УДК 004.056

**В.К. Губаев**
Студент 2 курса
ГАПОУ КО «Калужский технический колледж»

**Д.К. Никифоров**
заведующий информационно-аналитической службой
ГАПОУ КО «Калужский технический колледж»
кандидат физико-математических наук, доцент

# РАЗРАБОТКА КОМПЛЕКСА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМЫ ГОСУСЛУГ

**Аннотация.** Рассмотрены способы и методы защиты информации. В программе BPwin разработаны диаграммы обеспечения защиты информации и организации процесса дистанционного электронного голосования, описан каждый этап схемы процессов всего комплекса. Рассмотрена технология блокчейн и ее применение в онлайн-голосовании. Описан неразрывный процесс взаимодействия программных средств для обеспечения надежности, безопасности и конфиденциальности информации и принцип работы открытого и закрытого ключа шифрования. Сделаны выводы о преимуществах внедрения современных технологий для обеспечения надежной защиты информационных данных.

**Ключевые слова:** защита информации, BPwin, информационные технологии, методы защиты, дистанционное электронное голосование, блокчейн технологии.

**V.K. Gubaev, D.K. Nikiforov**

# DEVELOPMENT OF PROTECTION OF THE INFORMATION SYSTEM OF PUBLIC SERVICES

**Abstract.** Ways and methods of information protection are considered. In the BPwin program, diagrams have been developed for ensuring information security and organizing the process of remote electronic voting, each stage of the process diagram of the entire complex is described. Blockchain technology and its application in online voting are considered. An inextricable process of interaction between software tools to ensure the reliability, security and confidentiality of information and the principle of operation of a public and private encryption key are described. Conclusions are drawn about the advantages of introducing modern technologies to ensure reliable protection of information data.

**Keywords:** information security, BPwin, information technologies, security methods, remote electronic voting, blockchain technologies.

## Введение

В современном мире многое напрямую связано с хранением и обменом информации, которая обычно нуждается в сохранении конфиденциальности и тщательной защите. Порой собственных ресурсов организации бывает недостаточно для обеспечения надежной защиты и сохранности данных. Благодаря профессиональной разработке и установке систем, контролю и предотвращению утечки информации можно обеспечить стабильную работу организации.

Сегодня системы защиты информации имеют одну из самых важных ролей в деятельности любой организации. Грамотная и своевременная защита информации совместно с разработкой улучшенных систем безопасности предупредит любые потери, искажения и нарушения достоверности информации, а также сохранит ее полную конфиденциальность. Такой правильный и высококвалифицированный подход обеспечит пользователям безопасность и уверенность при использовании своих личных данных.

Технологии с каждым днем развиваются все больше, и мы обретаем все более объемные и разносторонние знания о средствах защиты информации, которых тоже становится все больше. Появление новых вирусов и новых систем взлома заставляет непрерывно работать над повышением эффективности защиты, а также разработкой более совершенных программ шифрования и блокировки утечки.

**Гипотеза**

Предполагаем, что наличие необходимых знаний в области информационной безопасности поможет предотвратить несанкционированный доступ, обеспечить эффективное применение мер по защите информации и предотвратить киберпреступления.

Для обоснования данной гипотезы были определены следующие задачи:

- Обобщить понятия применения современных дистанционных способов коммуникации.
- Изучить способы и методы защиты информации.
- В программе BPwin разработать диаграммы обеспечения защиты информации и организации процесса дистанционного электронного голосования, а также подробно рассмотреть каждый этап схемы процессов всего комплекса.
- Проанализировать работу технологии блокчейна на примере онлайн-голосования.
- Описать неразрывный процесс взаимодействия программных средств для обеспечения надежности, безопасности и конфиденциальности информации.
- Изучить принцип работы открытого и закрытого ключа шифрования голосов на дистанционном электронном голосовании.
- Сделать выводы о преимуществах внедрения современных технологий для упрощения технических процессов, связанных с хранением и обеспечением надежной защиты информационных данных.

