СОГЛАСОВАНО
Генеральный директор
ООО «ТСС»

_____ В.В. Сергиев
«23» ноября 2017 г.

УТВЕРЖДАЮ
Руководитель департамента
информатизации и связи
Краснодарского края

_____ Е.В. Юшков
«28» декабря 2017 г.

МОДЕЛЬ НАРУШИТЕЛЯ 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) и Модели угроз безопасности информации информационных систем (далее – ИС) ИОГВ Краснодарского края.

Модель нарушителя безопасности информации информационных систем исполнительных органов государственной власти Краснодарского края (далее – Модель нарушителя) содержит модель угроз (перечень угроз) и модель нарушителя (предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак на средства криптографической защиты информации (далее – СКЗИ) и среду функционирования криптосредств (далее – СФ), а также об ограничениях на эти возможности.

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

Модель нарушителя разработана на основании:

- Приказа ФСБ России от 10.07.2014 № 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»;
- Методических 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, утверждённых руководством 8 Центра ФСБ России от 31.03.2015 № 149/7/2/6-432.

СОДЕРЖАНИЕ

1 Общие положения

Разработка Модели нарушителя осуществляется с целью определения необходимого для применения класса СКЗИ.

Применение СКЗИ необходимо в связи с наличием угроз безопасности информации (в соответствии с Моделью угроз безопасности информации ИОГВ Краснодарского края), связанных с возможностью её перехвата (осуществления несанкционированных воздействий) нарушителем при передаче по каналам связи, нейтрализация которых возможна только с использованием СКЗИ.

Областью применения СКЗИ являются ИС ИОГВ Краснодарского края, в процессе эксплуатации которых осуществляется передача защищаемой информации по каналам связи (а том числе по информационно-телекоммуникационным сетям общего пользования).

Целью применения СКЗИ является обеспечение целостности, конфиденциальности и доступности информации, передаваемой между 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. В случаях, если в конкретных рассматриваемых ИС ИОГВ Краснодарского края перечень реализованных мер защиты информации меньше чем указанно в соответствующем разделе настоящей Модели нарушителя – для таких ИС ИОГВ Краснодарского края должны разрабатываться Частные модели нарушителя безопасности информационных систем.

2 Описание информационных систем

В зависимости от архитектуры, структуры (топологии) и назначения ИС, по результатам проведённого обследования объектов информатизации ИОГВ Краснодарского края, 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.

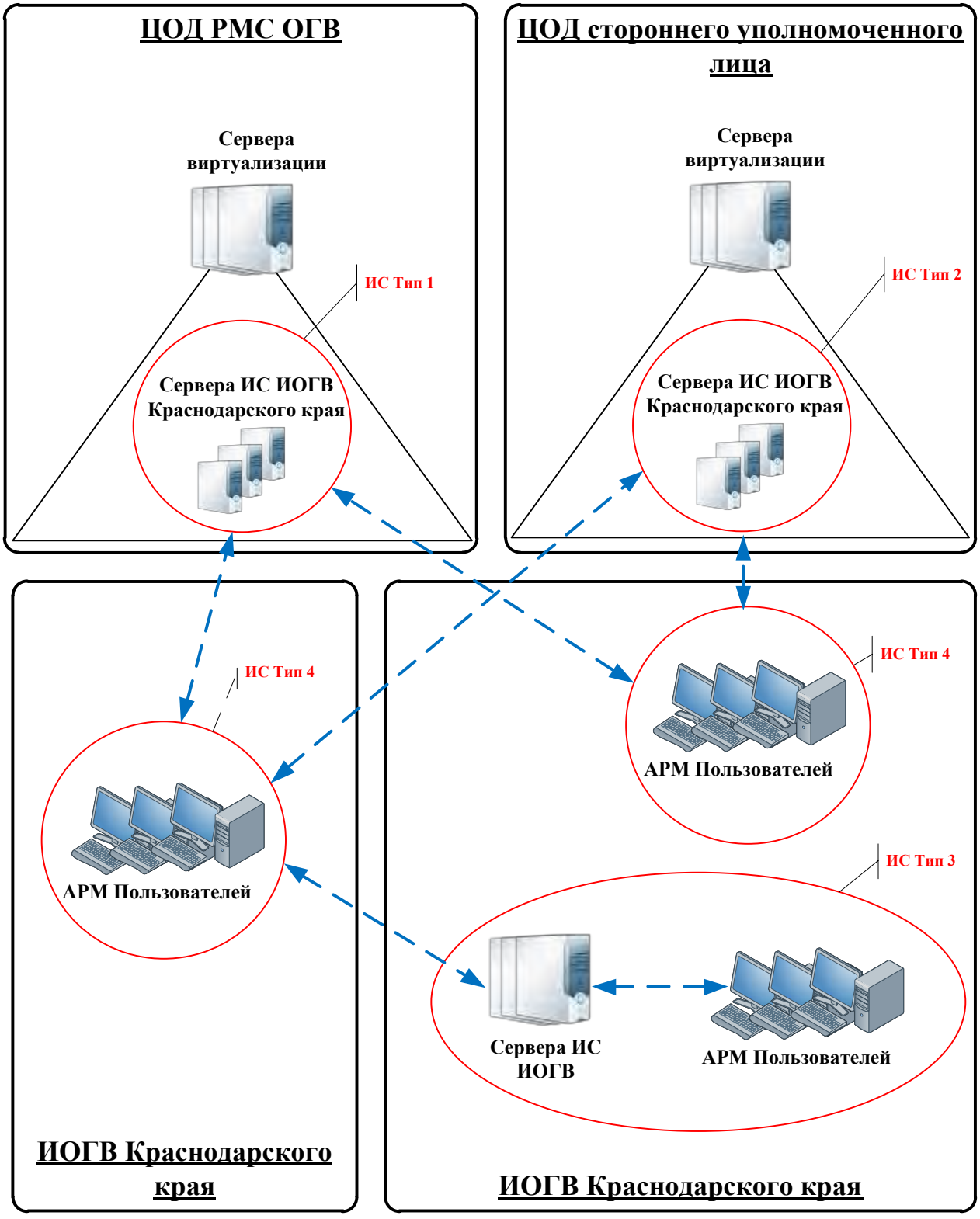


Рисунок 1 – Принципиальная схема организации ИС ИОГВ Краснодарского края

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 информационной системы.

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	+	+	+

[1] Конфиденциальность
[2] Целостность
[3] Доступность

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

Объектами защиты, безопасность которых необходимо обеспечить в ИС ИОГВ Краснодарского края, являются:

- документация на криптосредство и на технические и программные компоненты СФ;
- защищаемая информация;
- ключевая, аутентифицирующая и парольная информация;
- криптографически опасная информация;
- настроечная, конфигурационная информация;
- средства защиты информации (программные и аппаратные компоненты СЗИ);
- криптосредства (программные и аппаратные компоненты криптосредства);
- технические и программные компоненты СФ;
- данные, передаваемые по каналам связи;
- помещения, в которых находятся защищаемые ресурсы информационной системы.

2.4 Сведения о наличии каналов связи

Для ИС ИОГВ Краснодарского края Типа 1 и 2 характерно наличие нескольких высокоростных 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.

[4] За исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации

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 многоточёчный доступ к ССОП.

