СОГЛАСОВАНО
Генеральный директор
ООО «ТСС»

_____ В.В. Сергиев
«__» _____ 2017 г.

УТВЕРЖДАЮ
Руководитель департамента
информатизации и связи
Краснодарского края

_____ Е.В. Юшков
«__» _____ 2017 г.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ КРАСНОДАРСКОГО КРАЯ

г. Краснодар
2017 г.

Лист согласования

Департамент информатизации и связи Краснодарского края

Должность	Фамилия, имя, отчество	Подпись	Дата
Начальник управления связи	Стаценко А.Н.		18.12.2017
Начальник отдела информационной безопасности	Синеок С.В.		18.12.2017

Сведения о разработчике

Наименование организации: Общество с ограниченной ответственностью «ТелекомСтройСервис» (ООО «ТСС»)

Юридический и почтовый адрес: 350061, Российская Федерация, Краснодарский край, г. Краснодар, ул. Благоева, д. 24/1, литер А1.

ИНН: 2312156896

КПП: 231201001

E-mail: ib@tss23.ru

Разработано:

Должность	Фамилия, имя, отчество	Подпись	Дата
Начальник отдела защиты информации ООО «ТСС»	Барсуков О.И.		23.11.2017
Специалист по защите информации ООО «ТСС»	Редько А.С.		23.11.2017

АННОТАЦИЯ

Настоящий документ разработан на основании проведённого обследования объектов информатизации исполнительных органов государственной власти Краснодарского края (далее – ИОГВ Краснодарского края).

Модель угроз безопасности информации информационных систем исполнительных органов государственной власти Краснодарского края (далее – Модель угроз) содержит обобщённое описание угроз и потенциальных нарушителей безопасности информационных систем ИОГВ Краснодарского края, в которых обрабатывается защищаемая информация.

В настоящем документе в качестве объекта информатизации рассматривается совокупность информационных ресурсов (информации), средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации.

Модель угроз учитывает современное состояние и ближайшие перспективы развития информационных систем ИОГВ Краснодарского края.

Модель угроз разработана на основании:

— Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой заместителем директора ФСТЭК России 15 февраля 2008 года;

— Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой заместителем директора ФСТЭК России 14 февраля 2008 года.

Настоящий документ является основой для разработки Частных моделей угроз безопасности информации информационных систем ИОГВ Краснодарского края.

СОДЕРЖАНИЕ

1 Общие положения

Настоящий документ содержит единые исходные данные по угрозам безопасности информации (далее – УБИ), обрабатываемой в информационных системах (далее – ИС) ИОГВ Краснодарского края, которые:

— не связаны с деятельностью человека;
— обусловлены техногенным характером угроз;
— связаны с ошибочными действиями персонала;
— связаны с перехватом защищаемой информации по техническим каналам с целью ее копирования или неправомерного распространения;
— связаны с несанкционированным доступом (далее – НСД) к информации, обрабатываемой в ИС с целью изменения, копирования, неправомерного распространения защищаемой информации или деструктивных воздействий на элементы ИС и обрабатываемой в них защищаемой информации с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования защищаемой информации.

Целью разработки настоящей Модели угроз является:

— определение перечня актуальных угроз безопасности персональных данных, обрабатывающихся в информационных системах персональных данных (далее – ИСПДн) ИОГВ Краснодарского края;
— определение перечня актуальных угроз безопасности информации, обрабатывающейся в государственных информационных системах (далее – ГИС) ИОГВ Краснодарского края.
— описание идентифицированных угроз безопасности информации, определение степени актуальности угроз, возможности и способов их реализации, а также значимости последствий этих угроз.

Настоящим документом необходимо руководствоваться при решении следующих задач:

— анализ защищенности информационных систем ИОГВ Краснодарского края от УБИ в ходе организации и выполнения работ по обеспечению безопасности информации;
— разработка/модернизация системы защиты информации, обеспечивающая нейтрализацию предполагаемых УБИ с использованием методов и способов защиты информации, предусмотренных руководящими документами ФСТЭК России и ФСБ России;
— проведение мероприятий, направленных на предотвращение несанкционированного доступа к защищаемой информации и (или) передачи ее лицам, не имеющим права доступа к такой информации;
— осуществление контроля воздействий различного рода на технические средства ИС ИОГВ Краснодарского края, в результате которых может быть нарушено их функционирование;
— осуществление контроля обеспечения уровня защищенности ИС ИОГВ Краснодарского края.

В настоящем документе дано обобщённое описание ИС ИОГВ Краснодарского края как объектов защиты, возможных источников УБИ, основных классов

уязвимостей ИС, возможных видов деструктивных воздействий на защищаемую информацию, а также основных способов их реализации.

Рассматриваемые в настоящем документе УБИ, могут уточняться и дополняться по мере выявлении новых источников угроз, развития способов и средств реализации УБИ в ИС ИОГВ Краснодарского края, а также при разработке Частных моделей угроз безопасности конкретных ИС ИОГВ Краснодарского края.

В связи с тем, что в различных ИОГВ Краснодарского края степень информатизации различна (в т.ч. в связи с применением различных информационных технологий), а также разная степень зрелости систем обеспечения информационной безопасности (далее – СОИБ), при разработке настоящей Модели угроз приняты унифицированные допущения о компонентах ИС ИОГВ и мерах защиты информации, реализованных в них. Разработка Частных моделей угроз безопасности ИС ИОГВ Краснодарского края должна осуществляться с учётом применяемых информационных технологий и реализованных мер защиты информации в конкретных рассматриваемых ИС.

2 Описание информационных систем

В зависимости от архитектуры, структуры (топологии) и назначения ИС, по результатам проведённого обследования объектов информатизации ИОГВ Краснодарского края (Приложение А), были определены 4 типа информационных систем (сегментов информационных систем) ИОГВ Краснодарского края.

К типу 1 относятся серверные сегменты ИС ИОГВ Краснодарского края, размещаемые на вычислительных ресурсах Департамента информатизации и связи Краснодарского края в центре обработки данных региональной мультисервисной сети исполнительных органов государственной власти Краснодарского края (далее – ЦОД РМС ОГВ), предоставляемых им для обработки защищаемой информации.

К типу 2 относятся серверные сегменты ИС ИОГВ Краснодарского края при их размещении на сторонних вычислительных ресурсах (мощностях уполномоченного лица), предоставляемых для обработки защищаемой информации.

К типу 3 относятся ИС ИОГВ Краснодарского края, серверный и пользовательский сегменты которых располагаются в пределах локально-вычислительной сети (далее – ЛВС) одного ИОГВ Краснодарского края.

К типу 4 относятся пользовательские сегменты ИС ИОГВ Краснодарского края, осуществляющих доступ к ИС ИОГВ Краснодарского края типов 1,2 и 3, располагающиеся непосредственно в ИОГВ Краснодарского края.

Рассматриваемые сегменты информационных систем вне зависимости от мест их размещения являются локальными, однако каждая информационная система в целом может являться как локальной, так и распределённой.

Характер обрабатываемой информации не влияет на отнесение ИС ИОГВ Краснодарского края к тому или иному типу.

Принципиальная схема ИС ИОГВ Краснодарского края представлена на рисунке 1.

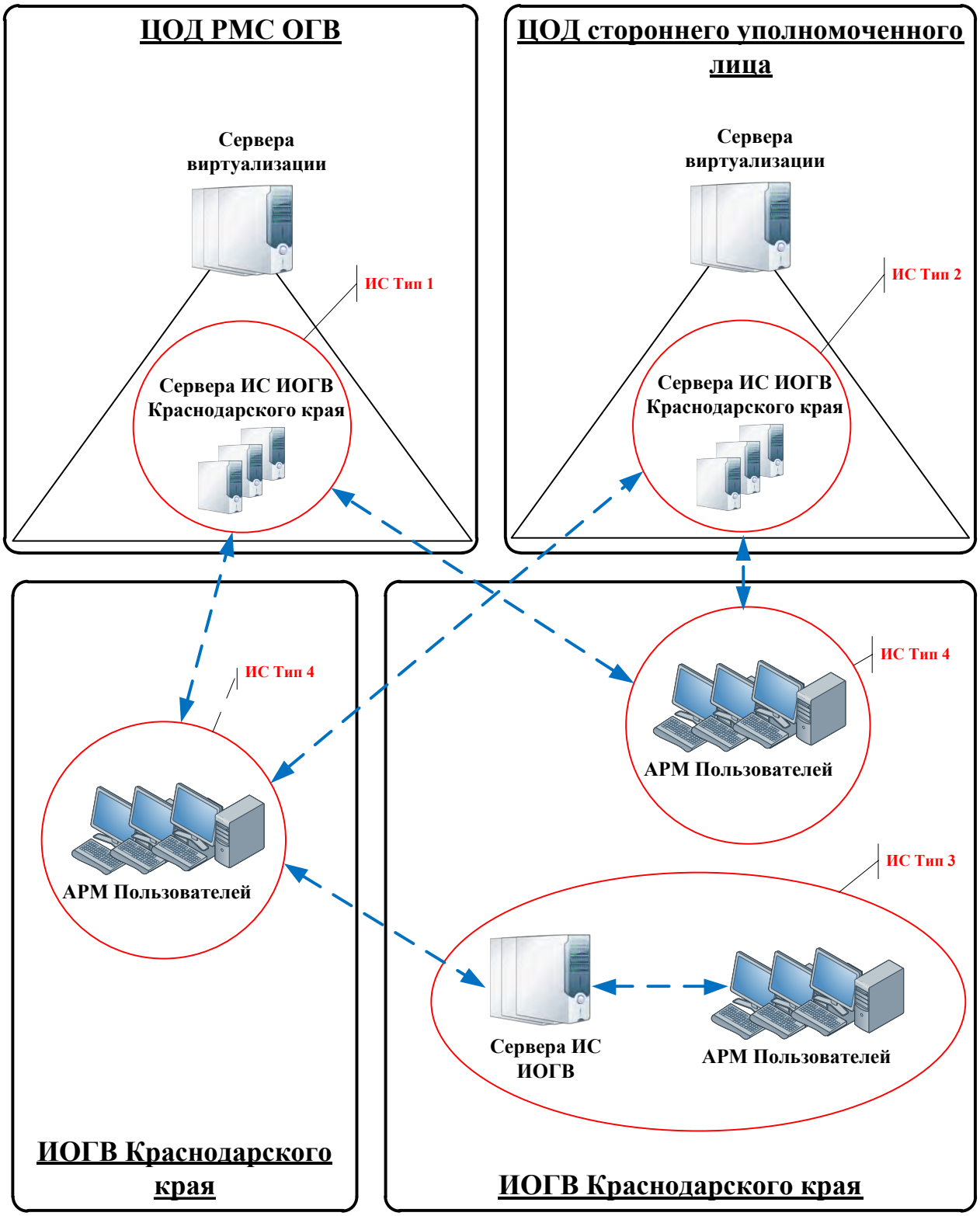


Рисунок 1 – Принципиальная схема организации ИС ИОГВ Краснодарского края

2.1 Состав защищаемой информации

Состав защищаемой информации, характерный для всех типов информационных систем, включает:

— служебную информацию:
  - с ограничительной пометкой «для служебного пользования» (далее – ДСП);
  - без ограничительной пометки «для служебного пользования» (далее – служебная информация);

— общедоступную информацию (в т.ч. обрабатываемую на общедоступных ресурсах (веб-порталах);

— информацию, составляющую коммерческую тайну третьих лиц (далее – коммерческая тайна);

— персональные данные:
  - персональные данные должностных лиц и работников ИОГВ Краснодарского края, а также членов их семей;
  - персональные данные граждан, претендующих на замещение вакантных должностей в ИОГВ Краснодарского края, а также членов их семей;
  - персональные данные лиц, уволенных с государственной службы (работы) в ИОГВ Краснодарского края, а также членов их семей;
  - персональные данные физических лиц (граждан), при предоставлении ИОГВ Краснодарского края государственных услуг (исполнении государственных функций).

Объем защищаемой информации индивидуален для каждой ИС.

2.2 Цели защиты информации

Цели защиты информации (характеристики информации, которые необходимо обеспечить), характерные для различных видов защищаемой информации, обрабатываемой в ИС ИОГВ Краснодарского края, представлены в таблице 1.

Таблица 1 – Цели защиты информации

№ п/п	Вид защищаемой информации		Характеристики информации		
			К[1]	Ц[2]	Д[3]
1	Служебная информация			+	+
2	ДСП		+	+	+
3	Общедоступная информация			+	+
4	Коммерческая тайна		+	+	+
5	Персональные данные:		+	+	+
5.1		персональные данные должностных лиц и работников ИОГВ Краснодарского края, а также членов их семей	+[4]	+	+

[1] Конфиденциальность
[2] Целостность
[3] Доступность
[4] За исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации

№ п/п	Вид защищаемой информации		Характеристики информации		
			К[1]	Ц[2]	Д[3]
5.2		персональные данные граждан, претендующих на замещение вакантных должностей в ИОГВ Краснодарского края, а также членов их семей	+	+	+
5.3		персональные данные лиц, уволенных с государственной службы (работы) в ИОГВ Краснодарского края, а также членов их семей	+	+	+
5.4		персональные данные физических лиц (граждан), при предоставлении ИОГВ Краснодарского края государственных услуг (исполнении государственных функций)	+	+	+

2.3 Объекты защиты

Типовые объекты защиты, безопасность которых необходимо обеспечить в ИС ИОГВ Краснодарского края, целесообразно разделить на следующие категории:

— информационные ресурсы (далее – ИР);
— системное программное обеспечение (далее – СПО) и прикладное программное обеспечение (далее – ППО);
— средства вычислительной техники;
— инженерно-техническое оборудование.

Перечень объектов защиты, характерных для различных типов ИС ИОГВ Краснодарского края, представлен в таблице 2.

Таблица 2 – Перечень объектов защиты

№ п/п	Объект защиты	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
Информационные ресурсы					
1	документы в файловом виде на АРМ пользователей			+	+
2	документы в файловом виде на серверах	+	+	+	
3	сведения, содержащейся в базах данных (далее - БД)	+	+	+	+[5]
4	сведения, содержащиеся на электронных носителях информации			+	+
5	сведения, содержащиеся на материальных носителях (документы в бумажном виде)			+	+
Системное и прикладное программное обеспечение					
1	системное программное обеспечение	+	+	+	+
2	прикладное программное обеспечение общего назначения	+	+	+	+
3	прикладное программное обеспечение специализированного назначения	+	+	+	+

[5] При отображении на мониторе АРМ пользователя информации при доступе к БД

№ п/п	Объект защиты	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
Средства вычислительной техники					
1	автоматизированные рабочие места пользователей (далее - АРМ)	-*[6]	-*	+	+
2	мобильные устройства (ноутбуки, мобильные телефоны, планшеты)			+	+
3	файловые сервера	+	+	+	
4	сервера баз данных	+	+	+	
5	веб-сервера (порталы)	+	+	+	
6	виртуальные сервера	+	+	+	
7	системы хранения данных	+	+	+	
8	системы резервного копирования	+	+	+	
9	коммуникационное оборудование[7]	+	+	+	+
10	электронные носители информации (flash-накопители, жёсткие диски, CD/DVD-диски)			+	+
11	средства защиты информации	+	+	+	+
Инженерно-техническое оборудование					
1	средства обеспечения электропитания	+	+	+	+
2	средства обеспечения гарантированного электропитания[8]	+	+	+	+
3	средства вентиляции и кондиционирования	+	+	+	+
4	системы контроля и управления доступом (далее – СКУД)	+	+	+	+
5	системы охранной сигнализации	+	+	+	+
6	системы пожарной сигнализации и средства пожаротушения	+	+	+	+

2.4 Сведения о наличии каналов связи

Для ИС ИОГВ Краснодарского края типа 1 и 2 характерно наличие нескольких высокосортных каналов связи для доступа к сетям связи общего пользования (далее – ССОП), в том числе и сетям связи международного информационного обмена (далее – СМИО). Также, для ИС ИОГВ Краснодарского края типа 1 и 2 характерно дублирование каналов связи (обеспечения отказоустойчивости).

Для ИС ИОГВ Краснодарского края типа 3 и 4 характерно наличие одного или нескольких каналов связи со средней и (или) низкой скоростью передачи данных для доступа к ССОП. Также возможно применение мобильных устройств доступа к ССОП.

[6] Под пользователями, в данном случае, понимаются субъекты доступа, эксплуатирующие информационные системы. АРМ администраторов (в т.ч. числе администраторов информационной безопасности), осуществляющих администрирование и обслуживание вычислительных мощностей ИС ИОГВ Типов 1 и 2 в качестве АРМ пользователей не рассматриваются.

[7] При разработке настоящей Модели угроз, учитывается, что в составе ЛВС ИС ИОГВ Краснодарского края типов 3 и 4 могут находится устройства беспроводного доступа (Wi-Fi роутеры)

[8] Под средствами обеспечения гарантированного электропитания понимаются: источники бесперебойного питания (далее – ИБП), бензиновые/дизельные генераторные установки (далее – ДГУ), резервные линии электропитания

Использование в качестве каналов связи для передачи информации технологии VPN MPLS, предоставляемой оператором связи (в том числе с применением сертифицированных ФСБ России средств криптографической защиты информации, передаваемой по каналам связи), считается подключением к ССОП.

Исходя из вышеописанного, необходимо считать, что ИС ИОГВ Краснодарского края имеют многоточечный доступ к ССОП.

2.5 Меры защиты информации

2.5.1 Характеристики обеспечения физической безопасности

Меры (методы и средства) обеспечения физической безопасности, характерные для различных типов ИС ИОГВ Краснодарского края, представлены в таблице 3.

Таблица 3 – Меры обеспечения физической безопасности

№ п/п	Меры обеспечения физической безопасности	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
Доступ в помещения и (или) на территорию					
1	Наличие постов охраны и контрольно-пропускного режима, исключающих неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа	+	+/-[9]	+/-	+/-
2	Наличие системы видеонаблюдения при входе на территорию	+	+/-	+	+
3	Наличие системы контроля и управления доступом (далее - СКУД)	+	+/-	+/-	+/-
4	Пропуск на объекты представителей сторонних организаций осуществляется в сопровождении должностного лица заинтересованного структурного подразделения	+	+/-	+	+
5	Внос (вынос) материальных ценностей осуществляется на основании материальных пропусков и в присутствии должностного лица заинтересованного структурного подразделения	+	+/-	+/-	+/-
6	Запись в Журнале учёта посетителей при их посещении	+	+/-	+/-	+/-
7	Регламентация контрольно-пропускного режима организационно-распорядительными документами	+	+/-	+	+
Оборудование помещений					
8	Наличие надёжных дверей в помещения	+	+/-	+/-	+/-
9	Наличие охранной сигнализации в помещениях	+	+/-	+/-	+/-
10	Наличие пожарной сигнализации в помещениях	+	+/-	+/-	+/-
11	Опечатывание и (или) установка на охрану служебных помещений по окончанию рабочего дня	+	+/-	+/-	+/-
12	Размещение устройств вывода (отображения) информации АРМ пользователей, исключающее ее несанкционированный	![10]	!	+/-	+/-

[9] Данная мера может быть реализована не во всех ИС ИОГВ Краснодарского края

[10] Данная мера не применима в связи с отсутствием АРМ пользователей в данном Типе ИС

№ п/п	Меры обеспечения физической безопасности	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
	просмотр посторонними лицами				
13	Наличие источников бесперебойного питания для АРМ пользователей	!	!	+/-	+/-
14	Наличие серверных помещений для размещения серверного и телекоммуникационного оборудования	+	+/-	+/-	+/-[11]
Оборудование серверных помещений					
15	Наличие надёжных дверей в помещения	+	+/-	+	+/-
16	Наличие охранной сигнализации в помещениях	+	+/-	+	+/-
17	Наличие пожарной сигнализации в помещениях	+	+/-	+	+/-
18	Наличие систем кондиционирования	+	+/-	+	+/-
19	Наличие источников бесперебойного питания для серверного и телекоммуникационного оборудования	+	+/-	+	+/-
20	Наличие систем гарантированного электропитания (резервные линии электропитания и (или) дизельные/бензиновые генераторные установки)	+	+/-	+/-	+/-

Границы контролируемых зон (далее – КЗ) ИС ИОГВ Краснодарского края устанавливаются по ограждающим конструкциям помещений размещения защищаемых компонентов ИС ИОГВ Краснодарского края или по внешнему периметру охраняемого здания.

2.5.2 Характеристики, связанные с организацией обеспечения информационной безопасности

Несмотря на наличие в отдельных ИОГВ Краснодарского края необходимых и достаточных (для обеспечения функционирования СОИБ) организационно-распорядительных документов, регламентирующих процедуры обработки и защиты информации (далее – ОРД), при разработке настоящей Модели угроз и определения актуальности УБИ считается, что такие ОРД отсутствуют[12].

2.5.3 Сведения о реализованных средствами ППО, СПО мерах по обеспечению информационной безопасности

Для ИС ИОГВ Краснодарского края характерно использование следующих механизмов обеспечения безопасности информации:

— идентификация и аутентификация пользователей при доступе в операционную систему (далее – ОС) и ППО по идентификатору (учётному имени пользователя) и паролю;

[11] Наличие серверных помещений для данного типа ИС ИОГВ Краснодарского края рассматривается только с точки зрения безопасности телекоммуникационного оборудования, располагающегося в них

[12] Исключением является прямое указание на наличие тех или иных ОРД

- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (управление идентификаторами пользователей в ОС и прикладном программном обеспечении);
- ограничение доступа к защищаемой информации до идентификации и аутентификации пользователя;
- защита обратной связи при вводе парольной информации (обеспечивается заменой вводимых знаков символами «*»);
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (реализуется посредством регистрации входа пользователей в систему средствами СПО и ППО);
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (реализуется средствами СПО и ППО путём назначения на учётные записи пользователей административных прав доступа (присвоение соответствующих ролей);
- управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей.

2.5.4 Сведения о применяемых средствах защиты информации

Сведения о применяемых средствах защиты информации и местах их размещения в ИС ИОГВ Краснодарского края представлены в таблице 4.

Таблица 4 – Средства защиты информации

№ п/п	Типы средств защиты информации	Тип ИС ИОГВ Краснодарского края			
		Тип 1	**Тип 2**	**Тип 3**	**Тип 4**
1	Сертифицированное ФСТЭК России средство защиты сред виртуализации от несанкционированного доступа	Сервера виртуализации	-	-	-
2	Сертифицированное ФСТЭК России средство антивирусной защиты сред виртуализации	Сервера виртуализации	-	-	-
3	Сертифицированное ФСТЭК России средство антивирусной защиты почтовых серверов	Почтовый сервер	-	-	-
4	Сертифицированное ФСТЭК России средство антивирусной защиты файловых серверов	Сервера ИС	-	+/-	+/-
5	Сертифицированное ФСТЭК России средство антивирусной защиты АРМ пользователей	*[13]	*	+/-	+/-
6	Сертифицированное ФСТЭК России средство межсетевого экранирования	На границе ЛВС	+/-	+/-	+/-
7	Сертифицированное ФСТЭК России средство обнаружения вторжений	На границе ЛВС	-	-	-
8	Сертифицированное ФСТЭК России средство анализа защищенности	АРМ Администратора ИБ	-	+/-	-
9	Сертифицированное ФСБ России средство криптографической защиты информации, передаваемой по каналам связи	На границе ЛВС	+/-	+/-	+/-

[13] Данная мера не применима в связи с отсутствием АРМ пользователей в данном Типе ИС

2.6 Категории лиц, имеющих доступ к ресурсам информационным системам

Сведения о категориях лиц, имеющих санкционированный доступ к ресурсам информационных систем ИОГВ Краснодарского края, представлены в таблице 5.

Таблица 5 – Категории лиц, являющихся зарегистрированными пользователями

№ п/п	Наименование	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
1	Пользователи – сотрудники ИОГВ Краснодарского края, участвующие в информационном взаимодействии, занимающиеся обработкой защищаемой информации и имеющие доступ к сервисам ИС ИОГВ Краснодарского края, в соответствии с наделёнными им правами			+	+
2	Пользователи – сотрудники ИОГВ Краснодарского края, занимающиеся обработкой защищаемой информации и осуществляющие доступ к сервисам ИС ИОГВ Краснодарского края по имеющимся каналам связи			+	+
3	Пользователи – граждане, осуществляющие доступ к сервисам ИС ИОГВ Краснодарского края посредством сети Интернет	+	+	+	
4	Системные администраторы и администраторы баз данных - сотрудники ИОГВ Краснодарского края по Краснодарскому краю, участвующие в информационном взаимодействии, не занимающиеся обработкой защищаемой информации	+	+	+	
5	Системные администраторы и администраторы баз данных - Исполнители (сторонние организации), действующие на основании заключённых государственных контрактов и осуществляющие конфигурирование и настройку программных и программно-технических средств, в том числе СЗИ, используемых в ИС ИОГВ Краснодарского края при информационном взаимодействии	+	+		
6	Администраторы безопасности – назначаются из состава сотрудников ИОГВ Краснодарского края, осуществляют мониторинг и аудит СЗИ, используемых в ИС ИОГВ Краснодарского края при информационном взаимодействии	+	+	+	+

Сведения о физических лицах, имеющих санкционированный (в т.ч. разовый) доступ к ресурсам ИС ИОГВ Краснодарского края, но не занимающихся обработкой защищаемой информации и не являющихся зарегистрированными пользователями ИС ИОГВ Краснодарского края, представлены в таблице 6.

Таблица 6 – Категории лиц, не являющихся зарегистрированными пользователями

№ п/п	Наименование	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
1	Технический и обслуживающий персонал (уборщики, электрики, сантехники, пожарная команда и т.д.)	+	+	+	+
2	Технические специалисты по обслуживанию технических средств ИС ИОГВ Краснодарского края и сопровождению используемого на них общесистемного и ППО, используемого при информационном взаимодействии	+	+	+	+
3	Работники, осуществляющие функции физической (в т.ч. периметровой) охраны и обеспечивающие поддержание установленных режимов безопасности и т.д.	+	+	+	+

2.7 Технология обработки информации и информационные потоки

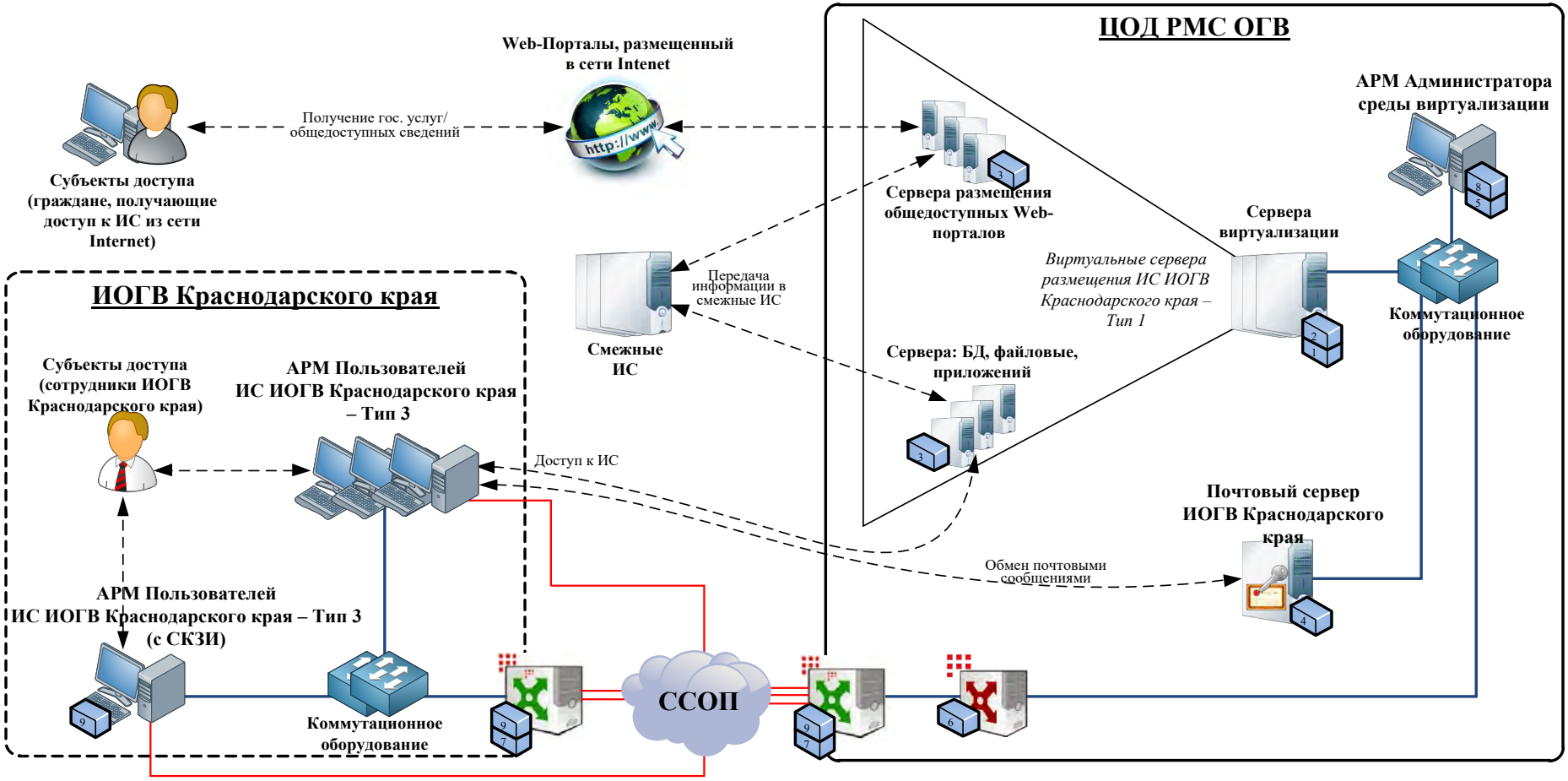
Для ИС ИОГВ Краснодарского края характерны следующие характеристики доступа к защищаемой информации:

- многопользовательский доступ к защищаемой информации;
- наличие разграничения прав доступа к защищаемой информации;
- способ доступа субъектов доступа (граждан, осуществляющих доступ к ИС из сети Интернет) к субъектам доступа (общедоступным ресурсам, размещённым в сети Интернет):
  - посредством Интернет-браузера;
- способ доступа субъектов доступа (сотрудников ИОГВ[14]) к субъектам доступа:
  - посредством Интернет-браузера;
  - посредством тонкого клиента;
  - посредством толстого клиента;
  - посредством терминального доступа;
- допустимые операции с записями БД в ИС для субъектов доступа (граждан, осуществляющих доступ к ИС из сети Интернет):
  - модификация и передача;
  - чтение и поиск;
  - запись и удаление;
- допустимые операции с записями БД в ИС для субъектов доступа (сотрудников ИОГВ):
  - модификация и передача;
  - чтение и поиск;
  - запись, удаление и сортировка;

[14] Доступ к ИС ИОГВ типа 1 и 2 может осуществляться по каналу связи, защищённому посредством средства криптографической защиты информации (далее – СКЗИ), передаваемой по каналам связи. В качестве такого средства может выступать как программно-аппаратный комплекс (далее –ПАК), устанавливаемый на границе ЛВС ИС ИОГВ Краснодарского края, так и программное СКЗИ, устанавливаемое на АРМ пользователя

Схемы информационного взаимодействия, характерные при взаимодействии ИС ИОГВ Краснодарского края представлены на рисунках 2-4.

Под смежными ИС понимаются любые ИС, взаимодействующие с конкретной рассматриваемой ИС ИОГВ Краснодарского края, при этом смежными ИС могут быть как ИС ИОГВ Краснодарского края типа 1, 2, 3, так и ИС сторонних организаций.



