Безопасность информационных систем голосования: риски и способы их минимизации

В последние годы выборы уходят в «цифру». Информационные системы делают почти все: ведут списки избирателей, передают протоколы, следят через видеонаблюдение и позволяют голосовать, не выходя из дома. С одной стороны, это удобно и быстро. С другой - формирует новые проблемы: от технических сбоев до кибератак. С развитием дистанционного электронного голосования (ДЭГ), многодневных кампаний и новых сервисов ЦИК, запрос общества на прозрачность и устойчивость систем вырос в разы. О чем идет речь, когда говорим об информационных системах голосования? Их можно разделить на три группы: база традиционных выборов - ГАС «Выборы», электронные списки, системы видеонаблюдения и сайты комиссий; платформы ДЭГ - федеральная система через «Госуслуги» и региональные решения; инфраструктура - дата-центры, каналы связи, криптозащита и системы мониторинга. Особенность систем состоит в том, что они должны одновременно обеспечивать несколько требований: доступность, тайну голосования, неизменность результата, проверяемость, защиту персональных данных, устойчивость к внешним воздействиям. Но чем выше анонимность бюллетеня, тем сложнее доказать избирателю, что его голос учтен именно так, как он проголосовал. Поэтому проектирование цифрового голосования является поиском баланса между безопасностью, удобством и доверием.

Мировой опыт показывает, что проблема не только в защите от хакеров, но и в доказуемости. В Эстонии электронное голосование - норма, в Швейцарии его периодически ставят на паузу для доработки безопасности, в Германии отказались от электронных машин в пользу бумаги, чтобы процесс был понятен человеку. Основные риски информационных систем голосования можно разделить на технические, организационные, кибернетические и социально-политические. К техническим рискам относятся сбои серверов, перегрузка каналов связи, ошибки программного кода, некорректная работа интерфейса, задержки при авторизации, сбои при передаче данных, несовместимость устройств пользователя с платформой. Даже кратковременная недоступность системы может вызвать общественный резонанс, так как выборы проходят в ограниченный срок, а каждый избиратель должен иметь равный доступ к процедуре.

Эксперты - доцент кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации кандидат технических наук, доцент Масалева М.В. и профессор кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации доктор технических наук, профессор Седнев В.А. провели исследование данных из открытых источников об инцидентах, связанных с применением информационных технологий в предшествующих избирательных кампаниях с 2020 года, которое показало, что основными рисками, которые создают трудности применения информационных технологий при голосовании, являются технические, которые, в свою очередь, связаны с организацией проведения избирательной кампании и кибберрисками.

Организационные риски - уровень подготовки специалистов, обеспечивающих работу информационных систем голосования. Даже защищенная система может пострадать из-за человеческого фактора: неверной настройки серверов, слабых процедур доступа, недостаточного обучения персонала, ошибок операторов. Особенно опасны ситуации, когда технические специалисты, избирательные комиссии и наблюдатели не имеют общего языка для описания проблем.

Киберриски представляют собой DDoS-атаки, попытки несанкционированного доступа, фишинг, компрометацию учетных записей, атаки на цепочку поставок, вредоносное программное обеспечение, атаки на криптографическую инфраструктуру. В отличие от обычных государственных сервисов, системы голосования являются особо привлекательной целью: успешная атака может не только нарушить работу сервиса, но и подорвать доверие к результатам.

Как минимизировать риски применения информационных технологий в избирательных кампаниях? *По мнению экспертов - доцента кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации кандидата технических наук, доцента Масалевой М.В. и профессора кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации доктора технических наук, профессора Седнева В.А.*, для обеспечения функционирования технологий, минимизации технических рисков и формирования доверия у граждан можно реализовывать следующие мероприятия: проводить независимый аудит, при этом код и криптографию должны проверять внешние эксперты, а результаты, хотя бы общие, публиковать, причем следует предоставить избирателю возможность убедиться, что его голос дошел до цели, не нарушая тайны голосования; разрабатывать резервные сценарии для недопущения технических сбоев в работе информационных технологий; внедрять не только мощные фильтры трафика для защиты от кибератак, но и учить пользователей не попадаться на фишинг, - если же сбой произошел, то следует дать возможность избирателям через официальные источники получить информацию о том, что произошло. Безопасность выборов - это не только про шифрование, но и про то, понимает ли человек, как работает система, при этом цифровая безопасность электоральных процессов - вопрос национальной безопасности.

Масалева М.В.,
кандидат технических наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве Российской Федерации
Седнев В.А.,
доктор технических наук, профессор,
профессор кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве Российской Федерации