2.5 Меры защиты информации

2.5.1 Характеристики обеспечения физической безопасности

При разработке настоящей Модели нарушителя учитывается, что в ИС ИОГВ Краснодарского края реализованы следующие меры обеспечения безопасности:

- имеются посты охраны и ведётся контрольно-пропускной режим, исключающий неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа, в том числе посредством применения систем контроля и управления доступом. Допуск сотрудников на территорию объектов ИОГВ Краснодарского края осуществляется по выданным им proximity-картам[5] (электронные пропуска), либо служебным удостоверениям. Пропуск на объекты представителей сторонних организаций осуществляется в сопровождении должностного лица заинтересованного структурного подразделения ИОГВ Краснодарского;
- служебные помещения оборудованы надёжными дверями, по окончанию рабочего дня опечатываются и ставятся под охрану;
- для размещения серверного и телекоммуникационного оборудования выделены отдельные серверных помещения, оснащённые системами кондиционирования, средствами пожарной сигнализации. Серверное и телекоммуникационное оборудование располагается в телекоммуникационных шкафах и подключается к сети электропитания посредством применения источников бесперебойного питания.
- граница контролируемой зоны установлена по ограждающим конструкциям помещений размещения защищаемых компонентов ИС ИОГВ Краснодарского края или внешнему периметру охраняемого здания.
- контрольно-пропускной режим на объектах регламентирован организационно-распорядительными документами.

2.5.2 Характеристики, связанные с организацией обеспечения информационной безопасности

Указания на наличие тех или иных организационно-распорядительных документов, регламентирующих процедуры обработки и защиты информации (далее – ОРД), необходимых и достаточных для обеспечения функционирования СОИБ даны ниже по тексту настоящей Модели нарушителя.

[5] На объектах, где установлена система контроля и управления доступом

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

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

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

При разработке настоящей Модели нарушителя учитывается, что ИС ИОГВ Краснодарского края оснащены следующими средствами защиты информации:

— защиты информации от несанкционированного доступа;
— антивирусной защиты серверов;
— антивирусной защиты АРМ пользователей;
— межсетевого экранирования;
— криптографической защиты информации, передаваемой по каналам связи.

2.6 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[6]) 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;

Схема информационного взаимодействия, характерная 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.

В настоящей Модели нарушителя не рассматриваются вопросы, связанные с доступом граждан (с целью получения государственных услуг) к общедоступным информационным ресурсам посредством сети Интернет.

[6] Доступ к ИС ИОГВ Типа 1 и 2 осуществляется по каналу связи, защищённому посредством СКЗИ, передаваемой по каналам связи. В качество такого средства может выступать как ПАК, устанавливаемый на границе ЛВС ИС ИОГВ Краснодарского края, так и программное СКЗИ, устанавливаемое на АРМ пользователя

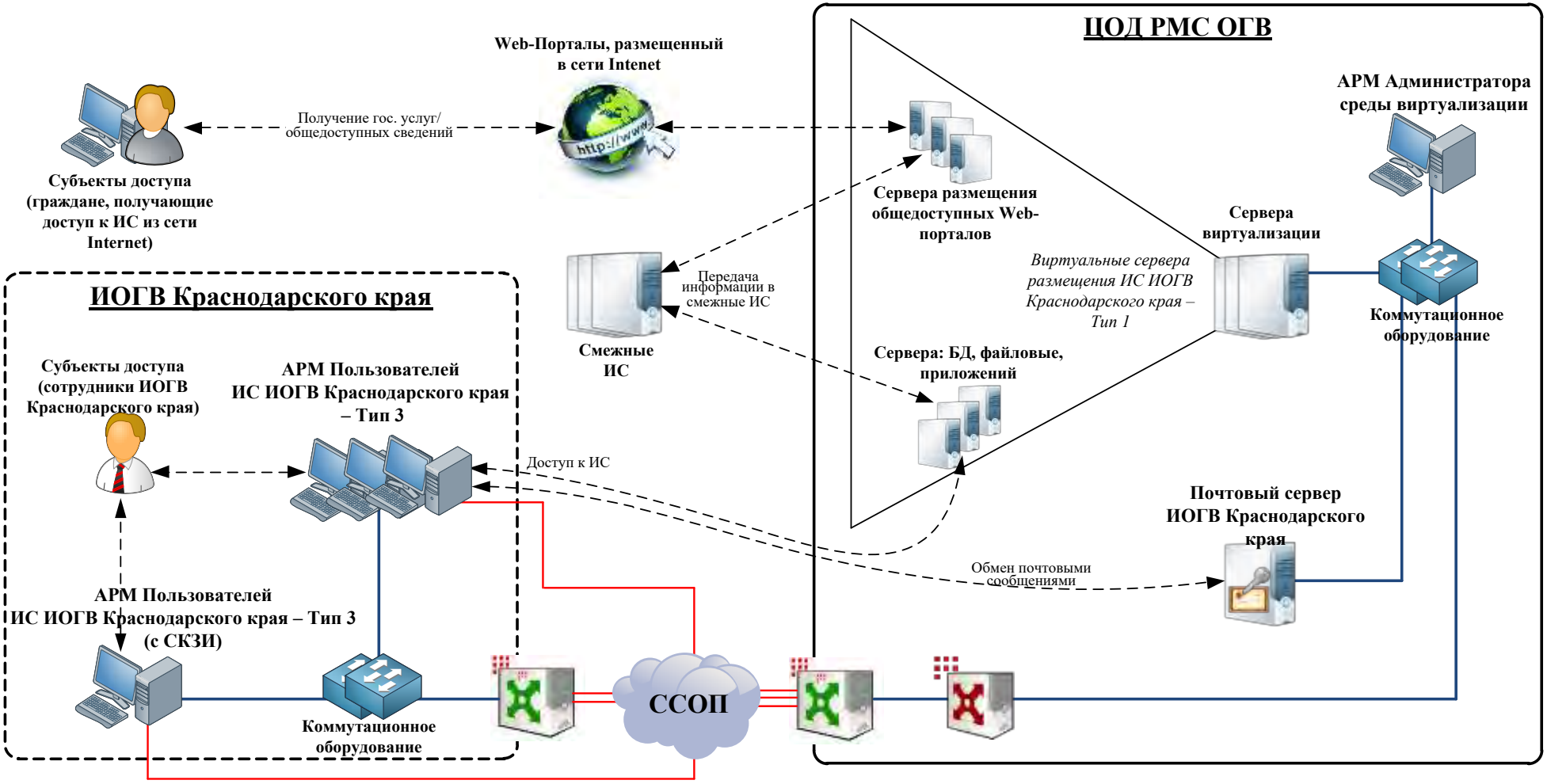
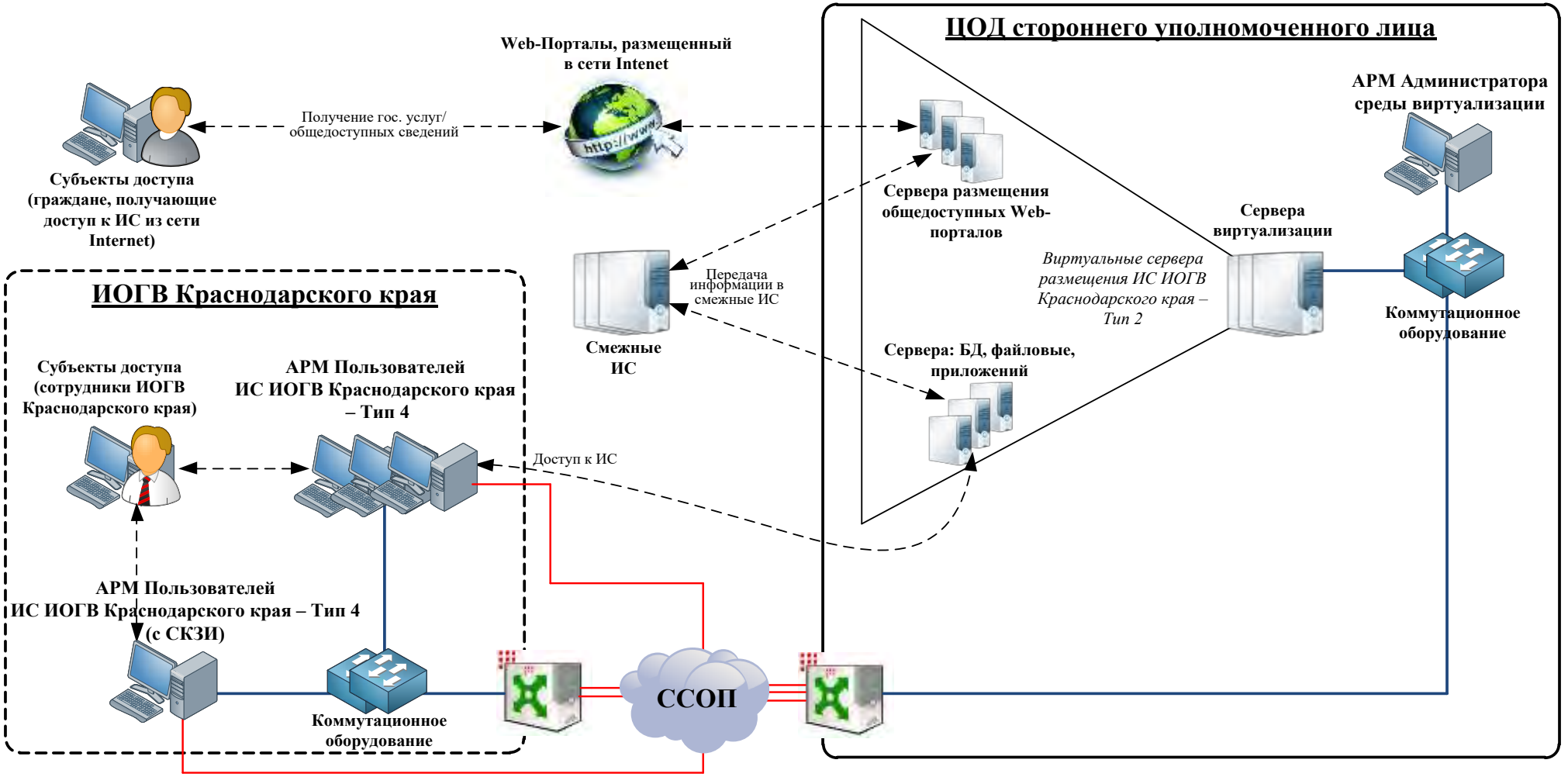