Условные обозначения:

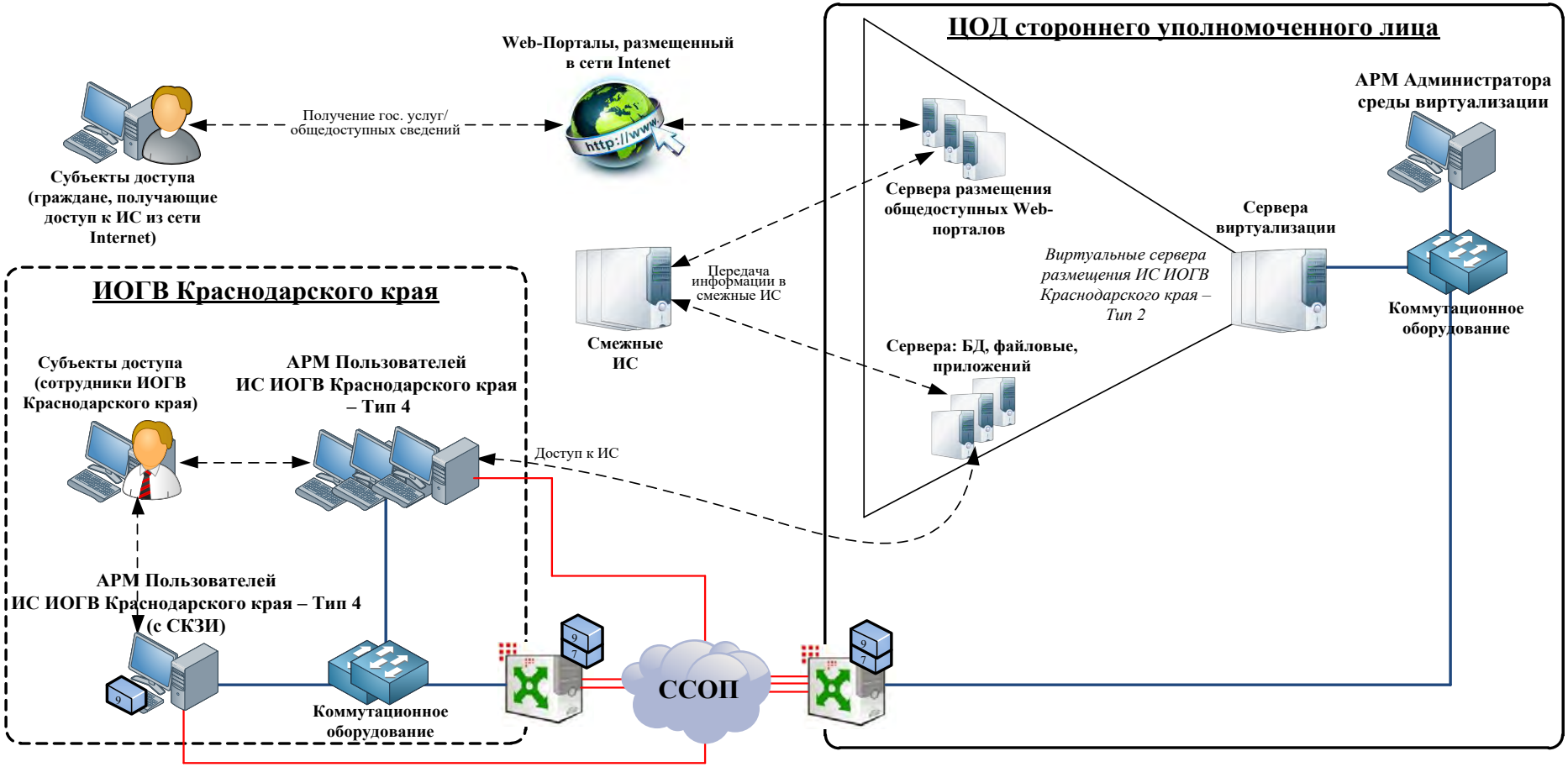
1	Сертифицированное ФСТЭК России средство защиты сред виртуализации
2	Сертифицированное ФСТЭК России средство антивирусной защиты сред виртуализации
3	Сертифицированное ФСТЭК России средство антивирусной защиты файловых серверов
4	Сертифицированное ФСТЭК России средство антивирусной защиты почтовых серверов
5	Сертифицированное ФСТЭК России средство антивирусной защиты АРМ пользователей
6	Сертифицированное ФСТЭК России средство обнаружения вторжений
7	Сертифицированное ФСТЭК России средство межсетевого экранирования
8	Сертифицированное ФСТЭК России средство анализа защищенности
9	Сертифицированное ФСБ России средство криптографической защиты информации, передаваемой по каналам связи

Информационные потоки

Передача информации в ЛВС

Незащищенные каналы передачи информации

Рисунок 2 – Схема информационного взаимодействия ИС ИОГВ Краснодарского края типов 1 и 4

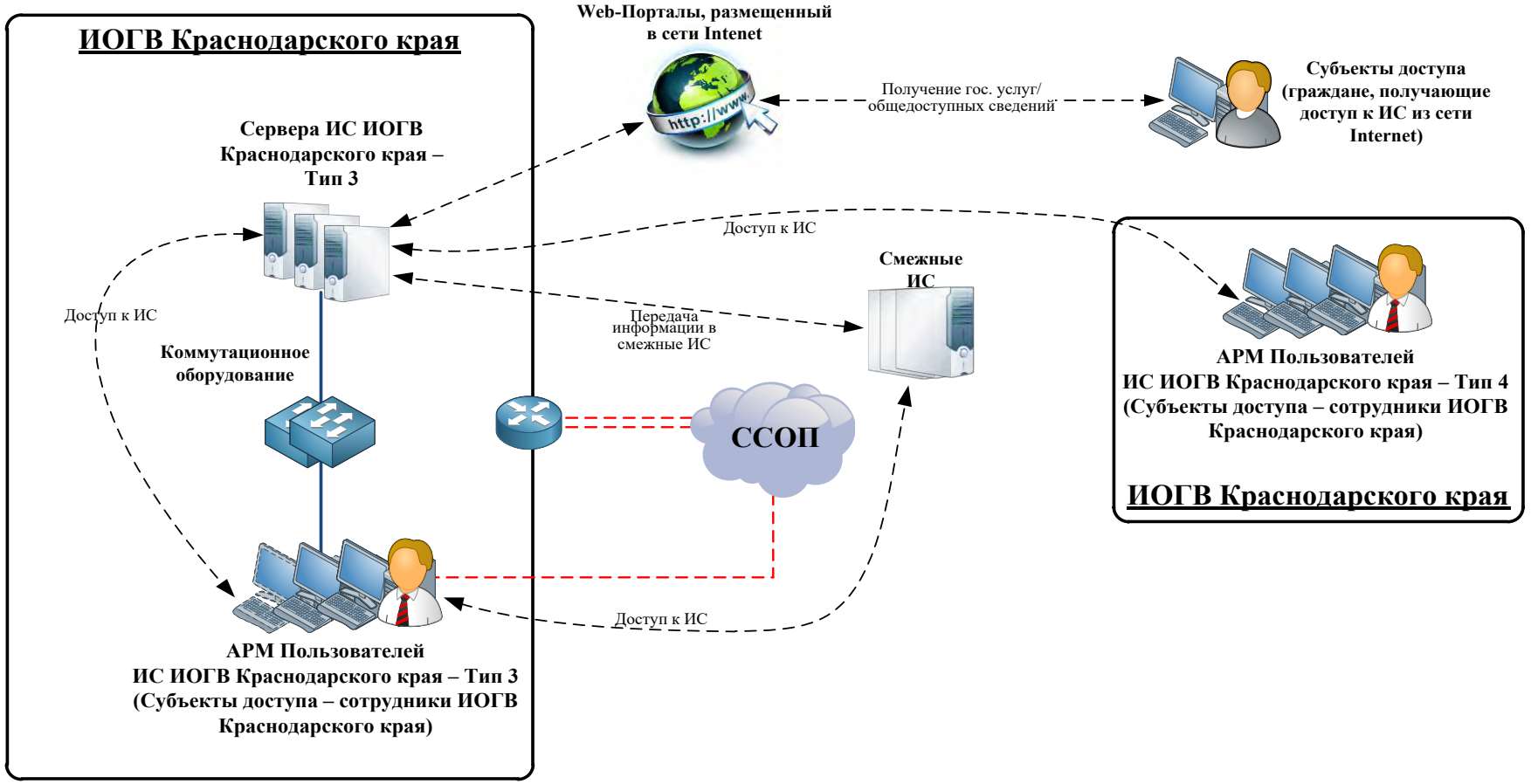


Условные обозначения:

1	Сертифицированное ФСТЭК России средство защиты сред виртуализации
2	Сертифицированное ФСТЭК России средство антивирусной защиты сред виртуализации
3	Сертифицированное ФСТЭК России средство антивирусной защиты файловых серверов
4	Сертифицированное ФСТЭК России средство антивирусной защиты почтовых серверов
5	Сертифицированное ФСТЭК России средство антивирусной защиты АРМ пользователей
6	Сертифицированное ФСТЭК России средство обнаружения вторжений
7	Сертифицированное ФСТЭК России средство межсетевого экранирования
8	Сертифицированное ФСТЭК России средство анализа защищенности
9	Сертифицированное ФСБ России средство криптографической защиты информации, передаваемой по каналам связи

- Информационные потоки
- Передача информации в ЛВС
- Незащищенные каналы передачи информации

Рисунок 3 – Схема информационного взаимодействия ИС ИОГВ Краснодарского края типов 2 и 4



Условные обозначения:

1	Сертифицированное ФСТЭК России средство защиты сред виртуализации
2	Сертифицированное ФСТЭК России средство антивирусной защиты сред виртуализации
3	Сертифицированное ФСТЭК России средство антивирусной защиты файловых серверов
4	Сертифицированное ФСТЭК России средство антивирусной защиты почтовых серверов
5	Сертифицированное ФСТЭК России средство антивирусной защиты АРМ пользователей
6	Сертифицированное ФСТЭК России средство обнаружения вторжений
7	Сертифицированное ФСТЭК России средство межсетевого экранирования
8	Сертифицированное ФСТЭК России средство анализа защищенности
9	Сертифицированное ФСБ России средство криптографической защиты информации, передаваемой по каналам связи

- Информационные потоки
- Передача информации в ЛВС
- Незащищенные каналы передачи информации

Рисунок 4 – Схема информационного взаимодействия ИС ИОГВ Краснодарского края типов 3 и 4

3 Потенциальные нарушители безопасности конфиденциальной информации

Модель нарушителя разрабатывается на основе классификации, приведённой в Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой Приказом ФСТЭК России от 15.02.2008 г.

По наличию права постоянного или разового доступа в контролируемую зону ИС ИОГВ Краснодарского края нарушители подразделяются на два типа:

— внешние нарушители – нарушители, не имеющие доступа к ИС, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
— внутренние нарушители – нарушители, имеющие доступ к ИС, включая пользователей ИС, реализующие угрозы непосредственно в ИС.

Предполагается, что существующая в ИОГВ система подбора кадров, действующие организационно-технические мероприятия исключают возможность сговора между нарушителями любых типов.

3.1 Оценка возможностей потенциальных внешних нарушителей

В общем случае, внешними нарушителями могут быть:

— разведывательные службы государств;
— криминальные структуры;
— конкурирующие организации;
— недобросовестные партнёры;
— внешние субъекты (физические лица).

Перечень потенциальных внешних нарушителей для ИС ИОГВ Краснодарского края приведён в таблице 7.

Таблица 7 – Перечень потенциальных внешних нарушителей

№ п/п	Внешние нарушители	Мотивация нарушителей	Тип ИС ИОГВ Краснодарского края			
			Тип 1	Тип 2	Тип 3	Тип 4
1	Разведывательные службы государств	Нарушение штатного режима функционирования и дестабилизация деятельности ИОГВ Краснодарского края	+	+		
2	Криминальные структуры	Мошенничество в сфере предоставления государственных услуг	+	+	+	+
3	Конкурирующие организации	-				
4	Недобросовестные партнёры	Ненадлежащее качество оказания услуг				
5	Внешние субъекты	Мошенничество в сфере предоставления	+	+	+	+

№ п/п	Внешние нарушители	Мотивация нарушителей	Тип ИС ИОГВ Краснодарского края			
			Тип 1	Тип 2	Тип 3	Тип 4
		государственных услуг; любопытство и (или) самореализация потенциальных нарушителей; использование вычислительных мощностей для проведения атак типа «отказ в обслуживание» сторонних организаций				

Информация, обрабатываемая в ИС ИОГВ Краснодарского края типов 1 и 2 (центры обработки данных) может представлять интерес для разведывательных служб государств, так как возможно получение доступа не к одной, а к ряду информационных систем.

Актуальность в качестве потенциальных нарушителей разведывательных служб государств для ИС ИОГВ Краснодарского края типа 3 должна определяться исходя из назначения конкретной рассматриваемой ИС ИОГВ Краснодарского края и характера обрабатываемой в ней информации. В общем случае, ИС ИОГВ Краснодарского края 3 типа не представляют интереса для разведывательных служб государств в связи с незначительным объёмом сведений, доступ к которым потенциальный нарушитель может получить – доступ возможен только к ИС отдельных ИОГВ Краснодарского края (несоизмерима стоимость и значимость информации с затратами на реализацию угроз).

Информация, обрабатываемая в ИС ИОГВ Краснодарского края типа 4 не представляет интереса для разведывательных служб государств в связи с:

— наличием разграничения прав доступа к ИС, доступ к которым осуществляется;
— малым объёмом сведений, доступ к которым потенциальный нарушитель может получить;
— несоизмеримой стоимостью и значимостью информации с затратами на реализацию угроз.

Конкурирующие организации у ИОГВ Краснодарского края отсутствуют.

Партнёры у ИОГВ Краснодарского края отсутствуют (единичные сотрудники органов государственной власти и прочих учреждений и организаций, взаимодействующих с ИОГВ Краснодарского края, рассматриваются как «Внешние субъекты»). Подведомственные ИОГВ Краснодарского края организации, осуществляющие функции по поддержке функционирования ИС ИОГВ Краснодарского края относятся к категории внутренних нарушителей.

Оценка возможностей внешнего нарушителя для ИС ИОГВ Краснодарского края представлена в таблице 8.

Таблица 8 – Возможности внешних нарушителей

№ п/п	Возможности внешнего нарушителя	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
1	Осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений	-	-	+	+
2	Осуществлять несанкционированный доступ через автоматизированные рабочие места, подключённые к сетям связи общего пользования и (или) сетям международного информационного обмена	-	-	+	+
3	Осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок	-	-	+	+
4	Осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИС, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны	+	+	+	+
5	Осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИС	+	+	+	+

Для обеспечения информационного взаимодействия между некоторыми ИОГВ Краснодарского края применяются сертифицированные ФСТЭК России средства межсетевого экранирования, а при передаче информации по каналам связи применяются сертифицированные ФСБ России СКЗИ (защита информации обеспечивается фрагментарно).

Осуществление НСД к каналам связи, выходящим за пределы служебных помещений ИС ИОГВ Краснодарского края типов 3 и 4, возможно в случае отсутствия необходимых мер, исключающих неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа на территорию ИОГВ.

Осуществление НСД через АРМ, подключённые к ССОП и (или) СМИО) для ИС ИОГВ Краснодарского края типов 3 и 4 возможно в следующих случаях:

— в составе ЛВС используются мобильные средства подключения к СМИО на АРМ пользователей, не оснащённых сертифицированными ФСТЭК России средствами межсетевого экранирования;
— отсутствует на границе ЛВС ИС сертифицированных ФСТЭК России средствами межсетевого экранирования при условии отсутствия на АРМ пользователей таких средств;
— имеется возможность несанкционированного доступа к АРМ пользователей посторонних лиц (на АРМ пользователей отсутствуют сертифицированные ФСТЭК России средства защиты информации от НСД);
— в составе ЛВС ИС наряду с защищёнными АРМ имеются АРМ, неоснащённые сертифицированными ФСТЭК России средствами защиты информации при условии отсутствия в составе ЛВС сертифицированных ФСТЭК России средств защиты информации, обеспечивающих сегментирование ЛВС.

Осуществление НСД к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок возможно для ИС ИОГВ Краснодарского края типов 3 и 4 для обеспечения информационной безопасности которых не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации на АРМ пользователей и серверах ИС.

Осуществление НСД через элементы информационной инфраструктуры ИС, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами КЗ возможно в следующих случаях:

— не регламентированы в ОРД процедуры модернизации/сопровождения/ремонта /утилизации элементов информационной инфраструктуры ИС;

— не осуществляется гарантированное уничтожение информации с носителей информации при их утилизации или передачи в ремонт посредством сертифицированных ФСТЭК России средств.

Осуществление НСД через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИС возможно в случае, если осуществляется подключение ИС, не оснащённых необходимыми сертифицированными ФСТЭК России средствами защиты информации и не аттестованными по требованиям безопасности информации (требования по подключению ИС также должны быть отражены в соответствующих технических условиях).

3.2 Оценка возможностей потенциальных внутренних нарушителей

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к защищаемой информации.

К первой категории относятся лица, имеющие санкционированный доступ к ИС, но не имеющие доступа к защищаемой информации.

Ко второй категории относятся зарегистрированные пользователи ИС ИОГВ Краснодарского края, осуществляющие ограниченный доступ к ресурсам ИС с автоматизированного рабочего места.

К третьей категории относятся зарегистрированные пользователи ИС ИОГВ Краснодарского края, осуществляющие удалённый доступ к защищаемой информации по локальным и (или) распределённым ИС.

К четвертой категории относятся зарегистрированные пользователи ИС ИОГВ Краснодарского края с полномочиями администратора безопасности сегмента ИС.

К пятой категории относятся зарегистрированные пользователи ИС ИОГВ Краснодарского края с полномочиями системного администратора ИС.

К шестой категории относятся зарегистрированные пользователи ИС ИОГВ Краснодарского края с полномочиями администратора безопасности ИС.

К седьмой категории относятся программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИС.

Перечень потенциальных внутренних нарушителей для ИС ИОГВ Краснодарского края представлен в таблице 9.

Таблица 9 – Перечень потенциальных внутренних нарушителей

№ п/п	Внутренние нарушители	Мотивация нарушителей	Тип ИС ИОГВ Краснодарского края			
			Тип 1	Тип 2	Тип 3	Тип 4
1	1 категория – Сотрудники, не являющиеся пользователями ИС	Несанкционированные изменения в БД с целью получения финансовой выгоды путём: продажи сведений, содержащихся в БД; внесение ложных сведений в БД, а также: любопытство или желание самореализации (подтверждение статуса), месть за ранее совершенные действия, непреднамеренные, неосторожные или неквалифицированные действия	+	+	+	+
2	2 категория – Пользователи ИС		-	-	+	+
3	3 категория – Удалённые пользователи ИС		+	+	+	-
4	4 категория – Администратор безопасности сегмента ИС		-	+	-	-
5	5 категория – Системный администратор ИС		-	+	-	-
6	6 категория – Администратор безопасности ИС		-	-	-	-
7	7 категория – Разработчики ИС	Внедрение дополнительных функциональных возможностей в программное обеспечение, причинение имущественного (и др. видов) ущерба путём обмана или злоупотребления доверием, непреднамеренные, неосторожные или неквалифицированные действия	-	-	-	-
8	8 категория – Подрядные организации, осуществляющие поставку, сопровождение и ремонт компонентов ИС		-	-	-	-

Категория 1 внутренних нарушителей (сотрудники, не являющиеся пользователями ИС) является актуальной для всех типов ИС ИОГВ Краснодарского края.

Категория 2 внутренних нарушителей (пользователи ИС) для ИС ИОГВ Краснодарского края типов 1 и 2 не рассматриваются в связи с их отсутствием.

Категория 2 внутренних нарушителей (пользователи ИС) для ИС ИОГВ Краснодарского края типов 3 и 4 является актуальной.

Категория 3 внутренних нарушителей (удалённые пользователи ИС[15]) неактуальна для ИС, в которых отсутствуют удалённые пользователи (ИС ИОГВ Краснодарского края типа 4).

[15] Под удалёнными пользователями для ИС ИОГВ Краснодарского края типов 1,2,3 понимаются пользователи общедоступных информационных ресурсов, получающих доступ из сети Интернет (граждане).

Категории 4, 5, 6 внутренних нарушителей (администраторы безопасности сегмента ИС, системные администраторы ИС, администраторы безопасности ИС) для ИС ИОГВ Краснодарского края типа 1[16] являются доверенными лицами и не относятся к категории нарушителей. Их доверенность и ответственность закрепляется положениями заключаемых на обслуживание информационных систем государственных контактов.

Категории 4, 5 внутренних нарушителей (администраторы безопасности сегмента ИС, системные администраторы ИС) для ИС ИОГВ Краснодарского края типа 2[17] не являются доверенными лицами и относятся к категории нарушителей. Категория 6 внутренних нарушителей (администраторы безопасности ИС) для ИС ИОГВ Краснодарского края типа 2 являются доверенными лицами и не относятся к категории нарушителей. Их доверенность должна обеспечиваться комплексом организационных мер по подбору персонала, закреплению ответственности и контролю лояльности.

Категории 4, 5, 6 внутренних нарушителей (администраторы безопасности сегмента ИС, системные администраторы ИС, администраторы безопасности ИС) для ИС ИОГВ Краснодарского края типа 3 являются доверенными лицами и не относятся к категории нарушителей. Их доверенность должна обеспечиваться комплексом организационных мер по подбору персонала, закреплению ответственности и контролю лояльности.

Категории 4,5 внутренних нарушителей (администраторы безопасности сегмента ИС, системные администраторы ИС) для ИС ИОГВ Краснодарского края типа 3 являются доверенными лицами и не относятся к категории нарушителей. Их доверенность должна обеспечиваться комплексом организационных мер по подбору персонала, закреплению ответственности и контролю лояльности. Категория 6 внутренних нарушителей (администраторы безопасности ИС) для ИС ИОГВ Краснодарского края типа 4 не рассматриваются в связи с их отсутствием в данном типе ИС ИОГВ Краснодарского края (данный тип является пользовательском сегментом ИС).

Категории 7, 8 внутренних нарушителей (разработчики ИС и подрядные организации, осуществляющие поставку, сопровождение и ремонт компонентов ИС) для ИС ИОГВ Краснодарского края типов 1,3,4 не относятся к категории нарушителей в случае закрепления их ответственности в государственных контрактах на развитие, обеспечение функционирования и техническое сопровождение ИС. Категории 7, 8 внутренних нарушителей для ИС ИОГВ Краснодарского края типа 2 не относятся к категории нарушителей в случае закрепления их ответственности в заключаемых (между поставщиком вычислительных мощностей (уполномоченным лицом) и его контрагентами) договорах.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах КЗ режимных и организационно-технических мер защиты. Оценка возможностей внутреннего нарушителя с учётом актуальных категорий внутренних нарушителей для ИС ИОГВ Краснодарского края приведена в таблице 10.

Удалённые пользователи АРМ (сотрудники ИОГВ), имеющие доступ к ИС ИОГВ Краснодарского края типов 1,2,3, относятся к ИС ИОГВ Краснодарского края типа 4

[16] Для данного типа ИС, указанные категории потенциальных нарушителей – сотрудники организации, осуществляющей администрирование и сопровождение ЦОД РМС ОГВ

[17] Для данного типа ИС, указанные категории потенциальных нарушителей – сотрудники организации, осуществляющей администрирование и сопровождение стороннего ЦОД, в котором осуществляется размещение ИС ИОГВ Краснодарского края

Таблица 10 – Возможности внутренних нарушителей

№ п/п	Возможности внутреннего нарушителя	Тип ИС ИОГВ Краснодарского края				Примечание
		Тип 1	Тип 2	Тип 3	Тип 4	
1	Имеет доступ к фрагментам информации, содержащей и распространяющейся по внутренним каналам связи ИС	+	+	+	+	Данной возможность обладают потенциальные нарушителя 1 категории, являющейся актуальными для всех типов ИС ИОГВ Краснодарского края
2	Располагает фрагментами информации о топологии ИС (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах	+	+	+	+	Данной возможность обладают потенциальные нарушителя 1 категории, являющейся актуальными для всех типов ИС ИОГВ Краснодарского края
3	Располагает именами и ведёт выявление паролей зарегистрированных пользователей	+	+	+	+	Данной возможность обладают потенциальные нарушителя 1 категории, являющейся актуальными для всех типов ИС ИОГВ Краснодарского края
4	Изменяет конфигурацию технических средств ИС, вносит в неё программно-аппаратные закладки и обеспечивает съем информации, используя непосредственное подключение к техническим средствам ИС	+	+	+	+	Данной возможность обладают потенциальные нарушителя 1 категории, являющейся актуальными для всех типов ИС ИОГВ Краснодарского края
5	Знает, по меньшей мере, одно легальное имя доступа	-	-	+	+	Данной возможность обладают потенциальные нарушителя 2 категории, являющейся актуальными для типов 3,4 ИС ИОГВ Краснодарского края
6	Обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации	-	-	+	+	Данной возможность обладают потенциальные нарушителя 2 категории, являющейся актуальными для типов 3,4 ИС ИОГВ Краснодарского края
7	Располагает конфиденциальными данными, к которым имеет доступ	-	-	+	+	Данной возможность обладают потенциальные нарушителя 2 категории, являющейся актуальными для типов 3,4 ИС ИОГВ Краснодарского края

№ п/п	Возможности внутреннего нарушителя	Тип ИС ИОГВ Краснодарского края				Примечание
		Тип 1	Тип 2	Тип 3	Тип 4	
8	Располагает информацией о топологии ИС на базе локальной и (или) распределённой ИС, через которую осуществляется доступ, и о составе технических средств ИС	-	-	-	-	Несмотря на то, что данной возможностью обладают нарушители 3 категории, являющейся актуальной для ИС ИОГВ Краснодарского края типов 1,2,3 – удалённые пользователи (граждане, осуществляющие доступ к общедоступным ресурсам посредством сети Интернет) сведениями о топологии ИС и о составе технических средств ИС (за исключением сведений, находящихся в свободном доступе в сети Интернет) не располагают.
9	Имеет возможность прямого (физического) доступа к фрагментам технических средств ИС	-	-	-	-	Несмотря на то, что данной возможностью обладают нарушители 3 категории, являющейся актуальной для ИС ИОГВ Краснодарского края типов 1,2,3 – удалённые пользователи (граждане, осуществляющие доступ к общедоступным ресурсам посредством сети Интернет) прямого доступа к фрагментам технических средств ИС не имеют.
10	Обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИС	-	+	-	-	Данной возможность обладают потенциальные нарушителя 4 категории, не являющейся актуальными для ИС ИОГВ Краснодарского края типов 1,3,4
11	Обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИС	-	+	-	-	Данной возможность обладают потенциальные нарушителя 4 категории, не являющиеся актуальными для ИС ИОГВ Краснодарского края типов 1,3,4
12	Имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИС	-	+	+	+	Несмотря на то, что данной возможностью обладают нарушители 4 категории, не являющейся актуальной для ИС ИОГВ Краснодарского края типов 3 и 4 - пользователи ИС могут обладать рядом административных прав на АРМ
13	Имеет доступ ко всем техническим средствам сегмента (фрагмента) ИС	-	+	-	-	Данной возможность обладают потенциальные нарушителя 4 категории, не являющейся актуальной для ИС ИОГВ Краснодарского края типов 1,3,4

№ п/п	Возможности внутреннего нарушителя	Тип ИС ИОГВ Краснодарского края				Примечание
		Тип 1	Тип 2	Тип 3	Тип 4	
14	Обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИС	+	+	+	+	Данной возможность обладают потенциальные нарушителя 4 категории, не являющейся актуальной для ИС ИОГВ Краснодарского края типов 1,3,4
15	Обладает полной информацией о системном и прикладном программном обеспечении ИС	-	+	-	-	Данной возможность обладают потенциальные нарушителя 5 категории, не являющейся актуальной для ИС ИОГВ Краснодарского края типов 1,3,4
16	Обладает полной информацией о технических средствах и конфигурации ИС	-	+	-	-	Данной возможность обладают потенциальные нарушителя 5 категории, являющейся актуальной для ИС ИОГВ Краснодарского края типов 1,3,4
17	Имеет доступ ко всем техническим средствам обработки информации и данным ИС	-	+	-	-	Данной возможность обладают потенциальные нарушителя 5 категории, являющейся актуальной для ИС ИОГВ Краснодарского края типов 1,3,4
18	Обладает правами конфигурирования и административной настройки технических средств ИС	-	+	+	+	Несмотря на то, что данной возможностью обладают нарушители 5 категории, являющейся актуальной для ИС ИОГВ Краснодарского края типов 3 и 4 - пользователи ИС могут обладать рядом административных прав на АРМ
19	Обладает полной информацией об ИС	-	+	-	-	Данной возможность обладают потенциальные нарушителя 6 категории, являющейся актуальной для ИС ИОГВ Краснодарского края типов 1,3,4
20	Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИС	-	+	+	+	Несмотря на то, что данной возможностью обладают нарушители 6 категории, являющейся актуальной для ИС ИОГВ Краснодарского края типов 3 и 4 - пользователи ИС могут иметь доступ к средствам защиты информации, установленным на АРМ
21	Обладает информацией об алгоритмах и программах обработки информации на ИС	-	-	-	-	Потенциальный нарушитель будет обладать данной возможностью в случае актуальности внутреннего нарушителя 7 категории
22	Обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное	-	-	-	-	Потенциальный нарушитель будет обладать данной возможностью в случае актуальности внутреннего нарушителя 7 категории

№ п/п	Возможности внутреннего нарушителя	Тип ИС ИОГВ Краснодарского края				Примечание
		Тип 1	Тип 2	Тип 3	Тип 4	
	обеспечение ИС на стадии ее разработки, внедрения и сопровождения					
23	Может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и защиты информации, обрабатываемой в ИС	-	-	-	-	Потенциальный нарушитель будет обладать данной возможностью в случае актуальности внутреннего нарушителя 7 категории
24	Обладает возможностями внесения закладок в технические средства ИС на стадии их разработки, внедрения и сопровождения	-	-	-	-	Потенциальный нарушитель будет обладать данной возможностью в случае актуальности внутреннего нарушителя 8 категории
25	Может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и защиты информации в ИС	-	-	-	-	Потенциальный нарушитель будет обладать данной возможностью в случае актуальности внутреннего нарушителя 8 категории

3.3 Потенциал возможных нарушителей

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом.

Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

— нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;
— нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;
— нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

При этом:

— низкий потенциал подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей;
— средний потенциал подразумевает наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей;
— высокий потенциал подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей.

Потенциал возможных нарушителей представлен в таблице 11.

Таблица 11 – Потенциал возможных нарушителей

№	Вид нарушителя	Потенциал нарушителя	Тип ИС ИОГВ Краснодарского края			
			Тип 1	Тип 2	Тип 3	Тип 4
Внешние нарушители						
1	Разведывательные службы государств	Высокий потенциал	+	+	-	-
2	Криминальные структуры	Средний потенциал	+	+	+	+
3	Конкурирующие организации	Средний потенциал	-	-	-	-
4	Недобросовестные партнёры	Низкий потенциал	-	-	-	-
5	Внешние субъекты	Низкий потенциал	+	+	+	+
Внутренние нарушители						
1	Сотрудники, не являющиеся пользователями ИС	Низкий потенциал	+	+	+	+
2	Пользователи ИС	Низкий потенциал	-	-	+	+

№	Вид нарушителя	Потенциал нарушителя	Тип ИС ИОГВ Краснодарского края			
			Тип 1	Тип 2	Тип 3	Тип 4
3	Удалённые пользователи ИС	Низкий потенциал	+	+	+	-
4	Администратор безопасности сегмента ИС	Средний потенциал	-	+	-	-
5	Системный администратор ИС	Средний потенциал	-	+	-	-
6	Администратор безопасности ИС	Средний потенциал	-	+	-	-
7	Разработчики ИС	Средний потенциал	-	-	-	-
8	Подрядные организации, осуществляющие поставку, сопровождение и ремонт компонентов ИС	Средний потенциал	-	-	-	-

4 Методологическая основа Модели угроз

В настоящем разделе приведено:
— методика определения актуальности УБИ;
— общая классификация УБИ;
— перечень УБИ, рассматриваемых для ИС ИОГВ Краснодарского края.

