Модель угроз и нарушителя безопасности информации, обрабатываемой в программно-техническом комплексе дистанционного электронного голосования

(выписка)

Москва, 2021

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

BIOS	(от англ. Basic input/output system) Базовая система ввода-вывода
DNS	(от англ. Domain name system) Система доменных имён
HSM	(от англ. Hardware Security Module) Аппаратный Модуль Безопасности
АРМ	Автоматизированное рабочее место
ГАС «Выборы»	Государственная автоматизированная система Российской Федерации «Выборы»
ГИС	Государственная информационная система
ЕПГУ	Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)»
ЕСПД	Единая сеть передачи данных
ЗИ	Защищаемая информация
ИБ	Информационная безопасность
ИК	Избирательная комиссия
ИС	Информационная система
ИТ	Информационные технологии
ИЭП	Инфраструктура электронного правительства
КЗ	Контролируемая зона
Модель	Модель угроз и нарушителя безопасности информации
МСЭ	Межсетевой экран
НДВ	Недекларированные возможности
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение / Производственное отделение
ППО	Прикладное программное обеспечение
ПТК ДЭГ	Программно-технический комплекс дистанционного электронного голосования
РФ	Российская Федерация
СКЗИ	Средство криптографической защиты информации
СМЭВ	Единая система межведомственного электронного взаимодействия
СОВ	Система обнаружения вторжений
СПО	Специальное программное обеспечение
СрЗИ	Средство защиты информации
ТС	Техническое средство

УБИ	Угроза безопасности информации
УИК	Участковая избирательная комиссия
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЦИК	Центральная избирательная комиссия Российской Федерации
ЦОД	Центр обработки данных
ЦП	Цифровая платформа реализации основных гарантий избирательных прав и права на участие в референдуме граждан Российской Федерации
ЭП	Электронная подпись

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств (далее – ТС) и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при её обработке в автоматизированной системе.

Блокирование информации – временное прекращение обработки информации.

Блокчейн – реестр, данные в который записываются блоками таким образом, что каждый новый блок включает информацию о предыдущем блоке.

Бюллетень – избирательный бюллетень, бюллетень для голосования на референдуме.

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

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

Выборы – форма прямого волеизъявления граждан, осуществляемого в соответствии с Конституцией Российской Федерации, федеральными законами, конституциями (уставами), законами субъектов Российской Федерации, уставами муниципальных образований в целях формирования органа государственной власти, органа местного самоуправления или наделения полномочиями должностного лица.

Голосование – подача голосов во время выборов или при коллективном решении какого-либо дела, вопроса.

Грид, грид-вычисления – система, образованная с помощью интеграции, виртуализации и управления сервисами и ресурсами в распределённой, гетерогенной среде.

Доступ к информации – возможность получения информации и ее использования.

Дистанционное электронное голосование – голосование без использования избирательного бюллетеня, изготовленного на бумажном носителе, с использованием ПТК ДЭГ, доступ к которому избирателю (участнику референдума) предоставляется с использованием находящихся в их владении или пользовании абонентских устройств на специальном портале, размещенном в информационно телекоммуникационной сети «Интернет» (далее – сеть Интернет).

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в ТС и системы обработки информации).

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

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

Избиратель – гражданин Российской Федерации, обладающий активным избирательным правом.

Информативный сигнал – электрические сигналы, акустические, электромагнитные поля, по параметрам которых может быть раскрыта конфиденциальная (защищаемая) информация, обрабатываемая в информационной системе.

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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

Источник угрозы безопасности информации – субъект доступа и материальный объект, являющиеся причиной возникновения угрозы безопасности информации.

Канал связи – совокупность технических устройств, обеспечивающих передачу сообщений любого вида от отправителя к получателю, осуществляемую с помощью электрических сигналов.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и исключена возможность хищения ТС обработки защищаемой информации и/или осуществления несанкционированного доступа к ним.

Конфиденциальность защищаемой информации – обязательное для соблюдения оператором или иным получившим доступ к защищаемой информации лицом требование не допускать её распространения без наличия законного основания.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Модель угроз – формализованный перечень возможных угроз.

Наблюдатель – гражданин Российской Федерации, уполномоченный осуществлять наблюдение за проведением голосования, подсчетом голосов и иной деятельностью комиссии в период проведения голосования, установления его итогов, определения результатов выборов, референдума, включая деятельность комиссии по проверке правильности установления итогов голосования и определения результатов выборов, референдума, в объеме, предусмотренном законодательством Российской Федерации и нормативными документами ЦИК России.

Нарушитель безопасности – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности защищаемой информации при её обработке ТС в информационных системах.

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

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

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

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

Перехват (информации) – неправомерное получение информации с использованием ТС, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

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

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

Сети общего пользования – информационно-телекоммуникационные сети, открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

Слепая подпись – разновидность электронной подписи, особенностью которой является то, что подписывающая сторона не может точно знать содержимое подписываемого документа.

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

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

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

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

Транзакция – сообщение и (или) запись в информационной системе, содержащие зашифрованные данные о волеизъявлении участника дистанционного голосования, подписанные его ЭП, а также дополнительные данные для проверки корректности заполненного бюллетеня без раскрытия информации о волеизъявлении (zkp).

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

Сетевой узел – компьютер, терминал или другое устройство, подключенное к сети и имеющее уникальный адрес, позволяющий другим узлам сети связываться с ним по каналам связи.

Уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой

информации через физическую среду до ТС, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

Шифровальные (криптографические) средства – криптосредства:

- средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;
- средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
- средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

Электронный бюллетень – бюллетень, подготовленный программно-техническими средствами в электронном виде, применяемый при проведении электронного голосования.

1 ОБЩИЕ ПОЛОЖЕНИЯ

В настоящем документе представлена выписка из Модели угроз и нарушителя безопасности информации (далее – Модель), обрабатываемой в программно-техническом комплексе дистанционного электронного голосования (далее – ПТК ДЭГ).

ПТК ДЭГ является отдельным, самостоятельным, взаимодействующим с Цифровой платформой (посредством переноса информации на съемных носителях), предназначенным для реализации основных гарантий избирательных прав и права на участие в референдуме граждан Российской Федерации (далее – ЦП) при подготовке и проведении дистанционного электронного голосования программно-техническим комплексом и не входит в состав инфраструктуры ЦП.

Модель содержит предположения о потенциале и возможностях нарушителей безопасности информации при создании способов, подготовке и проведении атак, а также систематизированный перечень угроз безопасности информации при ее обработке в ПТК ДЭГ.

В Модели рассматриваются угрозы безопасности информации ограниченного доступа (в том числе персональных данных) при их обработке в ПТК ДЭГ. В ПТК ДЭГ не предполагается обработка информации, относящейся к сведениям, составляющим государственную тайну (далее – ГТ), в связи с этим в настоящей Модели не рассматриваются вопросы обеспечения безопасности ГТ.

Модель формулирует основные исходные положения для определения требований по защите информации в ПТК ДЭГ. Положениями Модели необходимо руководствоваться на всех этапах жизненного цикла ПТК ДЭГ: развитии, эксплуатации, при проведении регламентных и ремонтно-профилактических работ, выводе ее из эксплуатации.

