

# Дистанционное электронное голосование (ДЭГ)

Подготовил Шаталин Данила м-45

# Дистанционное электронное голосование

- Дистанционное электронное голосование - это метод голосования, который позволяет избирателям проголосовать за кандидатов и инициативы на выборах или референдумах, используя интернет или другие электронные средства связи, не покидая своего дома.

# История развития в России и в других странах

- История развития Дистанционного электронного голосования началась в 1960-х годах в США, когда были разработаны первые электронные системы голосования. В России ДЭГ начали применяться сравнительно недавно, в 2012 году на региональных выборах в городе Москва. Впервые ДЭГ было применено в России на всенародном голосовании по поправкам к Конституции в 2020 году.
- В других странах Дистанционное электронное голосование также получило широкое распространение. Некоторые страны, такие как Эстония и Швейцария, уже многие годы успешно используют ДЭГ на выборах и референдумах. В других странах, таких как США, Канада, Великобритания, Франция, Нидерланды и Япония, ДЭГ применяется в определенных регионах или для определенных категорий избирателей.

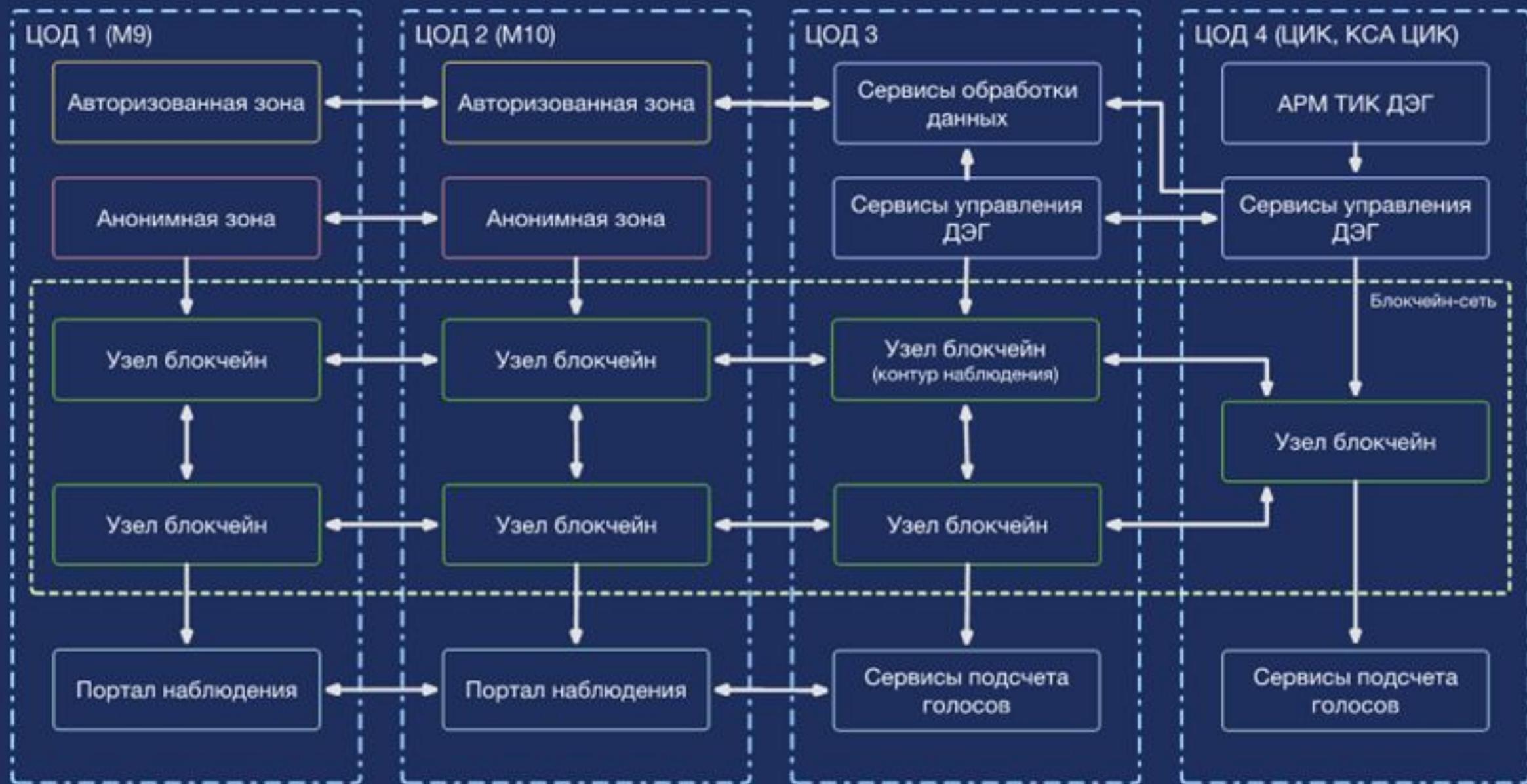
# Дэг в России

- В 2020 году ЦИК сообщила, что «Ростелеком» разрабатывает систему по ее заданию. В ЦИК пояснили, что «Ростелеком» с 2019 года в соответствии с поручением президента определен правительством единственным исполнителем заказываемых ЦИК работ по цифровизации избирательного процесса, предоставлению цифровых сервисов для участников избирательного процесса и созданию цифровой платформы реализации основных гарантий избирательных прав и права на участие в референдуме граждан РФ.