4.1 Методика определения актуальности угроз

Для построения модели угроз в соответствии с Федеральный закон Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных» должны необходимо руководствоваться нормативными документами ФСТЭК России.

Модель угроз применительно к конкретным ИС разрабатывается в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой Приказом ФСТЭК России от 14 февраля 2008 года (далее – Методика определения актуальных УБИ) на основе Базовой модели угроз и БДУ.

В данном разделе приведено описание методики определения актуальности угроз безопасности информации для ИС с учётом внесённых предположений и уточнений.

На основании нормативно-методического документа ФСТЭК России определяется степень исходной защищенности ИС. При определении степени исходной защищенности вводится числовой коэффициент Y1, его соответствие вербальному отображению представлено в таблице 12.

Таблица 12 – Коэффициент степени исходной защищенности ИС

Коэффициент СИЗ ИС	**Численное представление коэффициента Y_1**
Высокая	0
Средняя	5
Низкая	10

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путём показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данной ИС в складывающихся условиях обстановки. Для данного показателя характерны четыре градации, вербальному представлению которых, сопоставляется численный коэффициент Y2, представленный в таблице 13.

Таблица 13 – Вероятности реализации угроз безопасности

Вероятность реализации угроз	**Вероятность реализации угроз (описание)**	**Численное представление вероятности Y_2**
Маловероятно	Отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в хранилище носителей)	0

Вероятность реализации угроз	**Вероятность реализации угроз (описание)**	**Численное представление вероятности Y_2**
Низкая вероятность	Объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (применяются средства защиты информации)	2
Средняя вероятность	Объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны	5
Высокая вероятность	Объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности не приняты	10

Коэффициент реализуемости угрозы Y определяется соотношением (1)

$$Y = (Y1 + Y2)/20 \quad (1)$$

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

если $0 < Y < 0{,}3$, то возможность реализации угрозы признается низкой;

если $0{,}3 < Y < 0{,}6$, то возможность реализации угрозы признается средней;

если $0{,}6 < Y < 0{,}8$, то возможность реализации угрозы признается высокой;

если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИС. Этот показатель имеет три значения, которые представлены в таблице 14.

Таблица 14 – Показатель опасности угроз безопасности

Показатель опасности угрозы	**Показатель опасности (описание)**
Низкий	Незначительные негативные последствия для организации или субъектов ПДн при реализации угрозы
Средний	Негативные последствия для организации или субъектов ПДн при реализации угрозы
Высокий	Значительные негативные последствия для организации или субъектов ПДн при реализации угрозы

Выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИС, осуществляется в соответствии с определёнными правилами, представленными в таблице 15.

Таблица 15 – Матрица определения актуальности угроз безопасности

Возможность реализации угрозы	**Показатель опасности**		
	Низкий	**Средний**	**Высокий**
Низкая	Неактуальна	Неактуальна	Актуальна
Средняя	Неактуальна	Актуальна	Актуальна
Высокая	Актуальна	Актуальна	Актуальна
Очень высокая	Актуальна	Актуальна	Актуальна

С использованием перечня актуальных угроз, на основе

— Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных системах»;
— Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

должны формироваться конкретные организационно-технические требования по защите ИС от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИС. Перечень актуальных угроз и контрмеры должны определяться на этапе проектирования СОИБ.

4.2 Классификация угроз безопасности конфиденциальной информации

Под угрозами безопасности понимается совокупность условий и факторов, создающих потенциальную опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на неё.

Угрозы безопасности могут быть связаны как с непреднамеренными действиями персонала, так и со специально осуществляемыми неправомерными действиями отдельных лиц или групп лиц, а также иными источниками угроз.

При определении актуальности угроз безопасности по защите информации при информационном взаимодействии все угрозы безопасности информации подразделяются на:

— угрозы, не являющиеся атаками:
  - угрозы, не связанные с деятельностью человека;
  - угрозы социально–политического характера;
  - угрозы техногенного характера;
  - ошибочные действия (пользователей и обслуживающего персонала);
— угрозы, являющиеся атаками (атаки):
  - угрозы утечки информации по техническим каналам;
  - угрозы несанкционированного доступа.

4.3 Перечень угроз безопасности конфиденциальной информации

Перечень угроз составлен на основании агрегирования УБИ из Банка данных угроз безопасности информации ФСТЭК России приведённого на сайте http://bdu.fstec.ru/ (далее – БДУ), и Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой Приказом ФСТЭК России от 15 февраля 2008 года (далее – Базовая модель угроз), с учётом анализа среды, в которой осуществляется обработка защищаемой информации. Определение актуальности УБИ с учётом применяемых в ИС

ИОГВ Краснодарского края информационных технологий представлено в разделе 5.2 настоящей Модели угроз.

Общий перечень угроз, рассматриваемых с учётом потенциала возможных нарушителей УБИ, приведённом в таблице 11, представлен в таблице 16.

Описание угроз приведено в Приложении Б.

Таблица 16 – Перечень угроз безопасности информации

№ п/п	№ УБИ (по БДУ)	Наименование УБИ	Необходимый для реализации УБИ потенциал нарушителя		Актуальность рассмотрения УБИ для типа ИС ИОГВ Краснодарского края			
			Внутренний нарушитель	Внешний нарушитель	Тип 1	Тип 2	Тип 3	Тип 4
1. Угрозы, не являющиеся атаками								
1.1. Угрозы, не связанные с деятельностью человека								
1.1.1	-	Угроза стихийных бедствий и природных явлений	-	-	+	+	+	+
1.2. Угрозы социально–политического характера								
1.2.1	-	Угрозы социально–политического характера	-	-	+	+	+	+
1.3. Угрозы техногенного характера								
1.3.1	`	Угроза отказа электропитания серверного и телекоммуникационного оборудования	Низкий	Средний	+	+	+	+
1.3.2	-	Угроза отказа электропитания АРМ пользователей	Низкий	Средний	+	+	+	+
1.3.3	УБИ.180	Угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования	Низкий	Средний	+	+	+	+
1.4. Ошибочные действия								
1.4.1	-	Угроза разглашения конфиденциальной информации пользователями ИС	Низкий	-	+	+	+	+
1.4.2	-	Угроза разглашения конфиденциальной информации сотрудниками подрядных организаций	Средний	-	-	+	-	-
1.4.3	-	Угроза утраты мобильных технических средств пользователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации	Низкий	-	+	+	+	+
1.4.4	-	Угроза передача носителей информации лицам, не имеющих права доступа к хранимой на них информации	Низкий	-	+	+	+	+
1.4.5	УБИ.156	Угроза утраты носителей информации	Низкий	-	+	+	+	+
1.4.6	УБИ.106 УБИ.182	Угроза физического устаревания аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач	Низкий	-	+	+	+	+
1.4.7	УБИ.062 УБИ.109	Угроза некорректной настройки программного обеспечения	Средний	-	-	+	-	-
1.4.8	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Средний	Средний	+	+	+	+
1.4.9	УБИ.055	Угроза незащищённого удалённого администрирования информационной системы	Низкий	Низкий	+	+	+	+
1.4.10	УБИ.141	Угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу)	Средний	-	-	+	-	-
1.4.11	УБИ.054	Угроза недобросовестного исполнения обязательств поставщиком вычисли-	Низкий	Низкий	+	+	+	+

№ п/п	№ УБИ (по БДУ)	Наименование УБИ	Необходимый для реализации УБИ потенциал нарушителя		Актуальность рассмотрения УБИ для типа ИС ИОГВ Краснодарского края			
			Внутренний нарушитель	Внешний нарушитель	Тип 1	Тип 2	Тип 3	Тип 4
	УБИ.135 УБИ.142 УБИ.164	тельных мощностей (уполномоченным лицом)						
1.4.12	УБИ.065	Угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей)	Низкий	Низкий	+	+	+	+
1.4.13	УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Низкий	-	+	+	+	+
2. Угрозы, являющиеся атаками								
2.1. Угрозы утечки информации по техническим каналам								
2.1.1	УБИ.067	Угроза утечки акустической информации	Низкий	Низкий	+	+	+	+
2.1.2	УБИ.067	Угроза утечки видовой информации	Низкий	Низкий	+	+	+	+
2.1.3	-	Угроза утечки информации по каналу ПЭМИН	Высокий	Высокий	+	+	-	-
2.2. Угрозы несанкционированного доступа								
2.2.1	УБИ.139	Угроза преодоления физической защиты	-	Низкий	+	+	+	+
2.2.2	УБИ.157	Угроза физического выведения из строя АРМ, обрабатывающих защищаемую информацию	Низкий	Низкий	+	+	+	+
2.2.3	УБИ.157	Угроза физического выведения из строя серверов и систем хранения данных, обрабатывающих защищаемую информацию	Низкий	Низкий	+	+	+	+
2.2.4	УБИ.157	Угроза физического выведения из строя средств передачи информации	Низкий	Низкий	+	+	+	+
2.2.5	УБИ.160	Угроза хищения АРМ, обрабатывающих защищаемую информацию	Низкий	Низкий	+	+	+	+
2.2.6	УБИ.160	Угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию	Низкий	Низкий	+	+	+	+
2.2.7	УБИ.160	Угроза хищения средств передачи информации	Низкий	Низкий	+	+	+	+
2.2.8	УБИ.160	Угроза хищения носителей информации и мобильных технических средств	Низкий	Низкий	+	+	+	+
2.2.9	УБИ.023	Угроза изменения компонентов системы (аппаратной конфигурации) АРМ	Низкий	-	+	+	+	+
2.2.10	УБИ.023	Угроза изменения компонентов системы (аппаратной конфигурации) серверов	Низкий	-	+	+	+	+
2.2.11	УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Средний	Средний	+	+	+	+
2.2.12	УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	-	Высокий	+	+	-	-
2.2.13	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Низкий	Низкий	+	+	+	+

№ п/п	№ УБИ (по БДУ)	Наименование УБИ	Необходимый для реализации УБИ потенциал нарушителя		Актуальность рассмотрения УБИ для типа ИС ИОГВ Краснодарского края			
			Внутренний нарушитель	Внешний нарушитель	Тип 1	Тип 2	Тип 3	Тип 4
2.2.14	УБИ.008 УБИ.123	Угроза подбора пароля	Низкий	Низкий	+	+	+	+
2.2.15	УБИ.034 УБИ.122 УБИ.034 УБИ.122 УБИ.189 УБИ.192	Угроза использования уязвимостей используемого ПО	Низкий	Низкий	+	+	+	+
2.2.16	-	Угроза наличия недекларированных возможностей в СПО	-	Высокий	+	+	-	-
2.2.17	-	Угроза наличия недекларированных возможностей в ППО	-	Высокий	+	+	-	-
2.2.18	УБИ.009 УБИ.129 УБИ.154	Угроза установки уязвимых версий программного обеспечения	Низкий	Средний	+	+	+	+
2.2.19	УБИ.004 УБИ.018 УБИ.024 УБИ.045 УБИ.053 УБИ.144	Угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию	Низкий	-	+	+	+	+
2.2.20	УБИ.015 УБИ.111 УБИ.115 УБИ.117 УБИ.118 УБИ.158 УБИ.178	Угроза несанкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений	Низкий	Средний	+	+	+	+
2.2.21	УБИ.188	Угроза подмены программного обеспечения	Средний	-	+	+	+	+
2.2.22	УБИ.006 УБИ.022 УБИ.027 УБИ.145 УБИ.167 УБИ.170 УБИ.171 УБИ.191	Угроза внедрения вредоносного кода или данных на АРМ пользователей	Низкий	Низкий	+	+	+	+

№ п/п	№ УБИ (по БДУ)	Наименование УБИ	Необходимый для реализации УБИ потенциал нарушителя		Актуальность рассмотрения УБИ для типа ИС ИОГВ Краснодарского края			
			Внутренний нарушитель	Внешний нарушитель	Тип 1	Тип 2	Тип 3	Тип 4
2.2.23	УБИ.006 УБИ.022 УБИ.027 УБИ.145 УБИ.167 УБИ.170 УБИ.171 УБИ.191	Угроза внедрения вредоносного кода или данных на серверах	Низкий	Низкий	+	+	+	+
2.2.24	УБИ.172 УБИ.190	Угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет	Низкий	Низкий	+	+	+	+
2.2.25	УБИ.041 УБИ.042 УБИ.159	Угроза нарушения функционирования web-приложений	Низкий	Средний	+	+	+	+
2.2.26	УБИ.098 УБИ.099 УБИ.103 УБИ.104 УБИ.132 УБИ.151	Угроза получения сведений об информационной системе	Низкий	Низкий	+	+	+	+
2.2.27	УБИ.036 УБИ.037	Угроза исследования работы приложения	Средний	Средний	+	+	+	+
2.2.28	УБИ.088	Угроза несанкционированного копирования защищаемой информации	Низкий	Низкий	+	+	+	+
2.2.29	УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Низкий	Низкий	+	+	+	+
2.2.30	УБИ.011 УБИ.083 УБИ.125 УБИ.126	Угроза использования технологий беспроводного доступа	Низкий	Низкий	+	+	+	+
2.2.31	УБИ.048 УБИ.059 УБИ.073 УБИ.075 УБИ.076 УБИ.077 УБИ.078	Угроза несанкционированного доступа к компонентам среды виртуализации	Низкий	Низкий	+	+	+	+

№ п/п	№ УБИ (по БДУ)	Наименование УБИ	Необходимый для реализации УБИ потенциал нарушителя		Актуальность рассмотрения УБИ для типа ИС ИОГВ Краснодарского края			
			Внутренний нарушитель	Внешний нарушитель	Тип 1	Тип 2	Тип 3	Тип 4
	УБИ.079 УБИ.080 УБИ.084 УБИ.085 УБИ.119 УБИ.120							
2.2.32	УБИ.043 УБИ.140 УБИ.153 УБИ.173	Угроза приведения системы в состояние «отказ в обслуживании»	Низкий	Низкий	+	+	+	+
2.2.33	УБИ.069 УБИ.116 УБИ.130 УБИ.131 УБИ.174 УБИ.197	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	-	Средний	+	+	+	+
2.2.34	УБИ.069 УБИ.116 УБИ.130 УБИ.131 УБИ.174	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	-	Средний	+	+	+	+
2.2.35	УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	-	Средний	+	+	+	+
2.2.36	УБИ.165 УБИ.166 УБИ.169	Угроза наличия ошибок в ходе проектирования, разработки и отладки системы	Средний	-	-	+	-	-
2.2.37	УБИ.005 УБИ.150	Угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования	Средний	-	-	+	-	-
2.2.38	УБИ.015 УБИ.028 УБИ.033 УБИ.050 УБИ.063 УБИ.068 УБИ.100	Угроза слабости механизмов контроля входных данных	Низкий	Низкий	+	+	+	+

№ п/п	№ УБИ (по БДУ)	Наименование УБИ	Необходимый для реализации УБИ потенциал нарушителя		Актуальность рассмотрения УБИ для типа ИС ИОГВ Краснодарского края			
			Внутренний нарушитель	Внешний нарушитель	Тип 1	Тип 2	Тип 3	Тип 4
	УБИ.114 УБИ.117 УБИ.177							
2.2.39	УБИ.012 УБИ.121	Угроза слабости или некорректной настройки механизмов контроля целостности и резервирования данных	Низкий	Низкий	+	+	+	+
2.2.40	УБИ.167 УБИ.171	Угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика	Низкий	Низкий	+	+	+	+
2.2.41	УБИ.028 УБИ.031 УБИ.074 УБИ.086 УБИ.089 УБИ.090 УБИ.091 УБИ.124 УБИ.148 УБИ.152 УБИ.179 УБИ.185	Угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации	Низкий	Низкий	+	+	+	+
2.2.42	УБИ.003	Угроза анализа криптографических алгоритмов и их реализации	-	Средний	+	+	+	+
2.2.43	УБИ.176 УБИ.205	Угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информации	-	Низкий	+	+	+	+
2.2.44	УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Средний	Средний	+	+	+	+
2.2.45	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Низкий	Низкий	+	+	+	+
2.2.46	-	Угроза проникновения из смежных ИС с более низким уровнем защищенности	Низкий	Средний	+	+	+	+

5 Модель угроз

5.1 Определение исходной защищенности ИС

На основании Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой Приказом ФСТЭК России от 14 февраля 2008 года (далее – Методика определения актуальных угроз), определяется степень исходной защищенности ИС. Показатели исходной защищенности ИС ИОГВ Краснодарского края представлены в таблицах 17–20.

Таблица 17 – Показатели исходной защищенности ИС ИОГВ Краснодарского края 1 типа

	Технические и эксплуатационные характеристики ИС	**Высокая**	**Средняя**	**Низкая**
1.	По территориальному размещению			
1.1.	распределённая ИС (охватывает несколько областей, округов или государство в целом)			
1.2.	городская ИС (охватывает не более одного населённого пункта - города или посёлка)			
1.3.	корпоративная распределённая ИС (охватывает многие подразделения одной организации)			
1.4.	локальная (кампусная) ИС (развёрнута в пределах нескольких близко расположенных зданий)		1	
1.5.	локальная ИС (развёрнута в пределах одного здания)			
2.	По наличию соединения с сетями общего пользования (СОП)			
2.1.	ИС, имеющая многоточечный выход в СОП			1
2.2.	ИС, имеющая одноточечный выход в СОП			
2.3.	ИС, физически отделённая от СОП			
3.	По встроенным (легальным) операциям с записями БД			
3.1.	чтение, поиск			
3.2.	запись, удаление, сортировка			
3.3.	модификация, передача			1
4.	По разграничению доступа к защищаемой информации			
4.1.	ИС, к которой имеет доступ определённый перечень сотрудников организации, являющейся владельцем ИС, либо субъект защищаемой информации		1	
4.2.	ИС, к которой имеют доступ все сотрудники организации, являющейся владельцем ИС			
4.3.	ИС с открытым доступом			
5.	По наличию соединений с другими БД			
5.1.	интегрированная ИС (организация использует несколько БД ИС, при этом организация не является владельцем всех используемых БД)			1
5.2.	ИС, в которой используется одна БД, принадлежащая организации - владельцу данной ИС			
6.	По уровню обобщения (обезличивания)			

	Технические и эксплуатационные характеристики ИС	Высокая	Средняя	Низкая
6.1.	ИС, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)			
6.2.	ИС, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации			
6.3.	ИС, в которой предоставляемые пользователю данные не являются обезличенными			1
7.	По объёму защищаемой информации, который предоставляется сторонним пользователям ИС без предварительной обработки			
7.1.	ИС, предоставляющая всю БД с защищаемой информации			
7.2.	ИС, предоставляющая часть БД с защищаемой информации		1	
7.3.	ИС, не предоставляющая никакой информации			
	Количество баллов по уровням	0	3	4
	Уровень исходной защищенности ИС	0	0	низкий
	Коэффициент защищенности ИС (Y1)	10		

Таблица 18 – Показатели исходной защищенности ИС ИОГВ Краснодарского края 2 типа

	Технические и эксплуатационные характеристики ИС	Высокая	Средняя	Низкая
1.	По территориальному размещению			
1.1.	распределённая ИС (охватывает несколько областей, округов или государство в целом)			
1.2.	городская ИС (охватывает не более одного населённого пункта - города или посёлка)			
1.3.	корпоративная распределённая ИС (охватывает многие подразделения одной организации)			
1.4.	локальная (кампусная) ИС (развёрнута в пределах нескольких близко расположенных зданий)		1	
1.5.	локальная ИС (развёрнута в пределах одного здания)			
2.	По наличию соединения с сетями общего пользования (СОП)			
2.1.	ИС, имеющая многоточечный выход в СОП			1
2.2.	ИС, имеющая одноточечный выход в СОП			
2.3.	ИС, физически отделённая от СОП			
3.	По встроенным (легальным) операциям с записями БД			
3.1.	чтение, поиск			
3.2.	запись, удаление, сортировка			
3.3.	модификация, передача			1
4.	По разграничению доступа к защищаемой информации			
4.1.	ИС, к которой имеет доступ определённый перечень сотрудников организации, являющейся владельцем ИС, либо субъект защищаемой информации		1	
4.2.	ИС, к которой имеют доступ все сотрудники организации, являющейся владельцем ИС			
4.3.	ИС с открытым доступом			

	Технические и эксплуатационные характеристики ИС	Высокая	Средняя	Низкая
5.	По наличию соединений с другими БД			
5.1.	интегрированная ИС (организация использует несколько БД ИС, при этом организация не является владельцем всех используемых БД)			1
5.2.	ИС, в которой используется одна БД, принадлежащая организации - владельцу данной ИС			
6.	По уровню обобщения (обезличивания)			
6.1.	ИС, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)			
6.2.	ИС, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации			
6.3.	ИС, в которой предоставляемые пользователю данные не являются обезличенными			1
7.	По объёму защищаемой информации, который предоставляется сторонним пользователям ИС без предварительной обработки			
7.1.	ИС, предоставляющая всю БД с защищаемой информации			
7.2.	ИС, предоставляющая часть БД с защищаемой информации		1	
7.3.	ИС, не предоставляющая никакой информации			
	Количество баллов по уровням	0	3	4
	Уровень исходной защищенности ИС	0	0	низкий
	Коэффициент защищенности ИС (Y1)	10		

Таблица 19 – Показатели исходной защищенности ИС ИОГВ Краснодарского края 3 типа

	Технические и эксплуатационные характеристики ИС	Высокая	Средняя	Низкая
1.	По территориальному размещению			
1.1.	распределённая ИС (охватывает несколько областей, округов или государство в целом)			
1.2.	городская ИС (охватывает не более одного населённого пункта - города или посёлка)			
1.3.	корпоративная распределённая ИС (охватывает многие подразделения одной организации)			
1.4.	локальная (кампусная) ИС (развёрнута в пределах нескольких близко расположенных зданий)		1	
1.5.	локальная ИС (развёрнута в пределах одного здания)			
2.	По наличию соединения с сетями общего пользования (СОП)			
2.1.	ИС, имеющая многоточечный выход в СОП			1
2.2.	ИС, имеющая одноточечный выход в СОП			
2.3.	ИС, физически отделённая от СОП			
3.	По встроенным (легальным) операциям с записями БД			
3.1.	чтение, поиск			
3.2.	запись, удаление, сортировка			
3.3.	модификация, передача			1
4.	По разграничению доступа к защищаемой информации			

	Технические и эксплуатационные характеристики ИС	Высокая	Средняя	Низкая
4.1.	ИС, к которой имеет доступ определённый перечень сотрудников организации, являющейся владельцем ИС, либо субъект защищаемой информации		1	
4.2.	ИС, к которой имеют доступ все сотрудники организации, являющейся владельцем ИС			
4.3.	ИС с открытым доступом			
5.	По наличию соединений с другими БД			
5.1.	интегрированная ИС (организация использует несколько БД ИС, при этом организация не является владельцем всех используемых БД)			1
5.2.	ИС, в которой используется одна БД, принадлежащая организации - владельцу данной ИС			
6.	По уровню обобщения (обезличивания)			
6.1.	ИС, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)			
6.2.	ИС, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации			
6.3.	ИС, в которой предоставляемые пользователю данные не являются обезличенными			1
7.	По объёму защищаемой информации, который предоставляется сторонним пользователям ИС без предварительной обработки			
7.1.	ИС, предоставляющая всю БД с защищаемой информации			
7.2.	ИС, предоставляющая часть БД с защищаемой информации		1	
7.3.	ИС, не предоставляющая никакой информации			
	Количество баллов по уровням	0	3	4
	Уровень исходной защищенности ИС	0	0	низкий
	Коэффициент защищенности ИС (Y1)	10		

Таблица 20 – Показатели исходной защищенности ИС ИОГВ Краснодарского края 4 типа

	Технические и эксплуатационные характеристики ИС	Высокая	Средняя	Низкая
1.	По территориальному размещению			
1.1.	распределённая ИС (охватывает несколько областей, округов или государство в целом)			
1.2.	городская ИС (охватывает не более одного населённого пункта - города или посёлка)			
1.3.	корпоративная распределённая ИС (охватывает многие подразделения одной организации)			
1.4.	локальная (кампусная) ИС (развёрнута в пределах нескольких близко расположенных зданий)		1	
1.5.	локальная ИС (развёрнута в пределах одного здания)			
2.	По наличию соединения с сетями общего пользования (СОП)			
2.1.	ИС, имеющая многоточечный выход в СОП			1
2.2.	ИС, имеющая одноточечный выход в СОП			
2.3.	ИС, физически отделённая от СОП			
3.	По встроенным (легальным) операциям с записями БД			
3.1.	чтение, поиск			
3.2.	запись, удаление, сортировка			

	Технические и эксплуатационные характеристики ИС	Высокая	Средняя	Низкая
3.3.	модификация, передача			1
4.	По разграничению доступа к защищаемой информации			
4.1.	ИС, к которой имеет доступ определённый перечень сотрудников организации, являющейся владельцем ИС, либо субъект защищаемой информации		1	
4.2.	ИС, к которой имеют доступ все сотрудники организации, являющейся владельцем ИС			
4.3.	ИС с открытым доступом			
5.	По наличию соединений с другими БД			
5.1.	интегрированная ИС (организация использует несколько БД ИС, при этом организация не является владельцем всех используемых БД)			1
5.2.	ИС, в которой используется одна БД, принадлежащая организации - владельцу данной ИС			
6.	По уровню обобщения (обезличивания)			
6.1.	ИС, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)			
6.2.	ИС, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации			
6.3.	ИС, в которой предоставляемые пользователю данные не являются обезличенными			1
7.	По объёму защищаемой информации, который предоставляется сторонним пользователям ИС без предварительной обработки			
7.1.	ИС, предоставляющая всю БД с защищаемой информации			
7.2.	ИС, предоставляющая часть БД с защищаемой информации			
7.3.	ИС, не предоставляющая никакой информации	1		
	Количество баллов по уровням	1	2	4
	Уровень исходной защищенности ИС	0	0	низкий
	Коэффициент защищенности ИС (Y1)	10		

5.2 Определение актуальных угроз безопасности конфиденциальной информации

На основании экспертных оценок осуществляется определение вероятности реализации угроз, а также показатели их опасности. На их основе и с учётом коэффициента исходной защищенности ИС рассчитана степень актуальности угроз безопасности информации. Данные приведены в таблицах 21-24.

Таблица 21 – Актуальность угроз безопасности информации ИС ИОГВ Краснодарского края 1 типа

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
1. Угрозы, не являющиеся атаками								
1.1. Угрозы, не связанные с деятельностью человека								
1.1.1	Угроза стихийных бедствий и природных явлений	-	Информационная система	низкая	высокий	средняя	актуальна	Несмотря на невозможность прогнозирования данной угрозы и степени последствий от ее реализации, данная угроза является не актуальной, т.к. для данного типа ИС ИОГВ Краснодарского края характерно обеспечение отказоустойчивого функционирования ИС
1.2. Угрозы социально–политического характера								
1.2.1	Угрозы социально–политического характера	-	Информационная система	высокая	высокий	средняя	актуальна	Несмотря на невозможность прогнозирования данной угрозы и степени последствий от ее реализации, данная угроза является не актуальной, т.к. для данного типа ИС ИОГВ Краснодарского края отказоустойчивого обеспечение отказоустойчивого функционирования ИС
1.3. Угрозы техногенного характера								
1.3.1	Угроза отказа электропитания серверного и телекоммуникационного оборудования	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Линии и средства электропитания	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной в связи с применением ИБП для серверного оборудования, а также наличием ДГУ, обеспечивающей в случае необходимости, бесперебойную подачу электропитания
1.3.2	Угроза отказа электропитания АРМ пользователей	Внутренний нарушитель с низким потенциалом, Внешний нарушитель	Линии и средства электропитания	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной ввиду отсутствия в данном типе ИС ИОГВ Краснодарского края АРМ пользователей (за исключением АРМ Администраторов инфраструктуры, для обеспечения беспе-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		со средним потенциалом						ребойного электропитания которых применяются ИБП)
1.3.3	Угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в серверных помещениях, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной в связи с использованием систем кондиционирования в серверные помещения, а также ограничением физического доступа в них для потенциальных нарушителей
1.4. Ошибочные действия								
1.4.1	Угроза разглашения конфиденциальной информации пользователями ИС	Внутренний нарушитель с низким потенциалом	Защищаемая информация	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной ввиду отсутствия в данном типе ИС ИОГВ Краснодарского края пользователей ИС (Администраторы, обеспечивающие администрирование инфраструктуры, является доверенными лицами и не входят в число потенциальных нарушителей)
1.4.2	Угроза разглашения конфиденциальной информации сотрудниками подрядных организаций	Внутренний нарушитель с средним потенциалом	Защищаемая информация	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. подрядные организации относятся к неактуальным категориям потенциальных нарушителей для данного типа ИС ИОГВ Краснодарского края (требования о неразглашении конфиденциальной информации

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								подрядными организациями закрепляются в заключаемых государственных контрактах)
1.4.3	Угроза утраты мобильных технических средств пользователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации	Внутренний нарушитель с низким потенциалом	Мобильное техническое средство	высокая	средний	средняя	актуальна	Угроза является актуальной, т.к. процедуры контроля использования мобильных технических средств не регламентированы в ОРД и не реализованы, обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности не осуществляется.
1.4.4	Угроза передачи носителей информации лицам, не имеющих права доступа к хранимой на них информации	Внутренний нарушитель с низким потенциалом	Носитель информации	высокая	средний	средняя	актуальна	Угроза является актуальной, т.к. процедуры контроля использования носителей информации не регламентированы в ОРД и не реализованы, обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности не осуществляется.
1.4.5	Угроза утраты носителей информации	Внутренний нарушитель с низким потенциалом	Носитель информации	средняя	средний	средняя	актуальна	Угроза является актуальной, т.к. процедуры контроля использования носителей информации не регламентированы в ОРД и не реализованы. Также, в случае выноса носителей информации за пределы КЗ, информация на нах не шифруется
1.4.6	Угроза физического устаревания аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач	Внутренний нарушитель с низким потенциалом	Аппаратное средство, система хранения данных	средняя	средний	средняя	актуальна	Угроза является актуальной, т.к. в ОРД не определён жизненный цикл компонентов ИС и порядок вывода их из эксплуатации
1.4.7	Угроза некорректной настройки программного обеспечения	Внутренний нарушитель со средним потенциалом,	Системное программное обеспечение, прикладное программное	средняя	средний	средняя	актуальна	Несмотря на неактуальность для данного типа ИС ИОГВ Краснодарского края в качестве потенциальных нарушителей администраторов

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		Внешний нарушитель со средним потенциалом	обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр.					ИС/ИБ - данная угроза является актуальной, т.к. возможна некорректная настройка программного обеспечения (ввиду недостаточной компетенции сотрудников (необходимо проведение обучение сотрудников по вопросам установки и администрирования настраиваемых категорий ПО), которая может привести к возможности реализации данной угрозы внешним нарушителем. Также, на периодической основе должно осуществляться сканирование сертифицированными ФСТЭК России средствами анализа защищённости компонентов ИС на предмет некорректных настроек ПО.
1.4.8	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Средства защиты информации, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	средняя	высокий	средняя	актуальна	Несмотря на неактуальность для данного типа ИС ИОГВ Краснодарского края в качестве потенциальных нарушителей администраторов ИС/ИБ - данная угроза является актуальной, т.к. возможны ситуации, когда после ввода в эксплуатацию ПО и (или) оборудования не осуществляется изменение пароля, заданного по умолчанию (вследствие халатности сотрудников), что может в последующем привести к реализации несанкционированного доступа как внутренними, так и внешними нарушителями. Также, на периодической основе должно осуществляться сканирование компонентов ИС на предмет наличия заданной по умолчанию идентифи-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								кационной/аутентификационной информации сертифицированными ФСТЭК России средствами анализа защищенности.
1.4.9	Угроза незащищённого удалённого администрирования информационной системы	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Информационная система, сервер, рабочая станция, сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в связи с возможностью наличия на АРМ и серверах средств удалённого администрирования, аутентификационная информация которых может быть перехвачена нарушителем при доступе к ИС из-за пределов КЗ (при осуществлении удалённого администрирования без использования средств криптографической защиты информации (в данном случае аутентификационной), передаваемой по каналам связи)
1.4.10	Угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу)	Внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы	низкая	низкий	средняя	неактуальна	Угроза не является актуальной, т.к. для данного типа ИС ИОГВ Краснодарского края уполномоченное лицо является доверенным, ответственность которого закреплена в том числе в заключаемых с ним государственных контрактах
1.4.11	Угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом)	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Информационная система, сервер, носитель информации, метаданные, объекты файловой системы, системное программное обеспечение, аппаратное обеспечение, ка-	низкая	низкий	средняя	неактуальна	Угроза не является актуальной, т.к. для данного типа ИС ИОГВ Краснодарского края уполномоченное лицо является доверенным, ответственность которого закреплена в том числе в заключаемых с ним государственных контрактах

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
			нал связи					
1.4.12	Угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей)	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение	низкая	низкий	средняя	неактуальна	Угроза не является актуальной, т.к. для данного типа ИС ИОГВ Краснодарского края распределение ролей закреплено в заключаемых с уполномоченным лицом государственных контрактах
1.4.13	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Внутренний нарушитель со средним потенциалом	Мобильное устройство	высокая	средний	средняя	актуальна	Данная угроза является актуальной в связи с использованием личных мобильных устройств пользователей (незащищённых сертифицированными ФСТЭК России средствами защиты информации от НСД, средств антивирусной защиты информации и сертифицированными ФСБ России средствами криптографической защиты информации, передаваемой по каналам связи) в рабочих целях, в т.ч. для доступа к определённому количеству защищаемой информации (например, посредством электронной почты)
2. Угрозы, являющиеся атаками								
2.1. Угрозы утечки информации по техническим каналам								
2.1.1	Угроза утечки акустической информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Защищаемая информация, аппаратное обеспечение	маловероятно	средний	низкая	неактуальна	Угроза является не актуальной, т.к. в ИС отсутствуют функции голосового ввода информации и функции воспроизведения информации акустическими средствами ИС, также, акустическое озвучивание защищаемой информации не осуществляется
2.1.2	Угроза утечки видовой информации	Внутренний нарушитель с	Защищаемая информация	маловероятно	средний	низкая	неактуальна	Устройства отображения информации размещены таким образом, ко-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		низким потенциалом, Внешний нарушитель с низким потенциалом						торый исключает несанкционированный просмотр защищаемой информации
2.1.3	Угроза утечки информации по каналу ПЭМИН	Внутренний нарушитель с высоким потенциалом, Внешний нарушитель с высоким потенциалом	Аппаратное обеспечение	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. отсутствуют объективные предпосылки для реализации угроз данного класса, применение подобных средств разведки экономически необоснованно
2.2. Угрозы несанкционированного доступа								
2.2.1	Угроза преодоления физической защиты	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, т.к. реализован контрольно-пропускной и внутриобъектовый режим, помещения оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, ведётся журнал учёта посетителей
2.2.2	Угроза физического выведения из строя АРМ, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	АРМ	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной в связи с отсутствием АРМ пользователей в данном типе ИС ИОГВ Краснодарского края
2.2.3	Угроза физического выведения из строя серверов и систем хранения данных, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний	Сервер	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, т.к. реализован контрольно-пропускной и внутриобъектовый режим, помещения оборудованы надёжными дверьми, СКУД, охранной сигнали-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		нарушитель со средним потенциалом						зацией и системой видеонаблюдения, ведётся журнал учёта посетителей
2.2.4	Угроза физического выведения из строя средств передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, т.к. реализован контрольно-пропускной и внутриобъектовый режим, помещения оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, ведётся журнал учёта посетителей
2.2.5	Угроза хищения АРМ, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	АРМ	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной в связи с отсутствием АРМ пользователей в данном типе ИС ИОГВ Краснодарского края
2.2.6	Угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сервер	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, т.к. реализован контрольно-пропускной и внутриобъектовый режим, помещения оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, ведётся журнал учёта посетителей
2.2.7	Угроза хищения средств передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, т.к. реализован контрольно-пропускной и внутриобъектовый режим, помещения оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, ведётся журнал учёта посетителей
2.2.8	Угроза хищения носите-	Внутренний	Носитель инфор-	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, т.к.

