Автор: Бабенко А.И.,Бабенко И.В.
05.12.2024 17:20 - Обновлено 05.12.2024 17:21

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИФУНКЦИОНИРОВАНИЯ ДЕМОКРАТИЧЕСКОГО ИЗБИРАТЕЛЬНОГО ПРОЦЕССА

Бабенко А.И., старший преподаватель

Бабенко И.В., к.э.н., доцент

Кубанский государственный университет, г. Краснодар, Россия

Аннотация: Выборы являются важнейшей формой участия граждан государства в демократическом процессе и жизни страны. Современные цифровые технологии, преображающие различные процессы и улучшающие их удобство, коснулись и избирательной сферы. Но оправдано ли применение инновационных технологий? Авторами рассмотрены аспекты обеспечения информационной безопасности функционирования демократического избирательного процесса при его проведении в различных формах.

Ключевые слова: выборы, демократия, информационные системы, информационная безопасность, цифровизация, вмешательство, фальсификация, вредоносное программное обеспечение.

Выборы являются важнейшей формой участия граждан государства в демократическом процессе. Именно результат выборов определяет способность граждан реализовывать свои права и обязанности.

Существует два критерия надёжного избирательного процесса:

1) тайна голосования. Означает невозможность выяснить голос конкретного избирателя, в том числе во избежание давления на него [3];

2) достоверность голосования. Означает, что голосуют однократно и самостоятельно формируя своё волеизъявление реальные избиратели. Достоверность голосования должна быть проверяемой, для чего существует процедура наблюдения на выборах.

Внедрение инноваций в избирательный процесс позволяет обеспечить новшества в вопросе удобства волеизъявления, а также повысить экологичность (при отказе от бумажных бюллетеней). Однако обеспечивают ли инновационные формы участия в выборах и их проведения нужную информационной безопасность?

Существуют три эволюционные формы голосования:

1) бумажное голосование с ручным подсчётом бюллетеней, помещаемых в традиционные урны;

2) бумажное голосование с использованием устройств типа «терминал оптического сканирования» (в России таковым является устройство КОИБ), представляющих собой избирательные урны для помещения заполненного бумажного бюллетеня, оснащённые устройством сканирования бумажного носителя с целью определения обозначения выбора избирателя и сохранения его в постоянное запоминающее устройство (ПЗУ) данного аппаратно-программного комплекса, с возможностью дальнейшей печати аккумулированных итогов голосования на принтер или их передачи посредством сети ЭВМ для дальнейшей обработки;

3) электронное голосование – представляет собой волеизъявление избирателя, осуществляемое посредством воздействия (как правило, путём механического нажатия на кнопки или касания сенсорного экрана) на органы управления ЭВМ, с дальнейшим непосредственным сохранением волеизъявления в постоянное запоминающее устройство (ПЗУ), без использования промежуточного бумажного носителя в виде бюллетеня. Электронное голосование может осуществляться как на избирательных участках с использованием терминалов электронного голосования (ТЭГ), так и с использованием домашнего компьютера в дистанционном режиме (ДЭГ).

На наш взгляд, бумажный носитель обеспечивает проверяемость выборов. Необходимо выяснить, каким критериям должен отвечать достоверный голос на выборах. На наш взгляд, он должен отвечать следующим критериям:

1) голос должен быть направлен исключительно реальным избирателем (лицом, обладающим активным избирательным правом, т.е. правом избирать [3]);

2) голос должен быть сформирован без давления на избирателя или воздействия на

процесс фиксации голоса;

3) голос должен быть подан одним избирателем только однократно в рамках одной избирательной кампании;

4) после подачи голос не должен быть изменён без ведома избирателя.

Безусловно, проверка соответствия голосов данным критериям является сложной комплексной задачей. Необходимо помнить о том, что при обеспечить этих критериев важно не нарушить соблюдение тайны голосования.

Очевидно, что отмена тайны голосования привела бы к облегчению осуществления процесса наблюдения за достоверностью выборов, однако вместе с тем создала бы риски давления на избирателя, поэтому не является оптимальным решением.

При сохранении голосов избирателей в машиночитаемом виде в постоянном запоминающем устройстве технически возможна на том или ином этапе избирательного процесса скрытая установка вредоносных компьютерных программ, представляющих собой модифицированные алгоритмы сохранения и подсчёта голосов, приводящие к неправомерной модификации, уничтожению или блокированию достоверных сведений о волеизъявлении избирателей.

Возможность вмешательства в программные коды и/или обрабатываемую информацию систем обработки голосов была доказана на практике. Так, в статье Седы Давтян с соавторами была доказана возможность модификации содержимого ПЗУ устройств оптического сканирования бюллетеней компании Diebold, использующих в качестве рабочей операционной среды программный продукт
AV
-
OS
(
AccuVote
Operating
System
). После установки модифицированной версии
AV
-
OS
результаты голосования, передаваемые на принтер и в центральную систему управления базой данных (СУБД), перестали быть достоверными
[5].

