступа пользователей к защищаемым ресурсам;
- как возможность внедрения в ИСПДн программ с потенциально опасными последствиями;
- как риск проведения основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP;
- как недобросовестное выполнение персоналом КАИС КРО своих служебных обязанностей, в рамках выполнения требований по защите информации.

Выявлены угрозы, связанные с наличием недокументированных (недекларированных возможностей) в системном и прикладном программном обеспечении. При этом у потенциального нарушителя появляются следующие возможности:

- изменения настроек программных средств СЗИ;
- несанкционированного доступа к защищаемой информации с использованием штатных средств ИСПДн;
- перехвата и вскрытия паролей;
- изменения состава программного обеспечения и внедрение нештатного программного обеспечения;
- компрометации технологической (аутентификационной информации) штатных средств ИСПДн.

Технические меры противодействия (нейтрализации) актуальным угрозам КАИС КРО должны обеспечивать:

- надежную аутентификацию пользователей, администраторов и средств вычислительной техники КАИС КРО;
- контроль доступа к внешним устройствам;
- ограничение программной среды;
- регистрацию событий информационной безопасности;
- защиту машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

- защиту от несанкционированной модификации и контроль целостности используемых в КАИС КРО программных средств;
- целостность программных средств защиты информации;
- целостность обрабатываемой защищаемой информации;
- обнаружение и блокирование деструктивных воздействий вредоносных программ на системное и специальное программное обеспечение КАИС КРО;
- обнаружение и блокирование угроз, исходящих из потенциально опасных сетей связи;
- защиту технических средств КАИС КРО, в том числе средств защиты информации;
- управление конфигурацией КАИС КРО и ее системы защиты.

Кроме того, используемые средства защиты и программное обеспечение с защитными сервисами (ОС, СУБД) должны пройти проверку соответствия требованиям по безопасности информации, в том числе на отсутствие недекларированных возможностей.

Реализация указанных мер в системе защиты информации КАИС КРО позволит в наибольшей степени затруднить или исключить возможность реализации угроз безопасности информации, а также снизить величину ущерба в случае их реализации.

Анализ угроз КАИС КРО показал, что реализация нарушителем угроз безопасности ПДн, приводящих к нарушению **конфиденциальности, целостности** ПДн имеют «средний» показатель опасности, т.е. реализация угроз может привести к **негативным последствиям** для субъектов персональных данных, а реализация нарушителем угроз безопасности ПДн, приводящих к **доступности** ПДн имеют «низкий» показатель опасности, (реализация угроз может привести к **незначительным негативным** последствиям для субъектов персональных данных).

Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства РФ от 1.11.2012 № 1119, устанавливают четыре уровня защищенности персональных данных при их обработке в информационных системах. Необходимыми условиями определения уровня защищенности является установление типа угроз безопасности персональных данных, актуальных для информационной системы, и категории персональных данных, обрабатываемых в информационной системе

В соответствии с выводами настоящей Модели угроз КАИС КРО относится к системам, для которых актуальны **угрозы 1-го типа**.

По категории персональных данных, обрабатываемых в информационной системе, КАИС КРО является системой, обрабатывающей **иные категории персональных данных**.

В КАИС КРО одновременно обрабатываются персональные данные **более чем 100000 субъектов персональных данных**.

Таким образом, с учетом вышеизложенного, доработка системы защиты информации КАИС КРО должна быть направлена на обеспечение 1-го уровня защищенности персональных данных при их обработке в информационной системе:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных.

Приложение А

Угрозы доступа в операционную систему

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
1.1. Угрозы, реализуемые в ходе загрузки операционной системы							
Перехват управления загрузкой с изменением необходимой технологической информации, в т.ч. перехват паролей / идентификаторов, модификация базовой системы ввода- вывода (BIOS)	Лицо, имеющее санкционированный доступ в помещения, с ресурсами КАИС КРО, но не имеющее права доступа к ресурсам – А.2.1 степень опасности - низкая	АРМ пользователя Д.1 важность ресурса - средняя	Уязвимость системного ПО В.1.1	Изменение настроек программных средств СЗИ С.3.1	Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя
					Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
			Недостатки организации ТЗИ – В.3	Изменение конфигурации технических средств С.1.4	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
			Уязвимости СЗИ – В.4	Перехват и вскрытие паролей	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя

