Программно-технический комплекс дистанционного электронного голосования (ПТК ДЭГ)

Модель угроз и нарушителя безопасности информации

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» для информации, обрабатываемой в ПТК ДЭГ, устанавливаются следующие классификационные признаки:

- высокий уровень значимости (УЗ-1);
- ПТК ДЭГ имеет федеральный масштаб так как функционирует на всей территории Российской Федерации.

Для ПТК ДЭГ необходимо обеспечить выполнения требований, предъявляемых к 1 (первому) классу защищенности информационных систем

Уровень защищенности ПДн

В соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» установлено, что ПТК ДЭГ имеет следующие характеристики:

- для ПТК ДЭГ актуален 3 тип угроз;
- в ПТК ДЭГ обрабатываются ПДн, не относящиеся к категориям общедоступных, биометрических и специальных ПДн (иные категории ПДн);
- в ПТК ДЭГ обрабатываются ПДн субъектов, не являющихся сотрудниками оператора (более 100 000 субъектов ПДн).

В ПТК ДЭГ необходимо обеспечить третий уровень защищенности персональных данных при их обработке в ПТК ДЭГ (УЗ-3)

Основание разработки Модели угроз и нарушителя безопасности информации

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

Модель угроз прошла процедуры согласования с ФСБ России и ФСТЭК России

Типы нарушителей

С учетом наличия прав доступа и возможностей по доступу к информации и/или к компонентам ПТК ДЭГ нарушители подразделяются на два типа:

- внешние нарушители ИБ [тип 1] – лица, не являющееся пользователями ПТК ДЭГ или сотрудниками организации, эксплуатирующей инфраструктуру ПТК ДЭГ, и не имеющие санкционированного доступа к аппаратным и программным компонентам ПТК ДЭГ и информации, обрабатываемой в системе;
- внутренние нарушители ИБ [тип 2] – лица, являющиеся пользователями ПТК ДЭГ, и внешних, по отношению к ПТК ДЭГ организаций, имеющих постоянный или разовый доступ к информации, обрабатываемой в ПТК ДЭГ и компонентам ПТК ДЭГ, в рамках выполнения своих функциональных задач, а также лица, являющиеся сотрудниками организаций, не имеющие доступа к обрабатываемой информации, выполняющие хозяйственную деятельность и осуществляющие физический доступ к объектам доступа без цели их непосредственного использования.

Виды нарушителей

Тип нарушителя	Вид нарушителя
Внешний	Специальные службы иностранных государств (блоков государств)
	Террористические, экстремистские группировки.
	Преступные группы (криминальные структуры); Внешние субъекты (физические лица);
	Разработчики, производители, поставщики программных, технических и программно-технических средств
	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ (лица, обеспечивающие поставку, сопровождение и ремонт технических средств ПТК ДЭГ)
Внутренние	Пользователи ПТК ДЭГ (имеющие доступ к критичным для ПТК ДЭГ процессам)
	Пользователи ПТК ДЭГ (не имеющие доступ к критичным для ПТК ДЭГ процессам)
	Администраторы ПТК ДЭГ
	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ
	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

Угрозы информационной безопасности

Организационные меры и средства защиты информации, применяемые в ПТК, должны обеспечивать защиту от угроз безопасности информации, связанных с действиями нарушителей с высоким потенциалом

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

Угрозы связанные с использованием протоколов голосования

В ПТК ДЭГ рассматриваются угрозы, связанные с использованием протоколов голосования. К данным угрозам относятся:

- возможность со стороны нарушителя, используя ПО и технологические решения ПТК ДЭГ извлечь сведения о выборе избирателя, группы избирателей, всех избирателей, а также идентифицировать избирателя по выбору;
- возможность реализации голосования более одного раза;
- подмена голосов избирателей;
- некорректная запись голоса избирателя;
- досрочное прекращение голосования;
- деанонимизация избирателя;
- установление промежуточных итогов голосования до его завершения.

Средства защиты информации

В составе ПТК ДЭГ 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.

Средства криптографической защиты информации

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.

Средства криптографической защиты информации

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.