Модель, учитывая особенности ПТК ДЭГ, используемые технические средства и технологический процесс обработки информации, позволяет определить конкретные условия эксплуатации, защищаемые ресурсы, дать описания нарушителя и угроз безопасности информации, необходимые для выработки

основных исходных положений при разработке и предъявлении требований по защите информации в ПТК ДЭГ.

2 ИСХОДНЫЕ ДАННЫЕ ПО ОБЪЕКТУ ИНФОРМАТИЗАЦИИ

2.1 Назначение и цели создания ПТК ДЭГ

Дистанционное электронное голосование представляет собой голосование без использования избирательного бюллетеня, изготовленного на бумажном носителе, с использованием ПТК ДЭГ, доступ к которому избирателю (участнику референдума) предоставляется с использованием находящихся в их владении или пользовании абонентских устройств на специальном портале, размещенном в информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет).

ПТК ДЭГ обеспечивает реализацию следующих ключевых требований:

- обеспечение тайны голосования;
- генерация ключей шифрования и расшифрования, их разделение и сборка;
- начало и завершение голосования на выборах (референдуме);
- обеспечение наблюдения за ходом голосования, получение статистических отчетов о ходе голосования на выборах (референдуме);
- просмотр списка избирателей (участников референдума) ДЭГ ИК, отвечающей за подготовку и проведение дистанционного электронного голосования и предоставление возможности наблюдателям ознакомиться с данным списком;
- исключение избирателя (участника референдума) из списка избирателей (участников референдума) ДЭГ в период с завершения составления списка избирателей (участников референдума) ДЭГ и до окончания времени дистанционного электронного голосования на основании информации, поступившей в соответствующую ИК, при наличии официальных документов уполномоченных органов об утрате избирателем (участником референдума) активного избирательного права (права на участие в референдуме) и иным причинам, предусмотренным Порядком ДЭГ;
- невозможность изменения поданного, зафиксированного и учтенного голоса;

- невозможность исключения поданного голоса из подсчета поданных голосов и подведения итогов голосования;
- невозможность фиксации и учета голоса, поданного с нарушениями;
- прием голосов только от зарегистрированных и идентифицированных избирателей (участников референдума);
- учет при подсчете голосов только одного голоса от каждого избирателя (участника референдума);
- невозможность установления связи между поданным голосом и конкретным избирателем (участником референдума);
- невозможность демонстрации и подтверждения избирателем (участником референдума) своего выбора после голосования и принадлежности данного выбора избирателю (участнику референдума);
- возможность независимого подсчета поданных голосов;
- получение данных об итогах голосования на выборах (референдуме).

В ПТК ДЭГ обеспечена возможность использования различных мажоритарных и пропорциональных избирательных систем, предполагающих голосование по единому избирательному округу, одномандатным и многомандатным избирательным округам, а также возможность использования смешанной избирательной системы с учётом образуемых избирательных округов. При этом ПТК ДЭГ реализует возможность разбивки единого списка кандидатов на общую (общефедеральную, общерегиональную, общемуниципальную) группу и региональные (территориальные) группы при голосовании.

2.2 Класс защищенности ПТК ДЭГ

В соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Приказ ФСТЭК России № 17) класс защищенности информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы.

Анализ исходных данных о назначении, составе ПТК ДЭГ и циркулирующей в ней информации позволил выявить представленные ниже основные признаки, необходимые для классификации ПТК ДЭГ по требованиям безопасности информации, предъявляемым к государственным информационным системам.

Для информации, обрабатываемой в ПТК ДЭГ, необходимо обеспечить конфиденциальность, целостность и доступность.

Для ПТК ДЭГ устанавливаются следующие степени возможного ущерба от нарушения свойств безопасности информации:

- в случае нарушения конфиденциальности (неправомерный доступ, копирование, предоставление или распространение) – средняя;
- в случае нарушения целостности (неправомерное уничтожение или модифицирование) – высокая;
- в случае нарушения доступности (неправомерное блокирование) – средняя.

На основании вышеизложенного для информации, обрабатываемой в ПТК ДЭГ, в соответствии с Приложением № 1 к Приказу ФСТЭК России № 17 устанавливается высокий уровень значимости (УЗ-1).

ПТК ДЭГ имеет федеральный масштаб, так как функционирует на всей территории Российской Федерации.

Ввиду вышеуказанного, в соответствии с Приложением 1 к приказу ФСТЭК России №17, ПТК ДЭГ должна соответствовать 1 классу защищенности (К1).

2.3 Требуемый уровень защищенности персональных данных, обрабатываемых в ДЭГ

В соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» уровень защищенности персональных данных определяется в зависимости от типа актуальных угроз безопасности ПДн, объема, типа и категории обрабатываемых ПДн.

В соответствии информацией, изложенной в п. 9.1.1 настоящего документа, для ПТК ДЭГ являются актуальными угрозы 3-го типа (угрозы, не связанные с наличием НДВ в системном и прикладном программном обеспечении, используемом в информационной системе).

В ПТК ДЭГ обрабатываются персональные данные более чем 100 000 субъектов персональных данных, как являющихся, так и не являющихся сотрудниками оператора.

В ПТК ДЭГ не обрабатываются специальные категории ПДн (персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн).

В ПТК ДЭГ не обрабатываются биометрические ПДн (данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн).

В ПТК ДЭГ не обрабатываются общедоступные ПДн (персональные данные субъектов, полученные только из общедоступных источников персональных данных).

Таким образом, в ПТК ДЭГ обрабатываются иные ПДн.

Ввиду вышеуказанного, в соответствии с п. 11 Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», необходимо обеспечить третий уровень защищенности персональных данных при их обработке в ДЭГ (УЗ-3).

2.4 Архитектура ПТК ДЭГ

Схема архитектуры ПТК ДЭГ представлена в Приложении А.

Информационная инфраструктура ПТК ДЭГ развёрнута на базе вычислительных ресурсов, развернутых в георасределенных центрах обработки данных, функционирующих в режиме «Active/Standby».

ПТК ДЭГ размещается в 4 ЦОД (ЦОД-1, ЦОД-2, ЦОД-3, ЦОД-4). Также ПТК ДЭГ взаимодействует со следующими площадками: ЦИК РФ, Общественная палата, ПАО «Ростелеком».

Информационная инфраструктура ПТК ДЭГ развёрнута на базе вычислительных ресурсов, развёрнутых в георапределенных центрах обработки данных, функционирующих в режиме «Active/Standby».

Часть серверного оборудования ДЭГ может располагаться на отдельных территориальных площадках ЦИК и наблюдателей (общественная палата).

Помимо серверного и сетевого оборудования в состав технических средств ДЭГ входят АРМ операторов ПТК ДЭГ, администраторов, обеспечивающих функционирование вычислительной инфраструктуры, программного обеспечения и системы защиты информации ДЭГ.