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	лей информации и мобильных технических средств	нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	мации					реализован контрольно-пропускной и внутриобъектовый режим, помещения оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, ведётся журнал учёта посетителей
2.2.9	Угроза изменения компонентов системы (аппаратной конфигурации) АРМ	Внутренний нарушитель с низким потенциалом	АРМ	маловероятно	низкий	средняя	неактуальна	Угроза является неактуальной в связи с отсутствием АРМ пользователей в данном типе ИС ИОГВ Краснодарского края
2.2.10	Угроза изменения компонентов системы (аппаратной конфигурации) серверов	Внутренний нарушитель с низким потенциалом	Сервер	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. доступ в серверные помещения для потенциальных нарушителей ограничен реализованными контрольно-пропускным и внутриобъектовым режимом
2.2.11	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода, передачи информации	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. категории внутренних нарушителей, чей потенциал позволяет реализовать данную угрозу - не являются актуальными для данного типа ИС ИОГВ Краснодарского края. Для нейтрализации возможностей внешних нарушителей по реализации данной угрозы - используются сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений.
2.2.12	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение	низкая	средний	средняя	актуальна	Несмотря на использование сертифицированных ФСТЭК России средств межсетевого экранирования и обнаружения вторжений - угроза является актуальной в связи с отсутствием контроля использования аппаратного обеспечения, облада-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								ющим функциональными возможностями внеполосного доступа к ним
2.2.13	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	высокая	низкий	высокая	актуальна	Несмотря на реализованный контрольно-пропускной и внутриобъектовый режим, исключающий реализацию данной угрозы внешним нарушителем, данная угроза может быть реализована внутренним нарушителем вследствие его халатности
2.2.14	Угроза подбора пароля	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя, микропрограммное обеспечение BIOS/UEFI.	высокая	низкий	высокая	актуальна	Угроза является актуальной, т.к. используемые сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений не позволяют нейтрализовать угрозу подбора пароля
2.2.15	Угроза использования уязвимостей используемого ПО	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, информационная система, средство защиты информации	низкая	низкий	средняя	неактуальна	Угроза неактуальной, т.к. на периодической основе осуществляется анализ используемого ПО на предмет наличия в них уязвимостей с помощью сертифицированного ФСТЭК России средства анализа защищенности.

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.2.16	Угроза наличия недекларированных возможностей в СПО	Внешний нарушитель с высоким потенциалом	Системное программное обеспечение.	маловероятно	низкий	низкая	неактуальна	Актуальность данной угрозы должна определяться для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (топологии), назначения ИС, состава и критичности обрабатываемой в ней информации. В общем случае считается, что данная угроза является не актуальной, т.к. приобретается лицензионное СПО (или используется СПО с открытым кодом), ответственность разработчика которого определена в заключаемых на его поставку гос. контрактах
2.2.17	Угроза наличия недекларированных возможностей в ППО	Внешний нарушитель с высоким потенциалом	Прикладное программное обеспечение.	маловероятно	низкий	низкая	неактуальна	Актуальность данной угрозы должна определяться для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (топологии), назначения ИС, состава и критичности обрабатываемой в ней информации. В общем случае считается, что данная угроза является не актуальной, т.к. приобретается лицензионное ППО (или используется ППО с открытым кодом), ответственность разработчика которого определена в заключаемых на его поставку и (или) разработку гос. контрактах
2.2.18	Угроза установки уязвимых версий программного обеспечения	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Программное обеспечение, микропрограммное и аппаратное обеспечение BIOS/UEFI	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие права пользователей на установку программного обеспечения, а возможности внешнего нарушителя

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								ограничены посредством применения сертифицированных ФСТЭК России средств межсетевого экранирования, обнаружения вторжений и анализа защищенности.
2.2.19	Угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	высокая	средний	средняя	актуальна	Несмотря на то, что применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, осуществляющие контроль устанавливаемого и запускаемого ПО, а также контрольно-пропускным и внутриобъектовым режимом ограничены возможности внешнего нарушителя, угроза является актуальной, т.к. не осуществляется контроль вскрытия системных блоков АРМ пользователей.
2.2.20	Угроза несанкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение объекты файловой системы АРМ; сетевой узел, сетевой трафик, носитель информации.	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие установку и запуск приложений, а также наличием сертифицированных ФСТЭК России средств обнаружения вторжений и межсетевого экранирования, ограничивающих возможности внешних нарушителей.
2.2.21	Угроза подмены программного обеспечения	Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное про-	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. в данном типе ИС ИОГВ Краснодарского края отсутствуют пользователи ИС, а возможности внешнего нарушителя ограничены применяемыми средствами защиты инфор-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
			граммное обеспечение					мации
2.2.22	Угроза внедрения вредоносного кода или данных на АРМ пользователей	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, объект файловой системы, виртуальная машина сервера; сетевой узел	низкая	низкий	средняя	неактуальна	Угроза является не актуальной, т.к. для защиты АРМ пользователей применяются сертифицированные ФСТЭК России средства антивирусной защиты информации
2.2.23	Угроза внедрения вредоносного кода или данных на серверах	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, сетевой узел, объект файловой системы.	низкая	низкий	средняя	неактуальна	Угроза является не актуальной, т.к. для защиты серверов ИС применяются сертифицированные ФСТЭК России средства антивирусной защиты информации
2.2.24	Угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	высокая	средний	средняя	актуальна	Несмотря на то, что для защиты почтовых серверов и на АРМ пользователей применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, угроза является актуальной, т.к. не разработан регламент использования ресурсов сети Интернет и эксплуатации электронной почты, опи-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								сывающий необходимый порядок действия пользователей с целью недопущения вирусных заражений
2.2.25	Угроза нарушения функционирования web-приложений	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	высокая	средний	средняя	актуальна	Угроза является актуальной, т.к. отсутствуют специализированные средства межсетевого экранирования типа "Г", сертифицированные по требованиям ФСТЭК России.
2.2.26	Угроза получения сведений об информационной системе	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	средняя	низкий	высокая	актуальна	Угроза является актуальной, т.к. используемые сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений не позволяют нейтрализовать угрозы сканирования информационных систем
2.2.27	Угроза исследования работы приложения	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	средняя	средний	средняя	актуальна	Несмотря на неактуальность внутренних категорий нарушителей, способных реализовать данную угроз, угроза является актуальной для информационных систем, доступных из сети Интернет
2.2.28	Угроза несанкционированного копирования защищаемой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	высокая	высокий	средняя	актуальна	Угроза является актуальной, т.к. в ИС возможно подключение/использование съёмных носителей информации и не применяются специализированные средства защиты информации для контроля копирования защищаемой информации.

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.2.29	Угроза несанкционированного восстановления удалённой защищаемой информации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Машинный носитель информации	средняя	средний	средняя	актуальна	Угроза является актуальной, т.к. для удаления защищаемой информации не используются средства гарантированного уничтожения информации.
2.2.30	Угроза использования технологий беспроводного доступа	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение	маловероятно	низкий	низкая	неактуальна	Данная угроза является не актуальной, т.к. для доступа пользователей к ИС технологии беспроводного доступа не используются
2.2.31	Угроза несанкционированного доступа к компонентам среды виртуализации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина, сервер, сетевое оборудование, сетевой трафик, виртуальные устройства, гипервизор, виртуальные устройства хранения, обработки и передачи данных, объект файловой системы.	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России средства защиты сред виртуализации
2.2.32	Угроза приведения системы в состояние «отказ в	Внутренний нарушитель с	Информационная система, сетевой	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	обслуживании»	низким потенциалом Внешний нарушитель с низким потенциалом	узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик					ФСТЭК России средства обнаружения вторжений и межсетевого экранирования, а также осуществляется анализ постоянный мониторинг и анализ инцидентов
2.2.33	Угроза реализации атаки "человек посередине" при передаче информации в пределах контролируемой зоны	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер, информация, хранящаяся на компьютере во временных файлах (программное обеспечение)	низкая	низкий	средняя	неактуальна	Угроза является неактуальной т.к. в ЛВС применяются сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений, позволяющие нейтрализовать данную угрозу, а также доступ посторонних лиц в помещения ограничен.
2.2.34	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер	низкая	низкий	средняя	неактуальна	Угроза является неактуальной т.к. при передаче защищаемой информации за пределы КЗ применяются сертифицированные ФСБ России средства криптографической защиты информации, передаваемой по каналам связи.
2.2.35	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Внешний нарушитель со средним потенциалом	Аутентификационные данные пользователя (программное обеспечение)	высокая	средний	средняя	актуальна	Угроза является актуальной, т.к. порядок использования браузеров при доступе к административным функциям оборудования - не регламентирован.
2.2.36	Угроза наличия ошибок в ходе проектирования, разработки и отладки систе-	Внутренний нарушитель со средним	Программное обеспечение, техническое сред-	низкая	низкий	средняя	неактуальна	Угроза является неактуальной ввиду неактуальности для данного типа ИС ИОГВ Краснодарского края

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	мы	потенциалом	ство, информационная система, ключевая система информационной инфраструктуры					данной категории потенциальных нарушителей (в государственных контрактах на проектирование, разработку и отладку систем) закрепляется ответственность Поставщиков услуг. Для проведения работ по защите информации привлекаются только организации, имеющей соответствующие лицензии ФСТЭК России и ФСБ России. Однако, перед вводом систем в эксплуатацию должно осуществляться их тестирование (а для ИС, являющихся ГИС и (или) ИСПДн, дополнительно и аттестация по требованиям безопасности информации)
2.2.37	Угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	низкая	низкий	средняя	неактуальна	Угроза является неактуальной ввиду неактуальности для данного типа ИС ИОГВ Краснодарского края данной категории потенциальных нарушителей (в государственных контрактах на ремонт и обслуживания оборудования закрепляется ответственность Поставщиков услуг)
2.2.38	Угроза слабости механизмов контроля входных данных	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр, аппаратное	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие возможности нарушителей по доступу к программным компонентам информационных систем, а также контролирующие функционирование программ. Возможности внешнего нарушителя ограничены используемыми сертифицированными ФСТЭК России средствами обна-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
			обеспечение, метаданные					ружения вторжений и межсетевого экранирования.
2.2.39	Угроза слабости или некорректной настройки механизмов контроля целостности и резервирования данных	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, средствами которых обеспечивается контроль целостности, а также используются средства резервного копирования информации.
2.2.40	Угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России средства межсетевого экранирования, средства которых осуществляется фильтрация сетевого трафика
2.2.41	Угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, учётные данные пользователя, реестр, машинные носители информации, метаданные, микропрограммное обеспе-	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, средствами которых обеспечивается разграничение доступа к защищаемой информации

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
			чение, средство защиты информации					
2.2.42	Угроза анализа криптографических алгоритмов и их реализации	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСБ России средства криптографической защиты информации
2.2.43	Угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информации	Внешний нарушитель с низким потенциалом	Средство защиты информации, аппаратное устройство, программное обеспечение	низкая	низкий	средняя	неактуальна	Угроза является неактуальной в связи с тем, что используются сертифицированные ФСТЭК России и ФСБ России средства защиты информации, настройка которых осуществляется лицензиатами указанных ведомств. Этапу внедрения средств защиты информации предшествует этап проектирования системы защиты информации, учитывающее особенности функционирования ИС
2.2.44	Угроза несанкционированного воздействия на средство защиты информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Средство защиты информации	высокая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России и ФСБ России средства защиты информации, обеспечивающие ограничение возможностей потенциальных нарушителей по воздействию на средства защиты информации
2.2.45	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Средство защиты информации	высокая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. применяются сертифицированные ФСТЭК России средства защиты информации, доступ к администрированию которых пользователям ограничен

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.2.46	Угроза проникновения из смежных ИС с более низким уровнем защищенности	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Информационная система	средняя	средний	средняя	актуальна	Несмотря на наличие сертифицированных ФСТЭК России средств межсетевого экранирования, обеспечивающих сегментирование ИС различных уровней защищенности, угроза является актуальной, т.к. не разработаны технические условия подключения к сегментам ИС

Таблица 22 – Актуальность угроз безопасности информации ИС ИОГВ Краснодарского края 2 типа

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
1. Угрозы, не являющиеся атаками								
1.1. Угрозы, не связанные с деятельностью человека								
1.1.1	Угроза стихийных бедствий и природных явлений	-	Информационная система	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если поставщиком вычислительных мощностей (уполномоченным лицом) не обеспечение отказоустойчивого функционирования ИС, что возможно для ИС данного типа
1.2. Угрозы социально–политического характера								
1.2.1	Угрозы социально–политического характера	-	Информационная система	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если поставщиком вычислительных мощностей (уполномоченным лицом) не обеспечение отказоустойчивого функционирования ИС, что возможно для ИС данного типа
1.3. Угрозы техногенного характера								
1.3.1	Угроза отказа электропитания серверного и телекоммуникационного оборудования	Внутренний нарушитель с низким потенциалом,	Линии и средства электропитания	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если для обеспечения бесперебойного питания серверного и телекоммуникационного оборудования

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		Внешний нарушитель со средним потенциалом						не применяются ИБП и ДГУ, что возможно для ИС данного типа
1.3.2	Угроза отказа электропитания АРМ пользователей	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Линии и средства электропитания	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной ввиду отсутствия в данном типе ИС ИОГВ Краснодарского края АРМ пользователей
1.3.3	Угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в серверных помещениях, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля	высокая	средний	средняя	актуальна	Угроза является актуальной, в случае если в помещениях размещения серверного и телекоммуникационного оборудования отсутствуют системы кондиционирования и (или) доступ внешних нарушителей к данным помещениям не ограничен контрольно-пропускным и внутриобъектовым режимом, что возможно для ИС данного типа
1.4. Ошибочные действия								
1.4.1	Угроза разглашения конфиденциальной информации пользователями ИС	Внутренний нарушитель с низким потенциалом	Защищаемая информация	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной ввиду отсутствия в данном типе ИС ИОГВ Краснодарского края пользователей ИС

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
1.4.2	Угроза разглашения конфиденциальной информации сотрудниками подрядных организаций	Внутренний нарушитель с средним потенциалом	Защищаемая информация	высокая	средний	средняя	актуальна	Угроза является актуальной в связи с актуальностью категории нарушителей, имеющей потенциальную возможность для реализации угрозы
1.4.3	Угроза утраты мобильных технических средств пользователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации	Внутренний нарушитель с низким потенциалом	Мобильное техническое средство	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если процедуры контроля использования мобильных технических средств не регламентированы в ОРД и не реализованы, обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности не осуществляется, что возможно для ИС ИОГВ Краснодарского края данного типа.
1.4.4	Угроза передача носителей информации лицам, не имеющих права доступа к хранимой на них информации	Внутренний нарушитель с низким потенциалом	Носитель информации	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если процедуры контроля использования носителей информации не регламентированы в ОРД и не реализованы, обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности не осуществляется, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.5	Угроза утраты носителей информации	Внутренний нарушитель с низким потенциалом	Носитель информации	средняя	средний	средняя	актуальна	Угроза является актуальной в следующих случаях: - процедуры контроля использования носителей информации не регламентированы в ОРД и не реализованы; - в случае выноса носителей информации за пределы КЗ, информация на нах не шифруется, что возможно для ИС ИОГВ Краснодар-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								ского края данного типа
1.4.6	Угроза физического устаревания аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач	Внутренний нарушитель с низким потенциалом	Аппаратное средство, система хранения данных	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если в ОРД не определён жизненный цикл компонентов ИС и порядок вывода их из эксплуатации, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.7	Угроза некорректной настройки программного обеспечения	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр.	средняя	средний	средняя	актуальна	Угроза является актуальной в связи с актуальностью категории нарушителей, имеющей потенциальную возможность для реализации угрозы
1.4.8	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Средства защиты информации, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	средняя	средний	средняя	актуальна	Угроза является актуальной в связи с актуальностью категории нарушителей, имеющей потенциальную возможность для реализации угрозы
1.4.9	Угроза незащищённого удалённого администрирования информационной	Внутренний нарушитель с низким по-	Информационная система, сервер, рабочая станция,	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если на АРМ и (или) серверах имеются средства удалённого ад-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	системы	тенциалом, Внешний нарушитель с низким потенциалом	сетевое программное обеспечение					министрирования, аутентификационная информация которых может быть перехвачена нарушителем при доступе к ИС из-за пределов КЗ (при осуществлении удалённого администрирования без использования средств криптографической защиты информации (в данном случае аутентификационной), передаваемой по каналам связи)
1.4.10	Угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу)	Внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы	средняя	средний	средняя	актуальна	Угроза является актуальной, если в качестве уполномоченного лица, предоставляющие вычислительные мощности, выступает не Департамент информатизации и связи Краснодарского края
1.4.11	Угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом)	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Информационная система, сервер, носитель информации, метаданные, объекты файловой системы, системное программное обеспечение, аппаратное обеспечение, канал связи	средняя	средний	средняя	актуальна	Угроза является актуальной, если в качестве уполномоченного лица, предоставляющие вычислительные мощности, выступает не Департамент информатизации и связи Краснодарского края
1.4.12	Угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычис-	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с	Системное программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной, если в качестве уполномоченного лица, предоставляющие вычислительные мощности, выступает не Департамент информатизации и связи Краснодарского края

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	лительных мощностей)	низким потенциалом						
1.4.13	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Внутренний нарушитель со средним потенциалом	Мобильное устройство	средняя	средний	средняя	актуальна	Данная угроза является актуальной, если в рабочих целях используются личные мобильные устройства пользователей (незащищённых сертифицированными ФСТЭК России средствами защиты информации от НСД, средств антивирусной защиты информации и сертифицированными ФСБ России средствами криптографической защиты информации, передаваемой по каналам связи), в т.ч. для доступа к определённому количеству защищаемой информации (например, посредством электронной почты)
2. Угрозы, являющиеся атаками								
2.1. Угрозы утечки информации по техническим каналам								
2.1.1	Угроза утечки акустической информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Защищаемая информация, аппаратное обеспечение	маловероятно	средний	низкая	неактуальна	Угроза является не актуальной, т.к. в ИС отсутствуют функции голосового ввода информации и функции воспроизведения информации акустическими средствами ИС, также, акустическое озвучивание защищаемой информации не осуществляется
2.1.2	Угроза утечки видовой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Защищаемая информация	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной в связи с отсутствием АРМ пользователей в данном типе ИС ИОГВ Краснодарского края

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.1.3	Угроза утечки информации по каналу ПЭМИН	Внутренний нарушитель с высоким потенциалом, Внешний нарушитель с высоким потенциалом	Аппаратное обеспечение	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. отсутствуют объективные предпосылки для реализации угроз данного класса, применение подобных средств разведки экономически необоснованно
2.2. Угрозы несанкционированного доступа								
2.2.1	Угроза преодоления физической защиты	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.2	Угроза физического выведения из строя АРМ, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	АРМ	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной в связи с отсутствием АРМ пользователей в данном типе ИС ИОГВ Краснодарского края
2.2.3	Угроза физического выведения из строя серверов и систем хранения данных, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним	Сервер	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		потенциалом						сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.4	Угроза физического выведения из строя средств передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.5	Угроза хищения АРМ, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	АРМ	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной в связи с отсутствием АРМ пользователей в данном типе ИС ИОГВ Краснодарского края
2.2.6	Угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сервер	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данно-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								го типа
2.2.7	Угроза хищения средств передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.8	Угроза хищения носителей информации и мобильных технических средств	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.9	Угроза изменения компонентов системы (аппаратной конфигурации) АРМ	Внутренний нарушитель с низким потенциалом	АРМ	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной в связи с отсутствием АРМ пользователей в данном типе ИС ИОГВ Краснодарского края
2.2.10	Угроза изменения компонентов системы (аппаратной конфигурации) серверов	Внутренний нарушитель с низким потенциалом	Сервер	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.11	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	высокая	средний	средняя	актуальна	Угроза является актуальной в связи с актуальностью категории нарушителей, имеющей потенциальную возможность для реализации угрозы, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.12	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если отсутствует контроль использования аппаратного обеспечения, обладающим функциональными возможностями внеполосного доступа к ним, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.13	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	низкая	средний	средняя	актуальна	Несмотря на то что, может быть реализован контрольно-пропускной и внутриобъектовый режим, исключающий реализацию данной угрозы внешним нарушителем, данная угроза является актуальной, т.к. может быть реализована внутренним нарушителем вследствие его халатности
2.2.14	Угроза подбора пароля	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с	Системное программное обеспечение, прикладное программное обеспечение, микропрограммное	высокая	низкий	высокая	актуальна	Угроза является актуальной в связи с актуальностью категории нарушителей, имеющей потенциальную возможность для реализации угрозы

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		низким потенциалом	обеспечение, учётные данные пользователя, микропрограммное обеспечение BIOS/UEFI.					
2.2.15	Угроза использования уязвимостей используемого ПО	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, информационная система, средство защиты информации	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если на периодической основе не осуществляется анализ используемого ПО на предмет наличия в них уязвимостей с помощью сертифицированного ФСТЭК России средства анализа защищенности, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.16	Угроза наличия недекларированных возможностей в СПО	Внешний нарушитель с высоким потенциалом	Системное программное обеспечение.	маловероятно	низкий	низкая	неактуальна	Актуальность данной угрозы должна определяться для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (топологии), назначения ИС, состава и критичности обрабатываемой в ней информации. В общем случае считается, что данная угроза является не актуальной, т.к. приобретается лицензионное СПО (или используется СПО с открытым кодом), ответственность разработчика которого определена в заключаемых на его поставку гос. контрактах
2.2.17	Угроза наличия недекларированных возможностей в ППО	Внешний нарушитель с высоким потенциалом	Прикладное программное обеспечение.	маловероятно	низкий	низкая	неактуальна	Актуальность данной угрозы должна определяться для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (топологии), назначения ИС, состава и

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								критичности обрабатываемой в ней информации. В общем случае считается, что данная угроза является не актуальной, т.к. приобретается лицензионное СПО (или используется СПО с открытым кодом), ответственность разработчика которого определена в заключаемых на его поставку гос. контрактах
2.2.18	Угроза установки уязвимых версий программного обеспечения	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Программное обеспечение, микропрограммное и аппаратное обеспечение BIOS/UEFI	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие права пользователей на установку программного обеспечения, а также не ограничены возможности внешнего нарушителя посредством применения сертифицированных ФСТЭК России средств межсетевого экранирования, обнаружения вторжений и анализа защищенности, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.19	Угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	высокая	средний	средняя	актуальна	Угроза является актуальной в следующих случаях: - не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа для контроля, устанавливаемого и запускаемого ПО; - контрольно-пропускной и внутриобъектовый режим не обеспечивает ограничение возможностей внешнего нарушителя по допуску

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								их на территорию, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.20	Угроза несанкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение объекты файловой системы АРМ; сетевой узел, сетевой трафик, носитель информации.	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для ограничения установки и запуска приложений не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, а также отсутствуют сертифицированные ФСТЭК России средств обнаружения вторжений и межсетевого экранирования, ограничивающих возможности внешних нарушителей, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.21	Угроза подмены программного обеспечения	Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если пользователи (администраторы) обладают правами для установки программного обеспечения из сети Интернет, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.22	Угроза внедрения вредоносного кода или данных на АРМ пользователей	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, объект файловой системы, виртуаль-	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для защиты АРМ пользователей (администраторов) не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, что возможно для ИС ИОГВ Краснодарского края данного типа

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
			ная машина сервера; сетевой узел					
2.2.23	Угроза внедрения вредоносного кода или данных на серверах	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, сетевой узел, объект файловой системы.	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для защиты серверов ИС не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.24	Угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для антивирусной защиты периметра информационной системы не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, а пользователи (администраторы) ИС не проходят соответствующий инструктаж, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.25	Угроза нарушения функционирования web-приложений	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для защиты web-приложений не применяются специализированные средства межсетевого экранирования типа "Г", сертифицированные по требованиям ФСТЭК России, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.26	Угроза получения сведений об информационной	Внутренний нарушитель с	Сетевой узел, сетевое программ-	средняя	низкий	высокая	актуальна	Угроза является актуальной в связи с актуальностью категории наруши-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	системе	низким потенциалом, Внешний нарушитель с низким потенциалом	ное обеспечение, сетевой трафик, прикладное программное обеспечение					телей, имеющей потенциальную возможность для реализации угрозы
2.2.27	Угроза исследования работы приложения	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в связи с актуальностью категории нарушителей, имеющей потенциальную возможность для реализации угрозы
2.2.28	Угроза несанкционированного копирования защищаемой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	высокая	высокий	высокая	актуальна	Угроза является актуальной в случае, если возможно подключение/использование съёмных носителей информации и не применяются специализированные средства защиты информации для контроля копирования защищаемой информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.29	Угроза несанкционированного восстановления удалённой защищаемой информации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Машинный носитель информации	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для удаления защищаемой информации не используются средства гарантированного уничтожения информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.30	Угроза использования технологий беспроводного доступа	Внутренний нарушитель с низким потенциалом	Сетевой узел, учётные данные пользователя, сетевой трафик, ап-	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если для доступа к ИС применяются технологии беспроводного доступа, что возможно для ИС

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		Внешний нарушитель с низким потенциалом	паратное обеспечение					ИОГВ Краснодарского края данного типа
2.2.31	Угроза несанкционированного доступа к компонентам среды виртуализации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина, сервер, сетевое оборудование, сетевой трафик, виртуальные устройства, гипервизор, виртуальные устройства хранения, обработки и передачи данных, объект файловой системы.	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для защиты сред виртуализации не применяются сертифицированные ФСТЭК России средства защиты сред виртуализации, что возможно для ИС данного типа
2.2.32	Угроза приведения системы в состояние «отказ в обслуживании»	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если не применяются сертифицированные ФСТЭК межсетевого экранирования, и не осуществляется мониторинг и анализ инцидентов, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.33	Угроза реализации атаки "человек посередине" при передаче информации в пределах контролируемой зоны	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабо-	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если в ЛВС не применяются сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений, позволяющие нейтрализовать дан-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
			чая станция, сервер, информация, хранящаяся на компьютере во временных файлах (программное обеспечение)					ную угрозу и (или) доступ посторонних лиц в помещения не ограничен, что возможно для ИС ИОГВ Краснодарского края данного типа.
2.2.34	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер.	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если при передаче защищаемой информации за пределы КЗ не применяются сертифицированные ФСБ России средства криптографической защиты информации, передаваемой по каналам связи, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.35	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Внешний нарушитель со средним потенциалом	Аутентификационные данные пользователя (программное обеспечение)	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если порядок использования браузеров при доступе к компонентам ИС - не регламентирован, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.36	Угроза наличия ошибок в ходе проектирования, разработки и отладки системы	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры	средняя	средний	средняя	актуальна	Угроза является актуальной в следующих случаях: - если в договорах на проектирование, разработку и отладку систем (между поставщиком вычислительных мощностей и его контрагентами) не закрепляется ответственность Поставщиков услуг - для проведения работ по защите информации привлекаются только организации, имеющей соответствующие лицензии ФСТЭК России и ФСБ России - ИС вводятся в эксплуатацию без

