Беларусь. / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2023.

2. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 янв. 2021 г., № 91-З : принят Палатой представителей 18 дек. 2020 г. : одобрен Советом Республики 18 дек. 2020 г. : в ред. Закона Респ. Беларусь от 04.01.2022 г №144-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

УДК 339.543

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ТАМОЖЕННЫХ ОРГАНАХ

Новикова В.В.
Руководитель: ст. преподаватель Галай Т.А.
Белорусский национальный технический университет

Сегодня организация эффективной системы обеспечения информационной безопасности, которая будет способна защитить конфиденциальность информации и минимизирует риск её незаконного присвоения посторонними лицами является одной из приоритетных задач для таможенных органов. Внешняя торговля – непрерывный процесс, поэтому безопасность обмена данными должна обеспечиваться на каждом его этапе, быть максимально автоматизированной и приспособленной к изменениям в киберпространстве.

Информационная безопасность должна строиться на комплексе из трёх составляющих: целостности, доступности и конфиденциальности информации. Осуществляется защита конфиденциальных данных для всех важнейших видов: государственной, служебной, коммерческой, банковской тайн, персональных данных и интеллектуальной собственности.

В доступе таможенных органов находится множество разнообразной нуждающейся в защите информации. Данная информация касается как участников ВЭД, так и непосредственно внутренних вопросов деятельности таможен. Для организации защиты такой информации существует комплексная процедура защиты конфиденциальных данных в информационных системах. Она включает в себя защиту информации, обрабатываемой в автоматизированных системах; защиту данных, передаваемых между таможенными органами; использование средств защиты от несанкционированного доступа; использование электронной цифровой подписи и систем электронного документооборота [1, с. 87-88].

Защита информации, обрабатываемой в автоматизированных системах, осуществляется, в первую очередь, путём установки антивирусных программ. Защита от вирусов представляет собой комплекс мер по распознаванию и борьбе с обнаруженными вирусами, а также осуществление профилактических действий (например, запрет доступа к потенциально заражённым Интернет-ресурсам).

Оптимальная антивирусная программа должна сочетать в себе сразу несколько критериев: стабильная качественная работа с сведённым к нулю количеством программных ошибок, ёмкость базы данных идентифицированных вирусов, высокая скорость обработки большого количества данных, возможность работы на базе различных операционных систем, детекция ранее неизвестных программе вирусов, совместимость с максимально возможным количеством типов файлов, безостановочная фоновая работа. На протяжении всего развития информационных систем разработчики разных стран работали над созданием наиболее эффективного антивирусного программного обеспечения. Так, наиболее популярным из ныне существующих антивирусных программных средств относятся: антивирус Касперского, Dr. Web, McAfee VirusScan, Avira, ESET NOD32, Avast!, AVG Anti-Virus.

Защита данных, передаваемых между таможенными органами, организуется, в первую очередь, для защиты информации под грифом «для служебного пользования». Такие технологии защиты, в свою очередь, также не находятся в свободном доступе. К общепризнанным стандартам защиты служебной информации относятся:

– обеспечение доступа к защищаемой информации только для конкретных лиц путём составления список таких лиц или выдачей им индивидуальных ключей доступа;

– запрет на использование мобильных телефонов, оснащенных камерой и выходом в Интернет, использование служебной системы мобильной связи;

– ограничение доступа к помещениям, в которых происходит работа с конфиденциальной информацией путём оснащения их пропускной системой различных типов. Двери и окна в таких помещениях должны быть закрыты, жалюзи на окнах опущены;

– запрет на просмотр и обработку защищаемой информации в присутствии лиц, не имеющих к ней доступа;

– запрет на несанкционированное копирование информации на съемные носители;

– обязательное использование при работе на персональных компьютерах антивирусной защиты;

– своевременное периодическое резервное копирование информации.

Ключевая деятельность по обеспечению защиты автоматизированных систем таможенных органов от несанкционированного доступа - создание систем разграничения доступа (далее - СРД) субъектов к объектам защиты.

СРД состоит из трёх компонентов: аутентификация; авторизация; шифрование информации.

Аутентификация — это процесс проверки пользователя на принадлежность ему сведений, о которых известно проводящей аутентификацию системе. Иными словами, достоверно устанавливается, что человек или устройство является именно тем, кем себя объявляет. Аутентификация является барьером перед доступом к защищенной информации, поэтому ее методики должны максимально точно описывать каждого конкретного пользования и тем самым давать возможность сравнить заявляемые данные с существующими в системе. Для этого могут применяться более примитивные методы в виде одноразовых и многоразовых паролей, PIN-кодов, сертификатов, так и более сложные к фальсификации: биометрические характеристики, подпись мышью. Для усиления защиты прибегают к двухэтапной аутентификации, которая, помимо пароля вышеуказанных методов, включает в себя еще один дополнительный этап, проведение которого требует наличия определённого аппаратного обеспечения. В этих целях применяются:

– магнитные диски;

– элементы Touch Memory, включающие в себя постоянное запоминающее устройство и оперативное запоминающее устройство;

– пластиковые карты с магнитной полосой;

– карты со штрих-кодом, покрытым непрозрачным составом, считывание информации с которых происходит в инфракрасных лучах;

– смарт-карты, носителем ключевой информации в которых является специальная микросхема;

– маркеры eToken, представляющие собой подключаемое к USB-порту компьютера устройство, которое включает в себя аналогичную смарт-карте микросхему с процессором и защищенной от несанкционированного доступа памятью.