Сегменты ПТК ДЭГ могут располагаться в серверных стойках в рамках одного ЦОД, огражденных специализированной выгородкой, обеспечивающей невозможность несанкционированного доступа (контролируемую зону) к серверному оборудованию ПТК ДЭГ для пользователей и администраторов сторонних систем.[1]

Взаимодействие сегментов ПТК ДЭГ с сегментами ПТК ДЭГ или сторонними системами (например, ЕСИА), размещаемыми в рамках одного ЦОД, но выходящими за пределы КЗ (выгородки) должно осуществляться с применением средств криптографической защиты.

Взаимодействие сегментов ПТК ДЭГ с сегментами ПТК ДЭГ или сторонними системами (например, ЕСИА), размещаемыми в различных ЦОД, должно осуществляться с применением средств криптографической защиты.

Взаимодействие компонентов ПТК ДЭГ в рамках КЗ (выгородки) применение средств криптографической зашиты не требует.

[1] Настоящее инженерно-техническое решение (выгородка) должно быть реализовано в рамках целевой ПТК ДЭГ, так как решение по размещению оборудования ПТК ДЭГ на проведение общероссийской тренировки является временным.

Графический интерфейс ПТК ДЭГ реализован средствами веб-сервиса, поэтому может использоваться с помощью веб-браузеров. Доступ избирателей к ПТК ДЭГ предоставляется на портале с использованием их собственных абонентских устройств, имеющих возможность подключения к сети Интернет.

Программно-технический комплекс (ПТК) ДЭГ имеет два контура защиты – внешний и внутренний.

Внешний периметр защиты использует средства защиты инфраструктуры электронного правительства (ИЭП). Весь трафик, приходящий из сети международного информационного обмена Интернет инспектируется на внешнем периметре ИЭП, собранном из МСЭ с функцией обнаружения вторжений, на котором настроены правила фильтрации и включена система обнаружения и предупреждения вторжений.

Внутренний периметр разделяется на два сегмента: открытый и закрытый. В состав открытого сегмента входят публичные подсистемы, доступные через сеть Интернет, подсистема информационной безопасности и управления программно-технического комплекса ДЭГ. Периметр открытого контура реализован на кластере, собранном из МСЭ с функцией обнаружения вторжений, на котором настроены правила фильтрации и включена система обнаружения и предупреждения вторжений.

В состав закрытого сегмента входят компоненты анонимного голосования, хранения и подсчёта голосов, включая блокчейн. Периметр закрытого контура реализован на кластере, собранном из МСЭ отечественного производства с функцией обнаружения вторжений, на котором настроены правила фильтрации и включена система обнаружения и предупреждения вторжений.

При взаимодействии избирателей с ПТК ДЭГ они заходят на портал ДЭГ. В случае использования браузера «Спутник» с поддержкой отечественной криптографии исходящий трафик избирателей шифруется в виде ГОСТ TLS. Трафик, приходящий от избирателей, фильтруется на МСЭ внешнего периметра и направляется на балансировщик.

Балансировщик, в свою очередь, трафик, зашифрованный средствами ГОСТ TLS, перенаправляет на TLS-шлюз – криптографический сетевой программный комплекс. TLS-шлюз расшифровывает трафик и возвращает его на балансировщик, который распределяет его между средствами защиты web-приложений (WAF). Если трафик зашифрован RSA TLS, то он сразу перенаправляется на средства защиты web-приложений.[2]

После применения правил средствами защиты web-приложений, трафик направляется на МСЭ внутреннего периметра, где он фильтруется, инспектируется и маршрутизируется в открытый сегмент, который распределяет запросы между серверами web-приложений.

Взаимодействие открытого и закрытого сегментов ДЭГ происходит через МСЭ внутренних периметров, где трафик фильтруется, инспектируется и маршрутизируется между компонентами системы ДЭГ.

При взаимодействии компонентов системы ДЭГ, находящихся в разных ЦОД, трафик шифруется с использованием СКЗИ между ЦОД. Основное предназначение канала – репликация баз данных, включая взаимодействие узлов блокчейн.

Смежная система – ЕСИА, используемая для аутентификации избирателей, располагается в ЦОД-1 и ЦОД-2. При взаимодействии с ЕСИА трафик не покидает контролируемой зоны, т.к. ПТК ДЭГ находится за внешним периметром ИЭП.

Доступ к контуру управления инфраструктурой осуществляется через АРМ администраторов, как с площадок ЦОД, так и с внешних площадок через СКЗИ управления. Также через СКЗИ управления осуществляется доступ к услугам внешних сервисов информационной безопасности ПАО «Ростелеком», таким как сбор и корреляция событий ИБ, сессионная аналитика и анализ защищённости.

Взаимодействие ЦИК с ПТК ДЭГ осуществляется через выделенные СКЗИ для канала ЦИК. На стороне ИК ДЭГ трафик маршрутизируется в СКЗИ, где шифруется и, используя выделенную сеть, попадает на СКЗИ ЦОД ПТК ДЭГ, где

[2] Решение по применению протокола RSA является согласованным временным решением, до перехода физических лиц на использование протоколов, соответствующих ГОСТ

расшифровывается, фильтруется и маршрутизируется на МСЭ внутреннего периметра, на котором инспектируется и маршрутизируется на серверы ПТК ДЭГ.

В рамках планируемой архитектуры ПТК ДЭГ предполагается использование сети доставки контента (Content Delivery Networks, CDN).

CDN используется для оптимизации, ускорения раздачи статического контента избирателям и снижения нагрузки на инфраструктуру ПТК ДЭГ. CDN в рамках ДЭГ представляет собой географически распределённую сетевую инфраструктуру из 3-х точек присутствия, обеспечивающих доставку контента пользователям ПТК ДЭГ.

Для использования сети доставки контента создаётся отдельный домен со статическим контентом. Часть статических данных кэшируется на распределенных узлах CDN. Таким образом, избиратель при обращении к ПТК ДЭГ получает ответ с указанием домена, на котором хранится статический контент, после чего происходит обращение непосредственно на соответствующий узел CDN.

В точках присутствия CDN реализуется DNS-балансировка нагрузки на инфраструктуру ПТК ДЭГ. Система балансировки позволяет распределить трафик между ЦОД ПТК ДЭГ, таким образом пользователи автоматически перенаправляются к ближайшему или наименее загруженному участку в момент запроса, сводя к минимуму вероятность длительных задержек или сбоев в обслуживании.