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								их тестирования и аттестации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.37	Угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если в договорах на ремонт и обслуживание оборудования (между поставщиком вычислительных мощностей и его контрагентами) не закрепляется ответственность Поставщиков услуг, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.38	Угроза слабости механизмов контроля входных данных	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр, аппаратное обеспечение, метаданные.	средняя	средний	средняя	актуальна	Угроза является актуальной в следующих случаях: - не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие возможности нарушителей по доступу к программным компонентам информационных систем, а также контролирующие функционирование программ; - возможности внешнего нарушителя не ограничены посредством использования сертифицированных ФСТЭК России средства обнаружения вторжений и межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.39	Угроза слабости или некорректной настройки механизмов контроля целостности и резервирования данных	Внутренний нарушитель с низким потенциалом, Внешний	Системное программное обеспечение, прикладное программное обеспечение, мик-	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для контроля целостности не применяются средства защиты информации от несанкционированного доступа, сертифицированные

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		нарушитель с низким потенциалом	ропрограммное обеспечение, метаданные, объекты файловой системы, реестр					по требованиям ФСТЭК России и (или) средства резервного копирования информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.40	Угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для фильтрации сетевого трафика не применяются сертифицированные ФСТЭК России средства межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.41	Угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, учётные данные пользователя, реестр, машинные носители информации, метаданные, микропрограммное обеспечение, средство защиты информации	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для разграничения доступа к защищаемой информации не применяются сертифицированные ФСТЭК России средств защиты информации от несанкционированного доступа, что возможно для данного типа ИС ИОГВ Краснодарского края
2.2.42	Угроза анализа криптографических алгоритмов и их реализации	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если применяются средства криптографической защиты информации, не сертифицированные по

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								требованиям ФСБ России, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.43	Угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информации	Внешний нарушитель с низким потенциалом	Средство защиты информации, аппаратное устройство, программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной, в случае, если этапу внедрение средств защиты информации не предшествует этап проектирования системы защиты информации, учитывающее особенности функционирования ИС, а ее настройка осуществляется лицензиатами ФСТЭК России, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.44	Угроза несанкционированного воздействия на средство защиты информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Средство защиты информации	средняя	средний	средняя	актуальна	Угроза является актуальной, в случае если ИС не оснащены необходимыми сертифицированными ФСТЭК России средствами защиты информации, которые осуществляются: тестирование собственных функций, а также ограничение возможности по воздействие на сами средства защиты (комплексом применяемых средств защиты информации), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.45	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Средство защиты информации	средняя	средний	высокая	актуальна	Угроза является актуальной, в случае если возможность изменения настроек средств защиты информации не ограничена их функционалом, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.46	Угроза проникновения из смежных ИС с более низ-	Внутренний нарушитель с	Информационная система	средняя	средний	средняя	актуальна	Угроза является актуальной в случае отсутствия сегментирования

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	ким уровнем защищенности	низким потенциалом, Внешний нарушитель со средним потенциалом						ЛВС (в составе которой имеются ИС различных уровней защищенности) сертифицированными ФСТЭК России средствами межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа

Таблица 23 – Актуальность угроз безопасности информации ИС ИОГВ Краснодарского края 3 типа

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
1. Угрозы, не являющиеся атаками								
1.1. Угрозы, не связанные с деятельностью человека								
1.1.1	Угроза стихийных бедствий и природных явлений	-	Информационная система	низкая	средний	средняя	актуальна	Угроза является актуальной в случае отсутствия средств обеспечения отказоустойчивости, что характерно для данного типа ИС ИОГВ Краснодарского края
1.2. Угрозы социально–политического характера								
1.2.1	Угрозы социально–политического характера	-	Информационная система	низкая	средний	средняя	актуальна	Угроза является актуальной в случае отсутствия средств обеспечения отказоустойчивости, что характерно для данного типа ИС ИОГВ Краснодарского края
1.3. Угрозы техногенного характера								
1.3.1	Угроза отказа электропитания серверного и телекоммуникационного оборудования	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Линии и средства электропитания	низкая	средний	средняя	актуальна	Несмотря на наличие ИБП, применяемых для обеспечения бесперебойного электропитания серверного и телекоммуникационного оборудования, угроза является актуальной в случае отсутствия ДГУ (в случае длительного отсутствия электропитания будет нарушена доступность ИС), что возможно для

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								данного типа ИС ИОГВ Краснодарского края
1.3.2	Угроза отказа электропитания АРМ пользователей	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Линии и средства электропитания	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если не все АРМ оснащены ИБП, что возможно для данного типа ИС ИОГВ Краснодарского края
1.3.3	Угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в серверных помещениях, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной в связи с использованием систем кондиционирования в серверных помещениях, а также ограничением физического доступа к ним потенциальных нарушителей
1.4. Ошибочные действия								
1.4.1	Угроза разглашения конфиденциальной информации пользователями ИС	Внутренний нарушитель с низким потенциалом	Защищаемая информация	низкая	средний	средняя	актуальна	Несмотря на то, что ответственность пользователей закреплена в ОРД (при поступлении на работу), угроза является актуальной, в случае если на периодической основе не осуществляет обучение и повышении квалификации пользовате-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								лей по вопросам обеспечения информационной безопасности, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.2	Угроза разглашения конфиденциальной информации сотрудниками подрядных организаций	Внутренний нарушитель с средним потенциалом	Защищаемая информация	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. подрядные организации относятся к неактуальным категориям потенциальных нарушителей для данного типа ИС ИОГВ Краснодарского края (требования о неразглашении конфиденциальной информации подрядными организациями закрепляются в заключаемых государственных контрактах)
1.4.3	Угроза утраты мобильных технических средств пользователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации	Внутренний нарушитель с низким потенциалом	Мобильное техническое средство	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если процедуры контроля использования мобильных технических средств не регламентированы в ОРД и не реализованы, обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности не осуществляется, что возможно для ИС ИОГВ Краснодарского края данного типа.
1.4.4	Угроза передача носителей информации лицам, не имеющих права доступа к хранимой на них информации	Внутренний нарушитель с низким потенциалом	Носитель информации	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если процедуры контроля использования носителей информации не регламентированы в ОРД и не реализованы, обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности не осуществляется, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.5	Угроза утраты носителей	Внутренний	Носитель инфор-	высокая	средний	средняя	актуальна	Угроза является актуальной в сле-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	информации	нарушитель с низким потенциалом	мации					дующих случаях: - процедуры контроля использования носителей информации не регламентированы в ОРД и не реализованы; - в случае выноса носителей информации за пределы КЗ, информация на нах не шифруется, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.6	Угроза физического устаревания аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач	Внутренний нарушитель с низким потенциалом	Аппаратное средство, система хранения данных	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если в ОРД не определён жизненный цикл компонентов ИС и порядок вывода их из эксплуатации, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.7	Угроза некорректной настройки программного обеспечения	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр.	средняя	средний	средняя	актуальна	Несмотря на неактуальность для данного типа ИС ИОГВ Краснодарского края в качестве потенциальных нарушителей администраторов ИС/ИБ - данная угроза является неактуальной, т.к. возможна некорректная настройка программного обеспечения (ввиду недостаточной компетенции сотрудников (необходимо проведение обучение сотрудников по вопросам установки и администрирования настраиваемых категорий ПО), что может привести к возможности реализации данной угрозы внешним нарушителем. Также, данная угроза является актуальной в случае, если на периодической основе не осуществляться сканирование сертифицированными ФСТЭК России средствами анализа защищённости компонентов

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								ИС на предмет некорректных настроек ПО, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.8	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Средства защиты информации, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	средняя	средний	средняя	актуальна	Несмотря на неактуальность для данного типа ИС ИОГВ Краснодарского края в качестве потенциальных нарушителей администраторов ИС/ИБ – данная, угроза является актуальной, т.к. возможны ситуации, когда после ввода в эксплуатацию ПО и (или) оборудования не осуществляется изменение пароля, заданного по умолчанию (вследствие халатности сотрудников), что может в последующем привести к реализации несанкционированного доступа как внутренними, так и внешними нарушителями. Также, данная угроза является актуальной в случае, если на периодической основе не осуществляется сканирование компонентов ИС на предмет наличия заданной по умолчанию идентификационной/аутентификационной информации сертифицированными ФСТЭК России средствами анализа защищенности, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.9	Угроза незащищённого удалённого администрирования информационной системы	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с	Информационная система, сервер, рабочая станция, сетевое программное обеспечение	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если на АРМ и серверах имеются средства удалённого администрирования, аутентификационная информация которых может быть перехвачена нарушителем при до-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		низким потенциалом						ступе к ИС из-за пределов КЗ (при осуществлении удалённого администрирования без использования средств криптографической защиты информации (в данном случае аутентификационной), передаваемой по каналам связи), что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.10	Угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу)	Внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. для данного типа ИС ИОГВ Краснодарского края вычислительные мощности (уполномоченного лица) не применяются
1.4.11	Угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом)	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Информационная система, сервер, носитель информации, метаданные, объекты файловой системы, системное программное обеспечение, аппаратное обеспечение, канал связи	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. для данного типа ИС ИОГВ Краснодарского края вычислительные мощности (уполномоченного лица) не применяются
1.4.12	Угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей)	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким по-	Системное программное обеспечение	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. для данного типа ИС ИОГВ Краснодарского края вычислительные мощности (уполномоченного лица) не применяются

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		тенциалом						
1.4.13	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Внутренний нарушитель со средним потенциалом	Мобильное устройство	высокая	средний	высокая	актуальна	Данная угроза является актуальной в связи с использованием личных мобильных устройств пользователей (незащищённых сертифицированными ФСТЭК России средствами защиты информации от НСД, средств антивирусной защиты информации и сертифицированными ФСБ России средствами криптографической защиты информации, передаваемой по каналам связи) в рабочих целях, в т.ч. для доступа к определённому количеству защищаемой информации (например, посредством электронной почты)
2. Угрозы, являющиеся атаками								
2.1. Угрозы утечки информации по техническим каналам								
2.1.1	Угроза утечки акустической информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Защищаемая информация, аппаратное обеспечение	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, в случае если отсутствуют функции голосового ввода информации и функции воспроизведения информации акустическими средствами ИС, также, акустическое озвучивание защищаемой информации не осуществляется, что характерно для данного типа ИС ИОГВ Краснодарского края
2.1.2	Угроза утечки видовой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Защищаемая информация	высокая	средний	средняя	актуальна	Угроза является актуальной, в случае если устройства отображения информации не размещены таким образом, который исключает несанкционированный просмотр защищаемой информации, что характерно для данного типа ИС ИОГВ Краснодарского края

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.1.3	Угроза утечки информации по каналу ПЭМИН	Внутренний нарушитель с высоким потенциалом, Внешний нарушитель с высоким потенциалом	Аппаратное обеспечение	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. отсутствуют объективные предпосылки для реализации угроз данного класса (применение подобных средств разведки экономически необоснованно) и неактуальностью категорий нарушителя, чей потенциал позволяет реализовать данную угрозу
2.2. Угрозы несанкционированного доступа								
2.2.1	Угроза преодоления физической защиты	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.2	Угроза физического выведения из строя АРМ, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	АРМ	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.3	Угроза физического выведения из строя серверов и	Внутренний нарушитель с	Сервер	высокая	средний	низкая	актуальна	Угроза является актуальной в случае, если доступ в серверные по-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	систем хранения данных, обрабатывающих защищаемую информацию	низким потенциалом, Внешний нарушитель со средним потенциалом						мещения для потенциальных нарушителей не ограничен контрольно-пропускным и внутриобъектовым режимом, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.4	Угроза физического выведения из строя средств передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.5	Угроза хищения АРМ, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	АРМ	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.6	Угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель	Сервер	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудо-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		со средним потенциалом						ваны надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.7	Угроза хищения средств передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.8	Угроза хищения носителей информации и мобильных технических средств	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.9	Угроза изменения компонентов системы (аппаратной конфигурации) АРМ	Внутренний нарушитель с низким потенциалом	АРМ	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если не осуществляется контроль вскрытия системных блоков АРМ и контроль их аппаратной конфигурации, что возможно для ИС ИОГВ Краснодарского края

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								данного типа
2.2.10	Угроза изменения компонентов системы (аппаратной конфигурации) серверов	Внутренний нарушитель с низким потенциалом	Сервер	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если доступ в серверные помещения для потенциальных нарушителей не ограничен контрольно-пропускным и внутриобъектовым режимом, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.11	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	средняя	средний	средняя	актуальна	Несмотря на то, что категории внутренних нарушителей, чей потенциал позволяет реализовать данную угрозу - не являются актуальными для данного типа ИС ИОГВ Краснодарского края, угроза является неактуальной в случае, если для нейтрализации возможностей внешних нарушителей по реализации данной угрозы не используются сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.12	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. нарушитель, чей потенциал позволяет реализовать данную угрозу, является неактуальным для данного типа ИС ИОГВ Краснодарского края
2.2.13	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внутренний нарушитель с низким потенциалом, Внешний	Системное программное обеспечение, прикладное программное обеспечение, ап-	средняя	средний	высокая	актуальна	Несмотря на то что, может быть реализован контрольно-пропускной и внутриобъектовый режим, исключающий реализацию данной угрозы внешним нарушителем,

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		нарушитель с низким потенциалом	паратное обеспечение					данная угроза является актуальной, т.к. может быть реализована внутренним нарушителем вследствие его халатности
2.2.14	Угроза подбора пароля	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя, микропрограммное обеспечение BIOS/UEFI.	высокая	низкий	высокая	актуальна	Угроза является актуальной, т.к. используемые средства и меры защиты информации не позволяют нейтрализовать угрозу подбора пароля
2.2.15	Угроза использования уязвимостей используемого ПО	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, информационная система, средство защиты информации	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если на периодической основе не осуществляется анализ используемого ПО на предмет наличия в них уязвимостей с помощью сертифицированного ФСТЭК России средства анализа защищенности, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.16	Угроза наличия недекларированных возможностей в СПО	Внешний нарушитель с высоким потенциалом	Системное программное обеспечение.	маловероятно	низкий	низкая	неактуальна	Актуальность данной угрозы должна определяться для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (топологии), назначения ИС, состава и критичности обрабатываемой в ней информации. В общем случае считается, что данная угроза является не актуальной, т.к. приобретается

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								лицензионное СПО (или используется СПО с открытым кодом), ответственность разработчика которого определена в заключаемых на его поставку государственных контрактах
2.2.17	Угроза наличия недекларированных возможностей в ППО	Внешний нарушитель с высоким потенциалом	Прикладное программное обеспечение.	маловероятно	низкий	низкая	неактуальна	Актуальность данной угрозы должна определяться для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (топологии), назначения ИС, состава и критичности обрабатываемой в ней информации. В общем случае считается, что данная угроза является не актуальной, т.к. приобретается лицензионное ППО (или используется ППО с открытым кодом), ответственность разработчика которого определена в заключаемых на его поставку и (или) разработку государственных контрактах
2.2.18	Угроза установки уязвимых версий программного обеспечения	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Программное обеспечение, микропрограммное и аппаратное обеспечение BIOS/UEFI	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие права пользователей на установку программного обеспечения, а также не ограничены возможности внешнего нарушителя посредством применения сертифицированных ФСТЭК России средств межсетевого экранирования, обнаружения вторжений и анализа защищенности, что возможно для ИС ИОГВ Краснодарского края данного типа

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.2.19	Угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	высокая	средний	средняя	актуальна	Угроза является актуальной в следующих случаях: - не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа для контроля, устанавливаемого и запускаемого ПО; - контрольно-пропускной и внутриобъектовый режим не обеспечивает ограничение возможностей внешнего нарушителя по допуску их на территорию; - не осуществляется контроль вскрытия системных блоков АРМ пользователей, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.20	Угроза несанкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение объекты файловой системы АРМ; сетевой узел, сетевой трафик, носитель информации.	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для ограничения установки и запуска приложений не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, а также отсутствуют сертифицированные ФСТЭК России средств обнаружения вторжений и межсетевого экранирования, ограничивающих возможности внешних нарушителей, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.21	Угроза подмены программного обеспечения	Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, си-	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если пользователи обладают правами для установки программного обеспечения из сети Интернет, что возможно для ИС ИОГВ Крас-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
			стемное программное обеспечение					нодарского края данного типа
2.2.22	Угроза внедрения вредоносного кода или данных на АРМ пользователей	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, объект файловой системы, виртуальная машина сервера; сетевой узел	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для защиты АРМ пользователей не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.23	Угроза внедрения вредоносного кода или данных на серверах	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, сетевой узел, объект файловой системы.	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для защиты серверов ИС не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.24	Угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для антивирусной защиты периметра информационной системы не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, а пользователи ИС не проходят соответствующий инструктаж, что возможно для ИС ИОГВ Красно-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								дарского края данного типа
2.2.25	Угроза нарушения функционирования web-приложений	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае расположения в данном типе ИС серверов, на которых функционируют web-приложений и отсутствуют специализированные средства межсетевого экранирования типа "Г", сертифицированные по требованиям ФСТЭК России, что возможно для ИС ИОГВ Краснодарского края данного типа.
2.2.26	Угроза получения сведений об информационной системе	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	средняя	низкий	высокая	актуальна	Угроза является актуальной в случае, если используемые средства защиты информации не позволяют нейтрализовать угрозы сканирования информационных систем
2.2.27	Угроза исследования работы приложения	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	средняя	средний	средняя	актуальна	Несмотря неактуальность внутренних категорий нарушителей способных реализовать данную угроз, угроза является актуальной для информационных систем, доступных из сети Интернет
2.2.28	Угроза несанкционированного копирования защищаемой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	высокая	высокий	высокая	актуальна	Угроза является актуальной, т.к. в ИС возможно подключение/использование съёмных носителей информации и не применяются специализированные средства защиты информации для контроля копирования защищаемой информации

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.2.29	Угроза несанкционированного восстановления удалённой защищаемой информации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Машинный носитель информации	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для удаления защищаемой информации не используются средства гарантированного уничтожения информации
2.2.30	Угроза использования технологий беспроводного доступа	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если для доступа пользователей к ИС применяются технологии беспроводного доступа, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.31	Угроза несанкционированного доступа к компонентам среды виртуализации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина, сервер, сетевое оборудование, сетевой трафик, виртуальные устройства, гипервизор, виртуальные устройства хранения, обработки и передачи данных, объект файловой системы.	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если не применяются сертифицированные ФСТЭК России средства защиты сред виртуализации (при их наличии), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.32	Угроза приведения системы в состояние «отказ в обслуживании»	Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если не применяются сертифицированные ФСТЭК России средства обнаружения вторжений и

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		Внешний нарушитель с низким потенциалом	обеспечение, сетевое программное обеспечение, сетевой трафик					межсетевого экранирования, и не осуществляется мониторинг и анализ инцидентов, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.33	Угроза реализации атаки "человек посередине" при передаче информации в пределах контролируемой зоны	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер, информация, хранящаяся на компьютере во временных файлах (программное обеспечение)	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если в ЛВС не применяются сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений, позволяющие нейтрализовать данную угрозу, а также доступ посторонних лиц в помещения не ограничен, что возможно для ИС ИОГВ Краснодарского края данного типа.
2.2.34	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер.	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если при передаче защищаемой информации за пределы КЗ не применяются сертифицированные ФСБ России средства криптографической защиты информации, передаваемой по каналам связи, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.35	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Внешний нарушитель со средним потенциалом	Аутентификационные данные пользователя (программное обеспечение)	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если порядок использования браузеров при доступе к компонентам ИС - не регламентирован, а также используются соответствующий функционал браузеров, что возможно для ИС ИОГВ Краснодарского края данного типа

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.2.36	Угроза наличия ошибок в ходе проектирования, разработки и отладки системы	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры	средняя	средний	средняя	актуальна	Несмотря на неактуальности для данного типа ИС ИОГВ Краснодарского края данной категории потенциальных нарушителей (в государственных контракта на проектирование, разработку и отладку систем закрепляется ответственность Поставщиков услуг и то, то для проведения работ по защите информации привлекаются только организации, имеющие соответствующие лицензии ФСТЭК России и ФСБ России), угроза является актуальной, т.к. возможно фактическое введение ИС в эксплуатацию без их тестирования и аттестации Угроза является неактуальной ввиду неактуальности для данного типа ИС ИОГВ Краснодарского края данной категории потенциальных нарушителей (в государственных контрактах на ремонт и обслуживания оборудования закрепляется ответственность Поставщиков услуг)
2.2.37	Угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	низкая	низкий	средняя	неактуальна	Угроза является неактуальной ввиду неактуальности для данного типа ИС ИОГВ Краснодарского края данной категории потенциальных нарушителей (в государственных контрактах на ремонт и обслуживания оборудования закрепляется ответственность Поставщиков услуг)
2.2.38	Угроза слабости механизмов контроля входных данных	Внутренний нарушитель с низким по-	Сетевой узел, объекты файловой системы, приклад-	средняя	средний	средняя	актуальна	Угроза является актуальной в следующих случаях: - не применяются сертифицирован-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		тенциалом, Внешний нарушитель с низким потенциалом	ное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр, аппаратное обеспечение, метаданные.					ные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие возможности нарушителей по доступу к программным компонентам информационных систем, а также контролирующие функционирование программ; - возможности внешнего нарушителя не ограничены посредством использования сертифицированных ФСТЭК России средства обнаружения вторжений и межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.39	Угроза слабости или некорректной настройки механизмов контроля целостности и резервирования данных	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если для контроля целостности не применяются средства защиты информации от несанкционированного доступа, сертифицированные по требованиям ФСТЭК России и (или) средства резервного копирования информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.40	Угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для фильтрации сетевого трафика не применяются сертифицированные ФСТЭК России средств межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.41	Угроза слабости или некорректной настройки ме-	Внутренний нарушитель с	Объекты файловой системы, приклад-	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если для разграничения досту-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	ханизмов контроля и разграничения доступа к защищаемой информации	низким потенциалом, Внешний нарушитель с низким потенциалом	ное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, учётные данные пользователя, реестр, машинные носители информации, метаданные, микропрограммное обеспечение, средство защиты информации					па к защищаемой информации не применяются сертифицированные ФСТЭК России средств защиты информации от несанкционированного доступа, что возможно для данного типа ИС ИОГВ Краснодарского края
2.2.42	Угроза анализа криптографических алгоритмов и их реализации	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если применяются средства криптографической защиты информации, несертифицированные по требованиям ФСБ России, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.43	Угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информации	Внешний нарушитель с низким потенциалом	Средство защиты информации, аппаратное устройство, программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной, в случае, если этапу внедрение средств защиты информации не предшествует этап проектирования системы защиты информации, учитывающее особенности функционирования ИС, а ее настройка осуществляется лицензиатами ФСТЭК России, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.44	Угроза несанкционированного воздействия на средство защиты инфор-	Внешний нарушитель со средним	Средство защиты информации	средняя	средний	средняя	актуальна	Угроза является актуальной, в случае если ИС не оснащены необходимыми сертифицированными

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	мации	потенциалом, Внутренний нарушитель со средним потенциалом						ФСТЭК России средствами защиты информации, которые осуществляются: тестирование собственных функций, а также ограничение возможности по воздействие на сами средства защиты (комплексом применяемых средств защиты информации), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.45	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Средство защиты информации	средняя	средний	высокая	актуальна	Угроза является актуальной, в случае если возможность изменения настроек средств защиты информации не ограничена их функционалом, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.46	Угроза проникновения из смежных ИС с более низким уровнем защищенности	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Информационная система	средняя	средний	средняя	актуальна	Угроза является актуальной в случае отсутствия сегментирования ЛВС (в составе которой имеются ИС различных уровней защищенности) сертифицированными ФСТЭК России средствами межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа

Таблица 24 – Актуальность угроз безопасности информации ИС ИОГВ Краснодарского края 4 типа

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
1. Угрозы, не являющиеся атаками								
1.1. Угрозы, не связанные с деятельностью человека								
1.1.1	Угроза стихийных бедствий и природных явлений	-	Информационная система	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. в случае возможности реализации данной угрозы отсутствуют значительные негативные последствия
1.2. Угрозы социально–политического характера								
1.2.1	Угрозы социально–политического характера	-	Информационная система	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. в случае возможности реализации данной угрозы отсутствуют значительные негативные последствия
1.3. Угрозы техногенного характера								
1.3.1	Угроза отказа электропитания серверного и телекоммуникационного оборудования	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Линии и средства электропитания	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если не применяются ИБП для обеспечения бесперебойного электропитания телекоммуникационного оборудования, что возможно для данного типа ИС ИОГВ Краснодарского края
1.3.2	Угроза отказа электропитания АРМ пользователей	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Линии и средства электропитания	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если не все АРМ оснащены ИБП, что возможно для данного типа ИС ИОГВ Краснодарского края
1.3.3	Угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования	Внутренний нарушитель с низким потенциалом, Внешний нарушитель	Технические средства воздушного кондиционирования, включая трубопроводные системы для цирку-	низкая	средний	средняя	актуальна	Угроза является актуальной, в случае если в помещениях размещения телекоммуникационного оборудования отсутствуют системы кондиционирования и (или) доступ внешних нарушителей к данным поме-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		со средним потенциалом	ляции охлаждённого воздуха в серверных помещениях, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля					щениям не ограничен контрольно-пропускным и внутриобъектовым режимом
1.4. Ошибочные действия								
1.4.1	Угроза разглашения конфиденциальной информации пользователями ИС	Внутренний нарушитель с низким потенциалом	Защищаемая информация	низкая	средний	средняя	актуальна	Несмотря на то, что ответственность пользователей закреплена в ОРД (при поступлении на работу), угроза является актуальной, в случае если на периодической основе не осуществляет обучение и повышении квалификации пользователей по вопросам обеспечения информационной безопасности, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.2	Угроза разглашения конфиденциальной информации сотрудниками подрядных организаций	Внутренний нарушитель с средним потенциалом	Защищаемая информация	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. подрядные организации относятся к неактуальным категориям потенциальных нарушителей для данного типа ИС ИОГВ Краснодарского края (требования о неразглашении конфиденциальной информации подрядными организациями закрепляются в заключаемых государственных контрактах)
1.4.3	Угроза утраты мобильных технических средств поль-	Внутренний нарушитель с	Мобильное техническое средство	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если процедуры контроля ис-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	зователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации	низким потенциалом						пользования мобильных технических средств не регламентированы в ОРД и не реализованы, обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности не осуществляется, что возможно для ИС ИОГВ Краснодарского края данного типа.
1.4.4	Угроза передача носителей информации лицам, не имеющих права доступа к хранимой на них информации	Внутренний нарушитель с низким потенциалом	Носитель информации	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если процедуры контроля использования носителей информации не регламентированы в ОРД и не реализованы, обучение и повышение осведомлённости сотрудников по вопросам информационной безопасности не осуществляется, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.5	Угроза утраты носителей информации	Внутренний нарушитель с низким потенциалом	Носитель информации	высокая	средний	средняя	актуальна	Угроза является актуальной в следующих случаях: - процедуры контроля использования носителей информации не регламентированы в ОРД и не реализованы; - в случае выноса носителей информации за пределы КЗ, информация на нах не шифруется, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.6	Угроза физического устаревания аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач	Внутренний нарушитель с низким потенциалом	Аппаратное средство, система хранения данных	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если в ОРД не определён жизненный цикл компонентов ИС и порядок вывода их из эксплуатации, что возможно для ИС ИОГВ Краснодарского края данного типа

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
1.4.7	Угроза некорректной настройки программного обеспечения	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр.	средняя	средний	средняя	актуальна	Несмотря на неактуальность для данного типа ИС ИОГВ Краснодарского края в качестве потенциальных нарушителей администраторов ИС/ИБ - данная угроза является актуальной, т.к. возможна некорректная настройка программного обеспечения (ввиду недостаточной компетенции сотрудников (необходимо проведение обучение сотрудников по вопросам установки и администрирования настраиваемых категорий ПО), может привести к возможности реализации данной угрозы внешним нарушителем. Также, данная угроза является актуальной в случае, если на периодической основе не осуществляться сканирование сертифицированными ФСТЭК России средствами анализа защищённости компонентов ИС на предмет некорректных настроек ПО, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.8	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Средства защиты информации, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные сред-	средняя	средний	средняя	актуальна	Несмотря на неактуальность для данного типа ИС ИОГВ Краснодарского края в качестве потенциальных нарушителей администраторов ИС/ИБ - данная угроза является актуальной, т.к. возможны ситуации, когда после ввода в эксплуатацию ПО и (или) оборудования не осуществляется изменение пароля, заданного по умолчанию (вследствие халатности сотрудников), что может в последующем привести к реализации несанкционированного

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
			ства со встроенными функциями защиты					доступа как внутренними, так и внешними нарушителями. Также, данная угроза является актуальной в случае, если на периодической основе не осуществляется сканирование компонентов ИС на предмет наличия заданной по умолчанию идентификационной/аутентификационной информации сертифицированными ФСТЭК России средствами анализа защищенности, что возможно для ИС ИОГВ Краснодарского края данного типа
1.4.9	Угроза незащищённого удалённого администрирования информационной системы	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Информационная система, сервер, рабочая станция, сетевое программное обеспечение	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. в данном типе ИС ИОГВ Краснодарского края отсутствуют серверные сегменты ИС
1.4.10	Угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу)	Внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы	средняя	средний	средняя	актуальна	Угроза является актуальной, если в качестве уполномоченного лица, предоставляющие вычислительные мощности, выступает не Департамент информатизации и связи Краснодарского края
1.4.11	Угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом)	Внутренний нарушитель с низким потенциалом, Внешний	Информационная система, сервер, носитель информации, метаданные, объекты фай-	высокая	средний	высокая	актуальна	Угроза является актуальной, если в качестве уполномоченного лица, предоставляющие вычислительные мощности, выступает не Департамент информатизации и связи

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		нарушитель с низким потенциалом	ловой системы, системное программное обеспечение, аппаратное обеспечение, канал связи					Краснодарского края
1.4.12	Угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей)	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной, если в качестве уполномоченного лица, предоставляющие вычислительные мощности, выступает не Департамент информатизации и связи Краснодарского края
1.4.13	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Внутренний нарушитель со средним потенциалом	Мобильное устройство	высокая	средний	средняя	актуальна	Данная угроза является актуальной в связи с использованием личных мобильных устройств пользователей (незащищённых сертифицированными ФСТЭК России средствами защиты информации от НСД, средств антивирусной защиты информации и сертифицированными ФСБ России средствами криптографической защиты информации, передаваемой по каналам связи) в рабочих целях, в т.ч. для доступа к определённому количеству защищаемой информации (например, посредством электронной почты)
2. Угрозы, являющиеся атаками								
2.1. Угрозы утечки информации по техническим каналам								
2.1.1	Угроза утечки акустической информации	Внутренний нарушитель с низким потенциалом, Внешний	Защищаемая информация, аппаратное обеспечение	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, в случае если отсутствуют функции голосового ввода информации и функции воспроизведения информации акустическими средствами