[3] Источники угрозы определены в пункте 3.5 настоящего документа. Степень опасности каждого источника определена экспертным путем для КАИС КРО;
[4] Объекты воздействия описаны в пункте 3.3 настоящего документа. Важность ресурса определена как максимальная важность хотя бы одной из его составных частей. Важность составных частей определена экспертным путем для КАИС КРО;
[5] Частота (вероятность) реализации угрозы – определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация рассматриваемой угрозы персональных данных для КАИС КРО с учетом степени опасности и возможностей рассматриваемого источника угрозы;
[6] коэффициент реализуемости угрозы Y определяется соотношением $Y=(Y_1+Y_2)/20$, где Y_1 – уровень защищенности, рассчитанный в п.3.1 настоящего документа.

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
				С.3.2	Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
	Пользователь, КАИС КРО с персонального места - оператор А.2.3 степень опасности - средняя	АРМ пользователя Д.1 важность ресурса - средняя	Уязвимость системного ПО В.1.1	Изменение настроек программных средств СЗИ С.3.1	Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя
					Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
			Недостатки организации ТЗИ – В.3	Изменение конфигурации технических средств С.1.4	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
			Уязвимости СЗИ – В.4	Перехват и вскрытие паролей С.3.2	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями администратора БД КАИС КРО – А.2.4 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Уязвимость системного ПО В.1.1	Изменение настроек программных средств СЗИ С.3.1	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
			Недостатки организации ТЗИ – В.3	Изменение состава ПО и внедрение	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
				нештатного ПО С.3.3	Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями системного администратора/ администратора безопасности КАИС КРО – А.2.5 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Недостатки организации ТЗИ – В.3	Изменение состава ПО и внедрение нештатного ПО С.3.3	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
	Вредоносная программа А.3	АРМ пользователя Д.1 важность ресурса – средняя	Уязвимость системного ПО В.1.1	Изменение настроек программных средств СЗИ С.3.1	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
			Уязвимости СЗИ – В.4	Перехват и вскрытие паролей С.3.2	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
		Сервер Д.2 важность ресурса - очень высокая	Уязвимость системного ПО В.1.1	Изменение настроек программных средств СЗИ С.3.1	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
			Уязвимости СЗИ – В.4	Перехват и вскрытие паролей С.3.2	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
1.2. Угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем							
Несанкционированное ознакомление, модификация и блокирование защищаемой информации с использованием штатных программ ОС или специально разработанных программ	Лицо, имеющее санкционированный доступ в помещения с ресурсами КАИС КРО, но не имеющее права доступа к ресурсам – А.2.1 степень опасности - низкая	АРМ пользователя Д.1 важность ресурса – средняя	Уязвимость системного ПО В.1.1	НСД к ЗИ с использованием штатных средств ИСПДн (НДВ системного и прикладного ПО) С.2.1	Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя
					Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
					Воздействие на программы и данные прикладного ПО – Е.2.4.	низкая (2)	0.6 средняя
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	низкая (2)	0.6 средняя
				Перехват и вскрытие паролей – С.3.2	Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	низкая (2)	0.6 средняя
			Уязвимость прикладного и	НСД к ЗИ с использование	Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
			специального ПО B.1.2	м штатных средств ИСПДн C.2.1	Воздействие на программы и данные прикладного ПО – E.2.4.	низкая (2)	0.6 средняя
				Перехват и вскрытие паролей – C.3.2	Воздействие на ПО и защищаемую информацию – E.2.1	низкая (2)	0.6 средняя
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– E.2.5.	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – E.2.6	низкая (2)	0.6 средняя
			Уязвимости СЗИ B.4	Изменение настроек программных средств СЗИ – C.3.1	Несанкционированное копирование – E.1.2	низкая (2)	0.6 средняя
					Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
				Изменение состава ПО и внедрение нештатного ПО C.3.3	Внедрение вредоносной программы – E.2.6	низкая (2)	0.6 средняя
					Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
	Пользователь, КАИС КРО с персонального места - оператор A.2.3	АРМ пользователя Д.1 важность ресурса –	Недостатки организации ТЗИ – B.3	Изменение состава ПО и внедрение нештатного ПО C.3.3	Внедрение вредоносной программы – E.2.6	средняя (5)	0.75 высокая
					Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
	степень опасности - средняя	средняя	Уязвимости СЗИ B.4	Изменение настроек программных средств СЗИ – C.3.1	Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
				Изменение состава ПО и внедрение нештатного ПО C.3.3	Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями администратора БД КАИС КРО – A.2.4 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Уязвимость системного ПО B.1.1	НСД к ЗИ с использованием штатных средств ИСПДн C.2.1	Воздействие на программы и данные ОС - E.2.3	средняя (5)	0.75 высокая
				Изменение состава ПО и внедрение нештатного ПО C.3.2	Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
			Уязвимости СЗИ B.4	Изменение настроек программных средств СЗИ – C.3.1	Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
				Изменение состава ПО и	Внедрение вредоносной программы – E.2.6	низкая (2)	0.6 средняя