2.5 Структура ПТК ДЭГ

В состав ПТК ДЭГ входят следующие функциональные компоненты:

- компонент «Портал ДЭГ» - ресурс в сети Интернет, обеспечивающий идентификацию и верификацию пользователя, отображение доступных для него голосований, информирование об особенностях дистанционного голосования и порядке действий, формирование пользовательских ключей для процедуры анонимизации);
- компонент «Сервис анонимного волеизъявления» - ресурс в сети Интернет, предоставляющий возможность заполнения электронного бюллетеня;

- компонент «Центр наблюдения за голосованием» - ресурс в сети Интернет, предоставляющий статистическую информацию о ходе дистанционного электронного голосования и о состоянии компонента «Распределенное хранение данных и подсчет голосов», а также отдельные узлы распределенной базы данных «Распределенное хранение данных и подсчет голосов», хранящие собственную синхронизированную копию транзакций с зашифрованными данными;
- компонент «Список избирателей ДЭГ» (ведение списка избирателей, допущенных к голосованию в форме дистанционного голосования, валидация запроса на предоставление доступа к электронному бюллетеню, регистрация факта предоставления доступа к бюллетеню, обеспечение однократности голосования);
- компонент «Организация и проведение ДЭГ» (обеспечение автоматизации процессов загрузки исходных данных, проводимых кампаний и ключей шифрования и расшифрования, работа со списком избирателей (в том числе исключение избирателей (участников референдума) из списка ДЭГ и включение избирателей (участников референдума) в список ДЭГ (только для ранее исключенных)), получение статистических отчётов о ходе дистанционного электронного голосования, работа со средствами коллективного отображения информации в помещении ИК ДЭГ);
- компонент «Генерация и разделение ключей шифрования и расшифрования» (формирование ключей шифрования и расшифрования, разделение и сборка ключа расшифрования);
- компонент «Распределенное хранение данных и подсчет голосов» (получение зашифрованных бюллетеней, их хранение и функция подсчета голосов);
- компонент «Центр мониторинга ПТК ДЭГ» (формирование динамических онлайн-отчётов для оценки производительности и доступности серверов, сетевого оборудования, а также наблюдения за работой веб-приложений и баз данных).

Также, в структуру ПТК ДЭГ входят следующие АРМ, в соответствии с ролями пользователей ПТК ДЭГ:

- АРМ ДЭГ Председателя ИК;
- АРМ ДЭГ члена ИК;
- АРМ ДЭГ оператора ИК;
- АРМ администраторов ПТК ДЭГ (администраторы ИТ, ИБ, ИС, разработчиков).

АРМ администраторов ПТК ДЭГ, имеющие легитимные права доступа в соответствии со своими функциональными обязанностями, могут подключаться к ПТК ДЭГ:

- локально, находясь в контролируемой зоне;
- удаленно, находясь внутри инфраструктуры ЦОД за пределами КЗ;
- удаленно, с внешних площадок ПТК ДЭГ, осуществляющих взаимодействие по общедоступным каналам связи и сети Интернет.

Сведения, о категориях лиц, имеющих доступ к ПТК ДЭГ, приведены в п. 2.9.

Функциональная схема ПТК ДЭГ представлена на рисунке 1.

В состав ПТК ДЭГ входит программное обеспечение следующих видов:

- системное программное обеспечение (далее – СПО), включающее ОС семейства Linux, гипервизоры KVM;
- прикладное программное обеспечение (далее – ППО), включающее СУБД Postgres.

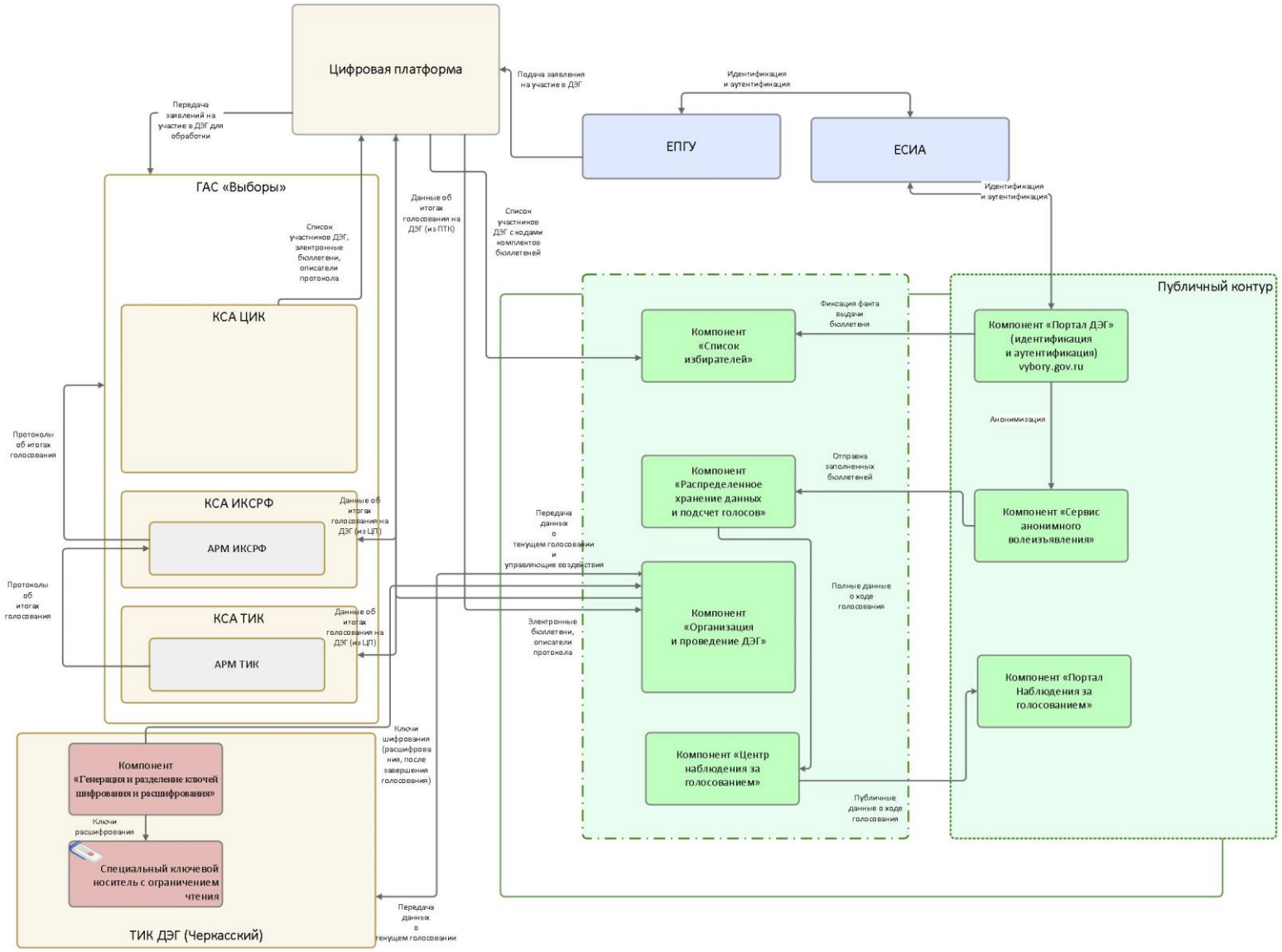


Рисунок 1 - Функциональная схема ПТК ДЭГ

2.6 Взаимосвязь со смежными системами

Описание взаимодействия ДЭГ с внешними информационными системами представлено в таблице 1.

