УДК 004.056.53

Петрушевская А.В.,
студент 3 курс, факультет
«Таможенного администрирования и безопасности»
Северо-Западный институт управления
Россия, г. Санкт-Петербург
Литвинова М.С.,
студент 3 курс,
факультет «Таможенного администрирования и безопасности»
Северо-Западный институт управления
Россия, г. Санкт-Петербург

МИНИМИЗАЦИЯ РИСКОВ ПО ИСКАЖЕНИЮ, ПОДДЕЛКЕ, ХИЩЕНИЮ ТАМОЖЕННОЙ ИНФОРМАЦИИ

Аннотация: *Статья посвящена внедрению и использованию новых информационных технологий – главным факторам, от которых зависит эффективность деятельности таможенных органов. В связи с этим актуальным является вопрос об угрозах информационной таможенной среде и способах её защиты. В статье авторами предложен новый метод по предотвращению искажения, подделке и хищения таможенной информации.*

Ключевые слова: *Российская Федерация, таможенная информация, парольная защита, информационная безопасность, вторичная аутентификация.*

Annotation: *The article is devoted to the introduction of new information technologies and using them which is considered to be the main factors of the efficiency of customs authorities. In this regard, the issue of possible threats to the information customs environment and how to protect it becomes particularly relevant. In the article, the authors proposed a new method to prevent customs data from changing, theft and deception.*

Key words: *Russian Federation, customs information, password protection, information security, secondary authentication.*

В начале XXI века работа с информационными технологиями затрагивает все виды современной профессиональной деятельности человека. Исключением не являются таможенные служащие. Преимущества, которые предоставляет информатизация, объясняют полномасштабное внедрение информационных технологий в работу таможенных структур и непрерывную деятельность по совершенствованию имеющихся технологий. Во-первых, таможенным органам необходимо собрать, обработать и сохранить большое количество данных. Именно информационные технологии ускоряют этот процесс, что впоследствии приводит к более быстрому осуществлению таможенных операций. Во-вторых, коррупционные риски в таможенных структурах значительно снижаются, т.к. информатизация способствует повышению прозрачности совершаемых таможенных операций. В-третьих, информационно-коммуникационные технологии позволяют выполнять таможенным органам одну из главнейших функций – обеспечивать экономическую безопасность Российской Федерации.

Несмотря на значимость процесса информатизации в работе Федеральной Таможенной Службы (далее – ФТС) России, за последние два десятилетия не было создано новых конкурентоспособных по отношению к зарубежным аналогам отечественных разработок в области информационных технологий. В настоящее время программные средства Единой автоматизированной информационной системы таможенных органов (далее – ЕАИС ТО) разрабатываются и эксплуатируются на программных платформах компаний Microsoft, IBM и Oracle. Вопрос импортозамещения информационных технологий является особенно актуальным, т.к. стало проблематичным осуществлять их обновление, сервисное обслуживание и ремонт из-за введения санкций против Российской Федерации рядом зарубежных стран. Так, 12 ноября 2015 г. ФТС России провела коллегию «О текущем состоянии, проблемах и перспективах развития импортозамещения технических средств и оборудования,

используемых в таможенных органах Российской Федерации», на которой был принят ряд решений по вопросам технического переоснащения подразделений таможенных органов РФ. Также была создана Концепция импортозамещения в таможенных органах Российской Федерации до 2020 года. Учитывая значительные усилия, направленные на совершенствование оснащенности таможенных структур передовыми информационными технологиями, в качестве объекта исследования данной статьи была выбрана информационная инфраструктура ФТС России, а в качестве предмета – возникновение различного рода рисков из-за применения информационных средств. Целью работы является создание усовершенствованного способа защиты данных таможенных органов. В соответствии с поставленной целью были выдвинуты следующие задачи:

- изучить существующие виды угроз информационной безопасности ЕАИС ТО;
- проанализировать способы защиты таможенной информации от несанкционированного доступа;

Помимо всех положительных аспектов использования информационных технологий, как было уже отмечено, существует ряд неблагоприятных воздействий на информационную таможенную инфраструктуру. К таким возможным воздействиям относятся [1]:

- заражение информационно-вычислительных ресурсов таможенных органов программными вирусами;
- перехват информации в сетях передачи данных и на линиях связи, с последующим дешифрованием и/или подменой данной информации;
- компрометация ключей криптографической защиты информации;
- распространение компьютерных вирусов, которые препятствуют выполнению функций систем защиты информации;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

В результате таких действий, как искажение, подделка, хищение информации, со стороны несанкционированных пользователей может быть нанесён значительный ущерб функционированию таможенных органов и

структурам, связанным с деятельностью ФТС России. Чтобы предотвратить возможность нанесения ущерба, существуют специальные методы предохранения таможенной информации от несанкционированного доступа.

Таблица 1.

Методы и средства защиты таможенной информации

Организационные	**Технические**
Законодательные	Физические
Административные	Криптографическое закрытие
	Управление доступом

Организационные формы защиты составляют нормативные документы ФТС России, которые регламентируют правила использования и обработки информации, в том числе информации ограниченного доступа, а также устанавливают меры ответственности за нарушение этих правил.