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
				внедрение нештатного ПО С.3.3	Воздействие на СЗИ – Е.2.8	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями системного администратора/ администратора безопасности КАИС КРО – А.2.5 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Уязвимость системного ПО В.1.1	Изменение состава ПО и внедрение нештатного ПО С.3.3	Воздействие на ПО и защищаемую информацию – Е.2.1	средняя (5)	0.75 высокая
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	средняя (5)	0.75 высокая
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
			Уязвимость прикладного и специального ПО В.1.2	Изменение состава ПО и внедрение нештатного ПО С.3.3	Воздействие на ПО и защищаемую информацию – Е.2.1	средняя (5)	0.75 высокая
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	средняя (5)	0.75 высокая
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
			Недостатки организации ТЗИ – В.3	Изменение состава ПО и внедрение нештатного ПО С.3.3	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
					Воздействие на программы и данные прикладного ПО – Е.2.4.	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – Е.2.6	низкая	0.6

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
						(2)	средняя
					Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
			Уязвимости СЗИ B.4	Изменение настроек программных средств СЗИ – C.3.1	Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
				Изменение состава ПО и внедрение нештатного ПО C.3.3	Воздействие на СЗИ – E.2.8	низкая (2)	0.6 средняя
1.3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ							
Угрозы доступа (проникновения) в среду функционирования прикладных программ	Лицо, имеющее санкционированный доступ в помещения с ресурсами КАИС КРО, но не имеющее права доступа к ресурсам – A.2.1 степень опасности - низкая	АРМ пользователя Д.1 важность ресурса – средняя	Недостатки организации ТЗИ – B.3	Изменение состава ПО и внедрение нештатного ПО C.3.3	Воздействие на ПО и защищаемую информацию – E.2.1	низкая (2)	0.6 средняя
					Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - E.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - E.2.3	низкая (2)	0.6 средняя
					Воздействие на программы и данные прикладного ПО – E.2.4.	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – E.2.6	низкая (2)	0.6 средняя
			Уязвимости СЗИ B.4	Изменение состава ПО и внедрение нештатного ПО C.3.3	Воздействие на ПО и защищаемую информацию – E.2.1	низкая (2)	0.6 средняя
					Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - E.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС -	низкая	0.6