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		нарушитель с низким потенциалом						ИС, также, акустическое озвучивание защищаемой информации не осуществляется, что характерно для данного типа ИС ИОГВ Краснодарского края
2.1.2	Угроза утечки видовой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Защищаемая информация	низкая	средний	средняя	актуальна	Угроза является актуальной, в случае если устройства отображения информации размещены таким образом, который не исключает несанкционированный просмотр защищаемой информации, что характерно для данного типа ИС ИОГВ Краснодарского края
2.1.3	Угроза утечки информации по каналу ПЭМИН	Внутренний нарушитель с высоким потенциалом, Внешний нарушитель с высоким потенциалом	Аппаратное обеспечение	низкая	низкий	средняя	неактуальна	Угроза является неактуальной, т.к. отсутствуют объективные предпосылки для реализации угроз данного класса (применение подобных средств разведки экономически необоснованно) и неактуальностью категорий нарушителя, чей потенциал позволяет реализовать данную угрозу
2.2. Угрозы несанкционированного доступа								
2.2.1	Угроза преодоления физической защиты	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.2	Угроза физического выве-	Внутренний	АРМ	высокая	средний	высокая	актуальна	Угроза является актуальной в слу-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	дения из строя АРМ, обрабатывающих защищаемую информацию	нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом						чае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.3	Угроза физического выведения из строя серверов и систем хранения данных, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сервер	маловероятно	средний	низкая	неактуальна	Угроза является неактуальной, т.к. в данном типе ИС ИОГВ Краснодарского края отсутствуют сервера и системы хранения данных
2.2.4	Угроза физического выведения из строя средств передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.5	Угроза хищения АРМ, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний	АРМ	высокая	средний	высокая	актуальна	Угроза является актуальной, в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: по-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		нарушитель со средним потенциалом						мещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.6	Угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сервер	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. в данном типе ИС ИОГВ Краснодарского края отсутствуют сервера и системы хранения данных
2.2.7	Угроза хищения средств передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.8	Угроза хищения носителей информации и мобильных технических средств	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если реализованный контрольно-пропускной и внутриобъектовый режим не обеспечивает нейтрализацию данной угрозы (например: помещения не оборудованы надёжными дверьми, СКУД, охранной сигнализацией и системой видеонаблюдения, не ведётся журнал учёта

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								посетителей), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.9	Угроза изменения компонентов системы (аппаратной конфигурации) АРМ	Внутренний нарушитель с низким потенциалом	АРМ	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если не осуществляется контроль вскрытия системных блоков АРМ и контроль их аппаратной конфигурации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.10	Угроза изменения компонентов системы (аппаратной конфигурации) серверов	Внутренний нарушитель с низким потенциалом	Сервер	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. в данном типе ИС ИОГВ Краснодарского края отсутствуют сервера и системы хранения данных
2.2.11	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	низкая	средний	средняя	актуальна	Несмотря на то, что категории внутренних нарушителей, чей потенциал позволяет реализовать данную угрозу - не являются актуальными для данного типа ИС ИОГВ Краснодарского края, угроза является неактуальной в случае, если для нейтрализации возможностей внешних нарушителей по реализации данной угрозы не используются сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.12	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. нарушитель, чей потенциал позволяет реализовать данную угрозу, является неактуальным для данного типа ИС ИОГВ Краснодарского края

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
2.2.13	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	высокая	средний	высокая	актуальна	Несмотря на то что может быть реализован контрольно-пропускной и внутриобъектовый режим, исключающий реализацию данной угрозы внешним нарушителем, данная угроза является актуальной, т.к. может быть реализована внутренним нарушителем вследствие его халатности
2.2.14	Угроза подбора пароля	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя, микропрограммное обеспечение BIOS/UEFI.	высокая	низкий	высокая	актуальна	Угроза является актуальной, т.к. используемые средства и меры защиты информации не позволяют нейтрализовать угрозу подбора пароля
2.2.15	Угроза использования уязвимостей используемого ПО	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, информационная система, средство защиты информации	низкая	средний	средняя	актуальна	Угроза является актуальной в случае, если на периодической основе не осуществляется анализ используемого ПО на предмет наличия в них уязвимостей с помощью сертифицированного ФСТЭК России средства анализа защищенности, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.16	Угроза наличия недекларированных возможностей в СПО	Внешний нарушитель с высоким потенциалом	Системное программное обеспечение.	маловероятно	низкий	низкая	неактуальна	Актуальность данной угрозы должна определяться для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (то-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								пологии), назначения ИС, состава и критичности обрабатываемой в ней информации. В общем случае считается, что данная угроза является не актуальной, т.к. приобретается лицензионное СПО (или используется СПО с открытым кодом), ответственность разработчика которого определена в заключаемых на его поставку гос. контрактах
2.2.17	Угроза наличия недекларированных возможностей в ППО	Внешний нарушитель с высоким потенциалом	Прикладное программное обеспечение.	маловероятно	низкий	низкая	неактуальна	Актуальность данной угрозы должна определяться для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (топологии), назначения ИС, состава и критичности обрабатываемой в ней информации. В общем случае считается, что данная угроза является не актуальной, т.к. приобретается лицензионное ППО (или используется ППО с открытым кодом), ответственность разработчика которого определена в заключаемых на его поставку и (или) разработку гос. контрактах
2.2.18	Угроза установки уязвимых версий программного обеспечения	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Программное обеспечение, микропрограммное и аппаратное обеспечение BIOS/UEFI	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие права пользователей на установку программного обеспечения, а также не ограничены возможности внешнего нарушителя посредством применения сертифицированных ФСТЭК России средств межсетевого экранирова-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								ния, обнаружения вторжений и анализа защищенности, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.19	Угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	высокая	средний	высокая	актуальна	Угроза является актуальной в следующих случаях: - не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа для контроля устанавливаемого и запускаемого ПО; - контрольно-пропускной и внутриобъектовый режим не обеспечивает ограничение возможностей внешнего нарушителя по допуску их на территорию; - не осуществляется контроль вскрытия системных блоков АРМ пользователей, что возможно для ИС ИОГВ Краснодарского края данного типа Угроза является актуальной в случае, если для ограничения установки и запуска приложений не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, а также отсутствуют сертифицированные ФСТЭК России средств обнаружения вторжений и межсетевого экранирования, ограничивающих возможности внешних нарушителей, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.20	Угроза несанкционированного доступа вслед-	Внутренний нарушитель с	Системное программное обеспе-	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если для ограничения установ-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	ствие наличия у пользователей излишних привилегий на установку и запуск приложений	низким потенциалом, Внешний нарушитель со средним потенциалом	чение, прикладное программное обеспечение, сетевое программное обеспечение объекты файловой системы АРМ; сетевой узел, сетевой трафик, носитель информации.					ки и запуска приложений не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, а также отсутствуют сертифицированные ФСТЭК России средств обнаружения вторжений и межсетевого экранирования, ограничивающих возможности внешних нарушителей, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.21	Угроза подмены программного обеспечения	Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если пользователи обладают правами для установки программного обеспечения из сети Интернет, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.22	Угроза внедрения вредоносного кода или данных на АРМ пользователей	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, объект файловой системы, виртуальная машина сервера; сетевой узел	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если для защиты АРМ пользователей не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.23	Угроза внедрения вредоносного кода или данных на серверах	Внутренний нарушитель с низким по-	Аппаратное обеспечение, системное программное	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для защиты серверов ИС не применяются сертифицирован-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		тенциалом, Внешний нарушитель с низким потенциалом	обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, сетевой узел, объект файловой системы.					ные ФСТЭК России средства антивирусной защиты информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.24	Угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если на АРМ пользователей не применяются сертифицированные ФСТЭК России средства антивирусной защиты информации, а пользователи ИС не проходят соответствующий инструктаж, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.25	Угроза нарушения функционирования web-приложений	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. в данном типе ИС ИОГВ Краснодарского края отсутствуют web-сервера
2.2.26	Угроза получения сведений об информационной системе	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	средняя	низкий	высокая	актуальна	Угроза является актуальной, т.к. используемые средства защиты информации не позволяют нейтрализовать угрозы сканирования информационных систем
2.2.27	Угроза исследования работы приложения	Внутренний нарушитель	Системное программное обеспе-	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. в данном типе ИС ИОГВ Краснодар-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		со средним потенциалом, Внешний нарушитель со средним потенциалом	чение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение					ского края отсутствуют серверные компоненты ИС, доступные из сети Интернет
2.2.28	Угроза несанкционированного копирования защищаемой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	высокая	высокий	высокая	актуальна	Угроза является актуальной, т.к. в ИС возможно подключение/использование съёмных носителей информации и не применяются специализированные средства защиты информации для контроля копирования защищаемой информации
2.2.29	Угроза несанкционированного восстановления удалённой защищаемой информации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Машинный носитель информации	высокая	средний	высокая	актуальна	Угроза является актуальной, т.к. для удаления защищаемой информации не используются средства гарантированного уничтожения информации
2.2.30	Угроза использования технологий беспроводного доступа	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если для доступа пользователей к ИС применяются технологии беспроводного доступа, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.31	Угроза несанкционированного доступа к компонентам среды виртуализации	Внутренний нарушитель с низким потенциалом Внешний	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, вир-	маловероятно	низкий	низкая	неактуальна	Угроза является неактуальной, т.к. в данном типе ИС не применяются среды виртуализации

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		нарушитель с низким потенциалом	туальная машина, сервер, сетевое оборудование, сетевой трафик, виртуальные устройства, гипервизор, виртуальные устройства хранения, обработки и передачи данных, объект файловой системы.					
2.2.32	Угроза приведения системы в состояние «отказ в обслуживании»	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если не применяются сертифицированные ФСТЭК межсетевого экранирования, и не осуществляется мониторинг и анализ инцидентов, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.33	Угроза реализации атаки "человек посередине" при передаче информации в пределах контролируемой зоны	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер, информация, хранящаяся на компьютере во временных файлах (программное обеспечение)	высокая	средний	высокая	актуальна	Угроза является актуальной в случае если в ЛВС не применяются сертифицированные ФСТЭК России средства межсетевого экранирования и обнаружения вторжений, позволяющие нейтрализовать данную угрозу и доступ посторонних лиц в помещения не ограничен, что возможно для ИС ИОГВ Краснодарского края данного типа.
2.2.34	Угроза реализации атаки "человек посередине" при	Внешний нарушитель с	Прикладное программное обеспе-	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если при передаче защищаемой

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	передаче информации за пределы контролируемой зоны	низким потенциалом	чение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер.					информации за пределы КЗ не применяются сертифицированные ФСБ России средства криптографической защиты информации, передаваемой по каналам связи, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.35	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Внешний нарушитель со средним потенциалом	Аутентификационные данные пользователя (программное обеспечение)	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если порядок использования браузеров при доступе к компонентам ИС - не регламентирован, а также используются соответствующий функционал браузеров, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.36	Угроза наличия ошибок в ходе проектирования, разработки и отладки системы	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры	средняя	средний	средняя	актуальна	Несмотря на неактуальности для данного типа ИС ИОГВ Краснодарского края данной категории потенциальных нарушителей (в государственных контрактах на проектирование, разработку и отладку систем закрепляется ответственность Поставщиков услуг и то, то для проведения работ по защите информации привлекаются только организации, имеющие соответствующие лицензии ФСТЭК России и ФСБ России), угроза является актуальной, т.к. возможно фактическое введение ИС в эксплуатацию без их тестирования и аттестации
2.2.37	Угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	низкая	низкий	средняя	неактуальна	Угроза является неактуальной ввиду неактуальности для данного типа ИС ИОГВ Краснодарского края данной категории потенциальных нарушителей (в государственных

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
								контрактах на ремонт и обслуживания оборудования закрепляется ответственность Поставщиков услуг)
2.2.38	Угроза слабости механизмов контроля входных данных	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр, аппаратное обеспечение, метаданные.	средняя	средний	средняя	актуальна	Угроза является актуальной в следующих случаях: - не применяются сертифицированные ФСТЭК России средства защиты информации от несанкционированного доступа, ограничивающие возможности нарушителей по доступу к программным компонентам информационных систем, а также контролирующие функционирование программ; - возможности внешнего нарушителя не ограничены посредством использования сертифицированных ФСТЭК России средства обнаружения вторжений и межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.39	Угроза слабости или некорректной настройки механизмов контроля целостности и резервирования данных	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	высокая	средний	высокая	актуальна	Угроза является актуальной в случае, если для контроля целостности не применяются средства защиты информации от несанкционированного доступа, сертифицированные по требованиям ФСТЭК России и (или) средства резервного копирования информации, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.40	Угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика	Внутренний нарушитель с низким потенциалом,	Сетевой узел, сетевое программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если для фильтрации сетевого трафика не применяются сертифицированные ФСТЭК России сред-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
		Внешний нарушитель с низким потенциалом						ства межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.41	Угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, учётные данные пользователя, реестр, машинные носители информации, метаданные, микропрограммное обеспечение, средство защиты информации	высокая	средний	средняя	актуальна	Угроза является актуальной в случае, если для разграничения доступа к защищаемой информации не применяются сертифицированные ФСТЭК России средств защиты информации от несанкционированного доступа, что возможно для данного типа ИС ИОГВ Краснодарского края
2.2.42	Угроза анализа криптографических алгоритмов и их реализации	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной в случае, если применяются средства криптографической защиты информации, не сертифицированные по требованиям ФСБ России, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.43	Угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информа-	Внешний нарушитель с низким потенциалом	Средство защиты информации, аппаратное устройство, программное обеспечение	средняя	средний	средняя	актуальна	Угроза является актуальной, в случае, если этапу внедрение средств защиты информации не предшествует этап проектирования системы защиты информации, учитывающее особенности функционирова-

№ п/п	Наименование УБИ	Источник угрозы	Объект воздействия	Вероятность реализации угрозы	Показатель опасности угрозы для ИС	Возможность реализации угрозы	Актуальность угрозы	Примечание
	ции							ния ИС, а ее настройка осуществляется лицензиатами ФСТЭК России, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.44	Угроза несанкционированного воздействия на средство защиты информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Средство защиты информации	средняя	средний	средняя	актуальна	Угроза является актуальной, в случае если ИС не оснащены необходимыми сертифицированными ФСТЭК России средствами защиты информации, которые осуществляются: тестирование собственных функций, а также ограничение возможности по воздействие на сами средства защиты (комплексом применяемых средств защиты информации), что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.45	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Средство защиты информации	средняя	средний	высокая	актуальна	Угроза является актуальной, в случае если возможность изменения настроек средств защиты информации не ограничена их функционалом, что возможно для ИС ИОГВ Краснодарского края данного типа
2.2.46	Угроза проникновения из смежных ИС с более низким уровнем защищенности	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Информационная система	средняя	средний	средняя	актуальна	Угроза является актуальной в случае отсутствия сегментирования ЛВС (в составе которой имеются ИС различных уровней защищенности) сертифицированными ФСТЭК России средствами межсетевого экранирования, что возможно для ИС ИОГВ Краснодарского края данного типа

6 Выводы

6.1 Категории потенциальных нарушителей

Потенциальным нарушителем безопасности информации могут быть нарушители категорий внешние и внутренние.

Потенциальными внешними нарушителями могут быть:

- для информационных систем исполнительных органов государственной власти Краснодарского края типов 1, 2:
  - разведывательные службы государств;
  - криминальные структуры;
  - внешние субъекты;
- для информационных систем исполнительных органов государственной власти Краснодарского края типов 3, 4:
  - криминальные структуры;
  - внешние субъекты.

Потенциальными внутренними нарушителями края могут быть:

- для информационных систем исполнительных органов государственной власти Краснодарского края типа 1:
  - сотрудники, не являющиеся пользователями информационных систем;
  - удалённые пользователи информационных систем.
- для информационных систем исполнительных органов государственной власти Краснодарского края типа 2:
  - сотрудники, не являющиеся пользователями информационных систем;
  - удалённые пользователи информационных систем;
  - администратор безопасности сегмента информационных систем;
  - системный администратор информационных систем.
- для информационных систем исполнительных органов государственной власти Краснодарского края типа 3:
  - сотрудники, не являющиеся пользователями информационных систем;
  - пользователи информационных систем;
  - удалённые пользователи информационных систем.
- для информационных систем исполнительных органов государственной власти Краснодарского края типа 4:
  - сотрудники, не являющиеся пользователями информационных систем;
  - пользователи информационных систем.

6.2 Актуальные угрозы безопасности конфиденциальной информации

В общем случае, актуальными для информационных систем исполнительных органов государственной власти Краснодарского края, являются следующие угрозы безопасности информации:

- угроза стихийных бедствий и природных явлений;
- угрозы социально–политического характера;
- угроза отказа электропитания серверного и телекоммуникационного оборудования;
- угроза отказа электропитания АРМ пользователей;
- угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования;
- угроза разглашения конфиденциальной информации пользователями ИС;
- угроза разглашения конфиденциальной информации сотрудниками подрядных организаций;
- угроза утраты мобильных технических средств пользователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации;
- угроза передача носителей информации лицам, не имеющих права доступа к хранимой на них информации;
- угроза утраты носителей информации;
- угроза физического устаревания аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач;
- угроза некорректной настройки программного обеспечения;
- угроза использования информации идентификации/аутентификации, заданной по умолчанию;
- угроза незащищённого удалённого администрирования информационной системы;
- угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу);
- угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом);
- угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей);
- угроза агрегирования данных, обрабатываемых с помощью мобильного устройства;
- угроза утечки видовой информации;
- угроза преодоления физической защиты;
- угроза физического выведения из строя АРМ, обрабатывающих защищаемую информацию
- угроза физического выведения из строя серверов и систем хранения данных, обрабатывающих защищаемую информацию;
- угроза физического выведения из строя средств передачи информации;
- угроза хищения АРМ, обрабатывающих защищаемую информацию;

- угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию;
- угроза хищения средств передачи информации;
- угроза хищения носителей информации и мобильных технических средств;
- угроза изменения компонентов системы (аппаратной конфигурации) АРМ;
- угроза изменения компонентов системы (аппаратной конфигурации) серверов;
- угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
- угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам;
- угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники;
- угроза подбора пароля;
- угроза использования уязвимостей используемого ПО;
- угроза установки уязвимых версий программного обеспечения;
- угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию;
- угроза несанкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений;
- угроза подмены программного обеспечения;
- угроза внедрения вредоносного кода или данных на АРМ пользователей;
- угроза внедрения вредоносного кода или данных на серверах;
- угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет
- угроза нарушения функционирования web-приложений;
- угроза получения сведений об информационной системе;
- угроза исследования работы приложения;
- угроза несанкционированного копирования защищаемой информации;
- угроза несанкционированного восстановления удалённой защищаемой информации;
- угроза использования технологий беспроводного доступа;
- угроза несанкционированного доступа к компонентам среды виртуализации;
- угроза приведения системы в состояние «отказ в обслуживании»;
- угроза реализации атаки «человек посередине» при передаче информации за пределы контролируемой зоны;
- угроза реализации атаки «человек посередине» при передаче информации за пределы контролируемой зоны;
- угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере;
- угроза наличия ошибок в ходе проектирования, разработки и отладки системы;
- угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования;
- угроза слабости механизмов контроля входных данных;

- угроза слабости или некорректной настройки механизмов контроля целостности и резервирования данных;
- угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика;
- угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации;
- угроза анализа криптографических алгоритмов и их реализации;
- угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информации;
- угроза несанкционированного воздействия на средство защиты информации;
- угроза несанкционированного изменения параметров настройки средств защиты информации;
- угроза проникновения из смежных ИС с более низким уровнем защищенности.

Актуальность следующих угроз должна определяться при разработки Частной модели угроз для конкретной ИС ИОГВ Краснодарского края исходя из ее архитектуры, структуры (топологии), назначения ИС, состава и критичности обрабатываемой в ней информации:

- угроза наличия недекларированных возможностей в СПО;
- угроза наличия недекларированных возможностей в ППО;

Перечень актуальных угроз безопасности информации для определённых типов информационных систем исполнительных органов государственной власти Краснодарского края приведён в таблице 25.

Таблица 25 – Актуальные угрозы безопасности информации ИС ИОГВ Краснодарского края

№ п/п	Наименование УБИ	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
1. Угрозы, не являющиеся атаками					
1.1. Угрозы, не связанные с деятельностью человека					
1.1.1	Угроза стихийных бедствий и природных явлений	актуальна	актуальна	актуальна	неактуальна
1.2. Угрозы социально–политического характера					
1.2.1	Угрозы социально–политического характера	актуальна	актуальна	актуальна	неактуальна
1.3. Угрозы техногенного характера					
1.3.1	Угроза отказа электропитания серверного и телекоммуникационного оборудования	неактуальна	актуальна	актуальна	актуальна
1.3.2	Угроза отказа электропитания АРМ пользователей	неактуальна	неактуальна	актуальна	актуальна
1.3.3	Угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования	неактуальна	актуальна	неактуальна	актуальна
1.4. Ошибочные действия					
1.4.1	Угроза разглашения конфиденциальной информации пользователями ИС	неактуальна	неактуальна	актуальна	актуальна
1.4.2	Угроза разглашения конфиденциальной информации сотрудниками подрядных организаций	неактуальна	актуальна	неактуальна	неактуальна
1.4.3	Угроза утраты мобильных технических средств пользователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации	актуальна	актуальна	актуальна	актуальна

№ п/п	Наименование УБИ	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
1.4.4	Угроза передача носителей информации лицам, не имеющих права доступа к хранимой на них информации	актуальна	актуальна	актуальна	актуальна
1.4.5	Угроза утраты носителей информации	актуальна	актуальна	актуальна	актуальна
1.4.6	Угроза физического устаревания аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач	актуальна	актуальна	актуальна	актуальна
1.4.7	Угроза некорректной настройки программного обеспечения	актуальна	актуальна	актуальна	актуальна
1.4.8	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	актуальна	актуальна	актуальна	актуальна
1.4.9	Угроза незащищённого удалённого администрирования информационной системы	актуальна	актуальна	актуальна	неактуальна
1.4.10	Угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу)	неактуальна	актуальна	неактуальна	актуальна
1.4.11	Угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом)	неактуальна	актуальна	неактуальна	актуальна
1.4.12	Угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей)	неактуальна	актуальна	неактуальна	актуальна
1.4.13	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	актуальна	актуальна	актуальна	актуальна
2. Угрозы, являющиеся атаками					
2.1. Угрозы утечки информации по техническим каналам					
2.1.1	Угроза утечки акустической информации	неактуальна	неактуальна	неактуальна	неактуальна
2.1.2	Угроза утечки видовой информации	неактуальна	неактуальна	актуальна	актуальна
2.1.3	Угроза утечки информации по каналу ПЭМИН	неактуальна	неактуальна	неактуальна	неактуальна
2.2. Угрозы несанкционированного доступа					
2.2.1	Угроза преодоления физической защиты	неактуальна	актуальна	актуальна	актуальна
2.2.2	Угроза физического выведения из строя АРМ, обрабатывающих защищаемую информацию	неактуальна	неактуальна	актуальна	актуальна
2.2.3	Угроза физического выведения из строя серверов и систем хранения данных, обрабатывающих защищаемую информацию	неактуальна	актуальна	неактуальна	неактуальна
2.2.4	Угроза физического выведения из строя средств передачи информации	неактуальна	актуальна	актуальна	актуальна
2.2.5	Угроза хищения АРМ, обрабатывающих защищаемую информацию	неактуальна	неактуальна	актуальна	актуальна
2.2.6	Угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию	неактуальна	актуальна	актуальна	неактуальна
2.2.7	Угроза хищения средств передачи информации	неактуальна	актуальна	актуальна	актуальна
2.2.8	Угроза хищения носителей информации и мобильных технических средств	неактуальна	актуальна	актуальна	актуальна
2.2.9	Угроза изменения компонентов системы (аппаратной конфигурации) АРМ	неактуальна	неактуальна	актуальна	актуальна
2.2.10	Угроза изменения компонентов системы (аппаратной конфигурации) серверов	неактуальна	актуальна	актуальна	неактуальна
2.2.11	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	неактуальна	актуальна	актуальна	актуальна
2.2.12	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	актуальна	актуальна	неактуальна	неактуальна
2.2.13	Угроза перезагрузки аппаратных и программ-	актуальна	актуальна	актуальна	актуальна

№ п/п	Наименование УБИ	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
	но-аппаратных средств вычислительной техники				
2.2.14	Угроза подбора пароля	актуальна	актуальна	актуальна	актуальна
2.2.15	Угроза использования уязвимостей используемого ПО	неактуальна	актуальна	актуальна	актуальна
2.2.16	Угроза наличия недекларированных возможностей в СПО	неактуальна	неактуальна	неактуальна	неактуальна
2.2.17	Угроза наличия недекларированных возможностей в ППО	неактуальна	неактуальна	неактуальна	неактуальна
2.2.18	Угроза установки уязвимых версий программного обеспечения	неактуальна	актуальна	актуальна	актуальна
2.2.19	Угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию	актуальна	актуальна	актуальна	актуальна
2.2.20	Угроза несанкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений	неактуальна	актуальна	актуальна	актуальна
2.2.21	Угроза подмены программного обеспечения	неактуальна	актуальна	актуальна	актуальна
2.2.22	Угроза внедрения вредоносного кода или данных на АРМ пользователей	неактуальна	актуальна	актуальна	актуальна
2.2.23	Угроза внедрения вредоносного кода или данных на серверах	неактуальна	актуальна	актуальна	актуальна
2.2.24	Угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет	актуальна	актуальна	актуальна	актуальна
2.2.25	Угроза нарушения функционирования web-приложений	актуальна	актуальна	актуальна	неактуальна
2.2.26	Угроза получения сведений об информационной системе	актуальна	актуальна	актуальна	актуальна
2.2.27	Угроза исследования работы приложения	актуальна	актуальна	актуальна	неактуальна
2.2.28	Угроза несанкционированного копирования защищаемой информации	актуальна	актуальна	актуальна	актуальна
2.2.29	Угроза несанкционированного восстановления удалённой защищаемой информации	актуальна	актуальна	актуальна	актуальна
2.2.30	Угроза использования технологий беспроводного доступа	неактуальна	актуальна	актуальна	актуальна
2.2.31	Угроза несанкционированного доступа к компонентам среды виртуализации	неактуальна	актуальна	актуальна	неактуальна
2.2.32	Угроза приведения системы в состояние «отказ в обслуживании»	неактуальна	актуальна	актуальна	актуальна
2.2.33	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	неактуальна	актуальна	актуальна	актуальна
2.2.34	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	неактуальна	актуальна	актуальна	актуальна
2.2.35	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	актуальна	актуальна	актуальна	актуальна
2.2.36	Угроза наличия ошибок в ходе проектирования, разработки и отладки системы	неактуальна	актуальна	актуальна	актуальна
2.2.37	Угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования	неактуальна	актуальна	неактуальна	неактуальна
2.2.38	Угроза слабости механизмов контроля входных данных	неактуальна	актуальна	актуальна	актуальна
2.2.39	Угроза слабости или некорректной настройки механизмов контроля целостности и резерви-	неактуальна	актуальна	актуальна	актуальна

№ п/п	Наименование УБИ	Тип ИС ИОГВ Краснодарского края			
		Тип 1	Тип 2	Тип 3	Тип 4
	рования данных				
2.2.40	Угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика	неактуальна	актуальна	актуальна	актуальна
2.2.41	Угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации	неактуальна	актуальна	актуальна	актуальна
2.2.42	Угроза анализа криптографических алгоритмов и их реализации	неактуальна	актуальна	актуальна	актуальна
2.2.43	Угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информации	неактуальна	актуальна	актуальна	актуальна
2.2.44	Угроза несанкционированного воздействия на средство защиты информации	неактуальна	актуальна	актуальна	актуальна
2.2.45	Угроза несанкционированного изменения параметров настройки средств защиты информации	неактуальна	актуальна	актуальна	актуальна
2.2.46	Угроза проникновения из смежных ИС с более низким уровнем защищенности	актуальна	актуальна	актуальна	актуальна

Актуальность угроз безопасности информации для конкретных информационных систем исполнительных органов государственной власти Краснодарского края должна определяться при разработке Частных моделей угроз безопасности информации данных информационных систем с учётом их архитектуры, структуры (топологии), назначения ИС, состава и критичности обрабатываемой в ней информации, реализованных мер защиты информации. Разработка Частных моделей угроз безопасности информации должна осуществляться с учётом положений настоящей Модели угроз.

Определение класса средств криптографической защиты информации, необходимого для использования в информационных системах исполнительных органов государственной власти Краснодарского края должно осуществляться при разработке Модели нарушителя безопасности информационных систем исполнительных органов государственной власти Краснодарского края.

7 Использованные источники

При проведении работ использовались следующие правовые, нормативно-технические, нормативно-методические и руководящие документы:

1. Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Страсбург, 28 января 1981 года;
2. Конституция Российской Федерации, 12 декабря 1993 года;
3. Федеральный закон Российской Федерации от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
4. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
5. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
6. Трудовой кодекс Российской Федерации от 30 декабря 2001 года № 197-ФЗ (ТК РФ);
7. Гражданский кодекс Российской Федерации (ГК РФ) от 30 ноября 1994 года № 51-ФЗ;
8. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения
9. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;
10. ГОСТ Р 51624-2000. Автоматизированные информационные системы в защищённом исполнении;
11. ГОСТ Р 52653-2006. Информационно-коммуникационные технологии в образовании. Термины и определения;
12. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения;
13. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
14. ГОСТ РО 0043-003-2012. Аттестация объектов информатизации. Общие положения;
15. Р 50.1.056-2005. Техническая защита информации. Основные термины и определения;
16. Р 50.1.056-2005. Техническая защита информации. Основные термины и определения;
17. Методические рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждены руководством 8 Центра ФСБ России от 31 марта.2015 года № 149/7/2/6 432;
18. Методический документ «Меры защиты информации в государственных информационных системах», утверждён ФСТЭК России от 11 февраля 2014 года;
19. Методические документы по профилям защиты межсетевых экранов, утверждённые ФСТЭК России от 12 сентября 2016 года;

20. Постановление Правительства России от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

21. Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

22. Постановление главы администрации (губернатора) Краснодарского края от 26 августа 2008 года №840 «О региональной мультисервисной сети исполнительных органов государственной власти Краснодарского края»;

23. Приказ ФСТЭК России от 15 февраля 2008 года «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

24. Приказ ФСТЭК России от 14 февраля 2008 года «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

25. Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных системах»;

26. Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

27. Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Приложение А

Сведения об информационных системах

В данном разделе приведены обобщённые сведения об ИС ИОГВ Краснодарского края, полученные в ходе проведения обследования объектов информатизации ИОГВ Краснодарского края.

Перечень ИС ИОГВ Краснодарского края, обследования которых осуществлялось, а также сведения о них (описание ИС; состав обрабатываемых в ИС сведений; цели защиты информации в ИС; перечень субъектов и способы информационного взаимодействия ИС; характеристики ИС) представлены в таблицах 26-28.

ЦОД РМС ОГВ представляет собой 2 контура:

- отказоустойчивый и катастрофоустойчивый кластер (далее – Кластер), размещённый на 3 площадках:
  - г. Краснодар, ул. Красная, 35;
  - г. Краснодар. ул. Красная, 180;
  - г. Краснодар, ул. Северная, 490.
- защищённый виртуальный кластер (далее – ЗВК), оснащённый сертифицированными ФСТЭК России и ФСБ России средствами защиты информации. ЗВК расположен по адресу: г. Краснодар, ул. Северная, 490.

Информационное взаимодействие между площадками размещения ЦОД РМС ОГВ осуществляется посредством РМС ОГВ. Схема инфраструктуры ЦОД РМС ОГВ представлена на рисунке 5.