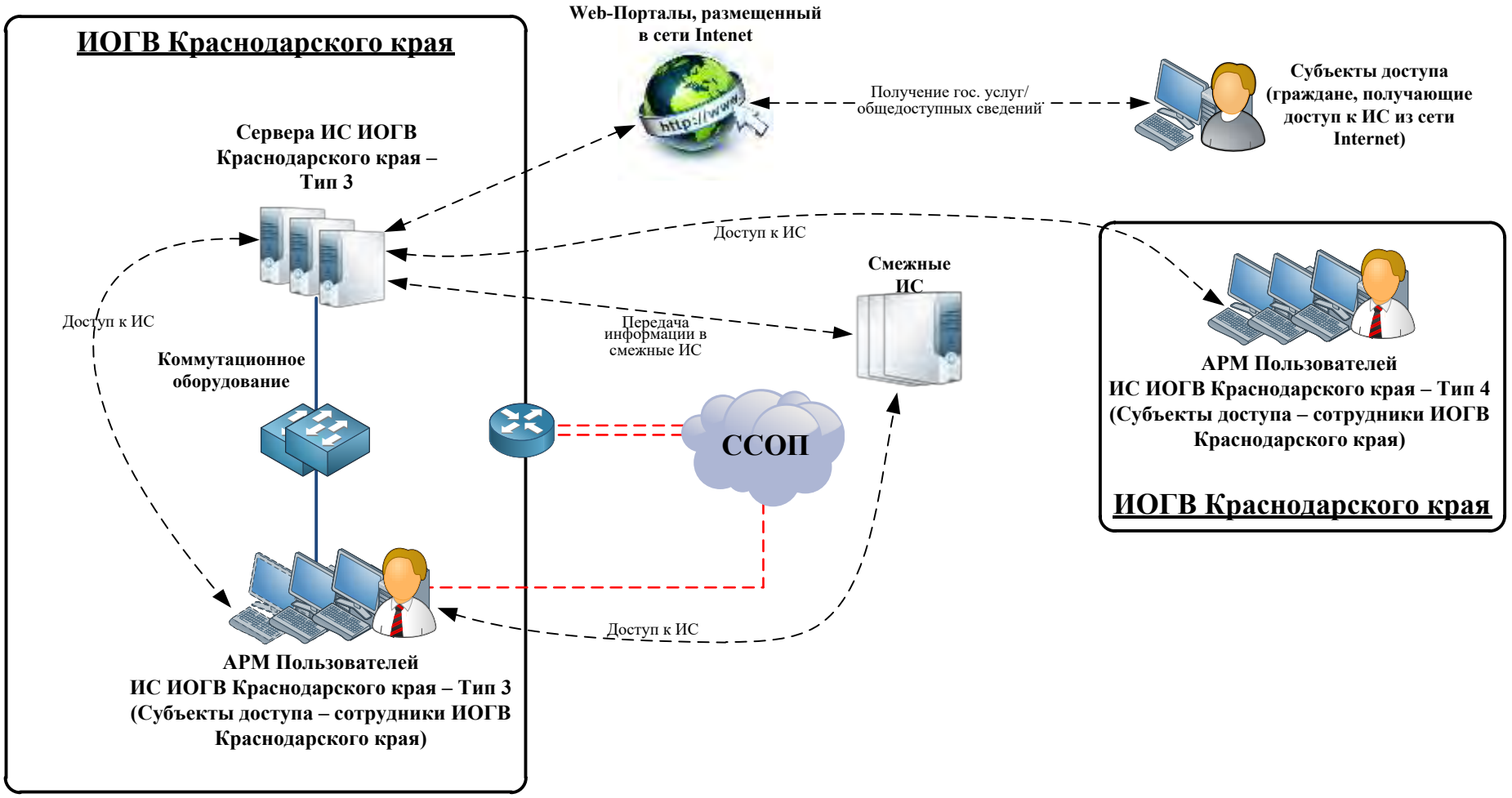
Рисунок 2 – Схема информационного взаимодействия ИС ИОГВ Краснодарского края типов 1 и 4



Условные обозначения:

- 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:

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

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

3 Модель угроз безопасности информации

Под угрозами безопасности информации 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, являющиеся атаками (атаки).

3.1 Угрозы, не являющиеся атаками

3.1.1 Угрозы, не связанные с деятельностью человека

Угрозами, не связанными с деятельностью человека являются бедствия и природные явления – землетрясения, наводнения, ураганы и др.