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
					E.2.3	(2)	средняя
					Воздействие на программы и данные прикладного ПО – E.2.4.	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – E.2.6	низкая (2)	0.6 средняя
	Пользователь, КАИС КРО с персонального места - оператор A.2.3 степень опасности - средняя	АРМ пользователя Д.1 важность ресурса – средняя	Недостатки организации ТЗИ B.3	Изменение состава ПО и внедрение нештатного ПО C.3.3	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - E.2.2	средняя (5)	0.75 высокая
					Воздействие на программы и данные ОС - E.2.3	средняя (5)	0.75 высокая
					Воздействие на программы и данные прикладного ПО – E.2.4.	средняя (5)	0.75 высокая
					Внедрение вредоносной программы – E.2.6	средняя (5)	0.75 высокая
			Уязвимости СЗИ B.4	Изменение состава ПО и внедрение нештатного ПО C.3.3	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - E.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - E.2.3	низкая (2)	0.6 средняя
					Воздействие на программы и данные прикладного ПО – E.2.4.	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – E.2.6	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями администратора БД КАИС КРО – A.2.4 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Недостатки организации ТЗИ **B.3**	Изменение состава ПО и внедрение нештатного ПО C.3.3	Воздействие на ПО, данные и драйвера, обеспечивающие загрузку ОС– E.2.2	средняя (5)	0.75 высокая
					Воздействие на программы и данные ОС - E.2.3	средняя (5)	0.75 высокая
					Воздействие на программы и данные прикладного ПО – E.2.4.	средняя (5)	0.75 высокая

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	средняя (5)	0.75 высокая
					Внедрение вредоносной программы – Е.2.6	средняя (5)	0.75 высокая я
			Уязвимости СЗИ В.4	Изменение состава ПО и внедрение нештатного ПО С.3.3	Воздействие на ПО, данные и драйвера, обеспечивающие загрузку ОС– Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
					Воздействие на программы и данные прикладного ПО – Е.2.4.	низкая (2)	0.6 средняя
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями системного администратора/ администратора безопасности КАИС КРО – А.2.5 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Недостатки организации ТЗИ В.3	Изменение состава ПО и внедрение нештатного ПО С.3.3	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	средняя (5)	0.75 высокая я
					Воздействие на программы и данные ОС - Е.2.3	средняя (5)	0.75 высокая я
					Воздействие на программы и данные прикладного ПО – Е.2.4.	высокая (10)	1.0 очень высокая
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	средняя (5)	0.75 высокая я
					Внедрение вредоносной программы – Е.2.6	высокая (10)	1.0 очень высокая
					Воздействие на СЗИ – Е.2.8	средняя (5)	0.75 высокая я
			Уязвимость прикладного и	Компрометация	Воздействие на ПО и защищаемую информацию – Е.2.1	средняя (5)	0.75 высокая я

Наименование угрозы	Источник угрозы, обозначение, степень опасности[3]	Объект воздействия, важность ресурса[4]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[5] (Y2)	Коэффициент реализуемости угрозы[6] (Y)
			специального ПО В.1.2	технологической (аутентификационной информации) штатных средств ИСПДн – С.2.2	Воздействие на программы и данные прикладного ПО – Е.2.4.	средняя (5)	0.75 высокая я
					Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	средняя (5)	0.75 высокая я
					Внедрение вредоносной программы – Е.2.6	средняя (5)	0.75 высокая я

Приложение Б

Угрозы создания нештатных режимов работы программных и программно-аппаратных средств

Наименование угрозы	Источник угрозы, обозначение, степень опасности[7]	Объект воздействия, важность ресурса[8]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[9] (Y2)	Коэффициент реализуемости угрозы[10] (Y)
Угрозы, реализованные путем физического доступа к элементам ИСПДн	Лицо, имеющее санкционированный доступ в помещения с ресурсами КАИС КРО, но не имеющее права доступа к ресурсам – А.2.1 степень опасности - низкая	АРМ пользователя Д.1 важность ресурса - средняя	Недостатки организации ТЗИ – В.3	Хищение, уничтожение, разрушение носителя защищаемых информационных ресурсов С.1.1	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
				Изменение конфигурации технических средств С.1.4	Внедрение программно-аппаратных закладок (ПАЗ) – Е.2.6	низкая (2)	0.6 средняя
		Отчуждаемые носители информации Д.3 важность ресурса - средняя	Недостатки организации ТЗИ – В.3	Хищение, уничтожение, разрушение носителя защищаемых информационных ресурсов С.1.1	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя

[7] Источники угрозы определены в пункте 3.5 настоящего документа. Степень опасности каждого источника определена экспертным путем для КАИС КРО;
[8] Объекты воздействия описаны в пункте 3.3 настоящего документа. Важность ресурса определена как максимальная важность хотя бы одной из его составных частей. Важность составных частей определена экспертным путем для КАИС КРО;
[9] Частота (вероятность) реализации угрозы – определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация рассматриваемой угрозы персональных данных для КАИС КРО с учетом степени опасности и возможностей рассматриваемого источника угрозы;
[10] коэффициент реализуемости угрозы Y определяется соотношением $Y = (Y_1+Y_2)/20$, где Y_1 – уровень защищенности, рассчитанный в п.3.1 настоящего документа.