## Как эти задачи могут решаться технически и организационно, на примере ДЭГ в России

- Инфраструктура федеральной системы ДЭГ на выборах в сентябре 2021 года включала 4 ЦОДа: площадки «Ростелекома» и два дополнительных [дата-центра](#). Система построена с возможностью масштабирования: первые три ЦОДа разворачивались на период голосования, а 4-й [ЦОД](#) остался в ведении ЦИК и сохранился и после завершения голосования. При этом у ЦИК остаются и все [данные](#) голосования.
- Также в состав инфраструктуры входят магистральные сети связи «Ростелекома», [ИТ](#)-оборудование, в котором в общем случае выделяется несколько слоев: сети передачи данных, [хранения](#), [виртуализации](#), [контейнеризации](#), [информационной безопасности](#) и [операционных систем](#). Дальше начинается сфера прикладного [ПО](#).

# Инфраструктурная схема ПТК ДЭГ



# Участники ДЭГ и их роли.

## ОСНОВНЫЕ УЧАСТНИКИ ПРОЦЕССА ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ (ДЭГ) И ИХ РОЛИ

TADVISER 2021



Гражданин РФ

Голосует в системе ДЭГ. Гражданин РФ, обладающий избирательным правом, с подтвержденной учетной записью на ЕПГУ, подавший заявление на ДЭ и получивший подтверждение.



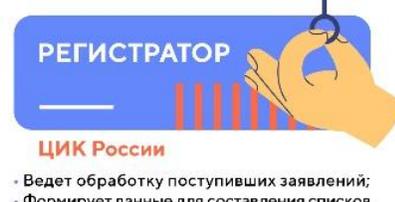
Минцифры России

Обеспечивает работу ЕСИА, через которую происходит система идентификации и аутентификации участника ДЭГ.



Минцифры России

Обеспечивает работу ЕПГУ, через который подаются гражданами заявления на участие в ДЭГ и передаются в ЦИК.



ЦИК России

- Ведет обработку поступивших заявлений;
- Формирует данные для составления списков участников ДЭГ;
- Является держателем ключей регистратора по каждому голосованию и сервиса подписи вслепую открытого ключа участника ДЭГ, обеспечивающего доступ к бюллетеню.



Территориальная избирательная комиссия ДЭГ

- Формирование списка участников ДЭГ;
- Отвечает за процессы, связанные с генерацией, загрузкой, сборкой ключей шифрования;
- Загрузка исходных данных о голосовании;
- Запуск подсчета голосов: формирование итогового бюллетеня и его расшифровка;
- Получение данных об итогах голосования;
- Подписание протокола об итогах голосования.