**Методы**

При написании данной статьи использовались: метод наблюдения, методы анализа и синтеза, метод гипотетико-дедуктивный, метод моделирования, а также метод обобщения.

В качестве основного метода исследования в работе было выбрано изучение способов обеспечения информационной безопасности и анализ информационных рисков предоставления государственных услуг в электронном виде. С целью подробного изучения была смоделирована схема процессов обеспечения защиты информации и разработан комплекс организации процесса электронного голосования, наглядно показывающий работу данной системы.

**Результаты и обсуждение**

Существует несколько способов и видов защиты информации, которые осуществляются по Федеральному закону "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [6]: правовой, физический, криптографический и технический.

Путём правового метода информация защищается благодаря разработке правовых норм и документов, реализуемых государством, а также через четкий контроль над их исполнением. Эти меры остановят тех, кто не готов ради информации игнорировать правила, нарушать законы и нести последующее наказание [4].

Далее идет физический метод защиты информации. Создание антивирусов и шифрования не помогут, если злоумышленник может просто пробраться в серверную и похитить жесткие диски с информацией. Поэтому серверные и информационные системы нужно в первую очередь защищать снаружи, с помощью физических средств защиты, таких как: решетки, двери, сигнализации, камеры наблюдения и сложные замки. Также

информацию из вне можно защитить посредством подбора надежных и ответственных сотрудников, через подписание договора с ними о неразглашении информации и системой уровней доступа для сотрудников.

Криптографическая защита выполняет две основные функции, во-первых шифрует данные. Даже если злоумышленник сможет получить доступ к данным, он увидит только зашифрованную информацию, для расшифровки которой требуется особый ключ. Во-вторых, она не только подтверждает подлинность информации, но и определяет личность отправителя, если файл попытаться изменить или подделать, это сразу будет видно.

Последний способ защиты информации - технический, путем использования программного обеспечения. Когда мы говорим о защите информации, то сразу вспоминаем антивирусы и пароли. Это как раз и является техническим методом защиты информации. К нему относятся: антивирусы, системы аккаунтов и паролей, программные межсетевые экраны (файерволы), инструменты виртуализации, DLP (предотвращают утечку информации) и SIEM (фиксируют подозрительную активность) системы [3].

В данной работе с помощью программы BPwin были разработаны и представленны схемы процессов защиты информации.

BPwin это приложение, предназначенное для поддержки процесса создания информационных систем. Оно является вполне развитым средством моделирования, позволяющим проводить документирование, анализ и улучшение процессов. С помощью этого приложения можно моделировать действия в процессах, определять порядок этих процессов и необходимые для них ресурсы. Модели BPwin создают структуру, благодаря которой становится понятен порядок взаимодействия элементов процесса между собой, нужный для понимания процессов и выявления управляющих событий [5]. Для построения больших моделей и анализа работы в организации в программе предусмотрена детализация, благодаря этому модели могут быть разбиты на группы. Каждая модель разбивается на более низкие уровни детализации, при этом их взаимосвязь между моделями и элементами сохраняется. При помощи BPwin любые модели можно разделить на составляющие части, провести работу с каждой из них, а затем интегрировать обратно в единую модель. На приведенных ниже схемах можно легко понять как происходит процесс защиты информации, а также как правильно и надежно обеспечить эту защиту.

«Еще ни одно программное решение не защищает информацию полностью, оно лишь блокирует одни возможности атаки, но оставляет пространство для других» - Федор Музалевский, RTM Group. Для построения надежной системы защиты информации нужно подобрать несколько программных средств и выстроить комплекс, где каждое средство взаимодействует с другими, именно поэтому на схеме каждый процесс неразрывно связан цепочкой с другим процессом и только при четком соблюдении всех процессов между собой можно достигнуть полного обеспечения защиты информации (ЗИ).