Наименование угрозы	Источник угрозы, обозначение, степень опасности[7]	Объект воздействия, важность ресурса[8]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[9] (Y2)	Коэффициент реализуемости угрозы[10] (Y)
	Лицо, обеспечивающее поставку, сопровождение и ремонт технических средств КАИС КРО - А.2.2 степень опасности - низкая	АРМ пользователя Д.1 важность ресурса – средняя	Недостатки организации ТЗИ – В.3	Хищение, уничтожение, разрушение носителя защищаемых информационных ресурсов С.1.1	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
				Изменение конфигурации технических средств С.1.4	Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
		Сервер Д.2 важность ресурса - очень высокая	Недостатки организации ТЗИ – В.3	Хищение, уничтожение, разрушение носителя защищаемых информационных ресурсов С.1.1	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
				Изменение конфигурации технических средств С.1.4	Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
		Коммутационное оборудование Д.4 важность ресурса - средняя	Недостатки организации ТЗИ – В.3	Изменение конфигурации технических средств С.1.4	Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя

Наименование угрозы	Источник угрозы, обозначение, степень опасности[7]	Объект воздействия, важность ресурса[8]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[9] (Y2)	Коэффициент реализуемости угрозы[10] (Y)
	Пользователь, КАИС КРО с персонального места - оператор А.2.3 степень опасности - средняя	АРМ пользователя Д.1 важность ресурса - средняя	Недостатки организации ТЗИ – В.3	Хищение, уничтожение, разрушение носителя защищаемых информационных ресурсов С.1.1	Несанкционированное копирование – Е.1.2	средняя (5)	0.75 высокая
				Изменение конфигурации технических средств С.1.4	Внедрение вредоносной программы – Е.2.6	средняя (5)	0.75 высокая
					Воздействие на СЗИ – Е.2.8	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями администратора БД КАИС КРО – А.2.4 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Недостатки организации ТЗИ – В.3	Хищение, уничтожение, разрушение носителя защищаемых информационных ресурсов С.1.1	Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
Угрозы преднамеренных действий внутренних нарушителей (лиц, допущенных к защищаемой информации)	Пользователь, КАИС КРО с персонального места - оператор А.2.3 степень опасности - средняя	АРМ пользователя Д.1 важность ресурса - средняя	Недостатки организации ТЗИ – В.3	Несоблюдение организационных мероприятий по ЗИ С.1.5.	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
					Воздействие на ПО и данные пользователя – Е.2.1	низкая (2)	0.6 средняя
		Сервер Д.2	Недостатки организации ТЗИ – В.3	Несоблюдение организационны	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя

Наименование угрозы	Источник угрозы, обозначение, степень опасности[7]	Объект воздействия, важность ресурса[8]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[9] (Y2)	Коэффициент реализуемости угрозы[10] (Y)
		важность ресурса - очень высокая		х мероприятий по ЗИ С.1.5.	Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
		Отчуждаемые носители информации Д.3 важность ресурса – средняя	Недостатки организации ТЗИ – В.3	Несоблюдение организационных мероприятий по ЗИ С.1.5.	Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями администратора БД КАИС КРО – А.2.4 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Недостатки организации ТЗИ – В.3	Несоблюдение организационных мероприятий по ЗИ С.1.5.	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
					Воздействие на ПО и данные пользователя – Е.2.1	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
	Зарегистрированный пользователь с полномочиями системного администратора/ администратора безопасности КАИС КРО – А.2.5 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Недостатки организации ТЗИ – В.3	Несоблюдение организационных мероприятий по ЗИ С.1.5.	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
					Воздействие на ПО и данные пользователя – Е.2.1	низкая (2)	0.6 средняя
					Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя