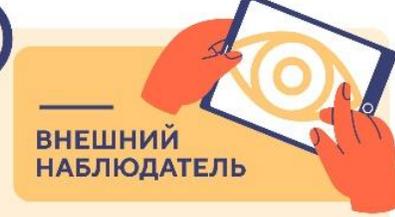
Избирательные комиссии, организующие выборы

определяющие результаты выборов на территории

- Подготовка в ГАС «Выборы» исходных данных (текст бюллетеня, форма протокола) для передачи организатору ДЭГ;
- После завершения голосования получают от организатора ДЭГ данные об итогах голосования для загрузки в ГАС «Выборы».



Наблюдает за процессом голосования из специализированного помещения, оснащенного средствами доступа к отдельным узлам компонента ПТК ДЭГ «Распределенное хранение и учет голосов».



Любой пользователь, наблюдающий за процессом голосования с портала наблюдения, публикующего статистические данные о голосовании в интернете. Может получить выгрузку транзакций из сети блокчейн в виде файлов, публикуемых на портале наблюдения.



**ФУНКЦИИ «РОСТЕЛЕКОМА»**



Предоставляет инфраструктуру ДЭГ и обеспечивает ее работу



Разработчик ПТК ДЭГ



Оказывает техподдержку ПТК ДЭГ

## Безопасность федеральной платформы

- В «Ростелекоме» и ЦИК уверяют, что система надежно защищена от [кибератак](#), надежна и обеспечивает тайну голосования. Федеральная система ДЭГ использует отечественную [блокчейн-платформу Waves Enterprise](#) с применением российских [криптографических алгоритмов](#) и средств защиты. [Блокчейн](#) позволяет хранить [зашифрованные](#) голоса избирателей в неизменном виде.
- Шифрование информации производится с помощью специального ключа, загруженного в блокчейн в ходе специальной процедуры, которая проходит в ТИК ДЭГ до начала голосования. Для расшифровки нужен другой специальный ключ, который создается и разделяется на несколько частей в ходе той же процедуры, а собирается только при подведении итогов. Части ключа расшифрования записываются на защищенные носители и передаются на хранение независимым «держателям» до окончания голосования. Одна из частей ключа также хранится в модуле [информационной безопасности](#) (Hardware Security Module, HSM) и оттуда не извлекается. Криптографический алгоритм позволяет проводить математические операции с зашифрованными данными, поэтому для подведения итогов расшифровывается суммарный зашифрованный бюллетень. Сами непосредственно бюллетени избирателей не расшифровывается ни во время, ни после установления итогов.
- Частично открыты коды системы. Так, в рамках раскрытия технической информации о системе ДЭГ, в сентябре 2021 года на ресурсе [GitHub](#) были размещены исходные коды основных компонентов системы, которая будет использована в голосовании в 2021 году [\[4\]](#). В частности, доступны коды портала голосования и анонимной зоны портала ДЭГ; утилиты разделения ключей; [смарт-контракт](#) и др.

## Анонимность голосования.

- Для обеспечения тайны голосования и анонимизации избирателя используется криптографический алгоритм «слепой электронной подписи». В этой статье мы рассмотрим его более подробно.

Сначала обратимся к известному и знакомому алгоритму электронной подписи, который широко применяется в информационных системах различного назначения. В основе электронной подписи лежат криптографические алгоритмы асимметричного шифрования. Асимметричное шифрование – это шифрование с помощью 2 ключей: один из них используется для шифрования, другой для расшифрования. Их называют открытый (публичный) и закрытый ключ. Открытый ключ известен окружающим, а закрытый – только владельцу электронной подписи и хранится в недоступном для других месте.