3.1.2 Угрозы социально–политического характера

Угрозами социально-политического характера являются забастовки, саботаж, локальные конфликты и т.д.

3.1.3 Угрозы техногенного характера

Угрозами техногенного характера являются:

— отказ электропитания серверного и телекоммуникационного оборудования;
— отказ электропитания АРМ пользователей;
— отказ подсистемы обеспечения температурного режима серверного и телекоммуникационного оборудования.

3.1.4 Ошибочные действия

Ошибочными действиями пользователей и обслуживающего персонала являются:

— разглашение конфиденциальной информации пользователями ИС;
— разглашение конфиденциальной информации сотрудниками подрядных организаций;
— утрата мобильных технических средств пользователями ИС или их передачи лицам, не имеющих права доступа к обрабатываемой на них информации;
— передача носителей информации лицам, не имеющих права доступа к хранимой на них информации;
— утрата носителей информации;
— физическое устаревание аппаратных компонентов ИС и (или) недостаточности вычислительных мощностей для решаемых задач;
— некорректная настройка программного обеспечения;

— использование информации идентификации/аутентификации, заданной по умолчанию;
— незащищённое удалённое администрирования информационной системы;
— привязка к поставщику вычислительных мощностей (уполномоченному лицу);
— недобросовестное исполнение обязательств поставщиком вычислительных мощностей (уполномоченным лицом);
— отсутствие распределения ролей между поставщиком вычислительных мощностей (уполномоченным лицом) и потребителем услуг (вычислительных мощностей);
— агрегирование данных, обрабатываемых с помощью мобильного устройства.

Защита от угроз, не являющихся атаками, регламентируется инструкциями, разработанными и утверждёнными в ИОГВ Краснодарского края с учётом условий эксплуатации ИС ИОГВ Краснодарского края и действующей нормативной базы.

3.2 Угрозы, являющиеся атаками

Атаки наносят наибольший урон и являются наиболее опасными угрозами, что обусловлено их тщательной подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак, многообразием применяемых средств проведения.

К основным атакам относятся:
— несанкционированный доступ (далее – НСД) к защищаемой информации;
— доступ к защищаемой информации на основе перехвата и анализа побочных сигналов, сопровождающих функционирование средств вычислительной техники (далее – СВТ);
— компьютерные атаки с использованием вредоносного ПО;

При информационном взаимодействии возможна реализация следующих угроз:
— угрозы утечки информации по техническим каналам;
— угрозы НСД.

3.2.1 Угрозы утечки информации по техническим каналам

Угрозы утечки информации по техническим каналам включают в себя:
— угрозы утечки акустической (речевой) информации;
— угрозы утечки видовой информации;
— угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее – ПЭМИН).

В ИС ИОГВ Краснодарского края функции голосового ввода информации или функции воспроизведения информации акустическими средствами отсутствуют. Акустический канал может позволить получить сведения об используемых для защиты информации криптосредствах только в случае, если пользователями ИС ведутся разговоры (как внутри, так и вне КЗ) на данную тематику. Комплекс организационных мер, реализованных в ИОГВ Краснодарского края, позволяет нейтрализовать данную угрозу. Таким образом, угрозы утечки акустической (речевой) информации являются неактуальными.

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие санкционированного доступа к информации, циркулирующей в ИС ИОГВ Краснодарского края, а также ТС просмотра, внедрённые в служебные помещения или скрытно используемые данными физическими лицами.

Угрозы утечки видовой (визуальной) информации реализуются за счёт просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения СВТ, входящих в состав ИС. Необходимым условием осуществления просмотра (регистрации) информации является наличие прямой видимости между указанными физическими лицами или средствами наблюдения и ТС ИС ИОГВ Краснодарского края, на которых визуально отображается защищаемая информация. Реализованный в ИОГВ Краснодарского края комплекс организационно-технических мер позволяет нейтрализовать данную угрозу. Таким образом, угрозы утечки видовой (визуальной) информации являются неактуальными.

Источником угроз утечки информации по каналам ПЭМИН являются внешние нарушители, не имеющие доступа к ИС ИОГВ Краснодарского края. 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. Реализованный в ИОГВ Краснодарского края комплекс организационно-технических мер ограничивает возможность перехвата информации по каналам ПЭМИН, однако полностью не исключают такой возможности.

3.2.2 Угрозы несанкционированного доступа

Угрозы, связанные с НСД, представляются в виде совокупности возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения, способов реализации угроз, объектов воздействия (носителей информации, директорий, каталогов, файлов) и возможных деструктивных действий.

Угрозы НСД с применением программных и программно-аппаратных средств реализуются за счёт несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение характеристик безопасности информации, и включают в себя:

- 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.

3.3 Источники угроз безопасности

Основными источниками угроз безопасности защищаемой информации при информационном взаимодействии могут быть:

— носитель вредоносной программы;
— аппаратная закладка;
— нарушитель.

3.3.1 Источник угроз безопасности - носители вредоносных программ

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер.

Если вредоносная программа ассоциируется с какой-либо прикладной программой, то в качестве её носителя рассматриваются:

— отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый жёсткий диск и т.п.;
— встроенные носители информации (жёсткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок);
— микросхемы внешних устройств.

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определённые расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то её носителями являются:

— пакеты передаваемых по компьютерной сети сообщений;
— файлы (текстовые, графические, исполняемые и т.д.).

Эффективная защита от вредоносных программ, которые могут распространяться через различные носители, может быть обеспечена за счёт обеспечения комплекса организационно-технических мер и систем антивирусной защиты.

3.3.2 Источник угроз безопасности - аппаратная закладка

Аппаратные закладки могут быть конструктивно встроенными и автономными.

Конструктивно встроенные аппаратные закладки создаются в ходе проектирования и разработки аппаратного обеспечения и могут проявляться в виде недекларированных возможностей различных элементов вычислительной системы.

Автономные аппаратные закладки являются законченными устройствами, выполняющими определённые функции перехвата, накопления, передачи или ввода/вывода информации.

Аппаратные закладки могут реализовать угрозы сбора и накопления информации конфиденциального характера.

Эффективная защита от аппаратных закладок может быть обеспечена за счёт соответствующей организации технической защиты информации на всех стадиях (этапах) жизненного цикла технических средств (этапы разработки, производства, хранения, транспортировки, ввода в эксплуатацию и эксплуатации).

3.3.3 Источник угроз безопасности - нарушитель

Под нарушителем понимается физическое лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

Все физические лица могут быть отнесены к следующим категориям:

— категория I (внешний нарушитель) - лица, не имеющие доступа в КЗ;

— категория II (внутренний нарушитель) - лица, имеющие право постоянного или разового доступа в КЗ.

Внешними нарушителями (лица типа I) могут быть:

— внешние субъекты (физические лица);

— пользователи ИС ИОГВ Краснодарского края, осуществляющие атаки из-за пределов КЗ.

Возможности внешних и внутренних нарушителей существенным образом зависят от действующих в пределах КЗ режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к защищаемой информации и контролю порядка проведения работ.

Внешний нарушитель не имеет непосредственного доступа к системам и ресурсам ИС ИОГВ Краснодарского края, находящимся в пределах КЗ. К нарушителю данного типа можно отнести физических лиц или организации, осуществляющие атаки с целью добывания информации, навязывания ложной информации, нарушения работоспособности ИС ИОГВ Краснодарского края, нарушения характеристик безопасности информации.

