УТВЕРЖДЕНА
приказом ФНС России
от « ___» _____ 2021 г.
№ _____

МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФЕДЕРАЛЬНОЙ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВЕДЕНИЯ ЕДИНОГО ГОСУДАРСТВЕННОГО РЕЕСТРА ЗАПИСЕЙ АКТОВ ГРАЖДАНСКОГО СОСТОЯНИЯ

СОГЛАСОВАНО
письмом ФСТЭК России
от « ___» _____ 202 г.
№ _____

СОГЛАСОВАНО
письмом ФСБ России
от « ___» _____ 202 г.
№ _____

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

– АРМ – Автоматизированное рабочее место;
– БД – База данных;
– ФГИС «ЕГР ЗАГС» – Федеральная государственная информационная система ведения Единого государственного реестра записей актов гражданского состояния;
– ИБ – Информационная безопасность;
– ИС – Информационная система;
– НСД – Несанкционированный доступ;
– ПДн – Персональные данные;
– ПЭМИН – Побочные электромагнитные излучения и наводки.
– ЦОД – Центр обработки данных;
– УБПДн – Угрозы безопасности персональных данных;
– СКЗИ – Средство криптографической защиты информации;
– ФЦОД – Федеральный центр обработки данных;
– РЦОД – Резервный центр обработки данных;
– СФ – среда функционирования.

1 ОБЩИЕ СВЕДЕНИЯ

Настоящая модель угроз и нарушителя Федеральной государственной информационной системы ведения Единого государственного реестра записей актов гражданского состояния (далее – ФГИС «ЕГР ЗАГС») разработана на основании:

- исходных данных о ФГИС «ЕГР ЗАГС», содержащихся в документации;
- требований специальных нормативных документов по обеспечению информационной безопасности (ИБ) и рекомендаций стандартов по обеспечению ИБ.

Целью разработки модели угроз является определение перечня угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ФГИС «ЕГР ЗАГС».

Документ разработан на основе методических и организационно-распорядительных документов ФСТЭК России, ФСБ России и ФНС России, а также банка данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

Определение актуальности угроз рассматривается применительно к нарушению основных свойств информации по конфиденциальности, доступности и целостности.

Под угрозами безопасности информации понимается совокупность условий и факторов, создающих опасность нарушения безопасности информации, в том числе случайного (несанкционированного) доступа к объектам защиты, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий с защищаемой информацией.

2 ОПИСАНИЕ ФГИС «ЕГР ЗАГС»

Объектами автоматизации ФГИС «ЕГР ЗАГС» являются:

- органы, уполномоченные на государственную регистрацию актов гражданского состояния:
  - органы ЗАГС;
  - органы исполнительной власти субъекта Российской Федерации, в компетенцию которого входит организация деятельности по государственной регистрации актов гражданского состояния на территории субъекта Российской Федерации;
  - органы местного самоуправления муниципальных районов, городских округов, городских, сельских поселений, на территориях которых отсутствуют органы ЗАГС, образованные в соответствии с Федеральным законом от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния», которым переданы полномочия органов ЗАГС;
  - многофункциональные центры предоставления государственных и муниципальных услуг, которым переданы полномочия на государственную регистрацию рождения (за исключением рождения, государственная регистрация которого производится одновременно с государственной регистрацией установления отцовства) и смерти в соответствии с Федеральным законом от 15.11.1997
  - № 143-ФЗ «Об актах гражданского состояния»;
- уполномоченный федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере государственной регистрации актов гражданского состояния и его территориальные подразделения;
- Министерство иностранных дел Российской Федерации;

– организация, уполномоченная Правительством Российской Федерации на изготовление свидетельств о государственной регистрации актов гражданского состояния.

Общее количество объектов автоматизации – 4,2 тысячи. Общее количество пользователей Системы, осуществляющих деятельность с использованием ФГИС «ЕГР ЗАГС», составляет 12,5 тыс.

Деятельность органов, осуществляющих в Российской Федерации полномочия по государственной регистрации актов гражданского состояния, осуществляется в соответствии с Федеральным законом от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния» и иными нормативными правовыми актами в сфере государственной регистрации актов гражданского состояния.

В полномочия указанных органов входит осуществление, в том числе, следующих функций:

– государственная регистрация актов гражданского состояния – рождения, заключения и расторжения брака, установления отцовства, усыновления (удочерения), перемены имени, смерти;
– составление записей актов гражданского состояния в форме электронных документов, подписываемых усиленной квалифицированной электронной подписью руководителя органа записи актов гражданского состояния или уполномоченного им работника органа записи актов гражданского состояния, а также на бумажных носителях для их последующего хранения;
– восстановление и аннулирование записей актов гражданского состояния;
– ведение делопроизводства в связи с направлением (и получением) дел о внесении исправлений и (или) изменений в записи актов гражданского состояния в другие органы ЗАГС Российской Федерации;

- обеспечение идентичности записей актов гражданского состояния, составленных на бумажных носителях и в форме электронного документа;
- проставление апостиля на гербовых свидетельствах (копиях свидетельств);
- учёт движения гербовых бланков свидетельств;
- перевод в электронную форму книг государственной регистрации актов гражданского состояния (актовых книг);
- включение в Единый государственный реестр записей актов гражданского состояния сведений о документах, выданных компетентными органами иностранных государств в удостоверение актов гражданского состояния, совершенных вне пределов территории Российской Федерации по законам соответствующих иностранных государств в отношении граждан Российской Федерации;
- сбор и предоставление аналитической (статистической) информации по зарегистрированным актам гражданского состояния;
- выдача гражданам первичных и повторных свидетельств о государственной регистрации актов гражданского состояния, в том числе на национальных языках субъектов Российской Федерации (в случаях, предусмотренных законами субъектов Российской Федерации), оформляемых на гербовых бланках строгой отчётности, изготавливаемых организацией, уполномоченной Правительством Российской Федерации на изготовление свидетельств о государственной регистрации актов гражданского состояния;
- исполнение заявлений граждан о внесении изменений и (или) исправлений в записи актов гражданского состояния и выдаче им повторных свидетельств о государственной регистрации актов

гражданского состояния, поступающих в органы ЗАГС при личном обращении граждан, через многофункциональные центры оказания услуг гражданам (МФЦ), через единый портал государственных и муниципальных услуг;

- учёт фактов оплаты государственной пошлины за государственную регистрацию актов гражданского состояния в соответствии с Налоговым кодексом Российской Федерации;
- обеспечение конфиденциальности и безопасности обработки персональных данных при государственной регистрации актов гражданского состояния;
- передача сведений о государственной регистрации актов гражданского состояния государственным органам и организациям в случаях и порядке, установленных законодательством Российской Федерации;
- исполнение запросов государственных органов и организаций, должностных лиц Российской Федерации в случаях и порядке, установленных законодательством Российской Федерации;
- исполнение межведомственных запросов органов, предоставляющих государственные услуги, или органов, предоставляющих муниципальные услуги, о предоставлении сведений о государственной регистрации актов гражданского состояния, необходимых для предоставления государственных и муниципальных услуг, поступающих через систему СМЭВ;
- истребование документов о государственной регистрации актов гражданского состояния с территории иностранных государств;
- взаимодействие в электронном виде с единым порталом государственных и муниципальных услуг, а также региональными порталами государственных и муниципальных услуг, в соответствии с Федеральным законом от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния»;

- взаимодействие в электронном виде с многофункциональными центрами предоставления государственных и муниципальных услуг;
- взаимодействие в электронном виде с информационными системами, являющимися поставщиками данных для ФГИС «ЕГР ЗАГС», в случаях и порядке, установленных законодательством Российской Федерации;
- передача книг записей актов гражданского состояния на бумажных носителях и в электронной форме в государственные архивы Российской Федерации после истечения 100-летнего срока их хранения в органах ЗАГС.

ФГИС «ЕГР ЗАГС» с точки зрения архитектуры относится к трёхзвенным клиент-серверным информационным системам, состоящим из:

- клиентской части, работающей в веб-браузере;
- серверов приложений, обеспечивающих взаимодействие клиентской части с системой управления базами данных (СУБД);
- сервера баз данных, на котором находится база данных и система управления базами данных (СУБД).

Централизованная часть системы размещается в системе центров обработки данных, создаваемых в соответствии с постановлением Правительства Российской Федерации от 05.12.2011 № 995 «Об осуществлении бюджетных инвестиций в проектирование и строительство объектов капитального строительства - центров обработки данных, подведомственных Федеральной налоговой службе». На базе центра обработки данных в г. Городец Нижегородской области создана и функционирует основная площадка системы. На базе центра обработки данных в г. Дубна размещена резервная площадка. Комплекс технических средств включает в себя следующие основные компоненты:

- ПАК машин баз данных на базе платформы СКАЛА-СР/Postgres под управлением операционной системы ALT Linux SPT и СУБД

версии Postgres Pro Enterprise (российская СУБД, разработанная на основе свободно-распространяемой СУБД PostgreSQL);

- ПАК вычислительной инфраструктуры (серверов приложений). В качестве базовой архитектуры для построения вычислительной инфраструктуры используется серверная виртуализация на базе платформ СКАЛА-Р серии 300 и СКАЛА-СР/Аналитика с применением учётно-аналитической системы Полиматика;
- ПАК виртуальной инфраструктуры пользовательского доступа (VDI). Представляет собой виртуальные рабочие места пользователей системы и технические средства, обеспечивающие доступ пользователей к ним по каналам связи, на базе платформы СКАЛА-Р серии 300;
- ПАК системы резервного копирования и восстановления данных;
- Активное сетевое оборудование.

Децентрализованная часть системы размещается на рабочих местах объектов автоматизации ЕГР ЗАГС и представляет собой типовой программно-аппаратный комплекс для работы с ЕГР ЗАГС в защищённом исполнении (защищённый компьютер). В состав программно-аппаратного комплекса входят:

- Операционная система ALT Linux SPT;
- Программный комплекс VPN Клиент «ЗАСТАВА» с СКЗИ «КриптоПро CSP»;
- Специальное программное обеспечение.

Взаимодействие программно-аппаратного комплекса с централизованной частью системы осуществляется через сеть Интернет: с использованием услуг единой сети передачи данных (IP VPN), оказываемых ПАО «Ростелеком» в соответствии с условиями государственного контракта от 27.11.2017 № 0173100007817000068-0003930-01, либо через собственный канал органа ЗАГС путём подключения к инфраструктуре пользовательского доступа.

По степени автоматизации ФГИС «ЕГР ЗАГС» относится к автоматизированным системам, в которых ряд действий выполняются

пользователями в интерактивном режиме. Пользователи системы на всех уровнях работают с единым унифицированным веб-интерфейсом. Взаимодействие с внешними информационными системами осуществляется централизовано на федеральном уровне с использованием СМЭВ.

3 СТРУКТУРНО-ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ ФГИС «ЕГР ЗАГС»

3.1 Состав данных

Основным элементом ФГИС «ЕГР ЗАГС» является информация ограниченного доступа (далее информация), не содержащая сведений, составляющих государственную тайну (в том числе персональные данные), и обрабатываемая в базах данных, используемых в ФГИС «ЕГР ЗАГС».

Состав данных приведён в Таблице 1.