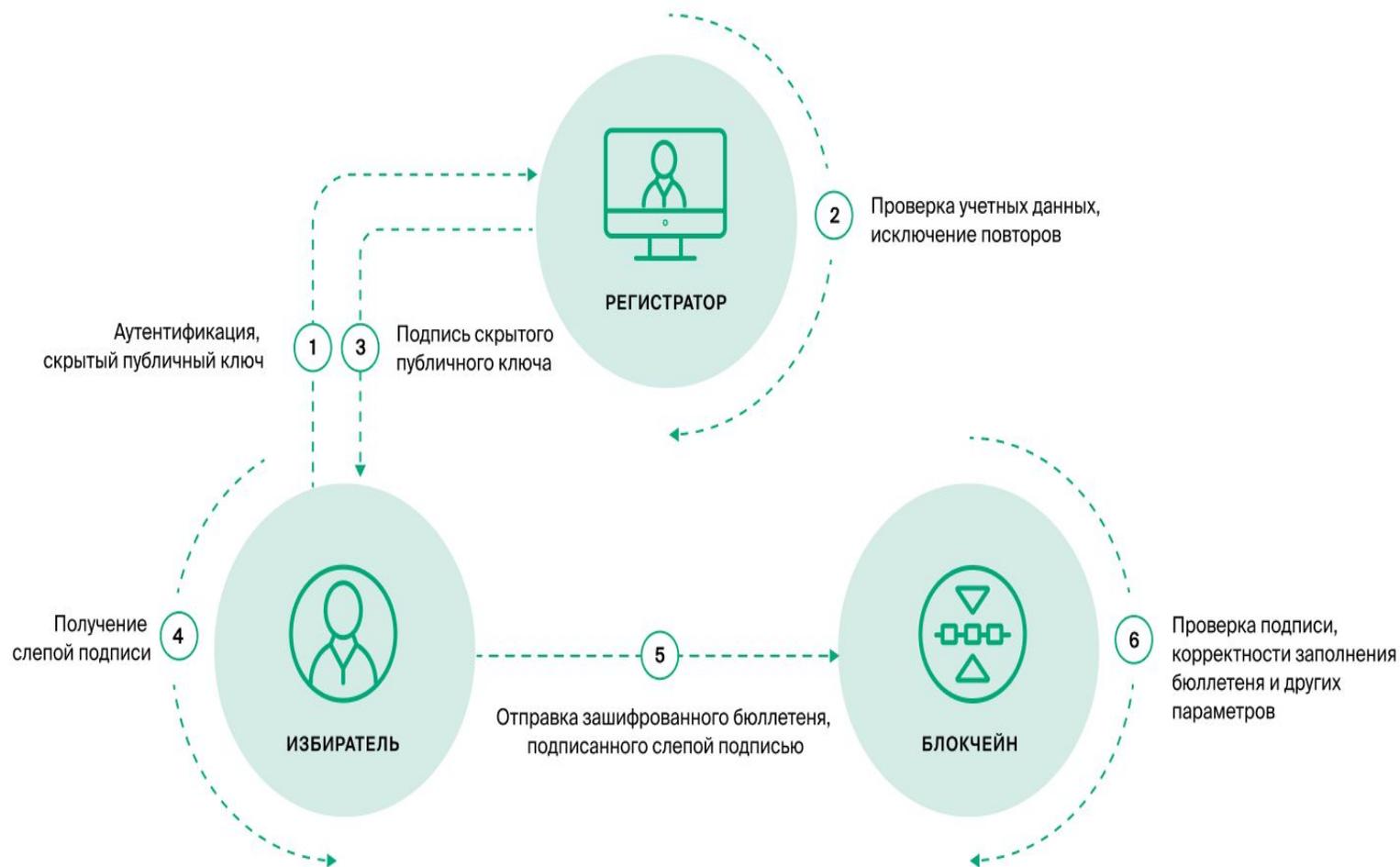
При подписании происходит следующее: сначала электронный документ, с помощью математических преобразований, приводится к последовательности символов определенного размера – это называется хэш функцией.