Таблица 26 – Перечень ИС, состав защищаемых в них сведений и субъекты информационного взаимодействия

№ п/п	Наименование ИС	Описание	Состав защищаемых сведений	Субъекты и способ взаимодействия	Характеристики информации, безопасность которых необходимо обеспечить		
					К[18]	Ц[19]	Д[20]
1	ИСАЭД «Синкопа»	Электронный документооборот ИОГВ Краснодарского края	Персональные данные граждан специальных категорий	1. Граждане (обращения посредством электронной почты, веб-портала, обращений в бумажном виде) 2. ИОГВ Краснодарского края (РМС ОГВ)	+	+	+
2	АИС «ЕЦУ»	Единый государственный центр услуг	Персональные данные граждан	1. Граждане (веб-портал) 2. ИОГВ Краснодарского края (РМС ОГВ) 3. РПГУ (РМС ОГВ)	+	+	+
3	РПГУ	Портал государственных и муниципальных услуг	Персональные данные граждан	1. Граждане (веб-портал) 2. АИС «ЕЦУ» (РМС ОГВ) 3. Реестр государственных и муниципальных услуг (РМС ОГВ)	+	+	+
4	РГУ	Информационная система, предоставляющая информацию о доступных в электронном виде государственных услугах	Общедоступная информация	1. ИОГВ Краснодарского края (РМС ОГВ) 2. АИС «ЕЦУ» (РМС ОГВ) 3. Федеральный реестр государственных и муниципальных услуг (РМС ОГВ) 4. РПГУ (РМС ОГВ)		+	+
5	Открытое правительство Краснодарского края	Форум общественных инициатив	Персональные данные пользователей	1. ИОГВ Краснодарского края (РМС ОГВ) 2. Граждане (Интернет)	+	+	+
6	ИС УНП	Система учёта начислений, реквизитов услуг и фактов оплаты	Персональные данные граждан	1. ГИС «ГМП» (Защищённый СКЗИ канал передачи данных) 2. Организации банковской системы Российской Федерации (Защищённый СКЗИ	+	+	+

[18] Конфиденциальность
[19] Целостность
[20] Доступность

№ п/п	Наименование ИС	Описание	Состав защищаемых сведений	Субъекты и способ взаимодействия	Характеристики информации, безопасность которых необходимо обеспечить		
					К[18]	Ц[19]	Д[20]
				канал передачи данных) 3. Администраторы доходов Краснодарского края (Защищённый СКЗИ канал передачи данных)			
7	РИС	Государственный реестр информационных систем Краснодарского края	Общедоступная информация	1. Департамент информатизации и связи Краснодарского края (РМС ОГВ) 2. Граждане (Интернет)		+	+
8	МСЭР	Информационная система планирования и мониторинга социально-экономического развития Краснодарского края	Служебная информация	1. ИОГВ Краснодарского края (Интернет с применением средств ЭП)		+	+
9	ИСПДн «Бухгалтерия и кадры»	Информационная система автоматизации процессов кадрового и бухгалтерского учёта	Персональные данные: - сотрудников и членов их семей - граждан, претендующих на замещение вакантных должностей - уволенных сотрудников	1. Сотрудники Департамент информатизации и связи Краснодарского края (документы в бумажном виде) 2. Организации банковской системы (Защищённый СКЗИ канал передачи данных) 3. ИОГВ Краснодарского края, в т.ч. ФОМС, ПФР, ФНС (Защищённый СКЗИ канал передачи данных)	+	+	+
10	АС «УРМ»	Автоматизированная система «Удалённое рабочее место» предназначена для автоматизации финансовой деятельности распорядителей и получателей бюджетных	Служебная информация	1. ИОГВ Краснодарского края (РМС ОГВ)		+	+

№ п/п	Наименование ИС	Описание	Состав защищаемых сведений	Субъекты и способ взаимодействия	Характеристики информации, безопасность которых необходимо обеспечить		
					К[18]	Ц[19]	Д[20]
		средств, а также для организации электронного взаимодействия между ФО и ГРБС, ГАИФ, РБС, АИФ, ПБС, ТПФО в процессе планирования и исполнения бюджета.					

Таблица 27 – Характеристики и установленные уровни защищенности ИС

№ п/п	Наименование ИС	Характеристики ИС					Установленный уровень защищенности ИС			
		Структура ИС	Масштаб ИС	Наличие подключения к ССОП	Режим обработки информации	Режим разграничения прав доступа	Уровень защищенности ПДн		Класс защищенности ГИС	
							Серверный сегмент	Пользовательский сегмент*[21]	Серверный сегмент	Пользовательский сегмент*
1	ИСАЭД «Синкопа»	Распределённая	Региональный	Да	МП	с РПД	2-УЗ	3-УЗ	К2	К3
2	АИС «ЕЦУ»	Распределённая	Региональный	Да	МП	с РПД	2-УЗ***[22]		К2**[23]	
3	РПГУ	Распределённая	Региональный	Да	МП	с РПД	Не установлен. Требуется	Не установлен. Не требуется	К2*	
4	РГУ	Распределённая	Региональный	Да	МП	с РПД	Не установлен. Не требуется		К2*	

[21] Пользовательский сегмент, субъектами доступа которого являются граждане, осуществляющие доступ к ИС и сети Интернет, не классифицируется по требования безопасности информации

[22] Требуется отдельное определение уровня защищенности ПДн, обрабатываемых в пользовательском и сервером сегментах ИС

[23] Требуется отдельное определение классов защищенности для сегментов ГИС (пользовательского и серверного)

№ п/п	Наименование ИС	Характеристики ИС					Установленный уровень защищенности ИС			
		Структура ИС	Масштаб ИС	Наличие подключения к ССОП	Режим обработки информации	Режим разграничения прав доступа	Уровень защищенности ПДн		Класс защищенности ГИС	
							Серверный сегмент	Пользовательский сегмент*[21]	Серверный сегмент	Пользовательский сегмент*
5	Открытое правительство Краснодарского края	Распределённая	Региональный	Да	МП	с РПД	4-УЗ***		К2*	
6	ИС УНП	Распределённая	Региональный	Да	МП	с РПД	3-УЗ***		К3*	
7	РИС	Распределённая	Региональный	Да	МП	с РПД	Не установлен. Требуется		Не установлен. Требуется	
8	МСЭР	Распределённая	Региональный	Да	МП	с РПД	Не установлен. Не требуется		К3*	
9	ИСПДн «Бухгалтерия и кадры»	Локальная	Объектовый	Да	МП	без РПД	4-УЗ		Не установлен. Не требуется	
10	АС «УРМ»	Распределённая	Региональный	Да	МП	с РПД	Не установлен. Не требуется		Не установлен. Требуется	

Таблица 28 – Места размещения компонентов ИС, состав СПО серверных компонентов ИС

№ п/п	Наименование ИС	Место размещения серверных мощностей	Место размещения АРМ пользователей	Состав серверного компонента ИС
1	ИСАЭД «Синкопа»	ЦОД РМС ОГВ	ИОГВ Краснодарского края	1. Сервер 1 (SUSE Linux Enterprise 11 x64) 2. Сервер 2 (SUSE Linux Enterprise 11 x64) 3. Сервер 3 (SUSE Linux Enterprise 11 x64) 4. Сервер 4 (SUSE Linux Enterprise 11 x64) 5. Сервер ДИО (OpenSUSE 12.3 x64)
2	АИС «ЕЦУ»	ЦОД РМС ОГВ	ИОГВ Краснодарского края	1. Сервер СИР - Балансировщик нагрузки (CentOS 6.5) 2. Сервер СИР - Node 1 (CentOS 6.5)

№ п/п	Наименование ИС	Место размещения серверных мощностей	Место размещения АРМ пользователей	Состав серверного компонента ИС
				3. Сервер СИР - Node N (CentOS 6.5) 4. Сервер СИР - БД (CentOS 6.5) 5. Сервер СИР - Портал (CentOS 7.2.1511) 6. Сервер СИР - Тестовый СИР (CentOS 6.5) 7. Продуктивный сервер ЕЦУ (CentOS 6.5)
3	РПГУ	ЦОД РМС ОГВ	ИОГВ Краснодарского края	1. Сервер 1 (CentOS 7.2.1511 (Core) 2. Сервер 2 (CentOS 7.2.1511 (Core)
4	РГУ	ЦОД РМС ОГВ	ИОГВ Краснодарского края	1. Сервер приложений (CentOS 6.6) 2. Сервер СУБД (CentOS 6.6)
5	Открытое правительство Краснодарского края	ЦОД РМС ОГВ	ИОГВ Краснодарского края	1. Кластер 1 (CentOS 6.5) 2. Кластер 2 (CentOS 6.5)
6	ИС УНП	ЦОД РМС ОГВ	ИОГВ Краснодарского края	1. Административный сервер (Microsoft Windows Server 2008 R2 Standard) 2. ИС УНП 1 (Microsoft Windows Server 2008 R2 Standard) 3. Сервер БД УНП (Microsoft Windows Server 2008 R2 Standard) 4. Веб сервер (Microsoft Windows Server 2008 R2 Standard) 5. ИС УНП 2 (Microsoft Windows Server 2008 R2 Standard) 6. Сервер БД УНП 2 (Microsoft Windows Server 2008 R2 Standard)
7	РИС	ЦОД РМС ОГВ	ИОГВ Краснодарского края	1. Сервер приложений (CentOS)
8	МСЭР	ЦОД РМС ОГВ	ИОГВ Краснодарского края	1. Сервер оперативной БД (Linux) 2. Сервер статистической БД (Linux) 3. Сервер многомерного анализа данных (Linux) 4. Сервер подсистемы отчётности (Linux) 5. Сервер подсистемы мониторинга достижений целевых показателей (Linux)
9	ИСПДн «Бухгалтерия и кадры»	ЦОД РМС ОГВ	Департамент информатизации и связи Краснодарского края	1. Сервер приложений и БД (Microsoft Windows Server 2008 R2 Standard)
10	АС «УРМ»	Министерство финансов Краснодарского края	ИОГВ Краснодарского края	Обследование ИС Министерства финансов Краснодарского края не входит в область проведения обследования

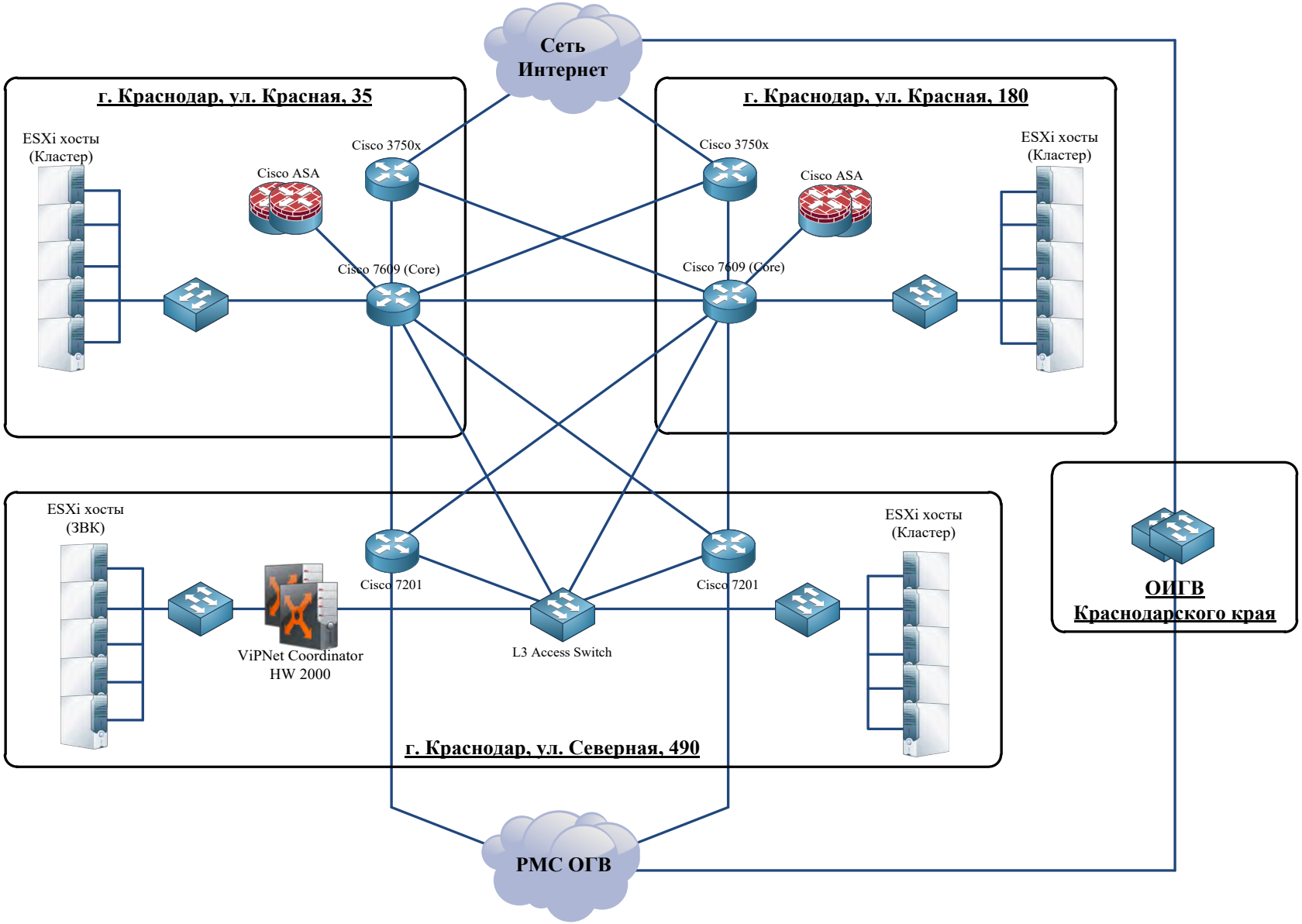


Рисунок 5 – Схема ЦОД РМС ОГВ

На основании данных сведений, было определено, что основными для типизации являются следующие параметры/характеристики ИС:

— расположение вычислительных мощностей, на которых располагаются серверные сегменты ИС ИОГВ Краснодарского края;
— расположение пользовательских сегментов ИС ИОГВ Краснодарского.
— организация, осуществляющая администрирование и сопровождение серверных мощностей расположения ИС ИОГВ Краснодарского края;

С учётом этих параметров типы рассмотренных ИС представлены в таблице 29.

Таблица 29 – Типизация ИС

№ п/п	Наименование ИС	Тип ИС	
		Серверный сегмент	Пользовательский сегмент[24]
1	ИСАЭД «Синкопа»	Тип 1	Тип 4
2	АИС «ЕЦУ»	Тип 1	Тип 4
3	РПГУ	Тип 1	Тип 4
4	РГУ	Тип 1	Тип 4
5	Открытое правительство Краснодарского края	Тип 1	Тип 4
6	ИС УНП	Тип 1	Тип 4
7	РИС	Тип 1	Тип 4
8	МСЭР	Тип 1	Тип 4
9	ИСПДн «Бухгалтерия и кадры»	Тип 1	Тип 4
10	АС «УРМ»	Тип 3	Тип 4

Учитывая, что уполномоченным лицом, предоставляющим мощности (вычислительные ресурсы) для размещения серверных сегментов ИС ИОГВ Краснодарского края может являться не только департамент информатизации и связи Краснодарского края (и соответственно серверные сегменты ИС могут располагаться за пределами ЦОД РМС ОГВ) – необходимо выделение отдельного типа ИС, предусматривающего данную ситуацию.

[24] При проведении обследования, в качестве пользовательского сегмента ИС выступал пользовательский сегмент ДИС Краснодарского края

Приложение Б

Описание угроз безопасности информации

Таблица 30 – Описание УБИ

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
1. Угрозы, не являющиеся атаками					
1.1. Угрозы, не связанные с деятельностью человека					
1.1.1	Угроза стихийных бедствий и природных явлений	Угроза заключается в возможности нарушения функционирования любых компонентов информационных систем в результате стихийных бедствий и природных явлений. Реализация данной угрозы возможна по независящим от возможных нарушителей причинам. Реализация данной угрозы возможна по независящим от возможных нарушителей причинам.	-	Информационная система	Нарушение конфиденциальности, доступности, целостности.
1.2. Угрозы социально–политического характера					
1.2.1	Угрозы социально–политического характера	Угроза заключается в возможности нарушения функционирования любых компонентов информационных систем в результате забастовок, саботажа, локальных конфликтов и т.д. Реализация данной угрозы возможна по независящим от возможных нарушителей причинам.	-	Информационная система	Нарушение конфиденциальности, доступности, целостности.
1.3. Угрозы техногенного характера					
1.3.1	Угроза отказа электропитания серверного и телекоммуникационного оборудования	Угроза заключается в возможности повреждения серверного и/или телекоммуникационного оборудования вследствие перебоев или отсутствия электропитания. Реализация данной угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на повреждение линий и/или средств электропитания	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Линии и средства электропитания	Нарушение доступности
1.3.2	Угроза отказа электропитания АРМ пользователей	Угроза заключается в возможности повреждения АРМ пользователей вследствие перебоев или отсутствия электропитания. Реализация данной угрозы возможна как вследствие естественных техногенных причин, так и путём проведения	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Линии и средства электропитания	Нарушение доступности

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		определённых мероприятий нарушителем, направленных на повреждение линий и/или средств электропитания			
1.3.3	Угроза отказа подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования	Угроза заключается в возможности повреждения части компонентов системы или системы в целом вследствие выхода температурного режима их работы из заданных требований из-за возникновения отказа входящих в неё подсистем вентиляции и температурных приборов. Реализация данной угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на удалённое отключение/вывод из строя компонентов подсистемы обеспечения температурного режима	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в серверных помещениях, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля	Нарушение доступности
1.4. Ошибочные действия					
1.4.1	Угроза разглашения конфиденциальной информации пользователями ИС	Угроза заключается в возможности умышленного или случайного раскрытия пользователями ИС конфиденциальной информации. Данная угроза обусловлена слабостями организационных мер по повышению осведомлённости пользователей ИС, отсутствием закреплённой ответственности. Реализация данной угрозы возможна вследствие халатности или злых намерений пользователей ИС	Внутренний нарушитель с низким потенциалом	Защищаемая информация	Нарушение конфиденциальности
1.4.2	Угроза разглашения конфиденциальной информации сотрудниками подрядных организаций	Угроза заключается в возможности умышленного или случайного раскрытия сотрудниками подрядных организаций конфиденциальной информации, ставшей известной вследствие проведения работ. Данная угроза обусловлена слабостями организационных мер по проверке контрагентов, отсутствием закреплённой ответственности. Реализация данной угрозы возможна вследствие халатности или злых намерений сотрудниками подрядных организаций ИС	Внутренний нарушитель с средним потенциалом	Защищаемая информация	Нарушение конфиденциальности
1.4.3	Угроза утраты мобиль-	Угроза заключается в возможности раскрытия информации,	Внутренний нарушитель с	Мобильное техниче-	Нарушение кон-

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
	ных технических средств пользователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации	хранящейся на утерянном/переданном мобильном техническом средстве (в случае отсутствия шифрования данных), или её потери (в случае отсутствия резервной копий данных). Данная угроза обусловлена слабостями мер регистрации и учёта мобильных технических средств, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	низким потенциалом	ское средство	фиденциальности, доступности.
1.4.4	Угроза передача носителей информации лицам, не имеющих права доступа к хранимой на них информации	Угроза заключается в возможности раскрытия информации, хранящейся на переданном носителе (в случае отсутствия шифрования данных), или её потери (в случае отсутствия резервной копий данных). Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	Внутренний нарушитель с низким потенциалом	Носитель информации	Нарушение конфиденциальности, доступности, целостности.
1.4.5	Угроза утраты носителей информации	Угроза заключается в возможности раскрытия информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или её потери (в случае отсутствия резервной копий данных). Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	Внутренний нарушитель с низким потенциалом	Носитель информации	Нарушение конфиденциальности, доступности.
1.4.6	Угроза физического устаревания аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач	Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания, а также при превышении максимально допустимой нагрузки на вычислительные мощности (объем жёстких дисков, процессорные мощности, объем оперативной памяти) Возможность реализации данной угрозы возрастает при использовании технических средств в условиях, не удовлетворяющих требованиям решаемых задач	Внутренний нарушитель с низким потенциалом	Аппаратное средство, система хранения данных	Нарушение доступности.
1.4.7	Угроза некорректной	Угроза заключается в возможности получения нарушителем	Внутренний нарушитель	Системное про-	Нарушение до-

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
	настройки программного обеспечения	доступа к дополнительному скрытому функционалу приложений (информация о котором не была опубликована разработчиком) или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций. Данная угроза обусловлена уязвимостями программного обеспечения, проявляющимися при его неправильной конфигурации, а также слабостями механизма контроля доступа к настройкам большинства приложений. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение конфигурации программного обеспечения. При реализации данной угрозы, в отличии от других подобных угроз, нарушитель действует «вслепую» – простым путём перебора всевозможных комбинаций	со средним потенциалом, Внешний нарушитель со средним потенциалом	граммное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр.	ступности, целостности
1.4.8	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Угроза заключается в возможности прохождения нарушителем процедуры авторизации, на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: - наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты; - успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Средства защиты информации, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		дискредитируемого объекта защиты			
1.4.9	Угроза незащищённого удалённого администрирования информационной системы	Угроза заключается в возможности осуществления опосредованного деструктивного программного воздействия на часть или все информационные системы, путём перехвата управления через механизмы удалённого администрирования. Данная угроза обусловлена недостаточностью внимания, уделяемого контролю вводимых пользователями данных (в том числе аутентификационных данных), а также уязвимостями небезопасных интерфейсов обмена данными (API), используемых средствами удалённого администрирования. Реализация данной угрозы возможна в случае получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Информационная система, сервер, рабочая станция, сетевое программное обеспечение	Нарушение конфиденциальности, доступности, целостности.
1.4.10	Угроза привязки к поставщику вычислительных мощностей (уполномоченному лицу)	Угроза заключается в возможности возникновения трудно решаемых (или даже неразрешимых) проблем технического, организационного, юридического или другого характера, препятствующих осуществлению потребителем услуг смены их поставщика. Данная угроза обусловлена отсутствием совместимости между форматами данных и программными интерфейсами, используемыми различными производителями. Реализация данной угрозы возможна при условии использования производителем нестандартного программного обеспечения или формата образов виртуальных машин и отсутствием средств преобразования образа виртуальной машины из используемого им формата в другой (используемый другим производителем)	Внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы	Нарушение доступности.
1.4.11	Угроза недобросовестного исполнения обязательств поставщиком вычислительных мощностей (уполномоченным лицом)	Угроза заключается в возможности нарушении конфиденциальности, целостности и доступности информации, обрабатываемой на предоставляемых уполномоченным лицом вычислительных мощностях, вследствие: технических сбоев , невыполнения требований к уровню качества и (или) снижение качества предоставляемых потребителям вычислительных мощностей , невыполнения требований по обеспечению безопасности информации.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Информационная система, сервер, носитель информации, метаданные, объекты файловой системы, системное программное обеспечение, аппаратное обеспече-	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		Данная угроза обусловлена невозможностью непосредственного контроля над действиями сотрудников уполномоченного лица со стороны их потребителей, слабостями процедуры контроля за выполнением технического обслуживания и соблюдения требований по обеспечению заданного уровня предоставления сервиса (в т.ч. по обеспечению безопасности информации) Реализация данной угрозы возможна в случаях: халатности со стороны сотрудников уполномоченного лица; недостаточности должностных и иных инструкций данных сотрудников; недостаточности мер по менеджменту и обеспечению безопасности защищаемой информации; ошибок при конфигурации (или выбора) используемого программного/аппаратного обеспечения инфраструктуры (в т.ч. средств защиты информации)		ние, канал связи	
1.4.12	Угроза отсутствия распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей)	Угроза заключается в возможности возникновения существенных разногласий между поставщиком и потребителем вычислительных мощностей по вопросам, связанным с определением их прав и обязанностей в части обеспечения информационной безопасности. Данная угроза обусловлена отсутствием достаточного набора мер контроля за распределением ответственности между различными ролями в части владения данными, контроля доступа, поддержки инфраструктуры и т. п. Возможность реализации данной угрозы повышается в случае использовании вычислительных мощностей, предоставляемых другими поставщиками (т.е. в случае использования схемы с участием посредников)	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение	Нарушение конфиденциальности, доступности, целостности.
1.4.13	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Угроза заключается в возможности осуществления нарушителем сбора и анализа информации, обрабатываемой с помощью мобильного устройства, за счёт использования специального программного обеспечения, встраиваемого пользователем в системное программное обеспечение мобильного устройства, а также встраиваемого в мобильные программы под видом программной платформы для их разработки другими компаниями. Данная угроза обусловлена наличием в мобильном устройстве множества каналов передачи данных, а также сложно-	Внутренний нарушитель со средним потенциалом	Мобильное устройство	Нарушение конфиденциальности

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		стью контроля потоков информации в таком устройстве. Реализация данной угрозы возможна при условии использования мобильных устройств пользователями. В качестве собираемой информации могут выступать: - персональные данные пользователя и контактирующих с ним лиц (пол, возраст, религиозные и политические взгляды и др.); - информация ограниченного доступа (история браузера, список контактов пользователя, история звонков и др.); данные об окружающей среде (текущее местоположение мобильного устройства, маршруты движения, наличие беспроводных сетей в радиусе доступа); - видеоданные, снимаемые видеокамерами мобильного устройства; - аудиоданные, снимаемые микрофоном устройства			
2. Угрозы, являющиеся атаками					
2.1. Угрозы утечки информации по техническим каналам					
2.1.1	Угроза утечки акустической информации	Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИС, при обработке информации в ИС возможно при наличии функций голосового ввода информации в ИС или функций воспроизведения информации акустическими средствами ИС. Утечка акустической (речевой) информации может быть осуществлена с помощью аппаратных закладок, за счёт съёма виброакустических сигналов, за счёт излучений, модулированных акустическим сигналом (микрофонный эффект и высокочастотное облучение), за счёт оптического излучения, модулированного акустическим сигналом.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Защищаемая информация, аппаратное обеспечение	Нарушение конфиденциальности
2.1.2	Угроза утечки видовой информации	Угрозы утечки видовой информации реализуются за счёт просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, ТС обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС. Кроме этого, просмотр (регистрация) информации возможен с использованием специальных электронных устройств	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Защищаемая информация	Нарушение конфиденциальности