Для простоты понимания все этапы обеспечения защиты информации были разделены на отдельные процессы. Обеспечение защиты можно разделить на «Обеспечение защиты информации при управлении доступом» и «Обеспечение защиты вычислительных систем» (рис.1). К первой относится: защита физического доступа (путем организационных мер и создания припятствий от несанкционированного доступа, управление учетными записями (например, контроль учетных записей уволенных и не активных сотрудников), идентификация, аутентификация и авторизация (однофакторная аутентификация пользователей, многофакторная аутентификация администраторов, пароли на BIOS, установка сложных паролей, а также разграничение доступа), идентификация, классификация, учет ресурсов и объектов доступа (контроль и учет состава ресурсов, операция по изменению, а также состав объектов доступа).

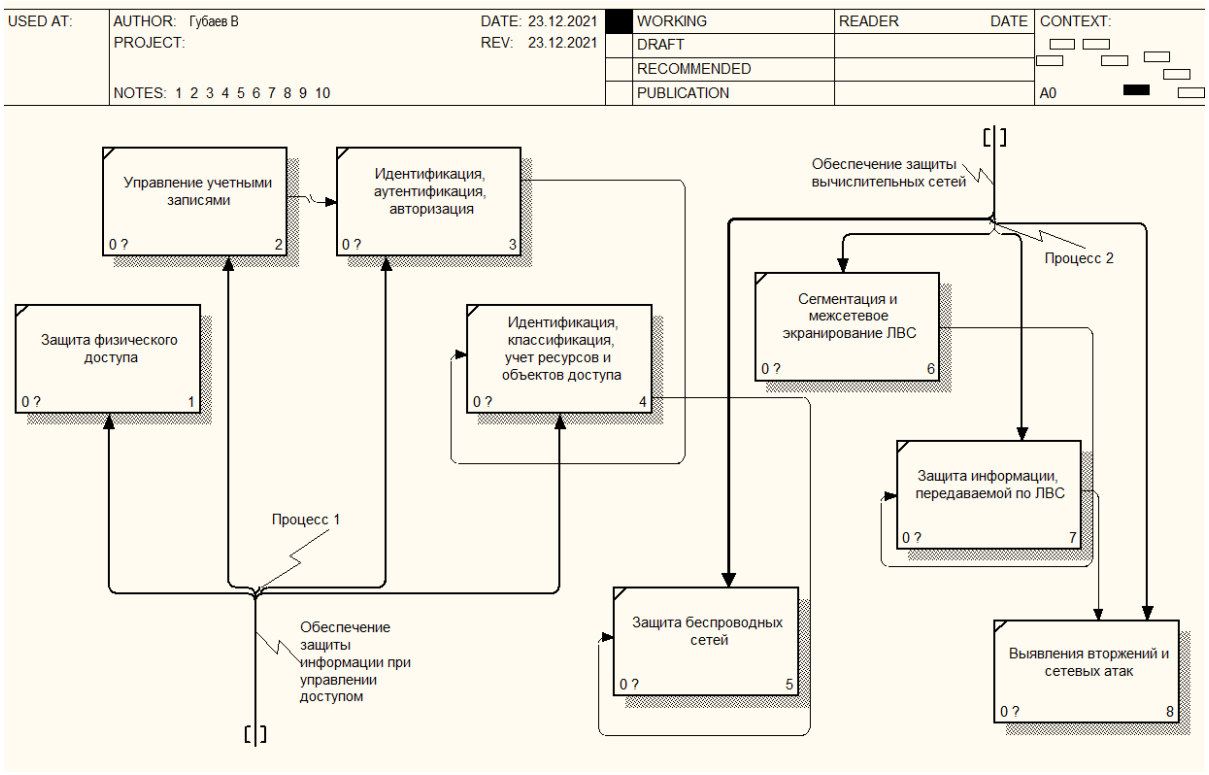


Рисунок 1. Схема процессов обеспечения ЗИ при управлении доступом и обеспечения защиты вычислительных сетей

Во второй процесс входит: защита беспроводных сетей (описать в ОРД правила взаимодействия, использовать WIPS, сохранять в логах сетевого оборудования информацию об изменении конфигурации), сегментация и межсетевое экранирование внутренних вычислительных сетей (далее ЛВС) (описание контуров безопасности, установление правил фильтрации, использование внешнего и внутреннего почтовых серверов), защита информации, передоваемой по ЛВС (использование двухстороннего TLS и VPN между подразделениями), выявление вторжений и сетевых атак (использование средств обнаружения вторжений, средств защиты от DDoS-атак, антиспама).