Внутренними нарушителями могут быть лица, имеющие доступ в КЗ и к ресурсам ИС ИОГВ Краснодарского края, включая пользователей ИС ИОГВ Краснодарского края, реализующих угрозы непосредственно внутри КЗ.

3.3.4 Потенциальные угрозы

Потенциальные угрозы обуславливаются наличием тех или иных возможностей у потенциальных нарушителей по реализации угроз. Исходный перечень потенциальных возможностей нарушителей, согласно Приказу ФСБ России от 10.07.2014 № 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», и класс СКЗИ применяемый для нейтрализации атак, при создании способов, подготовке и проведении которых используются данные возможности, представлены в таблице 2.

Рассмотрение актуальных угроз при обеспечении целостности обрабатываемой информации с использованием механизмов средств электронной подписи (далее – ЭП) не является предметом рассмотрения данного документа. Определение перечня актуальных угроз должно быть проведено в рамках отдельной работы и учитывать все возможные сценарии использования ЭП при выполнении ИОГВ Краснодарского края государственных функций.

Таблица 2 – Возможности потенциальных нарушителей и классы СКЗИ, требуемые для их нейтрализации

№	Возможности	Класс СКЗИ				
		КС1	КС2	КС3	КВ	КА
1	Создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ.	+	+	+	+	+
2	Создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ.	+	+	+	+	+
3	Проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее – контролируемая зона).	+	+	+	+	+
4	Проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак: – внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее – СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ; – внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.	+	+	+	+	+
5	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: – служебную информацию; – персональные данные; – ключевую, аутентифицирующую и парольную информацию СКЗИ; – программные компоненты СКЗИ; – аппаратные компоненты СКЗИ; – программные компоненты СФ; – аппаратные компоненты СФ (аппаратные средства, входящие в СФ, включая микросхемы с записанным микрокодом BIOS, осуществляющей инициализацию этих средств); – данные, передаваемые по каналам связи; – иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учётом применяемых в информационной системе информационных технологий, аппаратных средств (далее – АС) и программного обеспечения (далее – ПО).	+	+	+	+	+
6	Получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определённым кругом лиц, в том числе информационно-телекоммуникационная сеть «Интернет») информации об информационной системе, в	+	+	+	+	+

№	Возможности	Класс СКЗИ				
		КС1	КС2	КС3	КВ	КА
	которой используется СКЗИ. При этом может быть получена следующая информация: – общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы); – сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ; – содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ; – общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ; – сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее – канал связи); – все возможные данные, передаваемые в открытом виде по каналам связи, не защищённым от несанкционированного доступа к информации организационными и техническими мерами; – сведения обо всех проявляющихся в каналах связи, не защищённых от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ; – сведения обо всех проявляющихся в каналах связи, не защищённых от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ; – сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.					
7	Применение: – находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ; – специально разработанных АС и ПО.	+	+	+	+	+
8	Использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: – каналов связи, не защищённых от несанкционированного доступа к информации организационными и техническими мерами; – каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;	+	+	+	+	+
9	Проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определённым кругом лиц, если информационные системы, в которых используются	+	+	+	+	+

№	Возможности	Класс СКЗИ				
		КС1	КС2	КС3	КВ	КА
	СКЗИ, имеет выход в эти сети.					
10	Использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства).	+	+	+	+	+
11	Проведение атаки при нахождении в пределах контролируемой зоны.	-	+	+	+	+
12	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: – документацию на СКЗИ и компоненты СФ; – помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – СВТ), на которых реализованы СКЗИ и СФ.	-	+	+	+	+
13	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.	-	+	+	+	+
14	Использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	-	+	+	+	+
15	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ.	-	-	+	+	+
16	Возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	-	-	+	+	+
17	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	-	-	-	+	+
18	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	-	-	-	+	+

№	Возможности	Класс СКЗИ				
		КС1	КС2	КС3	КВ	КА
19	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	-	-	-	+	+
20	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.	-	-	-	-	+
21	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	-	-	-	-	+
22	Возможность располагать всеми аппаратными компонентами СКЗИ и СФ.	-	-	-	-	+

СКЗИ более высокого класса обеспечивает нейтрализацию всех потенциальных возможность, обеспечиваемых СКЗИ более низкого класса.

Знак «+» - возможность может быть нейтрализована.

Знак «-» - возможность не может быть нейтрализована.

4 Модель нарушителя

Нарушитель может действовать на различных этапах жизненного цикла СКЗИ и СФ, используемых в ИС ИОГВ Краснодарского края.

Под этими этапами в настоящем документе понимаются этапы разработки указанных средств, их производства, хранения, транспортировки, ввода в эксплуатацию, эксплуатации.

4.1 Этапы разработки, производства, хранения, транспортировки и ввода в эксплуатацию технических и программных СКЗИ и СФ

На этапах разработки, производства, хранения, транспортировки и ввода в эксплуатацию, используемых в ИС ИОГВ Краснодарского края технических и программных СКЗИ и СФ, обработка защищаемой информации не производится. Поэтому объектами угроз и атак на этих этапах являются только сами эти средства и документация на них.

Типовыми сценариями возможных действий нарушителей на данных этапах являются:

— внесение программных и/или аппаратных закладок в СКЗИ с последующей их активацией на стадии эксплуатации СКЗИ;

— внесение изменений в документацию СКЗИ.

Обеспечение безопасности указанных объектов достигается путём использования организационно-технических мер защиты как на предприятии изготовителе, так и в организации, эксплуатирующей СКЗИ, путём проведения обязательных проверок во время ввода в эксплуатацию СКЗИ и СФ на соответствие эталонным образцам и заданным алгоритмам функционирования.

СКЗИ для обеспечения безопасности информации при её обработке в информационных системах должны быть сертифицированы в системе сертификации ФСБ России.

4.2 Этап эксплуатации технических и программных СКЗИ и СФ

На данном этапе защита от угроз безопасности, не являющихся атаками, должна регламентироваться организационно-распорядительными документами, регламентирующими процессы обработки и защиты информации (разработанными с учётом особенностей эксплуатации ИС ИОГВ Краснодарского края и действующей нормативной базы), в которых описываются регламенты действий должностных лиц, допущенных к работе с защищаемой информацией. При этом возникновение угроз связано с ошибочными действиями или нарушениями тех или иных требований указанными лицами.

Угрозы безопасности, являющимися атаками, скрытно готовятся и осуществляются нарушителем целенаправленно и определяются его конкретными возможностями.

Типовыми сценариями возможных действий нарушителей на данных этапах являются:

— получения доступа к ключевая, аутентифицирующая и парольная информация, к документации на криптосредство и на технические и программные компоненты СФ;
— прослушивание каналов связи, находящихся за пределами КЗ, с целью получения (нарушения конфиденциальности) и/или модификации (нарушения целостности) передаваемой защищаемой информации;
— активация, внесённых в СКЗИ на предыдущих этапах, программных и/или аппаратных закладок с целью получения (нарушения конфиденциальности) и/или модификации (нарушения целостности) передаваемой защищаемой информации;
— получения физического доступа к СКЗИ с целью выведения их из строя.

