АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Макаренко Максим Сергеевич

студент института магистерской подготовки Белорусского государственного экономического университета, Республика Беларусь, г. Минск

Миронова Валерия Александровна

студент института магистерской подготовки Белорусского государственного экономического университета, Республика Беларусь, г. Минск

Шафалович Анна Анатольевна

научный руководитель, канд. юрид. наук, доцент кафедры теории и истории права Белорусского государственного экономического университета, Республика Беларусь, г. Минск

В современном мире информационная безопасность становится все более актуальной проблемой. В условиях развития электронного правительства, где большинство процессов осуществляется через сеть Интернет, защита персональных данных и иной конфиденциальной информации становится особенно важной.

Статьей 28 Конституции Республики Беларусь определено, что каждый имеет право на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство. Государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании [1].

Использование информационных систем, в свою очередь, порождает определенные риски. В Беларуси определен ряд государственных информационных систем и инфраструктурных решений, обеспечивающих возможность автоматизированного электронного взаимодействия всех участников информационного обмена, ключевыми из которых являются:

- общегосударственная автоматизированная информационная система (ОАИС);

- система межведомственного электронного документооборота государственных органов Республики Беларусь (СМДО);

- государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (ГосСУОК) [2].

Вместе с тем, информационные системы подвержены как внешним, так и внутренним угрозам со стороны нарушителей. Одной из основных угроз информационной безопасности является киберпреступность. Для борьбы с ней необходимо использовать современные технологии защиты информации. Защищенность автоматизированных систем непосредственно зависит от их архитектуры и встроенных программных средств по защите информации, что позволит гарантировать достоверность документов и исключить вероятность их фальсификации. Защита информации в рамках информационных систем должна включать в себя меры по их особому хранению, передаче и использованию. Это может быть достигнуто путем установления строгих правил доступа к персональным данным и конфиденциальной

информации, регулярной проверки систем на наличие уязвимостей и использования современных методов шифрования в рамках государственного управления.

Так, например, обеспечение безопасного доступа к информационным ресурсам внутри системы документооборота достигается применением одно- и многофакторной аутентификации субъекта при входе в систему и разграничением прав пользователей, осуществляемой за счет присвоения каждому участнику персонального идентификатора.

Меры, направленные на противодействие несанкционированному доступу к конфиденциальным данным, также обеспечиваются посредством централизованного управления процессом обработки охраняемой информации. Формирование защищенного электронного документооборота подразумевает контролируемое движение конфиденциальных документов по строго регламентированным пунктам приема, обработки, согласования, исполнения и хранения в условиях организационного и технологического обеспечения безопасности носителя информации и зафиксированных на нем данных [3].

Кроме того, защита информационных ресурсов требует проведения на постоянной основе аудита информационной безопасности. Результаты проведенного аудита составляют основу для формирования стратегии развития системы обеспечения информационной безопасности в автоматизированных информационных системах.

Для решения проблемы информационной защиты систем электронного документооборота целесообразно применение комплексного подхода, подразумевающего также использование совокупности программно-аппаратных средств и мер реагирования. Сопровождение такой системы включает в себя регулярное обновление антивирусного программного обеспечения, актуализацию средств защиты информации, круглосуточный мониторинг для прогнозирования моделей нарушителя и оперативной нейтрализации идентифицированных угроз, поддержание в актуальном состоянии и разработку новых нормативных документов в сфере защиты информации.

Таким образом, информационная система подвержена различным угрозам со стороны нарушителей. Для борьбы с ними необходимо использовать современные технологии защиты информации, в том числе меры по их особому хранению, передаче и использованию. Это может быть достигнуто путем:

- установления строгих правил доступа к конфиденциальной информации, пределов ее использования, а также четкого разграничения полномочий участников системы;

- совершенствования нормативной правовой базы в соответствующей сфере, в том числе установления четкого разграничения полномочий государственных органов и их работников в рамках функционирования системы электронного правительства;

- регулярной проверки систем на наличие уязвимостей и использования современных методов шифрования в рамках государственного управления;

- наличия возможности точной аутентификации пользователей системы, а также установления наличия прав доступа к той информации, которая им необходима;

- регулярного проведения внутреннего аудита безопасности компьютерных систем с целью выявления их исправности и уязвимости;

- передачи электронных версий документов по защищенным телекоммуникационным каналам связи;

- внутреннего мониторинга действий пользователей системы;

- обеспечения резервного копирования важных данных, позволяющего избежать потери информации в случае сбоев или аварийных ситуаций.

- обучения персонала, работающего с конфиденциальными данными, по вопросам

информационной безопасности;

- использования антивирусного программного обеспечения;

- возможного создания специального государственного органа, обеспечивающего контроль действий пользователей системы и движения документов в рамках взаимодействия государственных структур.

Таким образом, обеспечение информационной безопасности в условиях электронного правительства требует комплексного подхода, интегрирующего различные средства защиты информации в единую взаимосвязанную среду, обеспечивающую выполнение задач по информационной безопасности.

Список литературы:

1. Конституция Республики Беларусь.: с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г. и 27 февр. 2022 г. [Электронный ресурс]. – Режим доступа: https://president.gov.by/ru/gosudarstvo/constitution. – Дата доступа: 17.11.2023.

2. Электронное правительство [Электронный ресурс]. – Режим доступа: https://nces.by/e-government/. – Дата доступа: 17.11.2023.

3. Мирошниченко М.А., Бондаренко А.А., Пиналова Е.В., Актуальные проблемы обеспечения информационной безопасности систем электронного документооборота в рамках цифровой трансформации [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/zaschita-informatsii-v-usloviyah-primeneniya-dokumentoorientirovannyh-tehnologiy-na-primere-sistemy-elektronnoe-pravitelstvo-1/viewer. – Дата доступа: 17.11.2023.