Далее представлены одиночные процессы, в результате которых получено обеспечение защиты информации на этапах жизненного цикла АС и приложений (рис.2).

К контролю целостности и защищенности можно отнести: использование сканеров уязвимостей, тестирование на проникновение и устранение выявленных по результатам сканирования уязвимостей, хранение копий ОС, прикладного ПО, СЗИ, запрет установки или запуска неразрешенного ПО и т.д.

Защита от вредоностного кода включает в себя: различные антивирусы, тестирования на проникновение, решения по защите электронной почты с антивирусной проверкой почтовых сообщений, самостоятельный контроль.

Меры по предотвращению утечек информации: DLP-система с контентным анализом информации, контроль за внешними носителями, принтеры с авторизацией печати по карточке или логину-паролю, различные запреты и ограничения.

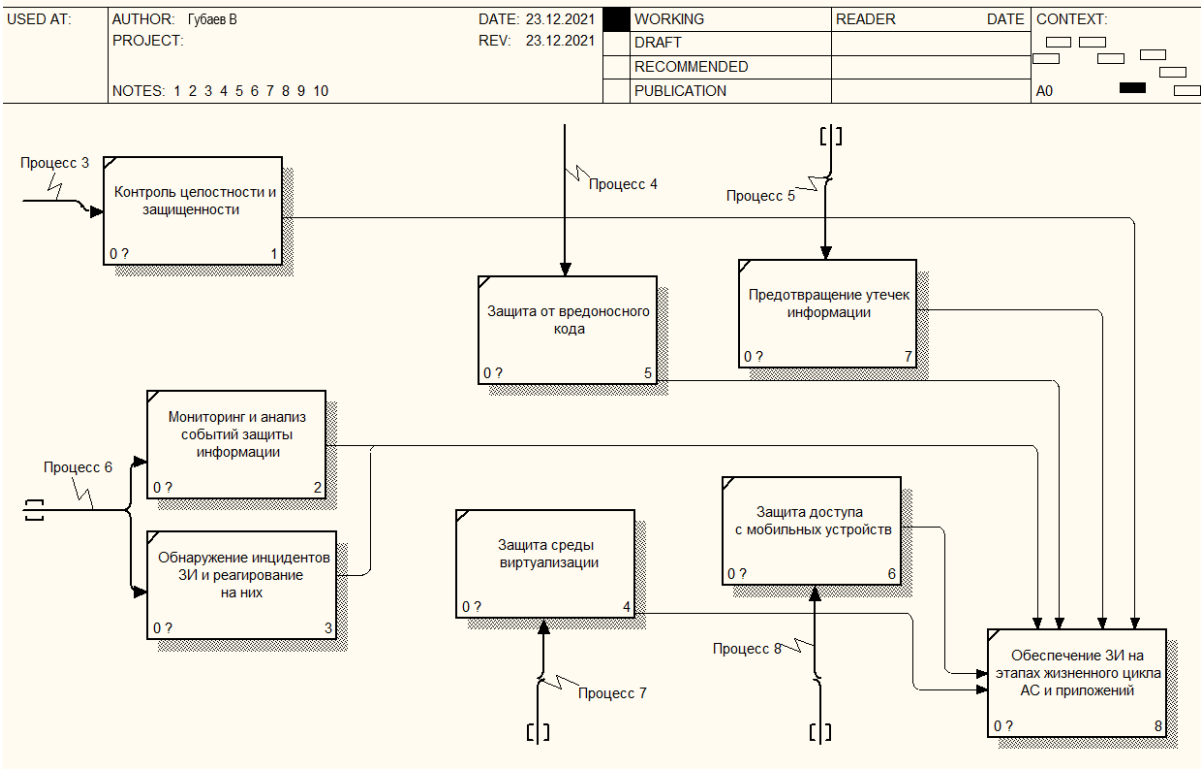


Рисунок 2. Схема процессов обеспечения ЗИ на этапах жизненного цикла АС и приложений