Авторизация является продолжением этапа аутентификации и направлена на предоставление ранее идентифицированному лицу возможности осуществления определённых действий. Из этого вытекает разница между ними - аутентификация проверяет то, что пользователь является тем, кем себя выдаёт. Авторизация же определяет круг доступных пользователю действий, т.е. круг его прав в данной информационной системе.

Шифрование — это процесс кодирования сообщения или информации таким образом, что только авторизованные стороны могут получить к нему доступ. Кодирование осуществляется с помощью криптографического

алгоритма [2, с. 111]. Расшифровка использует то же искусство криптографии, чтобы изменить зашифрованный текст обратно в открытый текст.

Немаловажной мерой по защите информации является использование электронной цифровой подписи и систем электронного документооборота. Электронная цифровая подпись (далее - ЭЦП) — реквизит электронного документа, получаемый в результате преобразования информации с использованием криптографических методов и особого ключа. ЭЦП доказывает факт подписания документа и позволяется идентифицировать подписанта как владельца сертификата ключа подписи. Для функционирования ЭЦП используются два ключа защиты: личный ключ, который доступен только непосредственно подписанту, и открытый ключ, который находится в открытом доступе и необходим для проверки подлинности ЭЦП.

Электронный документооборот, в свою очередь, позволяет создавать, обрабатывать, пересылать и хранить документы без применения бумажных носителей, то есть исключительно в цифровой форме. Отправитель создает документ, после чего подписывает его электронной цифровой подписью. Затем созданный документ отправляется по защищенным каналам связи. Получатель принимает документ, также подписывает собственной ЭЦП, а отправителю приходит уведомление, что документ был подписан.

Использование ЭЦП и электронного документооборота удобно для участников внешнеэкономической деятельности любого уровня – от малого бизнеса до крупных корпораций и правительств государств, так как он выводит обмен документами на качественно новый уровень. Со стороны таможенных органов, использование электронного документооборота позволяет минимизировать время таможенного оформления товаров. В целях обеспечения информационной безопасности использование исключительно цифровых форм документов также немаловажно, так как с помощью современных программных продуктов гораздо проще предотвратить утечку конфиденциальной информации, нежели обеспечивать защиту информации на бумажном носителе от реального хищения.

Таким образом, деятельность таможенных органов по обеспечению информационной безопасности должна носить непрерывный характер. Для достижения максимального результата такой деятельности необходимо ее постоянное совершенствование на основе развития информационных технологий, накопление и эффективное использование информационных ресурсов, и, наконец, обеспечение безопасности в автоматической информационной системе таможенных органов и контроль за состоянием информационной безопасности и технической защиты информации.

Литература

1. Мошкина, Н.А. Информационная безопасность таможенных органов и особенности ее обеспечения в условиях функционирования ЕАЭС / Н.А. Мошкина // Актуальные проблемы теории и практики таможенного дела в условиях международной экономической интеграции : материалы междунар. науч.-практ. конф., Респ. Беларусь, Минск, 20 марта 2019 г. / Белорус. гос. ун-т; редкол.: В. Г. Шадурский (отв. ред.) [и др.]. – Минск: БГУ, 2019. – С. 84-88

2. Даниленко, А. Ю. Безопасность систем электронного документооборота. Технология защиты электронных документов / А.Ю. Даниленко. - М.: Ленанд, 2015. - 232 с.

УДК 339.564

РЕГРЕССИОННЫЙ АНАЛИЗ И ПРОГНОЗИРОВАНИЕ ПОКАЗАТЕЛЕЙ СТОИМОСТИ ЭКСПОРТА ИЗ РЕСПУБЛИКИ БЕЛАРУСЬ В ПОЛЬШУ В 2019-2021 ГГ.

Новикова В.В.
Руководитель: ст. преподаватель Альшевская О.В.
Белорусский национальный технический университет

На протяжении всей суверенной истории Республики Беларусь, Польша является её важным торговым партнёром. Исходя из этого, изучение данных таможенной статистики, а также прогнозирование показателей внешней торговли с данной страной является стратегически значимым для дальнейшего развития экономических отношений и формирования эффективной внешнеторговой политики.

Исходные данные для анализа товарной структуры экспорта Республики Беларусь в Польшу по разделам ТН ВЭД ЕАЭС были получены с использованием Интерактивной информационно-аналитической системы распространения официальной статической информации, разработанной Национальным статистическим комитетом Республики Беларусь [1].

Товарная структура экспорта в Польшу сложилась в следующем виде. В 2019 году лидирующую позицию в экспорте занимали товары раздела V «минеральные продукты» - 27,20%. Наиболее крупными по объему экспорта также стали: раздел VI «продукция химической и связанной с ней отраслей промышленности» -17,20%, раздел IX «древесина; пробка и изделия из них; изделия из материалов для плетения» - 18,53%. В 2020 году товары этих разделов сохранили лидирующие позиции. В 2021 году наибольший