Таблица 1

Источник	Сведения
Ст. 22 143-ФЗ	**Содержание записи акта о рождении**
	фамилия, имя, отчество ребёнка
	пол
	место рождения ребёнка
	мертворождённый, живорождённый
	количество родившихся детей (один, двойня или более детей)
	сведения о документе, подтверждающем факт рождения ребёнка (сведения о выдаче медицинского свидетельства о рождении (дата выдачи, номер и серия)
	фамилия, имя, отчество, родителей (одного из родителей)
	дата рождения родителей (одного из родителей)
	место рождения родителей (одного из родителей)
	гражданство
	национальность (вносится по желанию заявителя)
	место жительства родителей (одного из родителей)
	фамилия, имя, отчество и место жительства заявителя либо наименование и юридический адрес органа или организации, заявивших о рождении ребёнка;
Ст. 29 143-ФЗ	**Содержание записи акта о заключении брака**
	фамилия до заключения брака
	фамилия после заключения брака

	имя, отчество,
	дата и место рождения
	возраст
	семейное положение до вступления в настоящий брак (в браке не состоял, разведён, вдов)
	место жительства каждого из лиц, заключивших брак
	национальность, образование и при наличии у данных лиц общих детей, не достигших совершеннолетия, их количество (вносятся по желанию лиц, заключивших брак)
	сведения о документе, подтверждающем прекращение предыдущего брака, в случае, если лицо (лица), заключившее брак, состояло в браке ранее
	реквизиты документов, удостоверяющих личности заключивших брак
	дата составления и номер записи акта о заключении брака
	наименование органа записи актов гражданского состояния, которым произведена государственная регистрация заключения брака
	серия и номер выданного свидетельства о браке
Ст. 37 143-ФЗ	**Содержание записи акта о расторжении брака**
	фамилия до расторжения брака
	фамилия после расторжения брака
	имя, отчество,
	дата и место рождения
	гражданство
	место жительства каждого из лиц, расторгнувших брак
	национальность, образование, первый или повторный брак и при наличии у супругов общих детей, не достигших совершеннолетия, их количество (вносятся по желанию заявителя)
	дата составления, номер записи акта о заключении брака
	наименование органа записи актов гражданского состояния, в котором произведена государственная регистрация заключения брака
	сведения о документе, являющемся основанием для государственной регистрации расторжения брака
	дата прекращения брака

	реквизиты документов, удостоверяющих личности расторгнувших брак
	серия и номер свидетельства о расторжении брака
Ст. 42 143-ФЗ	**Содержание записи акта об усыновлении**
	фамилия, имя, отчество ребёнка до усыновления
	фамилия, имя, отчество ребёнка после усыновления
	дата и место рождения ребёнка до усыновления
	дата и место рождения ребёнка после усыновления
	фамилия, имя, отчество, гражданство, национальность (при наличии в записи акта о рождении или в свидетельстве о рождении ребёнка) родителей (одного из родителей)
	дата составления, номер записи акта о рождении
	наименование органа записи актов гражданского состояния, которым произведена государственная регистрация рождения ребёнка
	фамилия, имя, отчество, гражданство, национальность (вносится по желанию усыновителя), место жительства усыновителя (усыновителей)
	дата составления, номер записи акта о заключении брака усыновителей
	наименование органа записи актов гражданского состояния, которым произведена государственная регистрация заключения брака усыновителей
	реквизиты решения суда об установлении усыновления ребёнка
	серия и номер выданного свидетельства об усыновлении
Ст. 55 143-ФЗ	**Содержание записи акта об установлении отцовства**
	фамилия, имя, отчество, лица, признанного отцом ребёнка
	дата и место рождения лица, признанного отцом ребёнка
	гражданство лица, признанного отцом ребёнка
	место жительства лица, признанного отцом ребёнка
	фамилия, имя, отчество (до установления отцовства)
	пол, дата и место рождения ребёнка
	дата составления, номер записи акта о рождении ребёнка
	наименование органа записи актов гражданского состояния, которым произведена государственная регистрация рождения ребёнка

	фамилия, имя, отчество ребёнка после установления отцовства
	фамилия, имя, отчество, дата и место рождения, гражданство, национальность (вносится по желанию заявителя) матери ребёнка
	сведения о документе, являющемся основанием для установления отцовства
	фамилия, имя, отчество, место жительства заявителя (заявителей)
	серия и номер выданного свидетельства об установлении отцовства
Ст. 55 143-ФЗ	**Содержание записи акта о перемене имени**
	фамилия, собственно имя, отчество, дата и место рождения, гражданство, национальность (вносится по желанию заявителя), место жительства лица до перемены имени
	фамилия, собственно имя, отчество лица после перемены имени
	дата и номер записи акта о рождении
	наименование органа записи актов гражданского состояния, которым произведена государственная регистрация рождения
	серия и номер выданного свидетельства о перемене имени
Ст. 67 143-ФЗ	**Содержание записи акта о смерти**
	фамилия, имя, отчество, дата и место рождения, последнее место жительства, пол, гражданство, национальность (если сведения о национальности указаны в документе, удостоверяющем личность умершего), место смерти умершего и момент смерти, а если момент смерти установить невозможно, дата смерти
	причина смерти (на основании документа, подтверждающего факт смерти)
	реквизиты документа, подтверждающего факт смерти
	фамилия, имя, отчество, место жительства заявителя либо наименование и юридический адрес органа, организации или учреждения, сделавших заявление о смерти
	серия и номер выданного свидетельства о смерти
	фамилия, имя, отчество, место жительства лица, которому выдано свидетельство о смерти

3.2 Обобщённая структура ФГИС «ЕГР ЗАГС»

Обобщённая структура ФГИС «ЕГР ЗАГС», представленная в Приложении № 1, определяет основные элементы системы и включает в себя:

- центры обработки данных;
- каналы связи;
- рабочие места ФГИС «ЕГР ЗАГС»;
- АРМы администраторов.

ФГИС «ЕГР ЗАГС» построена исходя из следующих технико-технологических предпосылок, важных с точки зрения информационной безопасности:

- единая база данных ФГИС «ЕГР ЗАГС» размещается на ЦОД в отдельном сегменте;
- рабочие места пользователей размещаются на объектах автоматизации; схема построения ФГИС «ЕГР ЗАГС» - «тонкий клиент». Основной режим работы «on line», при котором на АРМах защищаемые данные не хранятся;
- для обеспечения работы пользователей, в случае временного отсутствия связи, должен быть предусмотрен автономный режим печати актов гражданского состояния (временная работа в режиме «off line») с последующей передачей их в базу данных ЦОД при появлении связи. В этом случае на АРМ хранятся защищаемые данные в течение какого-то промежутка времени.

Основная часть пользователей ФГИС «ЕГР ЗАГС» в рамках функциональных обязанностей имеют возможность обратиться к любой записи в системе, в том числе для внесения дополнений (наложенных записей путём версионности с хранением всех версий записи и оснований внесения дополнений) в соответствии с законодательством.

ФГИС «ЕГР ЗАГС» разрабатывается на базе сертифицированных ФСТЭК России операционных систем и СУБД.

В ФГИС «ЕГР ЗАГС» производится обработка специальных категорий и иных персональных данных. Субъектами персональных данных являются все граждане Российской Федерации.

3.3 Объекты защиты в ФГИС «ЕГР ЗАГС»

К объектам защиты в ФГИС «ЕГР ЗАГС» относятся:

- персональные данные граждан Российской Федерации;
- средства защиты информации;
- среда функционирования СКЗИ (далее - СФ);
- информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- используемые информационной системой каналы (линии) связи, включая кабельные системы;
- помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

3.4 Состав передаваемых данных

В состав передаваемых данных входят персональные данные граждан и другая информация необходимая для оказания услуг по государственной регистрации актов гражданского состояния на территории Российской Федерации.

3.5 Классификация системы

ФГИС «ЕГР ЗАГС» имеет следующие классификационные признаки:

С точки зрения Государственной информационной системы классификация проводится на основе требований приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации,

не составляющей государственную тайну, содержащейся в государственных информационных системах».

Уровень значимости информации определяется степенью возможного ущерба для оператора ФГИС «ЕГР ЗАГС» и определён как «**высокий»** (в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможна высокая степень ущерба).

ФГИС «ЕГР ЗАГС» имеет федеральный масштаб и будет функционировать на территории Российской Федерации.

Класс защищённости информационной системы определён как **К1**.

Для ФГИС «ЕГР ЗАГС» актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении. Системное ПО имеет сертификаты ФСТЭК России. Прикладное ПО разрабатывается доверенным исполнителем государственных контрактов и на этапе эксплуатации должно контролироваться на неизменность, кроме того ПО дополнительно может быть проверено на отсутствие недекларированных возможностей специальными средствами контроля.

В ФГИС «ЕГР ЗАГС» обрабатываются специальные и иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора, вследствие чего в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в ФГИС «ЕГР ЗАГС» необходимо обеспечение **2 уровня защищённости** персональных данных в ФГИС «ЕГР ЗАГС».

В соответствии с приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при 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 защищённости», для третьего уровня защищённости ИСПДн, средства СКЗИ могут быть класса КС1 и выше.

В разделе 4 настоящего документа проводится определение класса СКЗИ для ФГИС «ЕГР ЗАГС» для предотвращения возможных атак на систему. Определение класса используемых СКЗИ (см. раздел 4) построено исходя из анализа возможностей нарушителя (атакующего потенциала).

4 МОДЕЛЬ НАРУШИТЕЛЯ И ХАРАКТЕРИСТИКА ИСТОЧНИКОВ УГРОЗ

4.1 Источники угроз

Источниками угроз деструктивных воздействий и хищения данных в ФГИС «ЕГР ЗАГС» могут быть:

– нарушители;

– вредоносная программа.

Настоящая модель учитывает сегментацию системы и концентрированность информации на разных участках, технологию обработки защищаемой информации и необходимость учёта при проектировании угроз нарушения всех свойств информации, в том числе её целостности и соответственно обеспечение некорректируемости информации.

Исходя из состава обрабатываемых данных и структуры ФГИС «ЕГР ЗАГС» (единая база в ЦОД и подключаемые рабочие места) можно выделить основной интерес потенциального нарушителя:

– к хранимой в ЦОД единой базе записей актов гражданского состояния;

– к остановке деятельности органов, осуществляющих в Российской Федерации полномочия по государственной регистрации актов гражданского состояния;

– по доступу к корректировке данных оператором АРМ.

Нарушители подразделяются на два типа:

– **внешние нарушители**;

– **внутренние нарушители**.

4.2 Модель нарушителя

Категории нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам защиты, а также анализа возможностей нарушителей по доступу к компонентам защиты исходя из

структурно-функциональных характеристик и особенностей функционирования ФГИС «ЕГР ЗАГС».

В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам защиты и (или) содержащейся в них информации или не иметь такого доступа.

Анализ прав доступа проводится, как минимум, в отношении следующих компонентов технических средств, входящих в состав ФГИС «ЕГР ЗАГС»:

– устройств ввода/вывода (отображения) информации;
– программных, программно-технических и технических средств обработки информации;
– активного (коммутационного) и пассивного оборудования каналов связи;
– средств защиты информации;
– каналов связи, выходящих за пределы контролируемой зоны.

Модель нарушителя содержит формализованное описание предположения о возможностях нарушителя информационной безопасности, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Нарушители безопасности информации представлены следующими типами по признаку возможности доступа к информационной системе:

– внешние нарушители – лица, не имеющие права доступа к информационной системе, её отдельным компонентам и реализующие УБИ из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
– внутренние нарушители – лица, имеющие право постоянного или разового доступа к информационной системе, её отдельным компонентам.