В процесс 6 входит: централизованный сбор событий, использование службы синхронизации времени, передача данных по защищенным протоколам, выделение массива для хранения данных, автоматическое уведомление администраторов об исчерпании дискового пространства, защита доступа к хранилищу данных, обеспечение целостности данных средствами СУБД, резервирование базы данных, создание и хранение базы данных об инцидентах. Такие решения как: запреты одновременного выполнения ролей и размещения серверных и пользовательских компонентов АС на одной ВМ, а также на параллельные сеансы RDP могут обеспечить защиту среды виртуализации. Для осуществления защиты доступа с мобильных устройств следует использовать: для аутентификации VPN или двухсторонней TLS, NAC, или клиент MDM.

Современные технологии позволяют облегчить жизнь человеку. Дистанционные способы коммуникации, такие как обучение и голосование, прочно входят в повседневную жизнь современного человека. Дистанционное электронное голосование (ДЭГ) - это голосование с помощью специального программного обеспечения без использования бумажного бюллетеня [2]. На Рисунке 3 разработана и представлена схема организации процесса электронного голосования, наглядно показывающая работу данной системы. Внедрение таких технологий предусматривает упрощение процедуры голосования как для избирателей, так и для избирательных комиссий.

Одним из способов защиты на ДЭГ является блокчейн. Если рассматривать децентрализованный блокчейн как непрерывную цепочку блоков, то в отличие от обычных централизованных баз данных изменять или удалять данные можно, но это трудоемко и дорого, поэтому является нецелесообразным на текущем этапе развития технологий. После голосования бюллетень, не содержащий каких-либо данных об избирателе, шифруется и добавляется в распределенную сеть, построенную на основе технологии блокчейна, для хранения и подсчета голосов. При этом специальные алгоритмы отвечают за то, чтобы данные не были расшифрованы до окончания голосования.