Наименование угрозы	Источник угрозы, обозначение, степень опасности[7]	Объект воздействия, важность ресурса[8]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[9] (Y2)	Коэффициент реализуемости угрозы[10] (Y)
					Воздействие на программы и данные прикладного ПО – Е.2.4.	низкая (2)	0.6 средняя
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
					Воздействие на СЗИ – Е.2.8	низкая (2)	0.6 средняя
	Лицо, осуществляющее разработку прикладного ПО КАИС КРО – А.2.6 степень опасности - высокая	Сервер Д.2 важность ресурса - очень высокая	Недостатки организации ТЗИ – В.3	Несоблюдение организационных мероприятий по ЗИ С.1.5.	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
					Воздействие на ПО и данные пользователя – Е.2.1	низкая (2)	0.6 средняя
					Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
					Воздействие на программы и данные прикладного ПО – Е.2.4.	средняя (5)	0.75 высокая
					Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
					Воздействие на СЗИ – Е.2.8	низкая (2)	0.6 средняя
					Нарушение и отказы функционирования средств обработки информации – Е.3.1	средняя (5)	0.75 высокая
					Нарушение и отказы функционирования средств ввода/вывода информации – Е.3.2	средняя (5)	0.75 высокая
					Нарушение и отказы функционирования средств хранения информации – Е.3.3	средняя (5)	0.75 высокая
					Нарушение и отказы функционирования средств защиты информации – Е.3.5	средняя (5)	0.75 высокая

Приложение В

Угрозы программно-математического воздействия

Класс вредоносной программы	Способ внедрения	Деструктивное воздействие	Частота реализации угрозы[11] (Y2)	Коэффициент реализуемости угрозы[12] (Y)
Загрузочные – А.3.1	Передача управления на оригинальный загрузочный сектор – С.5.1	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ - Е.2.2	низкая (2)	0.6 средняя
		Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
Файловые – А.3.2	Действия пользователя – С.5.2	Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
		Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя
		Воздействие на ПО, данные и драйвера, обеспечивающие загрузку ОС и СЗИ – Е.2.2	низкая (2)	0.6 средняя
		Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
		Воздействие на программы и данные прикладного ПО – Е.2.4.	низкая (2)	0.6 средняя
		Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– Е.2.5.	низкая (2)	0.6 средняя
		Внедрение вредоносной программы – Е.2.6	низкая (2)	0.6 средняя
Сетевые – А.3.3	Самостоятельная передача и запуск кода – С.5.3	Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
		Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя
		Воздействие на ПО, данные и драйвера, обеспечивающие загрузку ОС и СЗИ – Е.2.2	низкая (2)	0.6 средняя
		Воздействие на программы и данные ОС - Е.2.3	низкая	0.6

[11] Частота (вероятность) реализации угрозы – определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация рассматриваемой угрозы персональных данных для КАИС КРО с учетом степени опасности и возможностей рассматриваемого источника угрозы;

[12] коэффициент реализуемости угрозы Y определяется соотношением $Y = (Y_1+Y_2)/20$, где Y_1 – уровень защищенности, рассчитанный в п.3.1 настоящего документа.

Класс вредоносной программы	Способ внедрения	Деструктивное воздействие	Частота реализации угрозы[11] (Y2)	Коэффициент реализуемости угрозы[12] (Y)
			(2)	средняя
		Воздействие на программы и данные прикладного ПО – E.2.4.	низкая (2)	0.6 средняя
		Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– E.2.5.	низкая (2)	0.6 средняя
		Внедрение вредоносной программы – E.2.6	низкая (2)	0.6 средняя
Прочие вредоносные программы (утилиты) – A.3.4	Действия пользователя – C.5.2	Несанкционированное копирование – E.1.2	низкая (2)	0.6 средняя
		Перехват информации в каналах связи - E.1.3	низкая (2)	0.6 средняя
		Воздействие на ПО и защищаемую информацию – E.2.1	низкая (2)	0.6 средняя
		Воздействие на программы и данные ОС - E.2.3	низкая (2)	0.6 средняя
		Воздействие на программы и данные прикладного ПО – E.2.4.	низкая (2)	0.6 средняя
		Воздействие на промежуточные (оперативные) значения программ и данных в процессе их обработки– E.2.5.	низкая (2)	0.6 средняя
		Внедрение вредоносной программы – E.2.6	низкая (2)	0.6 средняя
		Воздействие на технологическую и сетевую информацию – E.2.7	низкая (2)	0.6 средняя