Таблица 1 - Описание взаимодействия ДЭГ с внешними информационными системами

Участники взаимодействия	Описание взаимодействия
ДЭГ – ЕСИА	Перенаправление запроса на авторизацию из ДЭГ в ЕСИА с целью идентификации и аутентификации избирателя. Передача в ДЭГ из ЕСИА информации о результатах идентификации и аутентификации избирателя. Передача в ДЭГ из ЕСИА ПДн избирателей, необходимых для проверки активного избирательного права в реестре участников онлайн голосования.
ДЭГ – ГАС «Выборы»	Передача в ДЭГ из ГАС «Выборы» реестра зарегистрированных участников онлайн голосования, исходной информации о выборах, описателей протоколов и форм бюллетеней. Передача из ДЭГ в ГАС «Выборы» итогов голосования. Обмен информацией осуществляется посредством съемных носителей информации. Сетевой связности ПТК ДЭГ и ГАС выборы нет. Требования к защите съемных носителей определяются организационно-распорядительной документацией. Технические меры защиты съемных носителей подразумевают реализацию решений по неизменности сведений, передаваемых на съемном носителе. Протокол (данные об итогах голосования) подписывается ЭП членов комиссии ИК ДЭГ.
ДЭГ – СМС-шлюз	Отправка избирателям СМС-кодов для верификации личности. Используется для подтверждения участия в голосовании как дополнительный фактор..
Цифровая платформа ЦИК России / ГАС «Выборы» - ДЭГ	Получение исходных данных для ДЭГ, а также загрузки данных об итогах голосования ДЭГ (осуществляется через воздушный зазор) Обмен информацией осуществляется посредством съемных носителей информации. Требования к защите съемных носителей определяются организационно-распорядительной документацией.

2.7 Категории лиц, имеющих доступ к компонентам ПТК ДЭГ и/или участвующих в процессах обработке информации

В ПТК ДЭГ можно выделить следующие группы субъектов доступа:

- зарегистрированные пользователи ПТК ДЭГ (лица, осуществляющие ограниченный доступ к ПТК ДЭГ в соответствии с назначенной ролью):

- избиратель (участник референдума);
- председатель и члены ИК ДЭГ;
- оператор ИК ДЭГ;
- наблюдатели;

– администраторы ИТ (лица, осуществляющие поддержку ИТ-инфраструктуры ПТК ДЭГ);
– администраторы ИБ (лица, осуществляющие поддержку ИБ-инфраструктуры ПТК ДЭГ);
– администраторы ИС (лица, осуществляющие поддержку сервисов ДЭГ);
– программисты-разработчики (поставщики) прикладного ПО и лица, обеспечивающие сопровождение ПТК ДЭГ;
– лица, обеспечивающие поставку, сопровождение и ремонт технических средств ДЭГ;
– обслуживающий персонал (лица, проводящие работы в помещениях, в которых размещаются технические средства ПТК ДЭГ, сотрудники, имеющие доступ в помещения, в которых размещаются технические средства ПТК ДЭГ, но не имеющие доступа к обрабатываемой в ДЭГ информации):
  - персонал, осуществляющий уборку помещений;
  - персонал, обеспечивающий физическую безопасность объектов, в которых размещены компоненты ПТК ДЭГ.

Председателю ИК ДЭГ доступны следующие функции ПТК ДЭГ по управлению процедурой голосования:

– просмотр голосований, проводимых комиссией;
– просмотр списка избирателей (участников референдума) по каждому голосованию, проводимому комиссией;
– изменение бюллетеня и фиксация документа, на основании которого вносятся изменения;
– запуск (открытие участка ДЭГ) и остановка голосования (закрытие участка ДЭГ);

- исключение избирателя (участника референдума) из списка;
- формирование и выгрузка списка участников ДЭГ на момент завершения голосования;
- запуск процедуры расшифрования бюллетеней и подсчета итогов голосования, проводимого комиссией;
- получение данных об итогах голосования, проводимого комиссией;
- получение статистических отчётов в ходе дистанционного электронного голосования.

Членам ИК ДЭГ доступны функции по просмотру информации о процедуре голосования в ПТК ДЭГ:

- просмотр голосований, проводимых комиссией;
- просмотр списка избирателей (участников референдума) по каждому голосованию, проводимому комиссией;
- просмотр статистических отчётов в ходе дистанционного электронного голосования.

Роль оператор ИК ДЭГ должна быть выделена для проведения технической подготовки к проведению голосования, и должна обладать такими функциями, как:

- загрузка исходных данных и техническая подготовка АРМ своей организующей комиссии ДЭГ к проведению голосования;
- загрузка ключей шифрования и расшифрования;
- просмотр голосований ПТК ДЭГ своей организующей комиссии ДЭГ;
- загрузка списков избирателей (участников референдума) по каждому голосованию своей организующей комиссии ДЭГ;
- просмотр списков избирателей (участников референдума) на голосованиях, проводимых своей организующей комиссией.

В качестве наблюдателей выступают лица, обращающиеся к веб-интерфейсу портала ДЭГ, посредством которого наблюдателям предоставляется статистическая информация о ходе голосования (состав информации определяется на этапе разработки технических решений).

Членам УИК доступны следующие функции:

- проверка факта выдачи бюллетеня избирателю (участнику референдума) ДЭГ;
- исключение избирателя (участника референдума) из списка избирателей (участников референдума) ДЭГ с целью выдачи бюллетеня на избирательном участке.

Роль администраторов ИТ ПТК ДЭГ предназначена для обеспечения работы ИТ-инфраструктуры ПТК ДЭГ в предусмотренных режимах функционирования.

Роль администраторов БИ ПТК ДЭГ предназначена для обеспечения работы системы защиты информации ПТК ДЭГ в предусмотренных режимах функционирования.

Администраторы ИТ ПТК ДЭГ разделяются, в зависимости от полномочий, доступных для каждой конкретной роли администратора:

- администраторы управления:
  - администраторы СУБД;
  - администраторы среды виртуализации;
  - администраторы общесистемного ПО;
  - администраторы сетевого оборудования;
  - администраторы СКЗИ.
- администраторы мониторинга:
  - сотрудники дежурной смены;
  - администраторы системы мониторинга.

Учитывая возможности администраторов управления по деструктивному воздействию на инфраструктуру ПТК ДЭГ, для реализации каналов связи необходимо применять СКЗИ в соответствии с п. 4.8.

При этом, в рамках реализации организационных и технических мер защиты информации, обеспечивается взаимный контроль действий администраторов управления (администраторов с разными ролями), в рамках ЦОД, а также взаимный мониторинг действий администраторов в рамках распределенной между ЦОД инфраструктурой мониторинга.

3 ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПТК ДЭГ (МОДЕЛЬ УГРОЗ)

3.1 Идентификация угроз

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю.

3.2 Определение актуальности угроз безопасности информации

Перечень актуальных угроз безопасности информации ПТК ДЭГ представлен в таблице 2.