Нарушители безопасности информации по признаку преднамеренности деструктивных действий могут подразделяться на следующие категории:

- лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в информационной системе, или нарушения функционирования информационной системы или обслуживающей её инфраструктуры (преднамеренные УБИ);
- лица, имеющие доступ к информационной системе, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

В информационной системе УБИ могут быть реализованы следующими видами нарушителей:

- специальные службы иностранных государств;
- террористические, экстремистские группировки;
- преступные группы (криминальные структуры);
- внешние субъекты (физические лица);
- конкурирующие организации;
- разработчики, производители, поставщики программных, технических и программно-технических средств;
- лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;
- лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);
- пользователи информационной системы;
- администраторы информационной системы;
- администраторы безопасности;
- бывшие работники (пользователи).

4.3 Описание классов нарушителей

Предположения о целях (мотивации) нарушителей делаются с учётом целей и задач ФГИС «ЕГР ЗАГС», вида обрабатываемой информации, а также с учётом результатов оценки степени возможных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации. Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации приведены в Таблице.

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
1	Специальные службы иностранных государств (блоков государств)	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов ЗАГС.
2	Преступные группы (криминальные структуры)	Внешний	Причинение имущественного ущерба путём мошенничества или иным преступным путём. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
3	Внешние субъекты (физические лица, не имеющие доступа к программно-аппаратным средствам ФГИС «ЕГР ЗАГС»)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путём мошенничества или иным преступным путём. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Любопытство или желание самореализации (подтверждение статуса).
4	Лица, не являющиеся пользователями информационных систем (включая обслуживающий персонал подрядных организаций, привлекаемый к проведению работ; лица, имеющие разовый или временный доступ в контролируемую зону);	Внутренний	Причинение имущественного ущерба путём обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
5	Пользователи информационной системы	Внутренний	Месть за ранее совершенные действия. Причинение

			имущественного ущерба путём мошенничества или иным преступным путём. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Любопытство или желание самореализации (подтверждение статуса).
6	Администраторы информационной системы и администраторы безопасности	Внутренний	Месть за ранее совершенные действия. Причинение имущественного ущерба путём мошенничества или иным преступным путём. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды

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.

Возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования информационной системы.

Угрозы безопасности информации могут быть реализованы нарушителями за счёт:

– несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));

– несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);

– несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

– несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

– несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;

– воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

4.4 Оценка возможностей

Возможности нарушителей всех классов по использованию штатных средств ФГИС «ЕГР ЗАГС» существенно ограничены следующими организационно-техническими мерами:

– меры по ограничению и контролю физического доступа к техническим средствам ФГИС «ЕГР ЗАГС»;

– меры по ограничению и контроля доступа к ресурсам технических средств ФГИС «ЕГР ЗАГС», реализованные механизмами применяемых средств защиты и штатных средств ФГИС «ЕГР ЗАГС» с ролевым разделением полномочий и минимально необходимыми права доступа для выполнения возложенных обязанностей;

– обеспечение подлинности информации с использованием квалифицированной электронной подписи, содержащей метку времени;

– меры по выполнению критических действий с защищаемой информацией коллегиально для обеспечения взаимного контроля с применением систем обработки обращений и мониторинга, выполнение работ вне системы обработки обращений запрещено;

– отсутствие в технологическом процессе информационной системы возможности корректировки данных в актах гражданского состояния.

Для ФГИС «ЕГР ЗАГС» актуальными считаются следующие классы нарушителей:

- специальные службы иностранных государств – высокий потенциал;

- администраторы информационной системы и администраторы безопасности – высокий потенциал;

– преступные группы (криминальные структуры) – средний потенциал;

– внешние субъекты (физические лица, не имеющие доступа к программно-аппаратным средствам ФГИС «ЕГР ЗАГС») – низкий потенциал;

– лица, не являющиеся пользователями информационных систем (включая обслуживающий персонал подрядных организаций, привлекаемый к проведению работ; лица, имеющие разовый или временный доступ в контролируемую зону) – низкий потенциал;

– пользователи информационной системы – низкий потенциал.

Внешние нарушители с базовым (низким) потенциалом имеют следующие возможности по реализации угроз безопасности информации:

- имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;
- имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему только из-за пределов контролируемой зоны.

Внешний нарушитель с потенциалом выше базового может осуществлять несанкционированный доступ:

- к каналам связи, выходящим за пределы контролируемой зоны;
- через автоматизированные рабочие места, подключённые к сетям связи общего пользования и (или) сетям международного информационного обмена;
- к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- через элементы информационной инфраструктуры ФГИС «ЕРН», которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;
- через элементы Объектов обслуживания Заказчиков при их подключении к ФГИС «ЕРН».

4.5 Анализ возможностей нарушителя и актуальности угроз ИБ

4.5.1 Возможности нарушителя в сегменте пользователя

На рабочих местах пользователей ФГИС «ЕГР ЗАГС» и в каналах связи ЦОД-АРМ функционирует фрагментарная информация, запросы в систему формализованы и формирование бланков строгой отчётности в режиме «тонкий клиент» производится в ЦОД. В этом случае наиболее значимой возможностью нарушителя может является – «физический доступ к СВТ, на которых реализованы СКЗИ и СФ».

Аппаратно-программная платформа (ПАК ЗК ЕГР ЗАГС – рабочие места пользователей ФГИС «ЕГР ЗАГС») оснащена встроенными аппаратными средствами контроля вскрытия корпуса системного блока с блокировкой функционирования. В качестве дополнительной меры защиты доступ к программной составляющей осуществляется только при предъявлении сертификата пользователя.

Ключевая информация и сертификаты, выпущенные УЦ ФГИС «ЕГР ЗАГС», хранятся на отчуждаемых защищенных носителях (ESMART). УЦ ФГИС «ЕГР ЗАГС» осуществляет ведение реестра пользователей, сертификатов, отозванных сертификатов.

Регистрация записей в информационной системе подтверждается электронной подписью сотрудника (пользователя информационной системы). А также в виду отсутствия доступа ко всем защищаемым сведениям информационной системы реализация УБИ со стороны пользователя системы маловероятна.

Но для внешнего нарушителя организационные, трудовые и материальные затраты на преодоление обеспечиваемой СКЗИ защиты защищаемой информации от нарушения её конфиденциальности или целостности существенно превышают аналогичные затраты на достижение аналогичных целей с помощью обмана, насилия, угроз в отношении

пользователей ФГИС «ЕГР ЗАГС» или использования неблагоприятных обстоятельств для них.

Указанными возможностями обладают спецслужбы и криминальные структуры, атаки которых, направленные на корректировку данных, могут проводиться с рабочих мест (клонов рабочих мест) пользователей ФГИС «ЕГР ЗАГС», в том числе в сговоре с пользователями.

Основной угрозой в этом случае является неконтролируемое внесение заведомо ложных сведений в базу данных. Угроза может быть реализована только в режиме «off line». Противодействие этой наиболее значимой угрозе осуществляется запретом внесения в ЕГР ЗАГС записей, не подписанных квалифицированной электронной подписью с меткой времени в установленном порядке в режиме «online».

Документы, выданные в режиме «off line», не имеют юридического значения, так как подпись документов осуществляется в режиме «online». Дополнительно реализация вышеуказанных атак существенно затруднена предоставлением информации - оснований для внесения записей из медицинских учреждений в случае смерти и рождения, решение суда и паспортные данные в случае развода и т.д. Кроме того в автоматизированном процессе предусмотрена регистрация записей прошедшей датой только по решению суда.

Таким образом, для предотвращения атак внутренних и внешних нарушителей на типовой ПАК ЗК ЕГР ЗАГС системы ФГИС «ЕГР ЗАГС» необходимо применение системы информационной безопасности, включающей в том числе, СКЗИ класса КС 3 с запретом доступа пользователю к ключевой информации и средства обеспечения некорректируемости данных актов гражданского состояния, созданных в режиме «off line» во время отсутствия связи с ФЦОД и РЦОД.

4.5.1 Возможности нарушителя в серверном сегменте

Серверная составляющая системы ФГИС «ЕГР ЗАГС» размещены в ЦОД ФНС России – площадки РЦОД в г. Городец Нижегородской области и ФЦОД в г. Дубна Московской области.

Физический доступ внешних нарушителей к компонентам информационной системы в ЦОД ФНС России исключен принятием мер к критически важным объектам РФ (распоряжение Правительства Российской Федерации от 23.03.2006 № 411-рс):

- режим физической охраны объекта 24/7/365;
- усиленный пропускной режим (разрешительные документы, запрет проноса оружия, взрывчатых веществ, электронных устройств);
- время реагирования территориальных правоохранительных органов в случае тревоги — 15 мин;
- сегментация рабочей зоны объекта с контролем доступа. Обработка и хранение сведений только в защищенной зоне ЦОД ФНС России;
- специальный допуск персонала для проведения работ;
- непрерывный видео-аудио контроль периметра и каждой рабочей зоны.

Нарушители, не являющиеся пользователями информационных систем – лиц, имеющих разовый или временный доступ в контролируемую зону, сопровождаются сотрудниками эксплуатирующей организации ФКУ «Налог – Сервис» ФНС России в пределах контролируемой зоны и не имеют возможности реализации УБИ.

Нарушители, не являющиеся пользователями информационных систем – персонал подрядных организаций, привлекаемый к проведению работ, выполняют работы в соответствии государственными контрактами. Исполнителями государственных контрактов являются проверенные и зарекомендовавшие себя компании, имеющие лицензии контролирующих органов на осуществление деятельности, которые по контрактным обязательствам несут ответственность в рамках законодательства Российской

Федерации. Выполнение данных работ контролируется сотрудниками эксплуатирующей организации – ФКУ «Налог – Сервис» ФНС России. Реализация УБИ данным типом нарушителя возможна только путем получения несанкционированного доступа в короткий промежуток времени, до момента реагирования на инцидент сотрудников эксплуатирующей организации, в который невозможно выполнить существенных УИБ.

В виду отсутствия в информационной системе общедоступных сервисов для работы пользователей, опубликованных в сети Интернет, внешнему нарушителю достижение целей хищения или корректировки данных возможно с помощью обмана, насилия, угроз в отношении администраторов информационной системы и администраторов безопасности ФГИС «ЕГР ЗАГС» или использования неблагоприятных обстоятельств для них.

Вышеуказанным возможностями обладают спецслужбы и криминальные структуры, атаки которых, направленные на корректировку и хищение данных, могут проводиться только в сговоре с администраторами информационной системы и администраторами безопасности.

Возможность корректировки данных и введение ложной информации со стороны администраторов информационной системы и администраторов безопасности исключена в виду хранения и обработки записей в информационной системе в формате xml + CAdES-T.

Для снижения риска хищения данных внутренними нарушителями с высоким потенциалом принят комплекс мер:

- выполнено разделение полномочий администраторов информационной системы и администраторов безопасности на следующие группы без возможности совмещения привилегий: администратор и оператор СКЗИ и СЗИ, администратор Телеком (внутренней сети), администратор БД, администратор ОС, администратор и оператор СРК, администратор и оператор систем мониторинга, администратор виртуализации;

- действия с защищаемой информацией проводятся коллегиально для обеспечения взаимного контроля через единый центр управления для координации выполнения работ;
- работы администраторов информационной системы фиксируются в системах обработки обращений и мониторинга, выполнение работ вне системы обработки обращений запрещено.