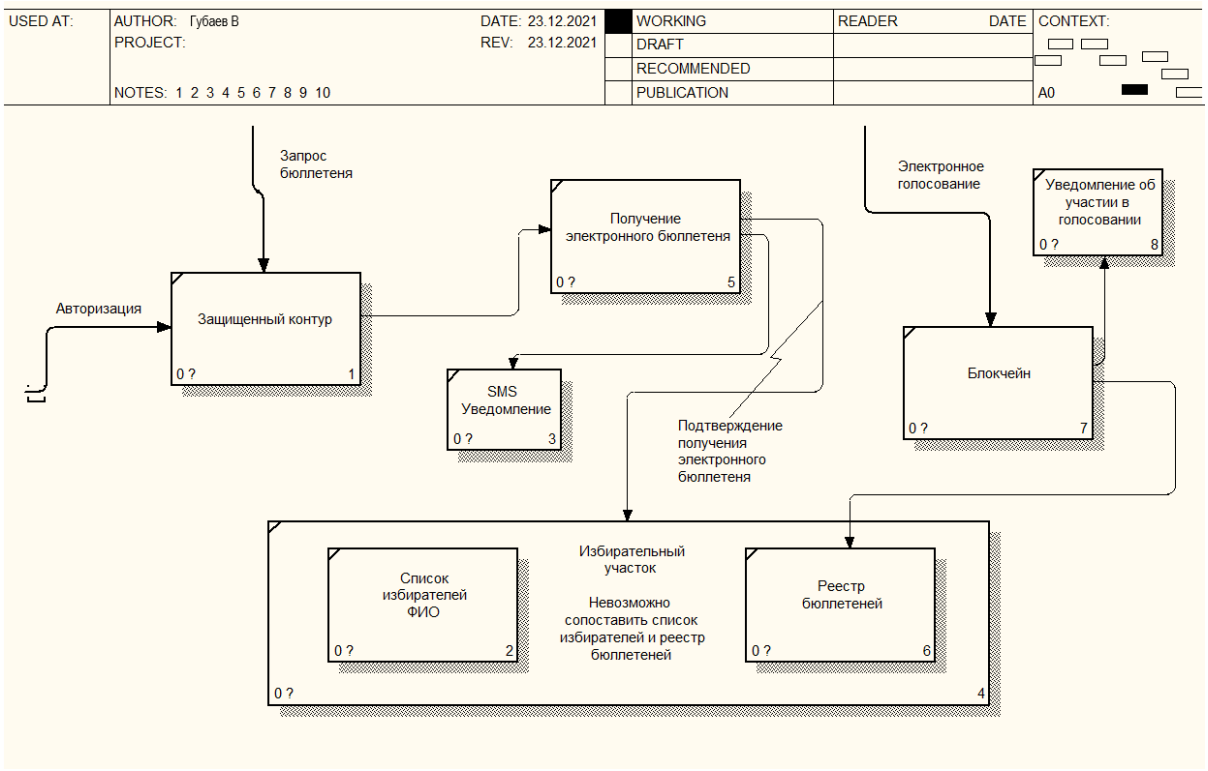


Рисунок 3. Организация процесса дистанционного электронного голосования

Если попытаться повлиять на данные одного из узлов, система IT изменения его просто не учтет, а взломанный узел будет исключен из сети блокчейн. Данные при этом не будут утеряны, так как они сохранены в других узлах сети.

Узнать результат голосования заранее невозможно. Он зашифрован двумя защищенными ключами (открытым и закрытым). На специальном компьютере, который не имеет подключения к сетям связи, происходит процедура генерации ключевой пары. Закрытый ключ разделяется на пять частей, которые записываются на защищенные носители и раздаются членам комиссии, независимым наблюдателям, представителям кандидатов или иным лицам по решению комиссии. Они обязаны носить свои носители и обеспечивать их конфиденциальность до окончания голосования. Сам компьютер при этом опечатывается. Открытый ключ шифрует все голоса, но расшифровать их можно только закрытым ключом, который разделен между несколькими участниками избирательного процесса (членами избирательной комиссии, наблюдателями, представителями кандидатов или партий). Каждая часть ключа отдельно бесполезна, система покажет итоги голосования только тогда, когда закрытый ключ будет соединен вновь [1].

В работе реализованы схемы процессов обеспечения защиты информации при управлении доступом и обеспечения защиты вычислительных сетей на этапах жизненного цикла автоматизированных систем и приложений с целью визуализации процесса правильного и надежного обеспечения защиты информации.

Рассмотрен процесс онлайн голосования и подробно изучена схема организации процесса электронного голосования с применением блокчейн технологии, наглядно показывающий работу данной системы.

Проведен анализ работы системы блокчейн, изучен открытый и закрытый ключ и выявлена необходимость развивать информационные технологии как принцип обеспечения эффективного управления государством и предоставления населению качественных услуг.

**Список литературы**


1. Губаев В.К., Никифоров Д.К. Блокчейн технологии в обеспечении защиты голосования на выборах. Сборник материалов II Всероссийской молодежной научно-практической конференции студентов, аспирантов и молодых ученых «Наука и творчество: вклад молодежи», Махачкала: Формат, 2021, – с. 34-36.
2. Губаев В.К., Никифоров Д.К. Дистанционное электронное голосование. Сборник трудов межрегиональной научно-практической конференции «Финансовая грамотность населения: проблемы, региональные практики и перспективы развития», Москва: ИП Карпов А.Н., 2021 – с. 225-230.
3. Официальный сайт ФСТЭК России [Электронный ресурс] - Режим доступа: https://fstec.ru/
4. Официальный сайт Центр Защиты Информации [Электронный ресурс] - Режим доступа: https://baltzi.ru/.
5. Сайт BPWIN - ITteach [Электронный ресурс] - Режим доступа: https://itteach.ru/bpwin/.
6. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.