Таблица 2 – Перечень актуальных угроз безопасности информации ПТК ДЭГ

Номер угрозы	**Наименование угроз**	**Вероятность (возможность) реализации угрозы**	**Степень возможного ущерба**	**Актуальность угрозы**
УБИ. 003	Угроза анализа криптографических алгоритмов и их реализации	Высокая	Высокая	Актуальная
УБИ. 004	Угроза аппаратного сброса пароля BIOS	Высокая	Высокая	Актуальная
УБИ. 006	Угроза внедрения кода или данных	Высокая	Высокая	Актуальная
УБИ. 007	Угроза воздействия на программы с высокими привилегиями	Высокая	Высокая	Актуальная
УБИ. 008	Угроза восстановления и/или повторного использования аутентификационной информации	Высокая	Высокая	Актуальная
УБИ. 009	Угроза восстановления предыдущей уязвимой версии BIOS	Высокая	Высокая	Актуальная
УБИ. 010	Угроза выхода процесса за пределы виртуальной машины	Высокая	Высокая	Актуальная
УБИ. 012	Угроза деструктивного изменения конфигурации/среды окружения программ	Высокая	Высокая	Актуальная
УБИ. 013	Угроза деструктивного использования декларированного функционала BIOS	Высокая	Высокая	Актуальная
УБИ. 014	Угроза длительного удержания вычислительных ресурсов пользователями	Высокая	Высокая	Актуальная
УБИ. 015	Угроза доступа к защищаемым файлам с использованием обходного пути	Высокая	Высокая	Актуальная
УБИ. 016	Угроза доступа к локальным файлам сервера при помощи URL	Высокая	Высокая	Актуальная
УБИ. 017	Угроза доступа/перехвата/изменения HTTP cookies	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 018	Угроза загрузки нештатной операционной системы	Высокая	Высокая	Актуальная
УБИ. 019	Угроза заражения DNS-кеша	Высокая	Высокая	Актуальная
УБИ. 022	Угроза избыточного выделения оперативной памяти	Высокая	Высокая	Актуальная
УБИ. 023	Угроза изменения компонентов информационной (автоматизированной) системы	Высокая	Высокая	Актуальная
УБИ. 025	Угроза изменения системных и глобальных переменных	Высокая	Высокая	Актуальная
УБИ. 026	Угроза искажения XML-схемы	Высокая	Высокая	Актуальная
УБИ. 027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Высокая	Высокая	Актуальная
УБИ. 028	Угроза использования альтернативных путей доступа к ресурсам	Высокая	Высокая	Актуальная
УБИ. 030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Высокая	Высокая	Актуальная
УБИ. 031	Угроза использования механизмов авторизации для повышения привилегий	Высокая	Высокая	Актуальная
УБИ. 032	Угроза использования поддельных цифровых подписей BIOS	Высокая	Высокая	Актуальная
УБИ. 033	Угроза использования слабостей кодирования входных данных	Высокая	Высокая	Актуальная
УБИ. 034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Высокая	Высокая	Актуальная
УБИ. 035	Угроза использования слабых криптографических алгоритмов BIOS	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 036	Угроза исследования механизмов работы программы	Высокая	Высокая	Актуальная
УБИ. 037	Угроза исследования приложения через отчёты об ошибках	Высокая	Высокая	Актуальная
УБИ. 039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Высокая	Высокая	Актуальная
УБИ. 041	Угроза межсайтового скриптинга	Высокая	Высокая	Актуальная
УБИ. 042	Угроза межсайтовой подделки запроса	Высокая	Высокая	Актуальная
УБИ. 044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Высокая	Высокая	Актуальная
УБИ. 045	Угроза нарушения изоляции среды исполнения BIOS	Высокая	Высокая	Актуальная
УБИ. 046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Высокая	Высокая	Актуальная
УБИ. 048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Высокая	Высокая	Актуальная
УБИ. 049	Угроза нарушения целостности данных кеша	Высокая	Высокая	Актуальная
УБИ. 051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Высокая	Высокая	Актуальная
УБИ. 053	Угроза невозможности управления правами пользователей BIOS	Высокая	Высокая	Актуальная
УБИ. 059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 061	Угроза некорректного задания структуры данных транзакции	Высокая	Высокая	Актуальная
УБИ. 062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Высокая	Высокая	Актуальная
УБИ. 063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Высокая	Высокая	Актуальная
УБИ. 067	Угроза неправомерного ознакомления с защищаемой информацией	Высокая	Высокая	Актуальная
УБИ. 068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Высокая	Высокая	Актуальная
УБИ. 069	Угроза неправомерных действий в каналах связи	Высокая	Высокая	Актуальная
УБИ. 071	Угроза несанкционированного восстановления удалённой защищаемой информации	Высокая	Высокая	Актуальная
УБИ. 072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Высокая	Высокая	Актуальная
УБИ. 073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Высокая	Высокая	Актуальная
УБИ. 074	Угроза несанкционированного доступа к аутентификационной информации	Высокая	Высокая	Актуальная
УБИ. 075	Угроза несанкционированного доступа к виртуальным каналам передачи	Высокая	Высокая	Актуальная
УБИ. 076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Высокая	Высокая	Актуальная
УБИ. 078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Высокая	Высокая	Актуальная
УБИ. 079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Высокая	Высокая	Актуальная
УБИ. 080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Высокая	Высокая	Актуальная
УБИ. 084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Высокая	Высокая	Актуальная
УБИ. 085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Высокая	Высокая	Актуальная
УБИ. 086	Угроза несанкционированного изменения аутентификационной информации	Высокая	Высокая	Актуальная
УБИ. 087	Угроза несанкционированного использования привилегированных функций BIOS	Высокая	Высокая	Актуальная
УБИ. 088	Угроза несанкционированного копирования защищаемой информации	Высокая	Высокая	Актуальная
УБИ. 089	Угроза несанкционированного редактирования реестра	Высокая	Высокая	Актуальная
УБИ. 090	Угроза несанкционированного создания учётной записи пользователя	Высокая	Высокая	Актуальная
УБИ. 091	Угроза несанкционированного удаления защищаемой информации	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 093	Угроза несанкционированного управления буфером	Высокая	Высокая	Актуальная
УБИ. 094	Угроза несанкционированного управления синхронизацией и состоянием	Высокая	Высокая	Актуальная
УБИ. 095	Угроза несанкционированного управления указателями	Высокая	Высокая	Актуальная
УБИ. 098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Высокая	Высокая	Актуальная
УБИ. 099	Угроза обнаружения хостов	Высокая	Высокая	Актуальная
УБИ. 100	Угроза обхода некорректно настроенных механизмов аутентификации	Высокая	Высокая	Актуальная
УБИ. 102	Угроза опосредованного управления группой программ через совместно используемые данные	Высокая	Высокая	Актуальная
УБИ. 103	Угроза определения типов объектов защиты	Высокая	Высокая	Актуальная
УБИ. 104	Угроза определения топологии вычислительной сети	Высокая	Высокая	Актуальная
УБИ. 108	Угроза ошибки обновления гипервизора	Высокая	Высокая	Актуальная
УБИ. 109	Угроза перебора всех настроек и параметров приложения	Высокая	Высокая	Актуальная
УБИ. 111	Угроза передачи данных по скрытым каналам	Высокая	Высокая	Актуальная
УБИ. 113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Высокая	Высокая	Актуальная
УБИ. 114	Угроза переполнения целочисленных переменных	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Высокая	Высокая	Актуальная
УБИ. 116	Угроза перехвата данных, передаваемых по вычислительной сети	Высокая	Высокая	Актуальная
УБИ. 117	Угроза перехвата привилегированного потока	Высокая	Высокая	Актуальная
УБИ. 118	Угроза перехвата привилегированного процесса	Высокая	Высокая	Актуальная
УБИ. 119	Угроза перехвата управления гипервизором	Высокая	Высокая	Актуальная
УБИ. 120	Угроза перехвата управления средой виртуализации	Высокая	Высокая	Актуальная
УБИ. 121	Угроза повреждения системного реестра	Высокая	Высокая	Актуальная
УБИ. 122	Угроза повышения привилегий	Высокая	Высокая	Актуальная
УБИ. 123	Угроза подбора пароля BIOS	Высокая	Высокая	Актуальная
УБИ. 124	Угроза подделки записей журнала регистрации событий	Высокая	Высокая	Актуальная
УБИ. 127	Угроза подмены действия пользователя путём обмана	Высокая	Высокая	Актуальная
УБИ. 128	Угроза подмены доверенного пользователя	Высокая	Высокая	Актуальная
УБИ. 129	Угроза подмены резервной копии программного обеспечения BIOS	Высокая	Высокая	Актуальная
УБИ. 130	Угроза подмены содержимого сетевых ресурсов	Высокая	Высокая	Актуальная
УБИ. 131	Угроза подмены субъекта сетевого доступа	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 132	Угроза получения предварительной информации об объекте защиты	Высокая	Высокая	Актуальная
УБИ. 139	Угроза преодоления физической защиты	Высокая	Высокая	Актуальная
УБИ. 140	Угроза приведения системы в состояние «отказ в обслуживании»	Высокая	Высокая	Актуальная
УБИ. 143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Высокая	Высокая	Актуальная
УБИ. 144	Угроза программного сброса пароля BIOS	Высокая	Высокая	Актуальная
УБИ. 145	Угроза пропуска проверки целостности программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 149	Угроза сбоя обработки специальным образом изменённых файлов	Высокая	Высокая	Актуальная
УБИ. 150	Угроза сбоя процесса обновления BIOS	Высокая	Высокая	Актуальная
УБИ. 151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Высокая	Высокая	Актуальная
УБИ. 152	Угроза удаления аутентификационной информации	Высокая	Высокая	Актуальная
УБИ. 153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Высокая	Высокая	Актуальная
УБИ. 154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Высокая	Высокая	Актуальная
УБИ. 155	Угроза утраты вычислительных ресурсов	Высокая	Высокая	Актуальная
УБИ. 156	Угроза утраты носителей информации	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Высокая	Высокая	Актуальная
УБИ. 158	Угроза форматирования носителей информации	Высокая	Высокая	Актуальная
УБИ. 159	Угроза «форсированного веб-браузинга»	Высокая	Высокая	Актуальная
УБИ. 160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Высокая	Высокая	Актуальная
УБИ. 162	Угроза эксплуатации цифровой подписи программного кода	Высокая	Высокая	Актуальная
УБИ. 163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Высокая	Высокая	Актуальная
УБИ. 165	Угроза включения в проект не достоверно испытанных компонентов	Высокая	Высокая	Актуальная
УБИ. 166	Угроза внедрения системной избыточности	Высокая	Высокая	Актуальная
УБИ. 167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Высокая	Высокая	Актуальная
УБИ. 168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Высокая	Высокая	Актуальная
УБИ. 169	Угроза наличия механизмов разработчика	Высокая	Высокая	Актуальная
УБИ. 170	Угроза неправомерного шифрования информации	Высокая	Высокая	Актуальная
УБИ. 171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Высокая	Высокая	Актуальная
УБИ. 172	Угроза распространения «почтовых червей»	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 173	Угроза «спама» веб-сервера	Высокая	Высокая	Актуальная
УБИ. 174	Угроза «фарминга»	Высокая	Высокая	Актуальная
УБИ. 175	Угроза «фишинга»	Высокая	Высокая	Актуальная
УБИ. 177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Высокая	Высокая	Актуальная
УБИ. 178	Угроза несанкционированного использования системных и сетевых утилит	Высокая	Высокая	Актуальная
УБИ. 179	Угроза несанкционированной модификации защищаемой информации	Высокая	Высокая	Актуальная
УБИ. 180	Угроза отказа подсистемы обеспечения температурного режима	Высокая	Высокая	Актуальная
УБИ. 181	Угроза перехвата одноразовых паролей в режиме реального времени	Высокая	Высокая	Актуальная
УБИ. 182	Угроза физического устаревания аппаратных компонентов	Высокая	Высокая	Актуальная
УБИ. 185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Высокая	Высокая	Актуальная
УБИ. 186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Высокая	Высокая	Актуальная
УБИ. 187	Угроза несанкционированного воздействия на средство защиты информации	Высокая	Высокая	Актуальная
УБИ. 188	Угроза подмены программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 189	Угроза маскирования действий вредоносного кода	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Высокая	Высокая	Актуальная
УБИ. 191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 192	Угроза использования уязвимых версий программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Высокая	Высокая	Актуальная
УБИ. 195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Высокая	Высокая	Актуальная
УБИ. 197	Угроза хищения аутентификационной информации из временных файлов cookie	Высокая	Высокая	Актуальная
УБИ. 198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Высокая	Высокая	Актуальная
УБИ. 201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Высокая	Высокая	Актуальная
УБИ. 205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Высокая	Высокая	Актуальная
УБИ. 208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Высокая	Высокая	Актуальная
УБИ. 209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Высокая	Высокая	Актуальная
УБИ. 212	Угроза перехвата управления информационной системой	Высокая	Высокая	Актуальная
УБИ. 213	Угроза обхода многофакторной аутентификации	Высокая	Высокая	Актуальная
УБИ. 214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Высокая	Высокая	Актуальная
УБИ. 215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Высокая	Высокая	Актуальная
УБИ. 217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Высокая	Высокая	Актуальная