При передаче информации по каналам связи она должна быть защищена с использованием СКЗИ или для её передачи должны использоваться защищённые каналы связи. Должна осуществляться защита информации, записываемой на отчуждаемые носители (магнитные, магнитооптические, оптические, карты флэш-памяти и т.п.).

4.3 Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что потенциальный нарушитель безопасности ИС ИОГВ Краснодарского края:

— не располагает всей технической документацией на технические и программные компоненты СФ;
— не располагает всей технической документацией, описанием используемых криптографических алгоритмов и исходными текстами ПО на СКЗИ;
— не располагает всеми данными об организации работы, линиях связи, структуре и используемом оборудовании ИС ИОГВ Краснодарского края в полном объёме;
— может получить из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определённым кругом лиц, в том числе информационно-телекоммуникационная сеть «Интернет») информацию об информационной системе, в которой используется СКЗИ;
— может располагать находящимися в свободном доступе или используемыми за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;
— может располагать всеми возможными данными, передаваемыми в открытом виде по каналам связи, не защищённым от НСД к информации организационно-техническими мерами;
— может располагать всеми проявляющимися в каналах связи, не защищённых от НСД к информации организационно-техническими мерами, нарушениями правил эксплуатации СКЗИ и СФ;
— может располагать всеми проявляющимися в каналах связи, не защищённых от НСД к информации организационно-техническими мерами, неисправностями и сбоями СКЗИ и СФ;

— может располагать сведениями, получаемыми в результате анализа сигналов от СКЗИ и СФ, которые может перехватить нарушитель на канале связи.

4.4 Ограничения на имеющуюся у нарушителя информацию об объектах

Обоснование ограничений на имеющуюся у нарушителя информацию об объектах представлено в таблице .

Таблица 3 – Ограничения на имеющуюся у нарушителя информацию об объектах

№ п/п	Информация	Ограничение	Обоснование ограничения
1	Содержание технической документации на технические и программные компоненты СФ	Доступна информация, находящаяся в свободном доступе. Доступна внутренним нарушителям частично в пределах компетенции согласно должностным функциям	В ИС ИОГВ Краснодарского края ограничен доступ к такой информации (в рамках исполнения функциональных обязанностей пользователем)
2	Все возможные данные, передаваемые в открытом виде по каналам связи, не защищённым от НСД к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.)	Доступны в каналах связи, незащищённых от НСД к информации	В ИС ИОГВ Краснодарского края передачи информации по каналам связи используются сертифицированные ФСБ России средства криптографической защиты информации
3	Сведения о линиях связи, по которым передаётся защищаемая информация: линии связи, проходящие в КЗ; линии связи, проходящие за пределами КЗ	Потенциальному нарушителю могут быть доступны следующие сведения о линиях связи, проходящих в КЗ и за её пределами: – общая информация об архитектуре ЛВС; – информация о типах используемого оборудования и кабелей. Более детальная информация о линиях связи нарушителю недоступна или доступна внутреннему нарушителю частично в пределах компетенции согласно должностным функциям	В ИС ИОГВ Краснодарского края ограничен доступ к такой информации (в рамках исполнения функциональных обязанностей пользователем).

№ п/п	Информация	Ограничение	Обоснование ограничения
4	Все сети связи, работающие на едином ключе	Сведения недоступны	Информация доступна только привилегированным администраторам безопасности
5	Проявляющиеся в каналах связи, не защищённых от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации СКЗИ и СФ	Доступны в каналах связи, незащищённых от НСД к информации	В ИОГВ Краснодарского края для передачи информации по каналам связи используются сертифицированные ФСБ России средства криптографической защиты информации
6	Проявляющиеся в каналах связи, не защищённых от НСД к информации организационно-техническими мерами, неисправности и сбои технических средств СКЗИ и СФ	Доступны в каналах связи, незащищённых от НСД к информации	В ИОГВ Краснодарского края для передачи информации по каналам связи используются сертифицированные ФСБ России средства криптографической защиты информации
7	Сведения, получаемые в результате анализа любых побочных сигналов от технических средств СКЗИ	Могут быть доступны	-
8	Исходные тексты прикладного программного обеспечения ИС	Могут быть доступны	Могут быть доступны в случае использования в ИС ИОГВ Краснодарского края непроприетарного ППО с закрытым исходным кодом

4.5 Предположения об имеющихся у нарушителя средствах атак

Состав и характеристики имеющихся у нарушителя средствах атак существенно зависят как от имеющихся у него возможностей по приобретению или разработке указанных средств, так и от реализованных в ИС ИОГВ Краснодарского края политик безопасности.

Предполагается, что потенциальный нарушитель безопасности ИС ИОГВ Краснодарского края:

— может использовать штатные средства в случае их расположения как вне КЗ, так и внутри КЗ;

— может располагать только доступными в свободной продаже аппаратными компонентами СКЗИ и СФ и за счёт реализованных в ИС ИОГВ Краснодарского

края организационных мер не имеет дополнительных возможностей по их получению;

— может самостоятельно и в одиночку осуществлять освоение способов, подготовку и проведение атак (т.е. отсутствует сговор нарушителей).

Вместе с тем, необходимо учитывать высокую социально-политическую значимость ИС ИОГВ Краснодарского края. Нарушение функционирования ИС ИОГВ Краснодарского края может привести к значительным негативным последствиям, как для отдельных субъектов (граждан), так и для государственных структур в масштабах субъекта Российской Федерации.

Угрозы безопасности ИС ИОГВ Краснодарского края могут быть связаны с неправомерной деятельностью криминальных структур или экстремистских группировок. В связи с этим предполагается, что потенциальный нарушитель также располагает следующей возможностью:

— может осуществлять создание способов, подготовку и проведение атак на каналы связи, выходящие за пределы КЗ, с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ.

Следует отметить, что реализация возможности привлечения отдельных специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, становится нецелесообразной при организации атак на каналы связи, выходящие за пределы КЗ ОИГВ Краснодарского края. Это обусловлено существенно меньшими объёмами передаваемой информации, эпизодичностью информационного взаимодействия, ограниченным объёмом передаваемой информации. Затраты, связанные с организацией атак с привлечением отдельных специалистов и с организацией работ в научно-исследовательских центрах, существенно превосходят возможную выгоду.

Таким образом, угрозы привлечения отдельных специалистов и организация работ в научно-исследовательских центрах для ИС ИОГВ Краснодарского края являются неактуальными.

4.6 Описание каналов атак

Основными каналами атак являются каналы сетей связи, не защищённые от НСД к информации организационно-техническими мерами. Кроме того, не исключается возможность использования в качестве канала атаки АРМ пользователя, в случае несоблюдения им требований правил работы.