Приложение Г
Угрозы при межсетевом взаимодействии

Наименование угрозы	Источник угрозы, обозначение, степень опасности[13]	Объект воздействия, важность ресурса[14]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[15] (Y2)	Коэффициент реализуемости угрозы[16] (Y)
Угрозы, реализуемые непосредственно в ИСПДн	Лицо, имеющее санкционированный доступ в помещения с ресурсами КАИС КРО, но не имеющее права доступа к ресурсам – А.2.1 степень опасности - низкая	АРМ пользователя Д.1 важность ресурса - средняя	Реализация протоколов межсетевого взаимодействия – В.2	Перехват информации С.4.1	Перехват информации в каналах передачи данных – Е.1.3	низкая (2)	0.6 средняя
				Модификация передаваемых данных – С.4.2.	Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя
					Воздействие на технологическую сетевую информацию – Е.2.7	низкая (2)	0.6 средняя
				Внедрение вредоносных программ – С.4.4	Воздействие на ПО и защищаемую информацию – Е.2.1	низкая (2)	0.6 средняя
					Воздействие на программы и данные ОС - Е.2.3	низкая (2)	0.6 средняя
				Удаленный несанкционированный доступ в систему - С.4.5	Утечка /разглашение ЗИ – Е.1.1	низкая (2)	0.6 средняя
					Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя

[13] Источники угрозы определены в пункте 3.5 настоящего документа. Степень опасности каждого источника определена экспертным путем для КАИС КРО;
[14] Объекты воздействия описаны в пункте 3.3 настоящего документа. Важность ресурса определена как максимальная важность хотя бы одной из его составных частей. Важность составных частей определена экспертным путем для КАИС КРО;
[15] Частота (вероятность) реализации угрозы – определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация рассматриваемой угрозы персональных данных для КАИС КРО с учетом степени опасности и возможностей рассматриваемого источника угрозы;
[16] коэффициент реализуемости угрозы Y определяется соотношением $Y = (Y_1+Y_2)/20$, где Y_1 – уровень защищенности, рассчитанный в п.3.1 настоящего документа.

Наименование угрозы	Источник угрозы, обозначение, степень опасности[13]	Объект воздействия, важность ресурса[14]	Уязвимость	Способ реализации	Деструктивное воздействие	Частота реализации угрозы[15] (Y2)	Коэффициент реализуемости угрозы[16] (Y)
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей	Лица, получившие доступ к информационным ресурсам КАИС КРО из внешних сетей телекоммуникаций, в том числе ССОП- А.1.2 степень опасности - высокая	Линии связи и коммутационное оборудование Д.4 важность ресурса – средняя	Реализация протоколов межсетевого взаимодействия – В.2	Модификация передаваемых данных – С.4.2.	Воздействие на технологическую сетевую информацию – Е.2.7	низкая (2)	0.6 средняя
				Перегрузка ресурсов - С.4.3	Воздействие на технологическую сетевую информацию – Е.2.7	низкая (2)	0.6 средняя
				Внедрение вредоносных программ – С.4.4	Перехват информации в каналах передачи данных – Е.1.3	низкая (2)	0.6 средняя
					Воздействие на технологическую сетевую информацию – Е.2.7	низкая (2)	0.6 средняя
		Сервер Д.2 важность ресурса - очень высокая	Реализация протоколов межсетевого взаимодействия – В.2	Удаленный несанкционированный доступ в систему – С.4.5	Несанкционированное копирование – Е.1.2	низкая (2)	0.6 средняя
					Перехват информации в каналах передачи данных – Е.1.3	низкая (2)	0.6 средняя
					Воздействие на технологическую сетевую информацию – Е.2.7	низкая (2)	0.6 средняя