Безусловно, подобная «модернизация» программного обеспечения электронных систем является уголовно-наказуемым деянием. Неправомерный доступ к ПЗУ устройства обработки голосов с целью внесения изменений в программные алгоритмы функционирования образует состав ст. 272 УК РФ [2]. Применение вредоносных программ, служащих для осуществления подобных действий (таких как модифицированные образы машинного кода прошивок устройств и прикладные программы, предназначенные исключительно для установки данных модифицированных образов), образует состав ст. 273 УК РФ
[2]. Более того, в случае отнесения объекта воздействия к КИИ (критической информационной инфраструктуре) – данные действия попадают под ст. 274.1 УК РФ
[2]. Также осуществление фальсификации избирательного процесса попадает под ст. 142.1 УК РФ
[2].

Необходимый элемент контроля функционирования подобных информационных систем – проверка содержимого постоянного запоминающего устройства (ПЗУ), наличие изученного представителями общественности эталонного образа содержимого ПЗУ. Такие требования предъявляются к информационным системам азартных игр, выполненным в виде игровых автоматов (ИА) и эксплуатируемым сегодня законно исключительно в границах игорных зон [1]. Безусловно, подобный, а то и больший, уровень проверки достоверности работы информационных систем следует применять и к выборам. Так как при использовании ИА возможны потери только в пределах вложенной суммы и только лишь игроком. Несанкционированные вмешательства в информационные системы избирательной отра сли несут куда более широкие и серьёзные последствия. Искажение содержащейся информации о голосах избирателей приводит к формированию недостоверного результата избирательной процедуры и, таким образом, недемократичности всех дальнейших политических решений. Реализация достоверного контроля содержимого всех машинных носителей на всех этапах избирательной процедуры представляется затруднительной и практически невозможной.

И если в случае с проведением выборов с использованием устройств типа «терминал оптического сканирования» для распознавания содержимого бюллетеней существует возможность верификации путём непосредственной перепроверки заполненных бюллетеней, то в случае с электронным голосованием без применения бумажных носителей голос после изъявления избирателем фактически существует исключительно в формате машинной записи в постоянном запоминающем устройстве (ПЗУ). При изменении данного голоса, вследствие применения вредоносных компьютерных программ или иных причин (например, потеря данных вследствие технического сбоя работы ПЗУ), не представляется возможным восстановить или обнаружить информацию об истинном содержании голоса.

Более того, при наблюдении за поступающими в агрегированное хранилище информационной системы голосами, например, от избирателей, находящихся у себя

дома, субъект наблюдения не может установить от кого конкретно поступают данные голоса, т.к. раскрытие данной информации было бы не совместимо с принципом тайны голосования. Проведение же традиционного голосования на участке позволяет наблюдателям лицезреть приходящих избирателей и контролировать работу со списком избирателей, не предоставляя при этом наблюдателям возможность установить содержание волеизъявления конкретного голоса, т.к. голос обозначается избирателем тайно и анонимизируется после помещения бюллетеня в урну, смешиваясь с другими находящимися в ней. Подобное сочетание максимальной проверяемости достоверности голосования в процессе наблюдения и полного соблюдения тайны волеизъявления – не представляется возможным, на наш взгляд, реализовать в рамках концепции дистанционного электронного голосования.

Известны сложные случаи при проведении электронного голосования и в других областях, не связанных непосредственно с политической избирательной процедурой. Например, при проведении зрительского голосования в рамках проекта «Голос.Дети» было осуществлено завышение числа зрительских голосов, отданных за одного из участников. Проведённая проверка систем силами экспертов по информационной безопасности подтвердила осуществление вмешательства в работу системы голосования путём применения программного продукта для ЭВМ, предназначенного для автоматизированной массовой подачи нелегитимных голосов. По мнению экспертов, не менее 8 тысяч голосов в виде сообщений и не менее 30 тысяч голосов в виде звонков было осуществлено с использованием программного обеспечения, имитирующего действия реальных голосующих [4].

Таким образом, можно сделать вывод о том, что применение электронно-вычислительных машин, их сетей и аппаратно-программных комплексов вместо традиционной концепции голосования с использованием простых подсчитываемых вручную избирательных урн и бумажных бюллетеней, не позволяет обеспечить должную проверяемость достоверности осуществления избирательных процессов.

Литература

1. МИ 2662-2005 Государственная система обеспечения единства измерений. Игровые автоматы с денежным выигрышем. Типовая методика контроля за соответствием утвержденному типу.

2. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 09.11.2024) (с изм. и доп., вступ. в силу с 20.11.2024).

3. Федеральный закон от 12.06.2002 N 67-ФЗ (ред. от 08.08.2024) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации».

4. Эксперт Group-IB про результаты «Голос.Дети»: «Мы точно установили факт того, что накрутка была»// BFM.RU. URL: https://www.bfm.ru/news/414369

5. Davtyan, Seda & Kentros, Sotirios & Kiayias, Aggelos & Michel, Laurent & Nicolaou, Nicolas & Russell, Alexander & See, Andrew & Shashidhar, Narasimha & Shvartsman, Alexander. (2009). Taking total control of voting systems: firmware manipulations on an optical scan voting terminal. 2049-2053. 10.1145/1529282.1529736.