4.7 Описание нарушителей (субъектов атак)

С учётом условий функционирования, реализованного комплекса организационно-технических мер по обеспечению информационной безопасности, имеющейся у нарушителя информации об объектах атак, имеющихся у нарушителя средствах атак, а также ограничениях по организации атак, предполагается:

— системные администраторы и администраторы баз данных, которые осуществляют техническое управление и обслуживание аппаратных и программных средств ИС ИОГВ Краснодарского края, включая их настройку, конфигурирование и распределение ключевой и парольной документации, ограничены в своих возможностях принятыми в ИОГВ Краснодарского края

организационно-техническими мерами, однако не исключаются из числа потенциальных нарушителей;

— администраторы безопасности, которые осуществляют техническое управление и обслуживание аппаратных и программных средств СКЗИ ИС ИОГВ Краснодарского края, включая их настройку, конфигурирование и распределение ключевой и парольной документации, ограничены в своих возможностях принятыми в ИОГВ Краснодарского края организационно-техническими мерами. Администраторы безопасности, назначаются из числа особо доверенных сотрудников и исключаются из числа потенциальных нарушителей;

— зарегистрированные пользователи ИС ИОГВ Краснодарского края, участвующие в информационном взаимодействии, в том числе, занимающиеся обработкой защищаемой информации, ограничены в своих возможностях принятыми в ИОГВ Краснодарского края организационно-техническими мерами, однако не исключаются из числа потенциальных нарушителей;

— физические лица, имеющие санкционированный (в т.ч. разовый) доступ к ресурсам ИС ИОГВ Краснодарского края, но не занимающиеся обработкой защищаемой информации и не являющиеся зарегистрированными пользователями ИС ИОГВ Краснодарского края ограничены в своих возможностях принятыми в ИОГВ Краснодарского края организационно-техническими мерами, однако не исключаются из числа потенциальных нарушителей;

— внешние нарушители, не имеющие непосредственного доступа к ресурсам ИС ИОГВ Краснодарского края, находящиеся в пределах КЗ. Этот тип нарушителя может осуществлять атаки на каналы связи, выходящие за пределы КЗ объектов ИОГВ Краснодарского края. Кроме того, внешний нарушитель может организовывать атаки на каналы связи ИС ИОГВ Краснодарского края и внешних организаций, использующих для доступа к ИС сеть Интернет.

5 Определение перечня актуальных угроз и класса СКЗИ

5.1 Определение перечня актуальных угроз

Определение перечня актуальных угроз (возможностей) является необходимым условием для выбора СКЗИ, с использованием которого они могут быть нейтрализованы.

Реализация угроз безопасности конфиденциальной информации (в том числе и персональных данных) в информационных системах (в соответствии с Методическими рекомендациями 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, утверждённых руководством 8 Центра ФСБ России от 31.03.2015 № 149/7/2/6-432 (далее – Методические рекомендации)) определяется возможностями источников атак.

Учитывая особенности функционирования ИС ИОГВ Краснодарского края, с точки зрения обеспечения безопасности информации при её передаче с использованием СКЗИ – рассматривать информационное взаимодействие между различными типами ИС ИОГВ Краснодарского края нецелесообразно.

Обобщённые возможности источников атак (с учётом объёма, содержания передаваемой конфиденциальной информации (в т.ч. персональных данных) для указанных выше типов информационного взаимодействия) представлены в таблице 4.

Определение требуемого класса СКЗИ для обеспечения безопасности защищаемой информации содержит три этапа:

— составление перечня актуальных угроз из числа перечисленных в исходном перечне потенциальных угроз;
— составление перечня неактуальных угроз из числа перечисленных в исходном перечне потенциальных угроз;
— анализ перечня актуальных угроз с выделением актуальной угрозы.

Перечень актуальных угроз (возможностей), а также обоснование отсутствия возможностей в таблице 5.

Согласно Методическим рекомендациям, таблица 5 заполняется в зависимости от положительных ответов в таблице 4, а именно:

— в случае, если выбрана только обобщённая возможность № 1, то в таблицах необходимо привести обоснование признания угроз 1.1-4.3 неактуальными;
— в случае, если максимально выбранная обобщённая возможность не выше № 2, то в таблицах обязательно актуальна хотя бы одна из угроз 1.1-1.4, а также необходимо привести обоснование признания угроз 2.1-4.3 неактуальными;
— в случае, если максимально выбранная обобщённая возможность не выше № 3, то в таблицах обязательно актуальна хотя бы одна из угроз 1.1-2.2, а также необходимо привести обоснование признания угроз 3.1-4.3 неактуальными;

— в случае, если максимально выбранная обобщённая возможность не выше № 5, то в таблицах обязательно актуальна хотя бы одна из угроз 1.1-3.3, а также необходимо привести обоснование признания угроз 4.1-4.3 неактуальными;
— в случае, если выбрана обобщённая возможность № 6, то заполнять таблиц нет необходимости.

Таблица 4 – Обобщённые возможности источников атак

№ п/п	Обобщённые возможности источников атак	Наличие возможности для типов информационного взаимодействия	Примечание
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	+	
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	+	
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	+	
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)		Данные пункты заполняются с учётом объёма, содержания обрабатываемых в ИС данных, а также возможным вредом субъекту персональных данных.
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)		
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)		

Таблица 5 – Уточнённые возможности нарушителей и направления атак

№ п/п	Утонённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия возможности
0.1	Создание способов, подготовка и проведение атак без	Актуально	

№	Утонённые возможности нарушителей и направления атак	Актуальность	Обоснование отсутствия возможности
	привлечения специалистов в области разработки и анализа СКЗИ.		
0.2	Создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ.	Актуально (на этапе эксплуатации)	
0.3	Проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств	Актуально	
0.4	Проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак: - внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ; - внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.	Актуально (на этапе ввода в эксплуатацию)	
0.5	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - защищаемую информацию; - ключевую, аутентифицирующую и парольную информацию СКЗИ; - программные компоненты СКЗИ; - аппаратные компоненты СКЗИ; - программные компоненты СФ; - аппаратные компоненты СФ (аппаратные средства, входящие в СФ, включая микросхемы с записанным микрокодом BIOS, осуществляющей инициализацию этих средств); - данные, передаваемые по каналам связи; - иные объекты, которые установлены при формировании	Актуально	

№	Утонённые возможности нарушителей и направления атак	Актуальность	Обоснование отсутствия возможности
	совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учётом применяемых в информационной системе информационных технологий, аппаратных средств и программного обеспечения.		
0.6	Получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определённым кругом лиц, в том числе информационно-телекоммуникационная сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация: - общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы); - сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ; - содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ; - общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ; - сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные; - все возможные данные, передаваемые в открытом виде по каналам связи, не защищённым от несанкционированного доступа к информации организационными и техническими мерами; - сведения обо всех проявляющихся в каналах связи, не защищённых от несанкционированного доступа к информации	Актуально	

№	Утонённые возможности нарушителей и направления атак	Актуальность	Обоснование отсутствия возможности
	организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ; - сведения обо всех проявляющихся в каналах связи, не защищённых от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ; - сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.		
0.7	Применение: - находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ; - специально разработанных АС и ПО.	Актуально	
0.8	Использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: - каналов связи, не защищённых от несанкционированного доступа к информации организационными и техническими мерами; - каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ.	Актуально (для внутренних каналов связи)	
0.9	Проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определённым кругом лиц, если информационные системы, в которых используются СКЗИ, имеет выход в эти сети.	Актуально	
0.10	Использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства).	Актуально	
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие	Актуально	

№	Утонённые возможности нарушителей и направления атак	Актуальность	Обоснование отсутствия возможности
	объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ		
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Актуально	
1.4	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	Актуально	
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Актуально	
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Не актуально	- проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей

№	Утонённые возможности нарушителей и направления атак	Актуальность	Обоснование отсутствия возможности
			помещений на замок и их открытия только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии ответственных сотрудников ИОГВ Краснодарского края; - осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учёт действий пользователей; - на АРМ и серверах, на которых установлены СКЗИ используются, сертифицированные средства антивирусной защиты; - не осуществляется обработка сведения, составляющих государственную тайну; - высокая стоимость и сложностью подготовки реализации возможности
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Не актуально	- не осуществляется обработка сведения, составляющих государственную тайну; - высокая стоимость и сложностью подготовки реализации возможности
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	Не актуально	- не осуществляется обработка сведения, составляющих государственную тайну; - высокая стоимость и сложностью подготовки реализации возможности

