

Пресс-брифинг Общественной палаты РФ

30 июня 2020 г.

Часть I: наблюдения и замечания

1. Электронное голосование проходит успешно с технической точки зрения, но необходимо понимать и помнить, что это — всего лишь первый шаг по длинной дороге.
2. С технической точки зрения система работает стабильно. Более того, мы, как эксперты, были приятно удивлены таким результатом — особенно с учётом 100-кратного роста нагрузки по сравнению с голосованием МГД 2019. Мы ожидали большего числа отказов.
3. Существенных отказов самой электоральной системы не зафиксировано. Был полчасовой отказ утром 25 числа «обложки» сайта голосования, при этом само голосование продолжало работать по прямой ссылке.
4. Были два технических отказа системы мониторинга для наблюдателей — в течение всей ночи с 25 на 26 не выгружались данные из блокчейна из-за превышения допустимого размера и времени формирования файла (файлы почти по 200 МБ), вечером 27 — часовой отказ мониторинга из-за внешней атаки. Детали атаки ожидаем от специалистов ДИТ Москвы.
5. Предварительный мониторинг работы блокчейна сбоев не выявил. Ожидаем от ДИТ Москвы полной выгрузки всех данных после окончания голосования.
6. Главной причиной отказа избирателям в допуске к голосованию стало несовпадение данных в базах различных ведомств. Около 40 тыс. отказов.
7. На втором месте — дублирование заявлений. Из-за возможности использования и мос.ру, и Госуслуг около 26 тыс. избирателей подали заявление через оба сервиса, в более позднем им было отказано, первое поданное удовлетворялось. Из-за недостаточно подробного информирования многие избиратели решили, что им в голосовании отказано полностью, а не только по одному из двух заявлений.
8. Наблюдались нестыковки в работе с обычными УИК. Из-за 1,6 млн. открепительных удостоверений в одной только Москве (1,1 млн. из них по ДЭГ) в некоторых УИК не успели учесть все открепительные, в некоторых были ложно учтённые избиратели, например, при полном совпадении ФИО. Такие случаи единичны, но они есть, их причиной является резко возросшая нагрузка на УИКи.
9. Около 1,6 % бюллетеней выданы, но результаты по ним не получены. Специалисты изучают причины этого, в большинстве случаев для избежания было бы достаточно более подробного информирования избирателей о поведении при незначительных сбоях.

10. Серьёзных вбросов недостоверной информации в Интернете не зафиксировано. В большинстве случаев избиратели выражают недовольство, следующее из недостаточной информированности о регламенте проведения ДЭГ. В отдельных случаях есть попытки заявлений, например, о возможности проголосовать через ДЭГ более одного раза — мы связывались с их авторами, они отказались предоставлять нам дополнительную информацию и доказательства.
11. Поступают единичные сообщения о голосовании под давлением, с обещанием руководства предприятий получить список голосов сотрудников через Госуслуги. На данный момент у нас нет никаких сведений, позволяющих утверждать, что это возможно. В блокчейне не сохраняется информация о личности проголосовавшего, по нему невозможно установить, кто именно какой голос отдал. Информация о возможности самостоятельной проверки поданного голоса соответствует действительности, но проверить его может только человек, непосредственно этот голос подавший, если в момент его подачи он записал выданный ему случайный идентификатор. В случае, если работодатель принуждает вас к голосованию за определённый вариант, утверждая, что потом проверит ваш голос — обязательно сообщайте об этом в Общественную палату и ни в коем случае не поддавайтесь давлению.
12. Что касается опасений подмены голосов, то ни наблюдатели, ни операторы системы не знают до самого конца голосования, за какой вариант вы проголосовали. Отданный голос шифруется на вашем устройстве, для его расшифровки нужен ключ, собираемый из нескольких частей, которые сейчас находятся у нескольких независимых людей — в том числе у представителей движения «Голос». До окончания голосования невозможно узнать его результаты. После окончания, если вы воспользовались упомянутой выше инструкцией, вы сможете сами проверить, правильно ли учтён ваш голос.
13. Что касается сообщений о скупке SIM-карт и баз данных для подставного голосования, то аккаунты, созданные после 5 июня, к голосованию допущены не были. Таких аккаунтов — около 15 тыс. штук, что относительно немного. Тем не менее, это временная, разовая мера, в долгосрочной перспективе она неэффективна.

Часть II: дальнейшее развитие системы.

1. Система должна быть выведена на федеральный уровень и распределена между несколькими игроками. Полный контроль над системой одного оператора — неправильная ситуация, так как потенциально этот оператор может злоупотребить своим положением с целью компрометации системы (фальсификации результатов, нарушения тайны голосования). Технически, по словам авторов, система уже готова к такой эксплуатации.
2. В системе должны быть реализованы меры защиты в соответствии с действующим законодательством по защите информации ГИС, а по окончании

реализации защитных мер, но до введения системы в промышленную эксплуатацию, она должна быть аттестована в качестве ГИС и пройти проверку ФСТЭК и других причастных служб.

3. Система должна быть документирована, должны быть в соответствии с действующими ГОСТами и принципом достаточности информации описаны её параметры, алгоритмы, программные интерфейсы.
4. Должна быть продумана, регламентирована и введена система надёжной верификации избирателя, например, возможность голосования только через верифицированный аккаунт Госуслуг, чтобы устранить возможность подставных голосований в будущем.
5. Система должна располагаться в выделенных специально под неё ЦОД, для которых предусмотрен режим доступа наблюдателей и меры по контролю за неизменностью выполняемого на серверах кода. Сейчас система работает на обычных ЦОД, в которые допуск наблюдателей не регламентирован.
6. Должны быть регламентированы права и обязанности наблюдателей на ТИК ДЭГ с учётом специфики электронного голосования, например, доступ к данным, порядок отчётности операторов системы о реагировании на инциденты и технические сбои, и так далее.
7. Должно быть существенно расширено и улучшено информирование избирателей о регламенте проведения ДЭГ, причинах отказов, действиях избирателя при этих отказах, механизмах защиты результатов голосования, обнаружения подмены голосов и т.п.
8. Должен быть рассмотрен вопрос об адаптации избирательного законодательства к техническим особенностям ДЭГ, например, возможности многократного голосования одного и того же избирателя с учётом только последнего поданного им голоса. Это решило бы вопрос и с 1,6 % «испорченных» бюллетеней, и с голосованием под давлением.
9. Должна быть в явном виде описана модель угроз ДЭГ и меры по нейтрализации этих угроз, от технических сбоев и внешних атак до манипуляций со стороны обслуживающего персонала. Меры как технические, так и, например, регламенты по аннулированию части бюллетеней.
10. С целью реализации этих мер должна быть разработана и публично обсуждена с участием экспертов дорожная карта по развитию и внедрению ДЭГ в России на период 2020-2024 г.г.
11. Применение системы ДЭГ должно быть расширено на региональные выборы, а также региональные и федеральные опросы общественного мнения. Должна проводиться последовательная цифровизация УИК.