Полученная символьная последовательность (хэш от документа) зашифровывается отправителем документа с помощью закрытого ключа и вместе с открытым ключом отправляется получателю. Получатель расшифровывает с помощью открытого ключа символьную последовательность, применяет к документу точно такую же хэш функцию и сравнивает результат преобразования с результатом расшифровки. Если все совпадает, то в документ не было внесено изменений после подписания его отправителем.

Описанные действия позволяют удостовериться, что документ не изменялся, но не позволяют убедиться в том, что отправитель действительно тот, за кого он себя выдает. Поэтому нам нужна третья сторона, которой доверяют и отправитель, и получатель. Для этого до отправки документа отправитель обращается к третьей стороне и просит ее подписать своей электронной подписью его открытый ключ. Теперь отправитель направляет получателю документ, свой открытый ключ, и подпись третьей стороны

- Теперь перейдем к тому, что такое «слепая подпись» и как она может помочь нам при анонимизации.

Представим, что в описанном выше примере отправитель — это избиратель, документ — это бюллетень, а получатель — избирательная комиссия, или как мы говорили «компонент учета и подсчета голосов». В качестве третьей стороны (валидатора) у нас будет выступать компонент «Список избирателей». В этом случае процесс может происходить следующим образом



# Основные криптографические алгоритмы

ТЕХНОЛОГИИ	СТАНДАРТЫ
Анонимизация избирателя	«Слепая» подпись регистратора. Поддерживаемые алгоритмы и стандарты 1) RSA 4096 2) алгоритмы с эллиптическими кривыми, определенные в Р 50.1.114-2016
Распределение ключа и генерация ключа шифрования	ГОСТ Р 34.12-2015 (опционально DKG Pedersen 91) Распределение ключа между держателями по схеме Шамира
Шифрование бюллетеня на стороне избирателя	Зашифрование данных по схеме Эль-Гамала (на эллиптических кривых) Неинтерактивные доказательства с нулевым разглашением (NIZK)
Подпись бюллетеня на стороне избирателя	ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
Проверка корректности данных в зашифрованных бюллетенях	Неинтерактивные доказательства с нулевым разглашением (NIZK)
Сложение зашифрованных бюллетеней	Зашифрование данных по схеме Эль-Гамала (на эллиптических кривых) со свойством аддитивного гомоморфизма
Распределенное расшифрование результатов голосования	Неинтерактивные доказательства с нулевым разглашением (NIZK)

## Модель угроз и нарушителя

- Модель угроз и нарушителя (МУиН) — это достаточно традиционный для IT-систем документ, описывающий, каким именно и с чьей стороны атакам и опасностям они могут подвергнуться. Банальные угрозы в целом всем очевидны — хакеры, DDoS, пожар, наводнение, землетрясение и экскаватор в поисках кабеля.
- Значительно интереснее угрозы, специфические для конкретной системы — те, которые повлекут не просто её отказ, а скажем так, недопустимое поведение: утрату или искажение обрабатываемых данных, раскрытие внутренней информации. В случае электоральных систем они крайне критичны, так как подозрение на успешную атаку на систему может привести к срыву выборов.
- есть три вида угроз:
  - социальная: т.н. голосование под давлением, когда человека принуждают к определённому выбору руководство или родственники;
  - электоральная: когда проводятся манипуляции на уровне процедур избирательной системы, например, вброс бюллетеней;
  - техническая: когда осуществляется непосредственная атака на инфраструктуру ПТК ДЭГ (причём как снаружи, так и изнутри).

## Модель угроз и нарушителя

- Обсуждаемая модель угроз работает с третьей категорией — она описывает, какие именно угрозы от каких именно злоумышленников, от иностранных спецслужб до недобросовестных сотрудников, могут быть направлены против ПТК ДЭГ.
- Полный текст модели угроз и нарушителя пока что ЦИК России не опубликован, однако на одном из заседаний экспертной группы при ЦИК была представлена презентация с основными тезисами, на базе которых МУиН формируется. На днях была выложена также [выписка из модели угроз](#), но ничего принципиально нового она нам не добавляет.

# 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)