В качестве итогового перечня потенциальных возможностей нарушителя, определяющих перечень угроз, будем использовать перечень возможностей, перечисленных пунктах 1 – 14 в таблице (см. Таблица 2). Для противодействия угрозам, осуществляемым с использованием возможностей, должны применяться СКЗИ класса КС3.

Таблица 2 – Предположения о возможностях нарушителей

№	Уточнённые возможности нарушителей и направления атак	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
*Возможности нарушителей, используемые при создании способов, подготовке и проведении атак, для нейтрализации которых должны применяться СКЗИ класса **КС 1***			
1.	Создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ	не актуально	
2.	Создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ	не актуально	
3.	Проведение атаки, находясь вне контролируемой зоны	**актуально**	
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;*	не актуально	
	– *внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.*	не актуально	
5.	Проведение атак на этапе эксплуатации СКЗИ на:		
	– *персональные данные;*	**актуально**	
	– *ключевую, аутентифицирующую и парольную информацию СКЗИ;*	не актуально	
	– *программные компоненты СКЗИ;*	не актуально	
	– *аппаратные компоненты СКЗИ;*	не актуально	
	– *программные компоненты СФ, включая программное обеспечение BIOS;*	не актуально	
	– *аппаратные компоненты СФ;*	не актуально	
	– *данные, передаваемые по каналам связи;*	не актуально	
	– *иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые*	не актуально	

№	Уточнённые возможности нарушителей и направления атак	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	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-телекоммуникационную 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);*	**актуально**	
	– *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;*	**актуально**	
	– *содержание конструкторской документации на СКЗИ;*	**актуально**	
	– *содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ*	**актуально**	
	– *общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;*	не актуально	
	– *сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);*	**актуально**	
	– *все возможные данные, передаваемые в открытом виде по каналам связи, не защищённым от несанкционированного доступа к информации организационными и техническими мерами;*	**актуально**	
	– *сведения обо всех проявляющихся в каналах связи, не защищённых от несанкционированного доступа к*	не актуально	

№	Уточнённые возможности нарушителей и направления атак	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	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;*	не актуально	
	– *сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.*	**актуально**	
7.	Применение:		
	– *находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;*	**актуально**	
	– *специально разработанных АС и ПО*	не актуально	
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;*	**актуально**	
	– *каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ.*	не актуально	
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, имеют выход в эти сети	**актуально**	
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**	
Возможности нарушителей, используемые при создании способов, подготовке и проведении атак, для нейтрализации которых должны применяться СКЗИ класса ***КС 2***			

№	Уточнённые возможности нарушителей и направления атак	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
11.	Проведение атаки при нахождении в пределах контролируемой зоны	**актуально**	
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.*	**актуально**	
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.*	**актуально**	
14.	Использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	актуально	
Возможности нарушителей, используемые при создании способов, подготовке и проведении атак, для нейтрализации которых должны применяться СКЗИ класса ***КС 3***			
15.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	**актуально**	
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	**актуально**	
Возможности нарушителей, используемые при создании способов, подготовке и проведении атак, для нейтрализации которых должны применяться СКЗИ класса ***КВ***			

№	Уточнённые возможности нарушителей и направления атак	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
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	не актуально	• в ФГИС «ЕРГ ЗАГС» не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; • высокая стоимость и сложность подготовки реализации возможности.
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	не актуально	• в ФГИС «ЕРГ ЗАГС» не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; • высокая стоимость и сложность подготовки реализации возможности.
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.	не актуально	• в ФГИС «ЕГР ЗАГС» не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; • высокая стоимость и сложность подготовки реализации возможности.
*Возможности нарушителей, используемые при создании способов, подготовке и проведении атак, для нейтрализации которых должны применяться СКЗИ класса **КА***			
20.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	не актуально	• в ФГИС «ЕГР ЗАГС» не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; • высокая стоимость и сложность подготовки реализации возможности.
21.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	не актуально	В ФГИС «ЕГР ЗАГС» не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
22.	Возможность располагать всеми аппаратными компонентами СКЗИ и СФ	не актуально	В ФГИС «ЕГР ЗАГС» не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

5 ОБОБЩЁННАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

5.1 Объекты воздействия

Актуальными объектами воздействия в ФГИС «ЕГР ЗАГС» являются:

– информация, обрабатываемая в ФГИС «ЕГР ЗАГС»;
– технологическая информация о компонентах ФГИС «ЕГР ЗАГС»
– технические средства обработки информации (АРМ, серверы, сетевое и коммуникационное оборудование и другие технические средства);
– носители информации;
– каналы связи;
– системное программное обеспечение;
– прикладное программное обеспечение;
– средства защиты информации;
– информация, используемая для аутентификации (ключевая, парольная информация СЗИ);
– программные компоненты СЗИ;
– аппаратные компоненты СЗИ;
– WSDL-интерфейсы;
– хранилища больших данных;
– объекты среды виртуализации (гипервизор, виртуальные машины, виртуальные устройства, образы виртуальных машин и т.д.).
– программное обеспечение BIOS.

Из-за отсутствия в составе ФГИС «ЕГР ЗАГС» компонентов, использующих соответствующие технологии, исключены:

– средства беспроводного доступа;
– облачная система;
– компоненты суперкомпьютеров;
– компоненты грид-систем;
– оборудование с числовым программным управлением;

– IoT устройства;
– автоматизированные средства управления технологическими процессами.

С учётом реализованных мер (указаны в разделе 4.5) по ограничению физического, сетевого и логического доступа к централизованным компонентам ФГИС «ЕГР ЗАГС» исключены:

– инженерное оборудование (средства кондиционирования и т.д.).

5.2 Каналы реализации угроз

Состав и содержание актуальных угроз безопасности информации определяются совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к защищаемой информации. Совокупность таких условий и факторов формируется с учётом характеристик ФГИС «ЕГР ЗАГС», свойств среды распространения информативных сигналов, содержащих защищаемую информацию и возможностей источников угроз (нарушителей).

Угроза безопасности реализуется в результате образования канала реализации угрозы между источником угрозы (нарушителем) и объектом защиты, что создаёт необходимые условия для нарушения безопасности ФГИС «ЕГР ЗАГС».

Основными элементами канала реализации угроз являются:

– источник угроз – субъект (нарушитель), материальный объект или физическое явление, создающие угрозу безопасности Объекту защиты;
– среда распространения или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ФГИС «ЕГР ЗАГС»;
– физический объект – материальный объект, в том числе физическое поле, в котором защищаемая информация находит своё отражение в

виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Основными каналами угроз безопасности информации являются:

– технические каналы;
– канал несанкционированного доступа (далее – НСД).

Среди технических каналов, выделяют каналы акустической (речевой) информации, видовой информации, информации по каналам побочных электромагнитных излучений и наводок. Реализация атак по техническому каналу потенциально возможна как в пределах контролируемой зоны, так и за её пределами.

Нарушители могут реализовывать атаки по каналу НСД

– через каналы передачи информации, в том числе выходящие за пределы контролируемой зоны;
– через автоматизированные рабочие места (далее – АРМ), в том числе подключённые к сетям связи общего пользования;
– через штатные средства информационных систем, в том числе через те, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны Внешний нарушитель имеет возможность реализации атак по каналу НСД с использованием протоколов межсетевого взаимодействия.

5.3 Определение типов угроз

В соответствии с частью 10, (п. «е») Требований к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, для ФГИС «ЕГР ЗАГС» актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в информационной системе.

При обработке информации в информационных системах, имеющих подключение к сетям связи общего пользования, возможна реализация следующих угроз безопасности персональным данным:

1) Угрозы деструктивных воздействий (искажение, уничтожение, подмена, блокирование) на информацию с использованием мошеннических манипуляционных схем данными и/или документами и «тонких» мест бизнес процессов:
   - угрозы фальсификации документов ФГИС «ЕГР ЗАГС»;
   - угрозы ввода в ФГИС «ЕГР ЗАГС» заведомо ложных данных с использованием мошеннических схем.
2) Угрозы хищения информации по техническим каналам:
   - угрозы утечки акустической (речевой) информации;
   - угрозы утечки видовой информации.
3) Угрозы деструктивных воздействий и хищение информации путём несанкционированного доступа к ПДн и операционной среды АРМ администратора и серверов путём получения физического доступа к ФГИС «ЕГР ЗАГС» или средствам вывода информации:
   - угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
   - угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ;
   - угрозы внедрения вредоносных программ при непосредственном физическом доступе.

4) Угрозы хищения аппаратно–технических средств, ФГИС «ЕГР ЗАГС»;
5) Угрозы хищения отчуждаемых носителей информации;
6) Угрозы хищения информации путём:
   - использования средств копирования на съёмные носители;
   - несанкционированной передачи по каналам связи;
   - НСД к ключам и атрибутам доступа.
7) Угрозы хищения информации в ходе ремонта, модификации и утилизации программно-аппаратных средств;
8) Угрозы деструктивных воздействий и хищения информации путём:
   - намеренного или непреднамеренного отключения средств защиты;
   - «Анализа сетевого трафика»:
     - с перехватом информации за пределами контролируемой зоны;
     - с перехватом передаваемой по внутренней сети информации.
   - сканирования, направленных на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ФГИС «ЕГР ЗАГС», топологии сети, открытых портов и служб, открытых соединений и др.;
   - навязывания ложного маршрута путём несанкционированного изменения маршрутно-адресных данных;
   - внедрения ложного объекта как внутри ИС, так и во внешних сетях;
   - подмены доверенного объекта;
   - выявления паролей по сети;
   - организации режима типа «Отказа в обслуживании»;
   - удаленного запуска приложений;

- внедрения по сети вредоносных программ;
- нанесения ущерба информации системы путём целенаправленного воздействия на данные с использованием РЭП.

5.4 Определение актуальных угроз

Актуальной считается угроза, которая может быть реализована в ФГИС «ЕГР ЗАГС».

Определение перечня актуальных угроз безопасности ФГИС «ЕГР ЗАГС» осуществлялось на основе Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой 14 февраля 2008 г. заместителем директора ФСТЭК России. Определение перечня актуальных угроз безопасности ФГИС «ЕГР ЗАГС» осуществлялось в следующей последовательности:

- определялся уровень исходной защищённости ФГИС «ЕГР ЗАГС» и соответствующий ему коэффициент Y1;
- с учётом используемых средств защиты информации и реализованных организационных мер по защите экспертным методом, в том числе путём дополнительного опроса персонала ФГИС «ЕГР ЗАГС», определялась вероятность возникновения угроз и соответствующие коэффициенты Y2, с использованием которых рассчитывались коэффициенты реализуемости угроз Y;
- проводилась экспертная оценка опасности реализации угроз безопасности ФГИС «ЕГР ЗАГС»;
- осуществлялся расчёт актуальности угроз безопасности ФГИС «ЕГР ЗАГС».

При определении актуальных угроз в качестве исходного перечня угроз использовался перечень угроз в соответствии с банком данных угроз безопасности информации ФСТЭК России, представленном на веб-сайте http://www.bdu.fstec.ru/ и в Приложении 2.