4 ВЫВОДЫ

Модель угроз разработана на основании постановления правительства Российской Федерации от 6 июля 2015 г. № 676 «Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

При разработке Модели угроз применялись методики, определённые в методическом документе ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» и Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности ФСБ России.

В качестве исходных данных для определения угроз безопасности информации использовался банк данных угроз безопасности информации (bdu.fstec.ru).

Организационные меры и средства защиты информации, применяемые в ПТК ДЭГ, должны обеспечивать защиту от угроз безопасности информации, связанных с действиями нарушителей с высоким потенциалом (спецслужбы иностранных государств).

Организационные меры и средства защиты информации, применяемые в ПТК ДЭГ, должны обеспечивать защиту от угроз безопасности информации, связанных с действиями, в том числе, внутренних нарушителей.

В составе ПТК ДЭГ, для нейтрализации угроз безопасности информации, необходимо использовать сертифицированные по требованиям безопасности информации средства защиты информации:

- средства защиты информации не ниже 4 класса и соответствующие 4 уровню доверия;

- средства контроля съемных машинных носителей информации не ниже 4 класса;
- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений не ниже 4 класса;
- средства антивирусной защиты не ниже 4 класса;
- средства межсетевого экранирования не ниже 4 класса;
- средства доверенной загрузки не ниже 4 класса.