Создание физических препятствий на пути злоумышленника, таких как строгая система пропусков на территорию и/или в помещения с аппаратурой, является физическим способом защиты информации. Данный способ преграждает путь к защищаемой информации только от «внешних» злоумышленников, однако он не защищает информацию от тех лиц, которые обладают правом входа на территорию и/или помещения с таможенными информационно-техническими средствами.

Следующий технический способ защиты – управление доступом – предусматривает такие ступени защиты, как идентификацию пользователей/персонала/ресурсов системы, авторизацию, регистрацию (протоколирование) обращений к защищаемым ресурсам, реагирование системы при попытке несанкционированного действия. Так, каждому объекту/субъекту системы присваивается персональный идентификатор (имя, код, пароль и т.д.), который устанавливает подлинность объекта или субъекта по предъявляемому им идентификатору. Авторизация системы предполагает проверку соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур

установленному регламенту. В случае осуществления злоумышленниками несанкционированных операций система может среагировать путём сигнализации, задержки в работе, отказа в запросе или окончательного отключения своей работы.

Таможенные органы также регламентируют порядок работы пользователей/персонала в собственных информационных системах, право доступа к отдельным файлам в таможенных базах данных и т. д. Самым распространенным методом установления подлинности субъекта таможенной информационной системы является метод паролей. Причина масштабного применения парольной защиты обуславливается простотой и дешевизной реализации, малыми затратами машинного времени, отсутствием необходимости в больших объемах памяти. Надёжность парольной защиты минимизируется из-за высокой вероятности изменения таблицы паролей, которая входит в состав программного обеспечения операционной системы. В связи с тем, что работа ЕАИС ТО реализуется на основе зарубежного программного обеспечения и программные средства разрабатываются на языках программирования иностранного производителя, можно заключить, что уровень уязвимости таблицы паролей – высок.

Как уже было отмечено, развитие отечественного производства в сфере информационно-технического обеспечения таможенных органов получило толчок несколько лет назад. Следовательно, российским разработчикам программных продуктов для ФТС России необходимо обеспечить дополнительную защиту таможенных данных от зарубежных высокоразвитых информационных технологий, которыми могут воспользоваться злоумышленники с целью нанесения ущерба российским таможенным данным. Помимо следования существующим способам по защите информации, авторы предлагают усовершенствованный метод парольной защиты – использование двухфазового пароля 3-D Secure с кодировкой, как отправителем информации, так и её получателем.

3-D Secure является XML-протоколом, который применяется в основном в банковской сфере: 3-D Secure добавляет ещё один шаг аутентификации для онлайн-платежей, позволяющий торговым точкам и банкам дополнительно убедиться, что платеж совершает именно держатель карты. От держателя карты требуется ввести код подтверждения, предоставляемый банком для каждой операции чаще всего в sms-сообщении, отправленном на привязанный к карте номер сотового телефона. Таким образом, 3-D Secure защищает клиентов банка от мошеннических операций.

Введение аналогичного способа защиты информации, с точки зрения авторов, было бы целесообразно при передаче и получении данных в таможенных органах. Новизна применения 3-D Secure метода в работе таможенных структур заключалась бы в том, что sms-запрос приходил бы не только отправителю информации, но и получателю данных. Перед отправкой пакета данных, пользователю системы необходимо запросить код-подтверждение, с помощью которого система идентифицирует подлинность субъекта и разрешает дальнейшую передачу информации. Как только пользователь системы получает sms-сообщение для вторичной аутентификации, ему следует ввести код в течение одной минуты. Если код вторичной аутентификации не вводится в течение отведённого времени, осуществляется повторный запрос для получения нового кода. Количество попыток запроса кода перед отправкой одного пакета документов – ограничено и равно трём. Если пользователь превышает допустимое количество попыток, то срабатывает отключение работы системы для данного пользователя. Аналогично работает 3-D Secure метод для пользователя, получающего таможенную информацию: чтобы открыть входящий пакет данных, необходимо сначала отправить запрос на получение кода-подтверждения и затем ввести его в нужную строку из sms-сообщения. Количество попыток отправления запроса также ограничено тремя разами. Подобный механизм позволит отследить количество отправлений одного и того же пакета документов, какие из адресатов чаще всего производят изменения в документах и др.

Информационная безопасность в силу ее значительного влияния на ключевые функции таможенных органов Российской Федерации становится в современных условиях одной из самостоятельных составляющих деятельности таможенных органов РФ. Однако необходимо понимать, что это сложная задача, которая требует капитального технического прорыва. Внедрение предложенного авторами метода – двухфазового пароля 3-D Secure с кодировкой у отправителя и получателя, которыми будут таможенные служащие и участники ВЭД, − является непростой задачей, однако, в то же время, использование подобной системы способно значительно усилить защищённость таможенных данных.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. СТРАТЕГИЯ РАЗВИТИЯ ТАМОЖЕННОЙ СЛУЖБЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ДО 2020 ГОДА: распоряжение Правительства Российской Федерации от 28 декабря 2012 г. N 2575-р. [Электронный ресурс]. URL: http://www.customs.ru/index.php?option=com_content&view=article&id=17220&