5.5 Показатели исходной защищённости

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищённости ФГИС «ЕГР ЗАГС» и частота (вероятность) реализации рассматриваемой угрозы. Под уровнем исходной защищённости ИС понимается обобщённый показатель, зависящий от технических и эксплуатационных характеристик ФГИС «ЕГР ЗАГС», приведённых в Таблице 3.

Таблица 3. Показатели исходной защищённости ФГИС «ЕГР ЗАГС»

Технические и эксплуатационные характеристики ИС	Уровень защищённости		
	Высокий	Средний	Низкий
1. По территориальному размещению: - распределённая ИС, которая охватывает несколько областей, краёв, округов или государство в целом;			+
- корпоративная распределённая ИС, охватывающая многие подразделения одной организации;		-	
- локальная (кампусная) ИС, развёрнутая в пределах нескольких близко расположенных зданий;		-	
- локальная ИС, развёрнутая в пределах одного здания.	-		
2. По наличию соединения с сетями общего пользования: - ИС, имеющая многоточечный выход в сеть общего пользования;			-
- ИС, имеющая одноточечный выход в сеть общего пользования;		+	
- ИС, физически отделённая от сети общего пользования.	-		
3. По встроенным (легальным) операциям с записями баз персональных данных: - чтение, поиск;	-		
- запись, удаление, сортировка;		+	
- модификация, передача.			-

4. По разграничению доступа к персональным данным: - ИС, к которой имеет доступ определённый перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн;		+	
- ИС, к которой имеют доступ все сотрудники организации, являющейся владельцем ИС;			
5. По наличию соединений с другими базами данных иных ИС: - интегрированная ИС (организация использует несколько баз данных ИС, при этом организация не является владельцем всех используемых баз ПДн);			-
- ИС, в которой используется одна база данных, принадлежащая организации - владельцу данной ИС.	+		
6. По уровню обобщения (обезличивания) информации: - ИС, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	-		
- ИС, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		-	
- ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).			+
7. По объёму ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки: - ИС, предоставляющая всю БД;			-
- ИС, предоставляющая часть базы данных;		-	
- ИС, не предоставляющие никакой информации.	+		
Сумма характеристик по столбцам:	**2**	**3**	**2**

ФГИС «ЕГР ЗАГС» имеет средний уровень исходной защищённости, т.к. более 70% (5/7*100%) характеристик, указанных в таблице, соответствуют уровню не ниже «среднего». Следовательно, коэффициент Y1 равен 5.

5.6 Вероятность реализации угрозы

Под вероятностью реализации угрозы понимается, определяемый экспертным путём, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ФГИС «ЕГР ЗАГС» в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 градациям этого показателя:

– **маловероятно** - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

– **низкая вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют её реализацию (Y2 = 2);

– **средняя вероятность** - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

- **высокая вероятность** - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

Итоговым значением вероятности угрозы являются:

– 0, для маловероятной угрозы;

– 2, для низкой вероятности угрозы;

– 5, для средней вероятности угрозы;

– 10, для высокой вероятности угрозы.

5.7 Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

– **низкая опасность** - если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;

– **средняя опасность** - если реализация угрозы может привести к негативным последствиям для субъектов ПДн;
– **высокая опасность** - если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

5.8 Оценка вероятности реализации и опасности угроз

5.8.1 Угрозы ввода в ФГИС «ЕГР ЗАГС» заведомо ложных данных с использованием мошеннических схем

Технология работы ФГИС «ЕГР ЗАГС» предполагает возможность печати документов на бланках строгой отчётности при отсутствии связи. Так как процедура печати и ввода записи в БД разнесены во времени, то появляется возможность распечатки документа с одними данными, с последующей их заменой и вводом в базу в виде, нужном нарушителю. Впоследствии может быть получена легализованная копия печатного документа на бланке строгой отчётности с искажёнными данными.

Мошеннические действия с одним лицом могут привести к значительным последствиям для Государства или третьих лиц, например, банков в случае фиктивных свидетельств о смерти лиц, взявших кредит.

Нарушители могут быть в сговоре: сотрудник ЗАГСа, получатель поддельного документа, сотрудник заинтересованной организации (например, сотрудник банка). Последние наблюдались в качестве нарушителей в схемах «фальшивых авизо». Ущерб причиняется банку или государству.

Для нейтрализации этой угрозы бланки строгой отчетности имеют уникальный номер, закрепленный в установленном порядке за уполномоченным сотрудником, который впоследствии подписывает квалифицированной электронной подписью с меткой времени в установленном порядке в режиме «online». Дополнительно в серверном сегменте реализовано подтверждение легитимности записей при помощи СМЭВ.

Вероятность реализации угрозы – **низкая (**$Y_2 = 2$).

Опасность угрозы – **высокая**.

5.8.2 Угрозы утечки акустической (речевой) информации

Предусмотренная технология обработки в ЦОД персональных данных, получаемых с АРМ, не подразумевает акустического ввода и обработки информации в серверном сегменте ФГИС «ЕГР ЗАГС».

Вероятность реализации угрозы – **маловероятно (**$Y_2 = 0$).

Опасность угрозы – **низкая**.

5.8.3 Угрозы утечки видовой информации

Предусмотренная технология обработки персональных данных в ЦОД не предусматривает видового отображения данных в серверном сегменте и АРМ администраторов ФГИС «ЕГР ЗАГС».

Утечка видовой информации с АРМ пользователей может привести к получению незначительной части информации ФГИС «ЕГР ЗАГС».

Вероятность реализации угрозы – **маловероятно (**$Y_2 = 0$).

Опасность угрозы – **низкая**.

5.8.4 Угрозы хищения информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН:

- утечка информации по сетям электропитания;
- утечка за счёт наводок на линии связи, технические средства, расположенные в помещении и системы коммуникаций;
- утечки побочные излучений технических средств;
- утечки за счёт, электромагнитного воздействия на технические средства;

Появление сторонних лиц близ аппаратно-технических средств ФГИС «ЕГР ЗАГС» и АРМ администраторов маловероятно в виду организации пропускного режима. В ФЦОД и РЦОД исключено наличие электрических линий, выходящих за границы контролируемой зоны линий. Дополнительно

организованно размещение трансформаторной подстанции в контролируемой зоне.

Информация на рабочих местах находится в ограниченном объёме и интереса для съёма с точки зрения ИТР и криминальных структур не представляет.

Наличие на ФЦОД и РЦОД интенсивных источников электромагнитных помех (большого числа одновременно работающих ПЭВМ и других технических средств, ограниченная часть которых в конкретный момент времени осуществляет обработку данных), что делает крайне сложным возможность выделения информативных сигналов из суммарного поля побочных электромагнитных излучений (наводок) и таким образом существенно снижает вероятность перехвата ПЭМИН от средств обработки данных. Кроме того, на ФЦОД и РЦОД имеется значительная контролируемая зона, в которой размещение устройств съёма данных маловероятно. Таким образом, вероятность реализации угрозы крайне маловероятна.

Вероятность реализации угрозы – **маловероятная (**$Y_2 = 0$).

Опасность угрозы – **средняя**.

5.8.5 Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой

Угрозы реализуются при непосредственном физическом доступе к ФГИС «ЕГР ЗАГС» и её элементам, как правило, с использованием отчуждаемых носителей.

Угрозы направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ФГИС «ЕГР ЗАГС».

Вероятность реализации угрозы – **низкая (**$Y_2 = 2$).

Опасность угрозы – **средняя**.

5.8.6 Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ

Угрозы реализуются при непосредственном физическом доступе к элементам ФГИС «ЕГР ЗАГС». Данный тип угроз возможен при неконтролируемом использовании носителей информации.

Вероятность реализации угрозы – **низкая (**$Y_2 = 2$).

Опасность угрозы – **высокая**.

5.8.7 Угрозы внедрения вредоносных программ при непосредственном физическом доступе

Угрозы реализуются при непосредственном физическом доступе к элементам ФГИС «ЕГР ЗАГС». Данный тип угроз возможен при неконтролируемом использовании отчуждаемых носителей информации или использовании сервисов почтовых или иных сообщений.

Внедрение вредоносных программ могут создавать условия для НСД в операционную среду компьютера и технических средств, а также способствуют формированию несанкционированных каналов доступа.

Вероятность реализации угрозы – **средняя (**$Y_2 = 5$).

Опасность угрозы – **высокая**.

5.8.8 Угрозы хищения аппаратно-технических средств ФГИС «ЕГР ЗАГС»

Угрозы реализуются при непосредственном физическом доступе нарушителей в помещения, где расположены элементы ФГИС «ЕГР ЗАГС», а

также на рабочих местах администраторов. Дополнительно реализации угрозы возможна при уборке помещений. Реализация угрозы НСД может привести к нарушению заданных характеристик безопасности.

Вероятность реализации угрозы – **маловероятно (**$Y_2 = 0$**).**

Опасность угрозы – **низкая**.

5.8.9 Угрозы хищения отчуждаемых носителей информации

Особенности обработки информации не предполагают использование отчуждаемых носителей информации.

Вероятность реализации угрозы – **маловероятно (**$Y_2 = 0$**).**

Опасность угрозы – **низкая**.

5.8.10 Угрозы хищения информации путём использования средств копирования на съёмные носители

Особенности обработки информации не предполагают использование съёмных носителей.

Вероятность реализации угрозы – **маловероятно (**$Y_2 = 0$**).**

Опасность угрозы – **низкая**.

5.8.11 Угрозы хищения информации путём несанкционированной передачи по каналам связи

Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, несанкционированной передачи данных по каналам связи с помощью использовании сервисов почтовых или иных сообщений, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы).

Вероятность реализации угрозы – **средняя (**$Y_2 = 5$**).**

Опасность угрозы – **высокая**.

5.8.12 Угрозы деструктивных воздействий и хищения информации путём НСД к ключам и атрибутам доступа

Угрозы осуществляются за счёт действия человеческого фактора пользователей ФГИС «ЕГР ЗАГС», которые нарушают положения парольной политики в части создания паролей (создают лёгкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Реализация угрозы может привести к нарушению заданных характеристик безопасности.

Вероятность реализации угрозы – **высокая (**$Y_2 = 10$**).**

Опасность угрозы – **высокая**.

5.8.13 Угрозы хищения информации в ходе ремонта, модификации и утилизации программно-аппаратных средств

Угрозы осуществляются за счёт действия человеческого фактора администраторов ФГИС «ЕГР ЗАГС», которые нарушают положения принятых правил работы с аппаратно-программными элементами ФГИС «ЕГР ЗАГС» или не осведомлены о них. На администраторов возложены задачи по администрированию СКЗИ и технических средств. Администраторы назначаются из числа особо доверенных, и они заинтересованы в сохранении свойств безопасности защищаемых объектов.

Реализация угрозы НСД может привести к нарушению заданных характеристик безопасности.

Вероятность реализации угрозы – **низкая (**$Y_2 = 2$).

Опасность угрозы – **средняя**.

5.8.14 Угрозы деструктивных воздействий и хищения информации путём намеренного или непреднамеренного отключения средств защиты

Угрозы осуществляются за счёт действия человеческого фактора пользователей и администраторов ФГИС «ЕГР ЗАГС», которые нарушают положения принятых правил работы с СЗИ и средствами защиты или не осведомлены о них. На администраторов возложены задачи по администрированию СКЗИ и технических средств. Администраторы назначаются из числа особо доверенных, и они заинтересованы в сохранении свойств безопасности защищаемых объектов.

Реализация угрозы НСД может привести к нарушению заданных характеристик безопасности.