В ПТК ДЭГ предполагаемый к использованию класс криптографической защиты для нейтрализации угроз безопасности информации при передаче персональных и иных данных по каналам связи между ЦОД ПТК ДЭГ определен как КА.

Предполагаемый к использованию класс криптографической защиты для нейтрализации угроз безопасности информации при передаче персональных и иных данных по каналам связи между ЦОД ПТК ДЭГ и серверными компонентами информационных систем ЦИК России определен как КА.

Предполагаемый к использованию класс криптографической защиты для нейтрализации угроз безопасности информации при передаче персональных и иных данных по каналам связи между компонентами ПТК ДЭГ в рамках КЗ ЦОД (за пределами выгородки) определен как КС3.

Для реализации подсистемы подключения пользователей к порталам ЕПГУ и ПТК ДЭГ для авторизации пользователей и получения бюллетеня голосования предполагаемый к использованию класс криптографической защиты для серверной компоненты класс СКЗИ определен как КС3.

Предполагаемый к использованию класс криптографической защиты в сегменте пользователей ПТК ДЭГ (избиратель) для подключения пользователей к порталам ЕПГУ и ПТК ДЭГ, авторизации пользователей и получения бюллетеня голосования, для нейтрализации угроз безопасности информации при передаче персональных данных по каналам связи, а также наложения и проверки ЭП определен как КС1.

Предполагаемый к использованию класс криптографической защиты на стороне администраторов управления, председателей и членов ИК ДЭГ (председатель ИК ДЭГ, оператор ИК ДЭГ, администраторы ИТ, администраторы ИБ), при взаимодействии с ПТК ДЭГ по каналам связи выходящими за пределы ЦОД, ввиду регулярного характера взаимодействия с системой и категории обрабатываемых данных (управляющая информация) определен как КА.

Предполагаемый к использованию класс криптографической защиты на стороне администраторов управления, председателей и членов ИК ДЭГ (председатель ИК ДЭГ, оператор ИК ДЭГ, администраторы ИТ, администраторы ИБ), при взаимодействии с ПТК ДЭГ по каналам связи не выходящими за пределы контролируемой зоны ЦОД, ввиду регулярного характера взаимодействия с системой и категории обрабатываемых данных (управляющая информация) определен как КС3.

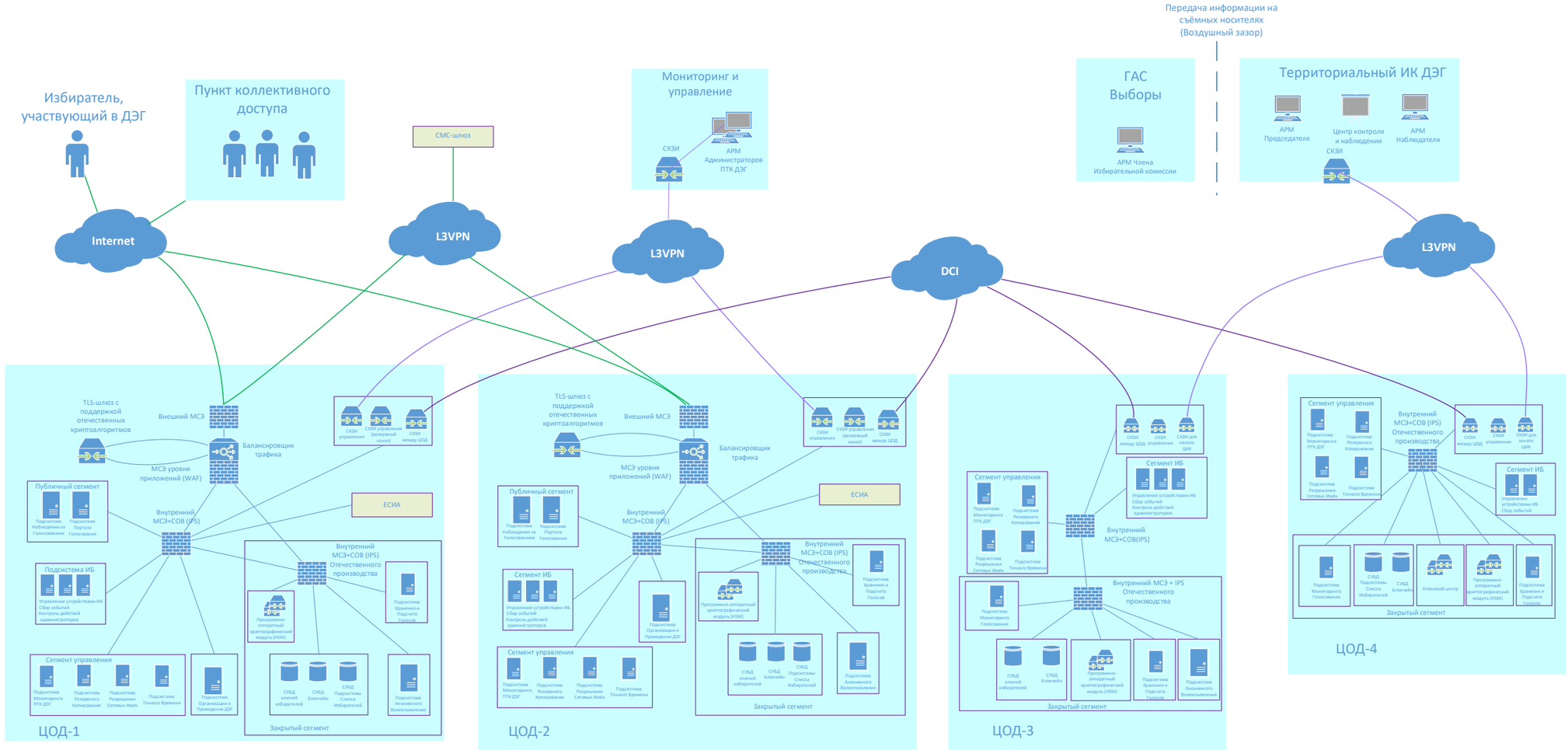
Предполагаемый к использованию класс криптографической защиты для реализации технологии блокчейн (подпись блоков) определен как класс СКЗИ КВ.

Предполагаемый к использованию класс криптографической защиты для ключевого центра определен как класс СКЗИ КА.

Репликация ключей между ЦОД должна осуществляться по протоколу репликации ключей между HSM класса КВ.

ПРИЛОЖЕНИЕ А

Схема архитектуры ПТК ДЭГ



Реализация каждого ЦОД включает в себя:
- Сертифицированные ОС
- Сертифицированные СУБД
- Средства доверенной загрузки
- Средства защиты гипервизоров
- Средства защиты контейнеризации
- Средства контроля действий привилегированных пользователей

Взаимодействие между ЦОД, защищаемое СКЗИ по классу КА, резервирование по классу КСЗ

Взаимодействие по сетям общего пользования

Взаимодействие по выделенным каналам, защищаемым СКЗИ по классу КА

Взаимодействие внутри контролируемой зоны

Внешние системы