МЕТОДЫ И СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ РЕСПУБЛИКИ БЕЛАРУСЬ

Картышева Д.А.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Информационная безопасность – защищённость информации от незаконного ознакомления, преобразования, уничтожения, а также защищённость информации от воздействий, направленных на нарушение их работоспособности.

Информационная безопасность таможенных органов – это состояние защищённости национальных интересов государства в информационной сфере деятельности таможенных органов.

При помощи определённых мер защиты поддерживается и обеспечивается защищённость национальных интересов, под которыми следует понимать управленческие меры, направленные на обеспечение информационной безопасности: административные руководящие документы (приказы, распоряжения и инструкции); аппаратные устройства или дополнительные программы, основной целью которых является предотвращение преступлений и злоупотреблений.

От эффективности деятельности таможенных органов в информационной сфере существенно зависит эффективность обеспечения экономической безопасности Республики Беларусь. [1]

На практике используют несколько групп методов защиты, в том числе:

– оказание воздействия на элементы защищаемой системы;

– преобразование данных, обычно – криптографическими способами;

– разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;

– создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;

– создание условий, которые мотивируют пользователей к должному поведению.

Каждый из приведённых методов защиты информации реализуется при помощи различных категорий средств. Основными средствами являются организационные и технические.

Разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности.

Чаще всего специалисты по безопасности:

– разрабатывают внутреннюю документацию, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;

– проводят инструктаж и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;

– разграничивают зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;

– внедряют программные продукты, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;

– составляют планы восстановления системы на случай выхода из строя по любым причинам. [2]

Для обеспечения информационной безопасности необходимо обеспечить:

– использование новых автоматизированных информационных технологий в таможенной деятельности и совершенствование действующих программных средств и подсистем, то есть повысить безопасность информационных систем таможенных органов;

– развитие системы управления рисками на основе осуществления таможенных процедур в соответствии с международными стандартами, основанными на последних достижениях в области информационных и управленческих технологий;

– укрепление взаимодействия с зарубежными и международными органами.

Таким образом, используя соответствующие методы и средства, таможенные органы обеспечивают информационную безопасность и, соответственно, обеспечивают защиту национальных интересов.

Литература

1. Информационная безопасность в таможенных органах: учебно-методическое пособие для студентов специальности 1-96 01 01 «Таможенное дело» / Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель. – Минск: БНТУ, 2019

2. О государственных секретах [Электронный ресурс]: Закон Респ. Беларусь, 19 июля 2010 г., № 170-З. // Режим доступа: https://kgb.by/ru/zakon170-3/. – Дата доступа: 23.03.2021

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ И ЕЁ ПРИМЕНЕНИЕ

Кирияк А.И., Стельмах Я.О.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Развитие Интернета принесло людям большое удобство и значительно облегчило их жизнь. Теперь с доставкой можно приобретать одежду и продукты, оплачивать коммунальные услуги или кредиты на сайтах, получить образование или освоить хобби в Интернете. Также стала доступна электронная цифровая подпись, которая даёт пользователю много преимуществ.

Уникальная последовательность символов, назначение которой заключается в подтверждении целостности, подлинности и неизменности документа, представленного в электронном виде, называется ***электронной цифровой подписью*** (сокращенно ***ЭЦП***). Этот реквизит является доказательством того, что документ подписан, и указывает, что он принадлежит владельцу действующего сертификата ключа ЭЦП.

В ситуациях, предусмотренных нормативно-правовыми актами страны, ЭЦП выступает аналогом личной подписи человека при совершении юридически значимых действий. Электронный документ (например, декларация о доходах индивидуального предпринимателя), подписанный ЭЦП, обретает ту же силу, что и бумажный вариант с личной подписью от руки. Естественно, что ЭЦП позволяет экономить время и силы для личного обращения. Любой пользователь может отправлять юридически ликвидные бумаги прямо из дома. [1]

Чтобы установить ЭЦП, надо иметь ключ (выглядит как обычная флешка, подсоединяется к компьютеру через USB-разъём). ЭЦП – это уникальный набор символов, который выдаётся в результате криптографического преобразования информации с применением ключа и с использованием специально созданного сложного алгоритма. Для создания ЭЦП чаще используется технология асимметричного шифрования – издаются закрытый ключ (Private key) и открытый ключ (Public key).

Закрытый ключ известен только владельцу сертификата и не может быть вычислен, даже если имеется вся информация, хранящаяся в открытом