Вероятность реализации угрозы – **низкая (**$Y_2 = 2$).

Опасность угрозы – **высокая**.

5.8.15 Угрозы деструктивных воздействий и хищения информации путём «Анализа сетевого трафика» с перехватом информации за пределами контролируемой зоны

Угрозы возможны с помощью использования специализированных программ-анализаторов пакетов при передаче по сегменту сети за пределами контролируемой зоны. При осуществлении угроз у нарушителей должна быть возможность встраивания специализированных программ-анализаторов в разрез существующих сетей провайдера.

В ходе реализации угрозы возможно получение права доступа к системе и дальнейшее извлечение или подмена, модификация конфиденциальной и идентификационной информации. В ФГИС «ЕГР ЗАГС» данные получаются путём взаимодействия с удалёнными рабочими местами пользователей.

Вероятность реализации угрозы – **низкая (**$Y_2 = 2$).

Опасность угрозы – **высокая**.

5.8.16 Угрозы деструктивных воздействий и хищения информации путём «Анализа сетевого трафика» с перехватом информации передаваемой по внутренней сети информации

Угрозы возможны с помощью использования специализированных программ-анализаторов пакетов при передаче по сегменту сети внутри сети. При осуществлении угроз у нарушителей должна быть возможность встраивания специализированных программ-анализаторов в существующую внутреннюю сеть ФГИС «ЕГР ЗАГС».

В ходе реализации угрозы возможно получение права доступа к системе и дальнейшее извлечение, подмена и модификация конфиденциальной и идентификационной информации. В ФГИС «ЕГР ЗАГС» данные получаются путём взаимодействия с удалёнными рабочими местами пользователей.

Вероятность реализации угрозы – **низкая (**$Y_2 = 2$).

Опасность угрозы – **высокая**.

5.8.17 Угрозы деструктивных воздействий и хищения информации путём сканирования, направленных на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ФГИС «ЕГР ЗАГС», топологии сети, открытых портов и служб, открытых соединений и др.

Угрозы сканирования направлены на выявление параметров сети через точку подключения к сетям общего доступа.

Внутри сети угроза сканирования возможна при несанкционированном подключении специализированного устройства или программного обеспечения к внутренней сети ФГИС «ЕГР ЗАГС».

Полученная информация при реализации угрозы даёт дополнительные сведения о системе и увеличивает вероятность реализации других угроз.

Вероятность реализации угрозы – **средняя (**$Y_2 = 5$).

Опасность угрозы – **средняя**.

5.8.18 Угрозы деструктивных воздействий и хищения информации путём навязывания ложного маршрута путём несанкционированного изменения маршрутно-адресных данных

Угрозы внедрения ложного или доверенного объекта возможны при использовании недостатков алгоритмов маршрутизации и реализуется путём внутрисегментного или межсегментного навязывания.

Для успешной реализации нарушителю необходимо установить хост внутри сегмента или воспользоваться недостатком маршрутизатора сетевого сегмента ФГИС «ЕГР ЗАГС». Данный вид угроз предотвращается современными протоколами маршрутизации или при использовании VPN сетей.

Успешная реализация угрозы может предоставить НСД к техническим средствам ФГИС «ЕГР ЗАГС».

Вероятность реализации угрозы – **низкая (**$Y_2 = 2$).

Опасность угрозы – **высокая**.

5.8.19 Угрозы деструктивных воздействий и хищения информации путём внедрения ложного объекта как внутри ИС, так и во внешних сетях

Эти угрозы основаны на использовании недостатков алгоритмов удаленного поиска. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного доступа, заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией.

При реализации угрозы существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведёт к требуемому изменению маршрутно-адресных данных. В дальнейшем

весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети

Вероятность реализации угрозы – **высокая (**$Y_2 = 10$).

Опасность угрозы – **высокая**.

5.8.20 Угрозы деструктивных воздействий и хищения информации путём подмены доверенного объекта

Угрозы возможны при использовании нестойких алгоритмов идентификации и аутентификации хостов. Для реализации нарушителю необходимо знать особенности сетевой структуры ФГИС «ЕГР ЗАГС».

Успешная угроза может привести к присвоению прав доверенного субъекта, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Дополнительно возможна передача служебных сообщений от имени управляющих устройств и изменять права доступа по своему усмотрению.

Вероятность реализации угрозы – **средняя (**$Y_2 = 5$).

Опасность угрозы – **высокая**.

5.8.21 Угрозы деструктивных воздействий и хищения информации путём выявления паролей по сети

Угрозы возможны при преодолении парольной защиты путём реализации перебора паролей, установки вредоносных программ, перехвата пакетов или подмены доверенного объекта.

Компрометация парольной защиты может привести к получению НСД к ФГИС «ЕГР ЗАГС» и различного рода последствиям.

Вероятность реализации угрозы – **средняя (**$Y_2 = 5$).

Опасность угрозы – **высокая**.

5.8.22 Угрозы деструктивных воздействий и хищения информации путём организации режима типа «Отказа в обслуживании»

Угрозы основаны на недостатках сетевого программного обеспечения, уязвимостях и возможны к реализации из неопределённого физического места (или множества мест). Однако для осуществления требует привлечения значительных аппаратных мощностей.

Угрозы особо опасны, когда ИС представляет собой распределённую ИС, подключённую к сетям общего пользования. При реализации угрозы возможно снижение производительности аппаратно-технических средств, переполнение очереди запросов, изменение логической связности между техническими средствами ФГИС «ЕГР ЗАГС», что может привести к частичному или полному отказу технических средства ФГИС «ЕГР ЗАГС», а также изменению маршрутно-адресных, идентификационных и аутентификационных данных.

Вероятность реализации угрозы – **средняя (**$Y_2 = 5$).

Опасность угрозы – **высокая.**

5.8.23 Угрозы деструктивных воздействий и хищения информации путём удаленного запуска приложений

Угрозы основаны на запуске исполняемых файлов на аппаратно-технических средствах ФГИС «ЕГР ЗАГС» и использовании недостатков программ. Для реализации угрозы, как правило, требуется, запуск исполняемого файла на атакуемом хосте, что возможно только при неконтролируемом запуске различных поступающих файлов по электронной почте или другом способом.

Последствия реализации угрозы могут привести к нарушению работы ФГИС «ЕГР ЗАГС», получения информации и перехвата управления над системой.

Вероятность реализации угрозы – **средняя (**$Y_2 = 5$).

Опасность угрозы – **высокая.**

5.8.24 Угрозы деструктивных воздействий и хищения информации путём внедрения по сети вредоносных программ

Угрозы основаны на запуске исполняемого кода на потенциально атакуемом аппаратно-техническом средстве и дальнейшем его распространении по сети путём передачи на удалённый сервер или рабочую станцию. Учитывая способность вредоносных программ скрывать своё присутствие, дублироваться и выполнять действия без инициативы.

Реализация угрозы может привести к повреждению файлов, перехвату информации, передачи управлению сторонним лицам.

Вероятность реализации угрозы – **высокая (**$Y_2 = 10$).

Опасность угрозы – **высокая.**

5.8.25 Угрозы деструктивных воздействий и хищения информации путём нанесения ущерба информации системы путём целенаправленного воздействия на данные с использованием РЭП

Радиоэлектронное подавление (РЭП) – это комплекс мероприятий и действий по снижению эффективности применения радиоэлектронных систем и средств путём воздействия на их приёмные устройства радиоэлектронными помехами. Включает радиотехническое, оптико-электронное и гидроакустическое подавление.

Реализация угрозы невозможна ввиду отсутствия использования радиоэлектронных систем и средств.

Обоснования вероятности угрозы аналогичны приведённым в п.п. 5.8.4.

Вероятность реализации угрозы – **Неприменимо(**$Y_2 = 0$).

Опасность угрозы – **средняя.**

5.9 Возможность реализации угрозы

Расчет возможности реализации угрозы Y будет определяться соотношением Y = (Y1+ Y2) / 20.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости 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.

Исходная защищённость Y1 – 5.

Таблица 4 содержит сводную таблицу вычисления возможности реализации угрозы.

Таблица 4 - Расчет возможности реализации угрозы

№ п/п	Угрозы	Вероятность реализации угрозы	Коэффициент	Возможность реализации угрозы
1.	Угрозы ввода в ФГИС «ЕГР ЗАГС» заведомо ложных данных с использованием мошеннических схем	10	0,75	Высокая
2.	Угрозы утечки акустической (речевой) информации	0	0,25	Низкая
3.	Угрозы утечки видовой информации	0	0,25	Низкая
4.	Угрозы хищения информации по каналам ПЭМИН	0	0,25	Низкая
5.	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	2	0,35	Средняя

6.	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	2	0,35	Средняя
7.	Угрозы внедрения вредоносных программ при непосредственном физическом доступе	5	0,5	Средняя
8.	Угрозы хищения аппаратно-технических средств ФГИС «ЕГР ЗАГС»	0	0,25	Низкая
9.	Угрозы хищения отчуждаемых носителей информации	0	0,25	Низкая
10.	Угрозы хищения информации путём использования средств копирования на съёмные носители	0	0,25	Низкая
11.	Угрозы хищения информации путём несанкционированной передачи по каналам связи	5	0,5	Средняя
12.	Угрозы деструктивных воздействий и хищения информации путём НСД к ключам и атрибутам доступа	10	0,75	Высокая
13.	Угрозы хищения информации в ходе ремонта, модификации и утилизации программно-аппаратных средств	2	0,35	Средняя
14.	Угрозы деструктивных воздействий и хищения информации путём намеренного или непреднамеренного отключения средств защиты	2	0,35	Средняя
15.	Угрозы деструктивных воздействий и хищения информации путём «Анализа сетевого трафика» с перехватом информации за пределами контролируемой зоны	2	0,35	Средняя
16.	Угрозы деструктивных воздействий и хищения информации путём «Анализа сетевого трафика» с перехватом информации передаваемой по внутренней сети информации	2	0,35	Средняя

17.	Угрозы деструктивных воздействий и хищения информации путём сканирования, направленных на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ФГИС «ЕГР ЗАГС», топологии сети, открытых портов и служб, открытых соединений и др.	5	0,5	Средняя
18.	Угрозы деструктивных воздействий и хищения информации путём навязывания ложного маршрута путём несанкционированного изменения маршрутно-адресных данных	2	0,35	Средняя
19.	Угрозы деструктивных воздействий и хищения информации путём внедрения ложного объекта как внутри ИС, так и во внешних сетях	10	0,75	Высокая
20.	Угрозы деструктивных воздействий и хищения информации путём подмены доверенного объекта	5	0,5	Средняя
21.	Угрозы деструктивных воздействий и хищения информации путём выявления паролей по сети	5	0,5	Средняя
22.	Угрозы деструктивных воздействий и хищения информации путём организации режима типа «Отказа в обслуживании»	5	0,5	Средняя
23.	Угрозы деструктивных воздействий и хищения информации путём удаленного запуска приложений	5	0,5	Средняя
24.	Угрозы деструктивных воздействий и хищения информации путём внедрения по сети вредоносных программ	10	0,75	Высокая
25.	Угрозы деструктивных воздействий и хищения информации путём нанесения ущерба информации системы путём целенаправленного	0	0,25	Низкая

	воздействия на данные с использованием РЭП			

5.10 Определение актуальности угрозы

Для отнесения угроз к актуальным в ФГИС «ЕГР ЗАГС» используется правила, приведённые в Таблица 5.