№	Утонённые возможности нарушителей и направления атак	Актуальность	Обоснование отсутствия возможности
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей	Не актуально	- не осуществляется обработка сведения, составляющих государственную тайну; - высокая стоимость и сложностью подготовки реализации возможности - проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; - осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учёт действий пользователей; - на АРМ и серверах, на которых установлены СКЗИ, используются сертифицированные антивирусной защиты.
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Не актуально	- не осуществляется обработка сведения, составляющих государственную тайну; - высокая стоимость и сложностью подготовки реализации возможности
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ	Не актуально	- не осуществляется обработка сведения,

№	Утонённые возможности нарушителей и направления атак	Актуальность	Обоснование отсутствия возможности
			составляющих государственную тайну; - высокая стоимость и сложностью подготовки реализации возможности

Исходя из условий функционирования ИС ОИГВ Краснодарского края, имеющегося комплекса организационных и технических мер защиты, а также сделанных предположений о возможностях нарушителя и ограничениях на эти возможности, определено, что актуальными угрозами для ИС ОИГВ Краснодарского края являются угрозы, перечисленные в таблице 5 под номерами: 0.1-2.2.

5.2 Определение необходимого класса СКЗИ

Выявленные актуальные угрозы могут быть нейтрализованы СКЗИ следующих классов:

— угрозы под номерами 0.1-0.10 таблиц выше, нейтрализуются СКЗИ класса КС1;
— угрозы под номерами 1.1-1.4 таблиц выше, нейтрализуются СКЗИ класса КС2;
— угрозы под номерами 2.1-2.2 таблиц выше, нейтрализуются СКЗИ класса КС3;
— угрозы под номерами 3.1-3.3 таблиц выше, нейтрализуются СКЗИ класса КВ.

Учитывая, что для ИС ИОГВ Краснодарского края, в общем случае, угрозы, связанные с наличием недекларированных возможностей в прикладном и системном программном обеспечении являются неактуальными (на основании Модели угроз безопасности информации информационных систем исполнительных органов государственной власти Краснодарского края), а также то, что СКЗИ более высокого класса обеспечивает нейтрализацию всех угроз, обеспечиваемых СКЗИ более низкого класса, определяем то, что для нейтрализация актуальных для ИС ИОГВ Краснодарского края угроз при информационном взаимодействии должны применяться СКЗИ класса не ниже КС3.

6 Выводы

На основе вышеизложенного в настоящей Модели нарушителя, можно сделать следующий вывод: для обеспечения защищённого информационного взаимодействия, средства криптографической защиты информации, устанавливаемые на каналы связи, выходящие за пределы контролируемой зоны информационных систем исполнительных органов государственной власти Краснодарского края, должны обеспечивать криптографическую защиту по уровню не ниже КС3.

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 Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных»;
5. Федеральный закон Российской Федерации от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения
7. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;
8. ГОСТ Р 51624-2000. Автоматизированные информационные системы в защищённом исполнении;
9. ГОСТ Р 52653-2006. Информационно-коммуникационные технологии в образовании. Термины и определения;
10. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения;
11. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
12. ГОСТ РО 0043-003-2012. Аттестация объектов информатизации. Общие положения;
13. Р 50.1.056-2005. Техническая защита информации. Основные термины и определения;
14. Р 50.1.056-2005. Техническая защита информации. Основные термины и определения;
15. 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»;
16. Постановление главы администрации (губернатора) Краснодарского края от 26 августа 2008 года №840 «О региональной мультисервисной сети исполнительных органов государственной власти Краснодарского края»;
17. Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных системах»;
18. 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»;

19. Методический документ «Меры защиты информации в государственных информационных системах», утверждён ФСТЭК России от 11 февраля 2014 года;
20. 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»;
21. Приказ 8 Центра ФСБ России от 21 февраля 2008 года № 149/54-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;
22. Приказ 8 Центра ФСБ России от 21 февраля 2008 года №149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, системах персональных данных с использованием средств автоматизации»
23. Методические рекомендации 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, утверждённых руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432.
24. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утверждённой приказом ФАПСИ от 13 июня 2001 года № 152.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

MLPS	-	Multiprotocol Label Switching — многопротокольная коммутация по меткам
VPN	-	Virtual Private Network — виртуальная частная сеть
АРМ	-	Автоматизированное рабочее место
БД	-	База данных
ДГУ	-	Бензиновые/дизельные генераторные установки
ИБП	-	Источник бесперебойного питания
ИОГВ	-	Исполнительные органы государственной власти
ИС	-	Информационная система
КЗ	-	Контролируемая зона
ЛВС	-	Локально-вычислительная сеть
НСД	-	Несанкционированный доступ
ОРД	-	Организационно-распорядительных документов, регламентирующих процедуры обработки и защиты информации
ОС	-	Операционная система
ПО	-	Программное обеспечение
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
СЗИ	-	Средство защиты информации
СКЗИ	-	Средство криптографической защиты информации
СМИО	-	Сеть международного информационного обмена
СОИБ	-	Система обеспечения информационной безопасности
СПО	-	Системное программное обеспечение
ССОП	-	Сеть связи общего пользования
СФ	-	Среда функционирования криптосредства
ТКУИ	-	Технический канал утечки информации
ФСБ России	-	Федеральная служба безопасности Российской Федерации
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЦОД	-	Центр обработки данных
ЭП	-	Электронная подпись

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе использованы следующие термины и определения:

Термин	Описание	Источник
Атака	Целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого	Методический рекомендации ФСБ России от 21.02.2008 № 149/5-144
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 её 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 автоматизированной информационной системы	Р 50.1.053-2005
Защита информации	Деятельность, направленная на	ГОСТ Р 51624-2000

Термин	Описание	Источник
	предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	
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»
Канал атаки	Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.	Методический рекомендации ФСБ России от 21.02.2008 № 149/5-144
Коммерческая тайна	Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов,	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»

Термин	Описание	Источник
	сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду	
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
Криптографически опасная информация	Информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.	Методический рекомендации ФСБ России от 21.02.2008 № 149/5-144
Криптосредство	Шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну	Методический рекомендации ФСБ России от 21.02.2008 № 149/5-144
Меры обеспечения информационной безопасности	Совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности	ГОСТ Р 53114-2008
Модель нарушителя	Предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности»	Методический рекомендации ФСБ России от 21.02.2008 № 149/5-144
Модель угроз	Перечень возможных угроз	Методический рекомендации ФСБ России от 21.02.2008 № 149/5-144
Нарушитель (субъект атаки)	Лицо (или инициируемый им процесс), проводящее (проводящий) атаку	Методический рекомендации ФСБ

Термин	Описание	Источник
		России от 21.02.2008 № 149/5-144
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
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	Меры обеспечения информационной безопасности, предусматривающие	ГОСТ Р 53114-2008

Термин	Описание	Источник
информационной безопасности	установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации	
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
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

Термин	Описание	Источник
		от 30 марта 1992 г.
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
Средство защиты от несанкционированного доступа	Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа	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
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»
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
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