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		съёма, внедрённых в служебных помещениях или скрыто используемых физическими лицами при посещении ими служебных помещений. Необходимым условием осуществления просмотра (регистрации) информации является наличие прямой видимости между средством наблюдения и носителем информации. Утечка видовой информации может быть осуществлена за счёт удалённого просмотра экранов дисплеев и других средств отображения информации; с помощью видеоаппаратных закладок.			
2.1.3	Угроза утечки информации по каналу ПЭМИН	Возникновение угрозы утечки информации по каналам ПЭМИН возможно за счёт перехвата ТС побочных (не связанных с прямым функциональным значением элементов ИС) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации ТС ИС. Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в ТС (средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приёма и обработки информации, средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других ТС обработки речевой, графической, видео- и буквенно-цифровой информации). Для регистрации ПЭМИН используется аппаратура в составе радиоприёмных устройств и оконечных устройств восстановления информации. Утечка информации по каналам ПЭМИН может быть осуществлена: за счёт побочных электромагнитных излучений электронно-вычислительной техники; за счёт наводок по цепям питания; за счёт радиоизлучений, модулированных информационным сигналом.	Внутренний нарушитель с высоким потенциалом, Внешний нарушитель с высоким потенциалом	Аппаратное обеспечение	Нарушение конфиденциальности
2.2. Угрозы несанкционированного доступа					
2.2.1	Угроза преодоления физической защиты	Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным сред-	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		ствам вычислительной техники системы путём преодоления системы контроля физического доступа, организованной в здании предприятия. Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.). Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.)			
2.2.2	Угроза физического выведения из строя АРМ, обрабатывающих защищаемую информацию	Угроза заключается в возможности умышленного выведения из строя нарушителем АРМ, обрабатывающих защищаемую информацию, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к АРМ, обрабатывающих защищаемую информацию. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к АРМ.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	АРМ	Нарушение доступности, целостности.
2.2.3	Угроза физического выведения из строя серверов и систем хранения данных, обрабатывающих защищаемую информацию	Угроза заключается в возможности умышленного выведения из строя нарушителем серверов и систем хранения данных, обрабатывающих защищаемую информацию, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к серверам и систем хранения данных, обрабатывающих защищаемую информацию. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к серверам и системам хранения данных.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сервер	Нарушение доступности, целостности.
2.2.4	Угроза физического выведения из строя средств передачи информации	Угроза заключается в возможности умышленного выведения из строя нарушителем средств передачи защищаемой информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам передачи защищаемой информации.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	Нарушение доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		Реализация данной угрозы возможна при условии получения нарушителем физического доступа к средству передачи защищаемой информации.			
2.2.5	Угроза хищения АРМ, обрабатывающих защищаемую информацию	Угроза заключается в возможности осуществления нарушителем кражи АРМ (и подключённых к нему устройств). Данная угроза обусловлена слабостями мер контроля физического доступа к АРМ, обрабатывающих защищаемую информацию. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к АРМ.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	АРМ	Нарушение конфиденциальности, доступности.
2.2.6	Угроза хищения серверов и систем хранения данных, обрабатывающих защищаемую информацию	Угроза заключается в возможности осуществления нарушителем кражи серверов и систем хранения данных, обрабатывающих защищаемую информацию. Данная угроза обусловлена слабостями мер контроля физического доступа к серверам системам хранения данных, обрабатывающих защищаемую информацию. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к серверам и системам хранения данных.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сервер	Нарушение конфиденциальности, доступности.
2.2.7	Угроза хищения средств передачи информации	Угроза заключается в возможности осуществления нарушителем кражи средств передачи информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам передачи информации. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к средствам передачи информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Средство передачи информации	Нарушение конфиденциальности, доступности.
2.2.8	Угроза хищения носителей информации и мобильных технических средств	Угроза заключается в возможности осуществления нарушителем кражи носителей защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к носителям защищаемой информации. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям защищаемой информации (внешним, съёмным и внутренним накопителям).	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации	Нарушение конфиденциальности, доступности.
2.2.9	Угроза изменения компонентов системы (аппаратной конфигурации) АРМ	Угроза заключается в возможности изменения аппаратной конфигурации АРМ со следующими целями: - получение нарушителем доступа к хранимым на них файлах, внедрения закладок, к сети Интернет (при его отсут-	Внутренний нарушитель с низким потенциалом	АРМ	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		ствии на АРМ), и т.п. путём несанкционированного изменения состава аппаратных средств АРМ, что в дальнейшем позволит осуществлять данному нарушителю (или другому – внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе; - хищение комплектующих АРМ; Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной конфигурации АРМ. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий доступа к АРМ.			
2.2.10	Угроза изменения компонентов системы (аппаратной конфигурации) серверов	Угроза заключается в возможности изменения аппаратной конфигурации сервера со следующими целями: - получение нарушителем доступа к хранимым на них файлах, внедрения закладок, к сети Интернет (при его отсутствии на сервере) и т.п. путём несанкционированного изменения состава аппаратных средств АРМ, что в дальнейшем позволит осуществлять данному нарушителю (или другому – внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе; - хищение комплектующих сервера; Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной конфигурации сервера. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий доступа к сервера.	Внутренний нарушитель с низким потенциалом	Сервер	Нарушение конфиденциальности, доступности, целостности.
2.2.11	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности прерывания нарушителем технологии обработки информации в дискредитируемой системе путём осуществления деструктивного программного (локально или удалённо) воздействия на средства хранения (внешних, съёмных и внутренних накопителей), обработки (процессора, контроллера устройств и т.п.) и (или) ввода/вывода/передачи информации (клавиатуры и др.), в результате которого объект защиты перейдёт в состояние «отказ в обслуживании». При этом вывод его из этого состояния может быть невозможен путём простой	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	Нарушение доступности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		перезагрузки системы, а потребует проведения ремонтно-восстановительных работ. Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации			
2.2.12	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Угроза заключается в возможности получения нарушителем привилегий управления системой путём использования удалённого внеполосного (по независимому вспомогательному каналу TCP/IP) доступа. Данная угроза обусловлена невозможностью контроля за механизмом, реализующего функции удалённого доступа на аппаратном уровне, на уровне операционной системы, а также независимостью от состояния питания аппаратных устройств, т.к. данный механизм предусматривает процедуру удалённого включения/выключения аппаратных устройств. Реализация данной угрозы возможна в условиях: - наличия в системе аппаратного обеспечения, поддерживающего технологию удалённого внеполосного доступа; - наличия подключения системы к сетям общего пользования (сети Интернет)	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение	Нарушение конфиденциальности, доступности, целостности.
2.2.13	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Угроза заключается в возможности сброса нарушителем состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом. Данная угроза обусловлена свойством оперативной памяти обнулять своё состояние при выключении и перезагрузке. Реализация данной угрозы возможна как аппаратным способом (нажатием кнопки), так и программным (локально или удалённо) при выполнении следующих условий: - наличие в системе открытых сессий работы пользователей; - наличие у нарушителя прав в системе (или физической возможности) на осуществление форсированной переза-	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	Нарушение доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		грузки			
2.2.14	Угроза подбора пароля	Угроза заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя. Данная угроза обусловлена слабостями механизма аутентификации, а так же значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: - время подбора в основном определяется не объёмом аутентификационной информации, а объёмом данных её хеш-кода; - восстановленная аутентификационная информация может не совпадать с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную».	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя, микропрограммное обеспечение BIOS/UEFI.	Нарушение конфиденциальности, доступности
2.2.15	Угроза использования уязвимостей используемого ПО	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействии на компоненты систему путём эксплуатации неправомерно полученных нарушителем дополнительных прав на управление дискредитированным объектом. Данная угроза обусловлена уязвимостями программного обеспечения, протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов. Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными; при наличии у нарушителя программного обеспечения (типа «эксплойт»), специально разработанного для реализации данной угрозы в дискредитируемой системе.	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, информационная система, средство защиты информации	Нарушение конфиденциальности, доступности, целостности.
2.2.16	Угроза наличия недекларированных возможностей в СПО	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) путём эксплуатации недекларированных возможностей в системном программном обеспечении. Данная угроза обусловлена наличием в системном про-	Внешний нарушитель с высоким потенциалом	Системное программное обеспечение.	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		граммном обеспечении функциональных возможностей, не описанных в документации. Реализация данной угрозы возможна при выявлении/наличии у нарушителя сведений о недокументированных функциональных возможностях в системном программном обеспечении.			
2.2.17	Угроза наличия недекларированных возможностей в ППО	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) путём эксплуатации недекларированных возможностей в прикладном программном обеспечении. Данная угроза обусловлена наличием в прикладном программном обеспечении функциональных возможностей, не описанных в документации. Реализация данной угрозы возможна при выявлении/наличии у нарушителя сведений о недокументированных функциональных возможностях в прикладном программном обеспечении.	Внешний нарушитель с высоким потенциалом	Прикладное программное обеспечение.	Нарушение конфиденциальности, доступности, целостности.
2.2.18	Угроза установки уязвимых версий программного обеспечения	Угроза заключается в возможности осуществления перехода на использование версий ПО (в том числе BIOS/UEFI), содержащей уязвимости, (например путём создания необходимости выполнения процедуры восстановления предыдущей версии программного обеспечения, предварительно подменённой нарушителем, либо внесения уязвимостей в программное обеспечение в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации или выполнения вредоносного кода при каждом запуске компьютера). Данная угроза обусловлена недостаточностью мер разграничения доступа и контроля целостности резервных копий программного обеспечения, а также слабостями технологий контроля за обновлением программного обеспечения (например, при осуществлении штатной процедуры восстановления работоспособности системы – «откат» системы к предыдущему работоспособному состоянию) Реализация данной угрозы возможна в ходе проведения	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Программное обеспечение, микропрограммное и аппаратное обеспечение BIOS/UEFI	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		ремонта и обслуживания компьютера в следующих условиях: нарушитель успешно подменил резервную копию программного обеспечения; возникла необходимость восстановления предыдущей версии программного обеспечения (данное условие может произойти как случайно, так и быть спровоцировано нарушителем). Также реализация данной угрозы возможна в случае наличия у пользователя прав на самостоятельную установку ПО			
2.2.19	Угроза несанкционированного доступа к BIOS с последующим внесением изменением в его конфигурацию	Угроза заключается в следующих возможностях нарушителя: 1) сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»); 2) подмены загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы; 3) изменения параметров и (или) логики работы программного обеспечения BIOS/UEFI путём программного воздействия из операционной системы компьютера или путём несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора; 4) осуществления несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера путём ввода «пустого» пароля; 5) изменения режимов работы аппаратных элементов компьютера путём несанкционированного переконфигурирования BIOS/UEFI, что позволяет: - за счёт изменения частоты системной шины, режима передачи данных по каналам связи и т.п. повлиять на общую производительность компьютера или вызвать сбои в его работе; - за счёт понижения входного напряжения, отключения систем охлаждения временно обеспечить неработоспособность компьютера; - за счёт задания недопустимых параметров работы устройств (порогового значения отключения устройства	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		при перегреве, входного напряжения и т.п.) привести к физическому выходу из строя отдельных аппаратных элементов компьютера; 6) неправомерного использования пользователями декларированного функционала BIOS/UEFI, ориентированного на администраторов. Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI, слабостями технологий разграничения доступа к управлению BIOS/UEFI, его функциям сброса пароля, администрирования и обновления. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера, наличия привилегий на изменение соответствующих параметров настройки BIOS/UEFI, наличия в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля непосредственно из-под операционной системы, наличия у нарушителя специальных программных средств, реализующих сброс пароля, а также прав в операционной системе для установки и запуска данных средств, при условии наличия BIOS/UEFI функционала обновления и (или) управления программным обеспечением BIOS/UEFI из операционной системы			
2.2.20	Угроза несанкционированного доступа вследствие наличия у пользователей излишних привилегий на установку и запуск приложений	Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, в т.ч.: доступа к скрытым/защищаемым каталогам или файлам; вывода данных на периферийные устройства; доступа к носителям информации; доступа к системным утилитам вследствие: наличия у него избыточных прав , в т.ч. унаследованных от пользователя или группы пользователей, выполняющих роль администраторов дискредитируемой системы; доступа к потоку данных, созданных приложением с дополнительными привилегиями. Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы; недостаточностью мер защиты информации от утечки и контроля потоков данных; уязвимостями программного обеспечения,	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение объекты файловой системы АРМ; сетевой узел, сетевой трафик, носитель информации.	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		использующего в своей работе участки кода, исполняемого с дополнительными правами, наследуемыми создаваемыми привилегированными потоками; уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации), приводящими к некорректному распределению прав доступа внутри древа наследуемых процессов; слабостью мер ограничения доступа к системным функциям. Реализация данной угрозы возможна при условиях: 1) наличие у нарушителя прав доступа к некоторым объектам файловой системы и каналам передачи данных; привилегий на установку и запуск программного обеспечения (в т.ч. системных утилит), виртуальных драйверов принтеров и др.; 2) наличие у дискредитируемого приложения слишком высоких привилегий доступа к файлам, обработка которых не предполагается с его помощью, а также участков кода, требующие исполнения с правами, превышающими права обычных пользователей			
2.2.21	Угроза подмены программного обеспечения	Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного обеспечения за счёт загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. Данная угроза обусловлена наличием у пользователя прав для установки программного обеспечения из сети Интернет. Реализация данной угрозы возможна при скачивании программного обеспечения в сети Интернет.	Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	Нарушение конфиденциальности, доступности, целостности.
2.2.22	Угроза внедрения вредоносного кода или данных на АРМ пользователей	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему вредоносного кода (в т.ч. скрытно устанавливаемых программ при посещении сайтов с неблагонадёжным содержимым); несанкционированного криптографического преобразования защищаемой информации с помощью известного только нарушителю секретного ключа; нарушение вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) дру-	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, объект файловой системы, виртуальная	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		гих виртуальных машин) Данная угроза обусловлена наличием слабостями мер антивирусной защиты; механизмов фильтрации сетевого трафика; механизмов разграничения доступа. Реализация данной угрозы возможна в случае работы с файлами, поступающими из не доверенных источников, или при наличии у пользователя привилегий установки программного обеспечения, а также при условии наличия выхода с дискредитируемого вычислительного устройства в сеть Интернет		машина сервера; сетевой узел	
2.2.23	Угроза внедрения вредоносного кода или данных на серверах	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему вредоносного кода (в т.ч. скрытно устанавливаемых программ при посещении сайтов с неблагонадёжным содержимым); несанкционированного криптографического преобразования защищаемой информации с помощью известного только нарушителю секретного ключа; Данная угроза обусловлена наличием слабостями мер антивирусной защиты; механизмов фильтрации сетевого трафика; механизмов разграничения доступа. Реализация данной угрозы возможна в случае работы с файлами, поступающими из не доверенных источников, или при наличии у пользователя привилегий установки программного обеспечения, а также при условии наличия выхода с дискредитируемого вычислительного устройства в сеть Интернет	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, сетевой узел, объект файловой системы.	Нарушение конфиденциальности, доступности, целостности.
2.2.24	Угроза внедрение вредоносного кода при использовании электронной почты и сети Интернет	Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа «почтовый червь», а также невольного участия в дальнейшем противоправном распространении вредоносного кода. Данная угроза обусловлена слабостями механизмов антивирусного контроля. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя электронного почтового ящика, а также наличия в его адресной книге хотя бы одно-	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		го адреса другого пользователя			
2.2.25	Угроза нарушения функционирования web-приложений	Угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы, или отправки дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс таким образом, что он будет выполнен на рабочей станции просматривающего этот сайт пользователя, либо в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта, а также уязвимостями браузеров и слабостями (или отсутствием) механизма проверки вводимых данных на веб-серверах. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему; в случае если пользователь сохраняет аутентификационную информацию с помощью браузера; либо в случае получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	Нарушение конфиденциальности Нарушение целостности Нарушение доступности
2.2.26	Угроза получения сведений об информационной системе	Угроза заключается в возможности нарушителя проведения процедуры сканирования дискредитируемой системы (портов, сетевых узлов) для получения различных сведений о системе (топологии, конфигурации, потенциальных уязвимостей и др.), позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, слабостями механизмов сетевого	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	Нарушение конфиденциальности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с отсутствием механизмов контроля входных и выходных данных. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика.			
2.2.27	Угроза исследования работы приложения	Угроза заключается в возможности проведения нарушителем исследования кода программы и анализа генерируемых этой программой отчётов об ошибках с целью определения её предполагаемой структуры и алгоритма работы для поиска в ней уязвимостей. Данная угроза обусловлена слабостями механизма защиты кода программы от исследования и размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчётах об ошибках. Реализация данной угрозы возможна в случаях наличия у нарушителя доступа к исходным файлам программы либо её дистрибутиву, при отсутствии механизма защиты кода программы от исследования, а также в случае наличия у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных.	Внутренний нарушитель со средним потенциалом, Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	Нарушение конфиденциальности, доступности.
2.2.28	Угроза несанкционированного копирования защищаемой информации	Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	Нарушение конфиденциальности

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		обработки защищаемой информации в нешифрованном виде.			
2.2.29	Угроза несанкционированного восстановления удалённой защищаемой информации	Угроза заключается в возможности осуществления прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации. Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удалённая с машинного носителя, в большинстве случаев может быть восстановлена. Реализация данной угрозы возможна при следующих условиях: - удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных (например, физическое уничтожение машинного носителя информации); - технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; - информация не хранилась в криптографически преобразованном виде	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Машинный носитель информации	Нарушение конфиденциальности
2.2.30	Угроза использования технологий беспроводного доступа	Угроза заключается в возможности получения нарушителем доступа к аутентификационной или другой защищаемой информации, либо ресурсам всей дискредитируемой информационной системы через используемые в её составе беспроводные каналы передачи данных, а также в возможности автоматического разрыва соединения беспроводной точки доступа с санкционированным клиентом беспроводной сети Данная угроза обусловлена слабостью технологий сетевого взаимодействия по беспроводным каналам передачи данных Реализация данной угрозы возможна при условии наличия у нарушителя специализированного программного обеспечения, реализующего функции эксплуатации уязвимостей протоколов идентификации/аутентификации беспроводных	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение	Нарушение конфиденциальности, доступности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		сетей, а также нахождения в точке приёма сигналов дискредитируемой беспроводной сети.			
2.2.31	Угроза несанкционированного доступа к компонентам среды виртуализации	Угроза заключается в возможности осуществления деструктивного программного воздействия (таких как: отказ легальным пользователям в выделении компьютерных ресурсов приведение виртуальной инфраструктуры в состояние «отказ в обслуживании»; деструктивное программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски; эксплуатация уязвимостей консоли управления гипервизором) на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин) Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации; уязвимостями программного обеспечения уровня управления; ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры; наличием у данного оборудования фиксированного сетевого адреса, наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной. Реализация данной угрозы возможна при условии успешного осуществления нарушителем несанкционированного доступа к программному обеспечению уровня управления виртуальной инфраструктурой, а также наличия у нарушителя специальных программных средств, способных эксплуатировать уязвимости технологий защиты виртуальных инфраструктур.	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина, сервер, сетевое оборудование, сетевой трафик, виртуальные устройства, гипервизор, виртуальные устройства хранения, обработки и передачи данных, объект файловой системы.	Нарушение конфиденциальности, доступности, целостности.
2.2.32	Угроза приведения системы в состояние «отказ в обслуживании»	Угроза заключается в возможности осуществления нарушителем воздействия на дискредитируемую систему с целью доведения её до состояния «отказ в обслуживании» Данная угроза обусловлена тем, что для обработки каждого сетевого запроса системой потребляется часть её ресурсов, а также слабостями сетевых технологий, связанными с	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой	Нарушение доступности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		ограниченностью скорости обработки потоков сетевых запросов, и недостаточностью мер контроля за управлением соединениями, мер контроля подлинности сетевых запросов на сторонних серверах, а также слабостями модели взаимодействия открытых систем. Реализация данной угрозы возможна при условии превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы (таких как способность переносить повышенную нагрузку или приобретать дополнительные ресурсы для предотвращения их исчерпания). Ключевым фактором успешности реализации данной угрозы является число запросов, которое может отправить нарушитель в единицу времени: чем больше это число, тем выше вероятность успешной реализации данной угрозы для дискредитируемой системы. Так же в распоряжении нарушителя должны быть сведения сторонних серверах с недостаточными мерами контроля подлинности сетевых запросов, о сетевом адресе дискредитируемой системы и специальное программного обеспечения, реализующего функции генерации сетевых пакетов.		трафик	
2.2.33	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	Угроза заключается в возможности нарушителя при взаимодействии «клиент-сервер» выдавать себя как за легитимного пользователя и выполнять приём/передачу данных от его имени, так и за сервер, тем самым ознакамливаясь с защищаемой информацией (в т.ч. аутентификационной, как передаваемой при подключении, так и хранящейся во временных файлах cookie), в т.ч. путём проведения различных мошеннических действий таких как скрытное перенаправление пользователя на поддельный сайт (выглядящий одинаково с оригинальным) или скрытой подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Данную угрозу можно охарактеризовать как «имитация действий клиента», «имитация действий сервера». Данная угроза обусловлена уязвимостями сетевого оборудования (маршрутизатора, DNS-сервера), а так же слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности содер-	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер, информация, хранящаяся на компьютере во временных файлах (программное обеспечение)	Нарушение конфиденциальности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		жимого электронного сообщения, а также при непринятии мер по стиранию остаточной информации из временных файлов (очистке временных файлов). Реализация данной угрозы возможна при наличии у нарушителя подключения к вычислительной сети, а также сведений о конфигурации сетевых устройств, типе используемого программного обеспечения и неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных.			
2.2.34	Угроза реализации атаки "человек посередине" при передаче информации за пределы контролируемой зоны	Угроза заключается в возможности нарушителя при взаимодействии «клиент-сервер» выдавать себя как за легитимного пользователя и выполнять приём/передачу данных от его имени, так и за сервер, тем самым ознакамливаясь с защищаемой информацией (в т.ч. аутентификационной), в т.ч. путём проведения различных мошеннических действий таких как скрытное перенаправление пользователя на поддельный сайт (выглядящий одинаково с оригинальным) или скрытой подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Данную угрозу можно охарактеризовать как «имитация действий клиента», «имитация действий сервера». Данная угроза обусловлена уязвимостями сетевого оборудования (маршрутизатора, DNS-сервера), а так же слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности содержимого электронного сообщения. Реализация данной угрозы возможна при наличии у нарушителя подключения к вычислительной сети, а также сведений о конфигурации сетевых устройств, типе используемого программного обеспечения и неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных.	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик, рабочая станция, сервер.	Нарушение конфиденциальности, целостности.
2.2.35	Угроза утечки пользовательских данных при использовании функ-	Угроза заключается в возможности утечки пользовательских данных за счёт использования реализованной в браузерах функции автоматического заполнение форм автори-	Внешний нарушитель со средним потенциалом	Аутентификационные данные пользователя (программное обес-	Нарушение конфиденциальности

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
	ций автоматического заполнения аутентификационной информации в браузере	зации. Реализация данной угрозы обусловлена хранением в браузерах в открытом виде пользовательских данных, используемых для автозаполнения форм авторизации. Реализация данной угрозы возможна при условии, что пользователь использует браузер, в котором реализована и активирована функция автоматического заполнения форм авторизации.		печение)	
2.2.36	Угроза наличия ошибок в ходе проектирования, разработки и отладки системы	Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, избыточных компонентов, а также возможностью перехвата управления программой за счёт использования отладочных механизмов. Реализация данной угрозы возможна при условии необоснованного выбора для применения в системе компонентов, внесения изменений в перечень задач, решаемых проектируемым программным обеспечением и если в программе не удалены отладочные механизмы.	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры	Нарушение конфиденциальности, доступности, целостности.
2.2.37	Угроза внедрения уязвимостей/ошибок в ходе проведения ремонта/обслуживания оборудования	Угроза заключается в возможности заставить компоненты системы выполнять вредоносный код при каждом запуске компьютера (например внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения, уже содержащего вредоносный код), а также в возможности выведения из строя компьютера из-за внесения критических ошибок в программное или аппаратное обеспечение в результате нарушения процесса его обновления/модернизации/ремонта. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения или аппаратного обеспечения. Реализация данной угрозы возможна как умышленно, так и неумышленно в ходе проведения ремонта и обслуживания компьютера как при установке корректной/совместимой версии обновления (из-за сбоев, помех и т.п.), так и при установке повреждённой/несовместимой версии обновления (из-за отсутствия механизма проверки целостности и	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	Нарушение конфиденциальности, доступности, целостности.

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		совместимости)			
2.2.38	Угроза слабости механизмов контроля входных данных	Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему либо в обход штатных механизмов (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения; доступ через командную строку в обход графического интерфейса; использование декларированных возможностей программных и аппаратных средств нестандартным способом; использование функций отладки; ввод данных неподдерживаемого формата; синхронное или асинхронное деструктивное программное воздействие на поток данных), а также осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы и механизма контроля входных данных Реализация данной угрозы возможна при условиях: - наличие у нарушителя доступа к программным и аппаратным средствам; - наличие у нарушителя прав доступа к некоторым объектам файловой системы; - возможности ввода произвольных данных в адресную строку; - возможности изменения интерфейса ввода входных данных; - отсутствие проверки вводимых пользователем данных; - наличие у нарушителя сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных; - наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр, аппаратное обеспечение, метаданные.	Нарушение конфиденциальности, доступности, целостности.
2.2.39	Угроза слабости или	Угроза заключается в возможности деструктивного про-	Внутренний нарушитель с	Системное про-	Нарушение кон-

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
	некорректной настройки механизмов контроля целостности и резервирования данных	граммного воздействия на часть функционала или всю информационную системы путём осуществления манипуляций с используемыми ей конфигурационными файлами, библиотеками, данными реестра (в том числе вследствие некорректного завершения работы операционной системы, возникновения ошибок в работе драйверов устройств и т.п.) в результате которых возможно, в т.ч. нарушение целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями, а также мер восстановления работоспособности как приложений, так и защищаемой информации. Реализация данной угрозы возможна в случае наличия у нарушителя прав осуществления записи в файловые объекты, связанные с конфигурацией/средой окружения программы; возникновения ошибок в работе отдельных процессов или всей операционной системы; недостаточности принятые мер по обеспечению резервирования данных	низким потенциалом, Внешний нарушитель с низким потенциалом	граммное обеспечение, прикладное программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	фиденциальности Нарушение целостности Нарушение доступности
2.2.40	Угроза слабости или некорректной настройки механизмов фильтрации сетевого трафика	Угроза заключается в возможности нарушения безопасности защищаемой информации при межсетевом взаимодействии, в т.ч. внутри сегментов ЛВС. Данная угроза обусловлена уязвимостями в сетевом программном обеспечении и слабостями механизмов межсетевого экранирования. Реализация данной угрозы возможна при условии наличия выхода с дискредитируемого вычислительного устройства в сеть Интернет, а также наличия доступа нарушителя к вычислительной сети.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	Нарушение конфиденциальности Нарушение целостности Нарушение доступности
2.2.41	Угроза слабости или некорректной настройки механизмов контроля и разграничения доступа к защищаемой информации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов доступа; за счёт ошибок в параметрах настройки средств разграничения доступа; путём извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей с машинных носителей информации; неправомерного доступа к аутентификационной информации других пользователей с помощью штат-	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение, сетевое программное обеспечение, учётные данные пользователя, реестр,	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		ных средств операционной системы или специальных программных средств; внесения изменений в используемый дискредитируемым приложением реестр; создания в системе дополнительной учётной записи пользователя, внесения изменений в журналы регистрации событий безопасности дискредитируемой системы, несанкционированного изменения параметров настройки средства защиты информации. Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации. Реализация данной угрозы возможна при условии наличия у нарушителя необходимых прав доступа.		машинные носители информации, метаданные, микропрограммное обеспечение, средство защиты информации	
2.2.42	Угроза анализа криптографических алгоритмов и их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	Нарушение конфиденциальности Нарушение целостности
2.2.43	Угроза нарушения функционирования технологических/информационных процессов вследствие некорректной работы средств защиты информации	Угроза заключается в возможности приведения системы в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации средствами защиты информации, вызванной необходимостью обработки передаваемой/обрабатываемой информации на предмет выявления и нейтрализации угроз безопасности информации и (или) за счёт нарушения работы компьютера и отказа в доступе к его данным за счёт ошибочного блокирования средством защиты информации файлов. На реализацию данной угрозы влияет не только номенклатура применяемых средств защиты информации, параметры их настройки, объём передаваемой/обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются сред-	Внешний нарушитель с низким потенциалом	Средство защиты информации, аппаратное устройство, программное обеспечение	Нарушение доступности

№ п/п	Наименование УБИ	Описание УБИ	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Последствия реализации угрозы
		ствами защиты информации			
2.2.44	Угроза несанкционированного воздействия на средство защиты информации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к программной среде управления средством защиты информации и изменения режима его функционирования. Угроза обусловлена наличием у средств защиты информации программной среды управления и взаимодействия с пользователями системы. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации.	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Средство защиты информации	Нарушение конфиденциальности, доступности, целостности.
2.2.45	Угроза несанкционированного изменения параметров настройки средств защиты информации	Угроза заключается в возможности осуществления нарушителем несанкционированного изменения параметров настройки средства защиты информации. Данная угроза обусловлена слабостями мер разграничения доступа к конфигурационным файлам средства защиты информации. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации, а также при наличии у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации	Внутренний нарушитель с низким потенциалом, Внешний нарушитель с низким потенциалом	Средство защиты информации	Нарушение конфиденциальности, доступности, целостности.
2.2.46	Угроза проникновения из смежных ИС с более низким уровнем защищенности	Угроза заключается в возможности осуществления нарушителем воздействия на дискредитируемую систему через смежные с ней системы, для которых предъявляются более низкие требования по защите информации. Нарушитель, получив доступ к систем, для которой установлен более низкий уровень защищенности (в связи с нереализацией тех или иных мер защиты информации, не являющимися обязательными для данной системы) может с меньшими усилиями получить доступ к дискредитируемой системе. Реализация данной угрозы возможна в случае отсутствия регламентации требований по подключению смежных информационных систем и (или) отсутствию сегментирования внутри вычислительной сети, в рамках которой функционируют информационные системы различных уровней защищенности.	Внутренний нарушитель с низким потенциалом, Внешний нарушитель со средним потенциалом	Информационная система	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

MPLS	-	Multiprotocol Label Switching — многопротокольная коммутация по меткам
VPN	-	Virtual Private Network — виртуальная частная сеть
АРМ	-	Автоматизированное рабочее место
БД	-	База данных
БДУ	-	Банк данных угроз безопасности информации ФСТЭК России
ГИС	-	Государственных информационных системах
ГОСТ	-	Государственный стандарт
ДГУ	-	Бензиновые/дизельные генераторные установки
ЗВК	-	Защищённый виртуальный кластер
ИБП	-	Источник бесперебойного питания
ИОГВ	-	Исполнительные органы государственной власти
ИР	-	Информационной ресурс
ИС	-	Информационная система
ИСПДн	-	Информационных системах персональных данных
КЗ	-	Контролируемая зона
ЛВС	-	Локально-вычислительная сеть
МП	-	Многопользовательский режим обработки информации
НСД	-	Несанкционированный доступ
ОРД	-	Организационно-распорядительных документов, регламентирующих процедуры обработки и защиты информации
ОП	-	Однопользовательский режим обработки информации
ОС	-	Операционная система
ПАК	-	Программно-аппаратный комплекс
ППО	-	Прикладное программное обеспечение
ПЭМИН	-	Побочные электромагнитные излучения и наводки
РМС ОГВ	-	Региональная мультисервисная сеть исполнительных органов государственной власти Краснодарского края
РПД	-	Разграничение прав доступа
СКЗИ	-	Средство криптографической защиты информации
СКУД	-	Система контроля и управления доступом
СМИО	-	Сеть международного информационного обмена
СОИБ	-	Система обеспечения информационной безопасности
СПО	-	Системное программное обеспечение
ССОП	-	Сеть связи общего пользования
ТКУИ	-	Технический канал утечки информации
УБИ	-	Угроза безопасности информации
УЗ	-	Уровень защищенности
ФСБ России	-	Федеральная служба безопасности Российской Федерации
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю
ЦОД	-	Центр обработки данных

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе использованы следующие термины и определения:

Термин	Описание	Источник
Атака «отказ в обслуживании»	Сетевая атака, приводящая к блокированию информационных процессов в автоматизированной системе	ГОСТ Р 53114-2008
Аттестация объекта информатизации	Комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации	ГОСТ РО 0043-003-2012
Аутентификация (субъекта доступа)	Действия по проверке подлинности субъекта доступа в автоматизированной информационной системе	Р 50.1.053-2005
Безопасности информации	Состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность	ГОСТ Р 50922-2006
Блокирование доступа (к информации)	Прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей)	ГОСТ Р 53114-2008
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы автоматизированной информационной системы	Р 50.1.053-2005
Доступ к информации	Возможность получения информации и ее использования	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Доступность	Состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно	Р 50.1.053-2005
Закладочное устройство	Техническое средство, скрытно устанавливаемое на объекте информатизации или в контролируемой зоне с целью перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы	Р 50.1.053-2005

Термин	Описание	Источник
	автоматизированной информационной системы	
Защита информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	ГОСТ Р 51624-2000
Идентификация	Действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов	Р 50.1.053-2005
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов	ГОСТ Р 52653-2006
Информация конфиденциального характера	Информация, не содержащая сведения, составляющие государственную тайну, доступ к которой ограничен законодательством Российской Федерации	ГОСТ РО 0043—003—2012
Информация, составляющая коммерческую тайну	Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введён режим коммерческой тайны	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
Инцидент информационной безопасности	Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.	ГОСТ Р ИСО/МЭК 27001-2006
Источник угрозы безопасности информации	Субъект, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности	Р 50.1.053-2005

Термин	Описание	Источник
	информации	
Коммерческая тайна	Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
Компьютерный вирус	Вредоносная программа, способная создавать вредоносные программы и (или) свои копии	Р 50.1.053-2005
Контролируемая зона	Пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и/или транспортных средств	ГОСТ Р 51624-2000
Конфиденциальность	Состояние информации (ресурсов автоматизированной информационной системы), при котором доступ к ней (к ним) осуществляют только субъекты, имеющие на него право	Р 50.1.053-2005
Меры обеспечения информационной безопасности	Совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности	ГОСТ Р 53114-2008
Модель угроз	Физическое, математическое, описательное представление свойств и характеристик угроз безопасности информации	ГОСТ Р 50922-2006
Нарушитель информационной безопасности организации	Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации	ГОСТ Р 53114-2008
недекларированные возможности (программного обеспечения)	Функциональные возможности программного обеспечения, не описанные в документации	Р 50.1.053-2005
Несанкционированный доступ к информации (ресурсам автоматизированной информационной системы)	Доступ к информации (ресурсам автоматизированной информационной системы), осуществляемый с нарушением установленных прав и (или) правил доступа к информации (ресурсам автоматизированной информационной системы)	Р 50.1.053-2005
Обработка информации	Совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации	ГОСТ Р 51624-2000

Термин	Описание	Источник
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	Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»
Объект доступа	Единица ресурса автоматизированной информационной системы, доступ к которой регламентируется правилами разграничения доступа	Р 50.1.053-2005
Объект информатизации	Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров	ГОСТ Р 51275-2006
Организационные меры обеспечения информационной безопасности	Меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации	ГОСТ Р 53114-2008
Перехват информации	Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов	Р 50.1.053-2005
Персональные данные	Любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»
побочное электромагнитное излучение	Электромагнитное излучение, наблюдаемое при работе технических средств обработки информации	ГОСТ Р 51275-2006
Потенциал нарушителя	Мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе	Банк данных угроз безопасности информации ФСТЭК России (На основе МД

Термин	Описание	Источник
		ФСТЭК России «Меры ЗИ в государственных ИС»)
Правила разграничения доступа	Правила, регламентирующие условия доступа субъектов доступа к объектам доступа	Р 50.1.053-2005
Программная закладка	Преднамеренно внесённые в программное обеспечение функциональные объекты, которые при определённых условиях инициируют реализацию недекларированных возможностей программного обеспечения	Р 50.1.053-2005
Программное воздействие	Несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ	ГОСТ Р 51275-2006
Разглашение информации	Несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации.	ГОСТ Р 53114-2008
Распределённая информационная система	Комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединённых в единую информационную систему средствами связи с использованием технологии удалённого доступа	ГОСТ РО 0043—003—2012
Санкционированный доступ к информации	Доступ к информации, не нарушающий правила разграничения доступа	Руководящий документ Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 года
Служебная тайна	Защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости	ГОСТ Р 51624-2000

Термин	Описание	Источник
Средство защиты информации от утечки по техническим каналам	Техническое средство, вещество или материал, предназначенные и (или) используемые для защиты информации от утечки по техническим каналам	Р 50.1.056-2005
Средство защиты от несанкционированного доступа	Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа	ГОСТ Р 53114-2008
Средство криптографической защиты информации	Средство защиты информации, реализующее алгоритмы криптографического преобразования информации	ГОСТ Р 50922-2006
Средство обнаружения вторжений	Программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности	ГОСТ Р 53114-2008
Субъект доступа	Лицо или единица ресурса автоматизированной информационной системы, действия которой по доступу к ресурсам автоматизированной информационной системы регламентируются правилами разграничения доступа	Р 50.1.053-2005
Техническое средство обеспечения информационной безопасности	Оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами	ГОСТ Р 53114-2008
Угроза безопасности информации	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на неё	ГОСТ Р 51624-2000
Уполномоченное лицо	Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключённого договора	Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Термин	Описание	Источник
Утечка (информации) по техническому каналу	Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.	Р 50.1.053-2005
Уязвимость	Свойство информационной системы, предоставляющее возможность реализации угроз безопасности, обрабатываемой в ней информации.	Р 50.1.056-2005
Целостность	Состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право.	Р 50.1.053-2005

ПЕРЕЧЕНЬ ИЛЛЮСТРАЦИЙ

ПЕРЕЧЕНЬ ТАБЛИЦ