Таблица 5 - Правила определения актуальности угроз

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

Таблица 1 - Определение актуальности угрозы

№ п/п	**Угрозы**	**Возможность реализации угрозы**	**Опасность угрозы**	**Актуальность**
1.	Угрозы ввода в ФГИС «ЕГР ЗАГС» заведомо ложных данных с использованием мошеннических схем	Высокая	Высокая	Актуальная
2.	Угрозы утечки акустической (речевой) информации	Низкая	Низкая	Неактуальная
3.	Угрозы утечки видовой информации	Низкая	Низкая	Неактуальная
4.	Угрозы хищения информации по каналам ПЭМИН	Низкая	Средняя	Неактуальная
5.	Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	Средняя	Средняя	Актуальная
6.	Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных	Средняя	Высокая	Актуальная

	функций операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ			
7.	Угрозы внедрения вредоносных программ при непосредственном физическом доступе	Средняя	Высокая	Актуальная
8.	Угрозы хищения аппаратно-технических средств ФГИС «ЕГР ЗАГС»	Низкая	Низкая	Неактуальная
9.	Угрозы хищения отчуждаемых носителей информации	Низкая	Низкая	Неактуальная
10.	Угрозы хищения информации путём использования средств копирования на съёмные носители	Низкая	Низкая	Неактуальная
11.	Угрозы хищения информации путём несанкционированной передачи по каналам связи	Средняя	Высокая	Актуальная
12.	Угрозы деструктивных воздействий и хищения информации путём НСД к ключам и атрибутам доступа	Высокая	Высокая	Актуальная
13.	Угрозы хищения информации в ходе ремонта, модификации и утилизации программно-аппаратных средств	Средняя	Средняя	Актуальная
14.	Угрозы деструктивных воздействий и хищения информации путём намеренного или непреднамеренного отключения средств защиты	Средняя	Высокая	Актуальная
15.	Угрозы деструктивных воздействий и хищения информации путём «Анализа сетевого трафика» с перехватом информации за пределами контролируемой зоны	Средняя	Высокая	Актуальная
16.	Угрозы деструктивных воздействий и хищения информации путём «Анализа сетевого трафика» с перехватом информации передаваемой по внутренней сети информации	Средняя	Высокая	Актуальная
17.	Угрозы деструктивных воздействий и хищения информации путём сканирования, направленных на выявление типа или типов	Средняя	Средняя	Актуальная

	используемых операционных систем, сетевых адресов рабочих станций ФГИС «ЕГР ЗАГС», топологии сети, открытых портов и служб, открытых соединений и др.			
18.	Угрозы деструктивных воздействий и хищения информации путём навязывания ложного маршрута путём несанкционированного изменения маршрутно-адресных данных	Средняя	Высокая	Актуальная
19.	Угрозы деструктивных воздействий и хищения информации путём внедрения ложного объекта как внутри ИС, так и во внешних сетях	Высокая	Высокая	Актуальная
20.	Угрозы деструктивных воздействий и хищения информации путём подмены доверенного объекта	Средняя	Высокая	Актуальная
21.	Угрозы деструктивных воздействий и хищения информации путём выявления паролей по сети	Средняя	Высокая	Актуальная
22.	Угрозы деструктивных воздействий и хищения информации путём организации режима типа «Отказа в обслуживании»	Средняя	Высокая	Актуальная
23.	Угрозы деструктивных воздействий и хищения информации путём удаленного запуска приложений	Средняя	Высокая	Актуальная
24.	Угрозы деструктивных воздействий и хищения информации путём внедрения по сети вредоносных программ	Высокая	Высокая	Актуальная
25.	Угрозы деструктивных воздействий и хищения информации путём нанесения ущерба информации системы путём целенаправленного воздействия на данные с использованием РЭП	Неприменимо	Средняя	Неактуальная

5.11 Перечень актуальных угроз

С целью исключения возможных угроз применяются меры защиты, согласно требованиям приказа ФСТЭК России № 17 от 11 февраля 2013 года.

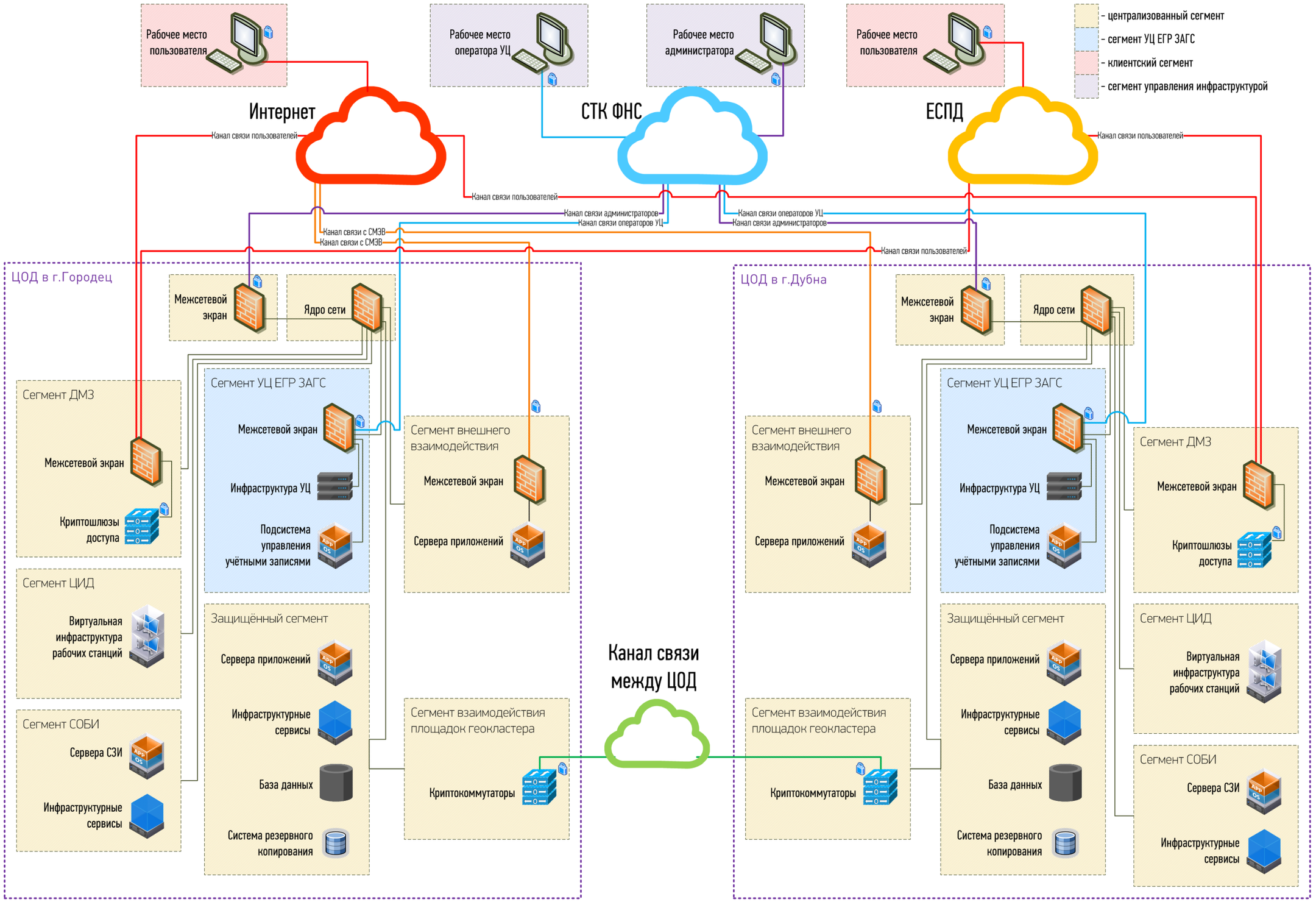
В результате анализа установлено, что актуальными угрозами информационной безопасности являются:

- угрозы ввода в ФГИС «ЕГР ЗАГС» заведомо ложных данных с использованием мошеннических схем;
- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ;
- угрозы внедрения вредоносных программ при непосредственном физическом доступе;
- угрозы хищения информации путём несанкционированной передачи по каналам связи;
- угрозы деструктивных воздействий и хищения информации путём НСД к ключам и атрибутам доступа;
- угрозы хищения информации в ходе ремонта, модификации и утилизации программно-аппаратных средств;
- угрозы деструктивных воздействий и хищения информации путём намеренного или непреднамеренного отключения средств защиты;
- угрозы деструктивных воздействий и хищения информации путём «Анализа сетевого трафика» с перехватом информации за пределами контролируемой зоны;

- угрозы деструктивных воздействий и хищения информации путём «Анализа сетевого трафика» с перехватом информации передаваемой по внутренней сети информации;
- угрозы деструктивных воздействий и хищения информации путём сканирования, направленных на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ФГИС «ЕГР ЗАГС», топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы деструктивных воздействий и хищения информации путём навязывания ложного маршрута путём несанкционированного изменения маршрутно-адресных данных;
- угрозы деструктивных воздействий и хищения информации путём внедрения ложного объекта как внутри ИС, так и во внешних сетях;
- угрозы деструктивных воздействий и хищения информации путём подмены доверенного объекта;
- угрозы деструктивных воздействий и хищения информации путём выявления паролей по сети;
- угрозы деструктивных воздействий и хищения информации путём организации режима типа «Отказа в обслуживании»;
- угрозы деструктивных воздействий и хищения информации путём удаленного запуска приложений;
- угрозы деструктивных воздействий и хищения информации путём внедрения по сети вредоносных программ.

Анализ перечня угроз из БДУ ФСТЭК России, для построения системы ИБ ФГИС «ЕГР ЗАГС», приведён в приложении № 2.

