Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.53

Малачевский
Артур Сергеевич

Защищенная система электронного голосования

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии
по специальности 1-45 81 01 "Инфокоммуникационные системы и сети"

_____

Научный руководитель

Борискевич Анатолий Антонович
профессор, доктор технических наук
доцент кафедры СиУТ

_____

Минск 2017

ВВЕДЕНИЕ

В развитых странах стали осуществляться целевые программы по автоматизации работы государственных служб. Одной из наиболее актуальных проблем является организация выборов и процессов голосования через глобальную сеть Интернет. В США, Великобритании, Ирландии, Швейцарии и других для избрания членов центральных и местных органов власти используются системы электронного голосования (СЭГ), позволяющие избирателям дистанционно сделать свой выбор.

Преимуществами проведения выборов через сеть общего пользования являются: отсутствие необходимости появления на избирательном участке; осуществление подсчета голосов в более короткие сроки; увеличение явки на выборы «молодого» электората, пользующегося мобильными устройствами. Наряду с достоинствами СЭГ возникают трудности ее внедрения, так как необходимо: внедрение электронных удостоверений личности и соответствующей инфраструктуры открытых ключей; разработка надежного протокола голосования на основе криптографических алгоритмов; разработка ПО и аппаратуры; тестирование СЭГ на различном уровне.

Основная цель при организации избирательного процесса – гарантия получения достоверного результата. Поэтому на всех этапах проведения выборов необходимо обеспечить защиту сведений от модификации и уничтожения. Отличием СЭГ от системы бумажно-электронного голосования является наличие канала передачи данных (КПД) между избирателем и счетной комиссией. При бумажном голосовании нарушению целостности информации

препятствуют наблюдатели и система видеоконтроля на избирательном участке. Проведение дистанционного голосования должно сопровождаться мерами безопасности, направленными на защиту КПД. Одним из эффективных методов защиты информации при передаче по каналу связи является шифрование. Целью создания СЭГ является повышение уровня защищенности информации, циркулирующей при организации и проведении дистанционных выборов.

Целью работы является исследование и проектирование эффективного комплекса мер безопасности, разработка алгоритма работы и взаимодействия процессов современной системы электронного голосования. Для достижения поставленной цели в ходе работы решены следующие задачи: определение общих требований к СЭГ; определение этапов избирательного процесса и разработка алгоритма работы СЭГ; проектирование алгоритмов взаимодействия процессов СЭГ; проведение анализа безопасности модели; анализ полученных данных о безопасности системы; Областью применения данных алгоритмов является: мультимедийные, инфокоммуникационные системы.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью работы является исследование и проектирование эффективного комплекса мер безопасности, разработка алгоритма работы и взаимодействия процессов современной системы электронного голосования.

Для достижения поставленной цели в ходе работы решены следующие задачи:

1) определение общих требований к СЭГ;

2) определение этапов избирательного процесса и разработка алгоритма работы

СЭГ;

3) проектирование алгоритмов взаимодействия процессов СЭГ;

4) проведение анализа безопасности модели;

5) анализ полученных данных о безопасности системы.

Областью применения данных алгоритмов является: мультимедийные, инфокоммуникационные системы.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, формулируются цель и основные задачи исследуемой работы.

В первой главе проводится анализ существующих систем электронного голосования.

В п.1.1 рассматриваются особенности внедрения СЭГ.

В п.1.2 представлены риски электронного голосования.

Во второй главе представлены алгоритмы взаимодействия СЭГ.

В п.2.1 приведено общее описание алгоритма электронного голосования. Рассмотрены требования к системе, представлены основные фазы процессов системы. Представлены компоненты системы и их базовые функции.

В п.2.2 представлен модифицированный, путем внедрения дополнительной защиты целостности информации, алгоритм работы СЭГ.

В п.2.3 приведены методы анализа безопасности работы алгоритма системы электронного голосования. Рассмотрен метод анализа системы путем создания дерева атак. Методом анализа рисков выявлены параметры для мультипараметрической системы.

В п.2.4 приведен подробный алгоритм работы СЭГ, а также подробный алгоритм взаимодействия процессов системы.

В третьей главе представлены результаты анализа безопасности алгоритмов системы электронного голосования.

В п.3.1 определены характеристики окружающей среды для проведения анализа безопасности системы.

В п.3.2 представлен анализ безопасности смоделированного окружения. Установлено обоснование свойств безопасности СЭГ.

В п.3.3 представлен анализ безопасности системы против специфических атак направленных на голоса избирателей. Рассмотрены крупномасштабные атаки, представлены расчеты вероятностей подобных атак.

В п.3.4 представлен анализ безопасности системы против специфических атак направленных на лишение прав избирателей. Выявлено, что проверка целостности системных журналов, лог файлов, крайне важна для достижения завершенности безопасных свойств, при которых избиратели с правом голоса могут голосовать и участвовать в подсчете финального результата выборов

В п.3.5 представлен анализ безопасности системы против специфических атак направленных на нарушение конфиденциальности. Определено, что покупка и продажа голосов, а также нарушение конфиденциальности маловероятна, что дает основание считать процесс голосования тайным.

В п.3.6 представлено обоснование безопасности других требований системы.

В заключении сформулированы основные результаты, полученные в диссертационной работе.

В приложении предоставлен графический материал.

ЗАКЛЮЧЕНИЕ

Рассмотрены преимущества систем электронного голосования, а также риски и недостатки. Определены общие требования и свойства системы, этапы избирательного процесса в системе электронного голосования. Представлены алгоритмы работы системы электронного голосования, а также алгоритмы работы и взаимодействия внутренних процессов системы. Сформированы характеристики окружающей среды для дальнейшего проведения анализа безопасности представленной системы. Выявлены требования к безопасности системы и ее характеристики в смоделированной окружающей среде. Проведен анализ безопасности представленной системы электронного голосования, а также анализ полученных данных о безопасности системы. Все определенные

свойства системы были оправданы для представленного алгоритма системы электронного голосования. Данный алгоритм системы электронного голосования является безопасным в определенной модели среды. Областью применения данного алгоритма является: мультимедийные, инфокоммуникационные системы.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1. Малачевский А.С., Лапко С.А. Модификация защищенной системы электронного голосования / В печати