ПРИЛОЖЕНИЕ №1



24.02.2021 6:21

kompburo /Н.И./9152dd5b3beba97c206027b060d0302f5020077ba8e868b8cbfac442a38a18fe

ПРИЛОЖЕНИЕ №2

Анализ перечня угроз, рекомендуемых ФСТЭК России, для построения системы ИБ ФГИС «ЕГР ЗАГС»

Идентификатор УБИ	Наименование УБИ	Обоснование неприменимости	Вероятность	Возможность	Опасность	Актуальность
1	Угроза автоматического распространения вредоносного кода в грид-системе	Угроза не применима ввиду отсутствия в составе ИС грид-систем	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
2	Угроза агрегирования данных, передаваемых в грид-системе	Угроза не применима ввиду отсутствия в составе ИС грид-систем	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
3	Угроза анализа криптографических алгоритмов и их реализации		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
4	Угроза аппаратного сброса пароля BIOS		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
5	Угроза внедрения вредоносного кода в BIOS		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
6	Угроза внедрения кода или данных		Средняя (Y2=5)	Средняя (Y=0,5)	Высокая	Актуальная
7	Угроза воздействия на программы с высокими привилегиями		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
8	Угроза восстановления и/или повторного использования аутентификационной информации		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
9	Угроза восстановления предыдущей уязвимой версии BIOS		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
10	Угроза выхода процесса за пределы виртуальной машины		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
11	Угроза деавторизации санкционированного клиента беспроводной сети	Угроза не применима ввиду отсутствия в ИС средств беспроводного доступа	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
12	Угроза деструктивного изменения конфигурации/среды окружения программ		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
13	Угроза деструктивного использования декларированного функционала BIOS		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
14	Угроза длительного удержания вычислительных ресурсов пользователями		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
15	Угроза доступа к защищаемым файлам с использованием обходного пути		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
16	Угроза доступа к локальным файлам сервера при помощи URL		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
17	Угроза доступа/перехвата/изменения HTTP cookies		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
18	Угроза загрузки нештатной операционной системы		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
19	Угроза заражения DNS-кеша		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
20	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
21	Угроза злоупотребления доверием потребителей облачных услуг	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
22	Угроза избыточного выделения оперативной памяти		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
23	Угроза изменения компонентов информационной (автоматизированной) системы		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная

24.02.2021 6:21
kompburo /Н.И./9152dd5b3beba97c206027b060d0302f5020077ba8e868b8cbfac442a38a18fe

24	Угроза изменения режимов работы аппаратных элементов компьютера		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
25	Угроза изменения системных и глобальных переменных		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
26	Угроза искажения XML-схемы		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
27	Угроза искажения вводимой и выводимой на периферийные устройства информации		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
28	Угроза использования альтернативных путей доступа к ресурсам		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
29	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Угроза не применима ввиду отсутствия в ИС суперкомпьютеров	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию		Высокая (Y2=10)	Высокая (Y=0,75)	Средняя	Актуальная
31	Угроза использования механизмов авторизации для повышения привилегий		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
32	Угроза использования поддельных цифровых подписей BIOS		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
33	Угроза использования слабостей кодирования входных данных		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
34	Угроза использования слабостей протоколов сетевого/локального обмена данными		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
35	Угроза использования слабых криптографических алгоритмов BIOS		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
36	Угроза исследования механизмов работы программы		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
37	Угроза исследования приложения через отчёты об ошибках		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
38	Угроза исчерпания вычислительных ресурсов хранилища больших данных		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
40	Угроза конфликта юрисдикций различных стран	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
41	Угроза межсайтового скриптинга		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
42	Угроза межсайтовой подделки запроса		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
43	Угроза нарушения доступности облачного сервера	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
44	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
45	Угроза нарушения изоляции среды исполнения BIOS		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
47	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Угроза не применима ввиду отсутствия в составе ИС грид-систем	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная

48	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин		Средняя (Y2=5)	Средняя (Y=0,5)	Высокая	Актуальная
49	Угроза нарушения целостности данных кеша		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
50	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
52	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
53	Угроза невозможности управления правами пользователей BIOS		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
54	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
55	Угроза незащищённого администрирования облачных услуг	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
56	Угроза некачественного переноса инфраструктуры в облако	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
57	Угроза неконтролируемого копирования данных внутри хранилища больших данных		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
58	Угроза неконтролируемого роста числа виртуальных машин		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
60	Угроза неконтролируемого уничтожения информации хранилищем больших данных		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
61	Угроза некорректного задания структуры данных транзакции		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
62	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
63	Угроза некорректного использования функционала программного и аппаратного обеспечения		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
64	Угроза некорректной реализации политики лицензирования в облаке	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
65	Угроза неопределённости в распределении ответственности между ролями в облаке	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
66	Угроза неопределённости ответственности за обеспечение безопасности облака	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
67	Угроза неправомерного ознакомления с защищаемой информацией		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
68	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
69	Угроза неправомерных действий в каналах связи		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
70	Угроза непрерывной модернизации облачной инфраструктуры	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
71	Угроза несанкционированного восстановления удалённой защищаемой информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная

72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
74	Угроза несанкционированного доступа к аутентификационной информации		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
75	Угроза несанкционированного доступа к виртуальным каналам передачи		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
76	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
77	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
78	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
80	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
81	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Угроза не применима ввиду отсутствия в составе ИС грид-систем	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
82	Угроза несанкционированного доступа к сегментам вычислительного поля	Угроза не применима ввиду отсутствия в ИС суперкомпьютеров	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
83	Угроза несанкционированного доступа к системе по беспроводным каналам	Угроза не применима ввиду отсутствия в ИС средств беспроводного доступа	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
84	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
85	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
86	Угроза несанкционированного изменения аутентификационной информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
87	Угроза несанкционированного использования привилегированных функций BIOS		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
88	Угроза несанкционированного копирования защищаемой информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
89	Угроза несанкционированного редактирования реестра		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
90	Угроза несанкционированного создания учётной записи пользователя		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
91	Угроза несанкционированного удаления защищаемой информации		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
92	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
93	Угроза несанкционированного управления буфером		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная

94	Угроза несанкционированного управления синхронизацией и состоянием		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
95	Угроза несанкционированного управления указателями		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
96	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
97	Угроза несогласованности правил доступа к большим данным		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
98	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
99	Угроза обнаружения хостов		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
100	Угроза обхода некорректно настроенных механизмов аутентификации		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
101	Угроза общедоступности облачной инфраструктуры	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
102	Угроза опосредованного управления группой программ через совместно используемые данные		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
103	Угроза определения типов объектов защиты		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
104	Угроза определения топологии вычислительной сети		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Угроза не применима ввиду отсутствия в ИС суперкомпьютеров	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
107	Угроза отключения контрольных датчиков		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
108	Угроза ошибки обновления гипервизора		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
109	Угроза перебора всех настроек и параметров приложения		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
110	Угроза перегрузки грид-системы вычислительными заданиями	Угроза не применима ввиду отсутствия в составе ИС грид-систем	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
111	Угроза передачи данных по скрытым каналам		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Угроза не применима ввиду отсутствия в составе ИС оборудования с ЧПУ	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
114	Угроза переполнения целочисленных переменных		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
116	Угроза перехвата данных, передаваемых по вычислительной сети		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
117	Угроза перехвата привилегированного потока		Средняя (Y2=5)	Средняя (Y=0,5)	Высокая	Актуальная
118	Угроза перехвата привилегированного процесса		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
119	Угроза перехвата управления гипервизором		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная

120	Угроза перехвата управления средой виртуализации		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
121	Угроза повреждения системного реестра		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
122	Угроза повышения привилегий		Средняя (Y2=5)	Средняя (Y=0,5)	Высокая	Актуальная
123	Угроза подбора пароля BIOS		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
124	Угроза подделки записей журнала регистрации событий		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Угроза не применима ввиду отсутствия в ИС средств беспроводного доступа	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
126	Угроза подмены беспроводного клиента или точки доступа	Угроза не применима ввиду отсутствия в ИС средств беспроводного доступа	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
127	Угроза подмены действия пользователя путём обмана		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
128	Угроза подмены доверенного пользователя		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
129	Угроза подмены резервной копии программного обеспечения BIOS		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
130	Угроза подмены содержимого сетевых ресурсов		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
131	Угроза подмены субъекта сетевого доступа		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
132	Угроза получения предварительной информации об объекте защиты		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
133	Угроза получения сведений о владельце беспроводного устройства	Угроза не применима ввиду отсутствия в ИС средств беспроводного доступа	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
134	Угроза потери доверия к поставщику облачных услуг	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
135	Угроза потери и утечки данных, обрабатываемых в облаке	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
137	Угроза потери управления облачными ресурсами	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
139	Угроза преодоления физической защиты		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
140	Угроза приведения системы в состояние «отказ в обслуживании»		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
141	Угроза привязки к поставщику облачных услуг	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
144	Угроза программного сброса пароля BIOS		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная

145	Угроза пропуска проверки целостности программного обеспечения		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Угроза не применима ввиду отсутствия в ИС суперкомпьютеров	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Угроза не применима ввиду отсутствия в составе ИС грид-систем	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
149	Угроза сбоя обработки специальным образом изменённых файлов		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
150	Угроза сбоя процесса обновления BIOS		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Угроза не применима ввиду отсутствия в составе ИС технологий WSDL	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
152	Угроза удаления аутентификационной информации		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
154	Угроза установки уязвимых версий обновления программного обеспечения BIOS		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
155	Угроза утраты вычислительных ресурсов		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
156	Угроза утраты носителей информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
158	Угроза форматирования носителей информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
159	Угроза «форсированного веб-браузинга»		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Угроза не применима ввиду отсутствия в ИС суперкомпьютеров	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
162	Угроза эксплуатации цифровой подписи программного кода		Средняя (Y2=5)	Средняя (Y=0,5)	Высокая	Актуальная
163	Угроза перехвата исключения/сигнала из привилегированного блока функций		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Угроза не применима ввиду отсутствия в составе ИС облачной системы	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
165	Угроза включения в проект не достоверно испытанных компонентов		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
166	Угроза внедрения системной избыточности		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
167	Угроза заражения компьютера при посещении неблагонадёжных сайтов		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
168	Угроза «кражи» учётной записи доступа к сетевым сервисам		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
169	Угроза наличия механизмов разработчика		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная

170	Угроза неправомерного шифрования информации		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
171	Угроза скрытного включения вычислительного устройства в состав бот-сети		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
172	Угроза распространения «почтовых червей»		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
173	Угроза «спама» веб-сервера		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
174	Угроза «фарминга»		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
175	Угроза «фишинга»		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
178	Угроза несанкционированного использования системных и сетевых утилит		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
179	Угроза несанкционированной модификации защищаемой информации		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
180	Угроза отказа подсистемы обеспечения температурного режима		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
181	Угроза перехвата одноразовых паролей в режиме реального времени	Угроза не применима ввиду отсутствия в ИС технологий одноразовых паролей	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
182	Угроза физического устаревания аппаратных компонентов		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Угроза не применима ввиду отсутствия в ИС АСУ ТП	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Угроза неприминима ввиду отсутствия в ИС мобильных устройств	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
185	Угроза несанкционированного изменения параметров настройки средств защиты информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
187	Угроза несанкционированного воздействия на средство защиты информации		Средняя (Y2=5)	Средняя (Y=0,5)	Средняя	Актуальная
188	Угроза подмены программного обеспечения		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
189	Угроза маскирования действий вредоносного кода		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
192	Угроза использования уязвимых версий программного обеспечения		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Угроза неприминима ввиду отсутствия в ИС мобильных устройств	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная

195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Угроза не применима ввиду отсутствия нарушителя с высоким потенциалом	Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Угроза неприминима ввиду отсутствия в ИС мобильных устройств	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
197	Угроза хищения аутентификационной информации из временных файлов cookie		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Угроза неприминима ввиду отсутствия в ИС мобильных устройств	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Угроза неприминима ввиду отсутствия в ИС мобильных устройств	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
202	Угроза несанкционированной установки приложений на мобильные устройства	Угроза неприминима ввиду отсутствия в ИС мобильных устройств	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
203	Угроза утечки информации с неподключенных к сети Интернет компьютеров		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты		Средняя (Y2=5)	Средняя (Y=0,5)	Низкая	Неактуальная
206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Угроза не применима ввиду отсутствия нарушителя с высоким потенциалом	Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
212	Угроза перехвата управления информационной системой		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная
213	Угроза обхода многофакторной аутентификации		Низкая (Y2=2)	Средняя (Y=0,35)	Высокая	Актуальная
214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации		Низкая (Y2=2)	Средняя (Y=0,35)	Средняя	Актуальная
215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная

216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Угроза не применима ввиду отсутствия в ИС Smart-карт	Маловероятно (Y2=0)	Неприменимо	Неприменимо	Неактуальная
217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения		Низкая (Y2=2)	Средняя (Y=0,35)	Низкая	Неактуальная