УДК 656.073

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Павлова Я.В.

Санкт-Петербургский имени В.Б. Бобкова филиал Российской таможенной академии

ENSURING INFORMATION SECURITY OF THE CUSTOMS BODIES OF THE RUSSIAN FEDERATION

Y.V. Pavlova

St. Petersburg named after V.B. Bobkova branch of the Russian Customs Academy

Аннотация

В статье рассмотрены вопросы, связанные с обеспечением информационной безопасности таможенных органов Российской Федерации. Приведена нормативно-правовая база, регламентирующая данные отношения. Рассмотрены виды угроз и варианты развития системы защиты информации.

Ключевые слова: информационные технологии, информационная безопасность, информационная система, межведомственное электронное взаимодействие, защита информации.

Abstract

The article considers issues related to ensuring information security of the customs authorities of the Russian Federation. The regulatory framework governing these relationships is provided. The types of threats and options for the development of an information protection system are considered.

Keywords: information technology, information security, information system, interagency electronic interaction, information security.

Деятельность Федеральной таможенной службы направлена на обеспечение экономической безопасности Российской Федерации. В процессе выполнения своего функционала, а именно действий, направленных на выполнение таможенного администрирования, представители таможенных органов получают доступ к таким сведениям, как конфиденциальные данные участников ВЭД, персональные данные физических лиц и сведениям, относящимся к государственной тайне. С развитием информационно-коммуникационных технологий безусловно происходит усовершенствование и усложнение угроз, а это в свою очередь заставляет совершенствовать системы, выполняющие функции по защите информации. Из-за этого перед таможенной службой ставится одна из основополагающих задач – гарантия конфиденциальности, доступности и целостности информации. При проектировании системы безопасности необходимо учитывать все существующие и предполагаемые угрозы и уязвимости. Для выполнения данной задачи необходимо осуществлять непрерывный контроль, причем он должен учитывать весь жизненный цикл информации: от появления – до потери актуальности или полного уничтожения. Правильно подобранная концепция управления информационной безопасностью позволяет снизить риски до приемлемых параметров [1].

В обширном смысле под безопасностью понимается защита законных интересов объектов от различных видов угроз. На сегодняшний день информация – один из самых важных и ценных активов любой организации. Защиту информации по определенным параметрам можно условно можно разделить на две составляющие [2]. Первая – собственно защита самой информации, то есть содержательной части, смысловой нагрузки. Вторая – защита информации от внешних воздействий, сюда включено и её полное уничтожение. Другими словами, защищать нужно не только саму информацию, но также информационные системы, помещения, в которых данные ресурсы расположены, сотрудников, имеющих доступ к информации с ограниченным доступом. Для этого используют следующие виды контроля: административный, логический и физический контроль. Административный контроль подразумевает набор локальных актов, правил и стандартов. Логический контроль или иначе технические средства контроля включает в себя защиту и контроль доступа к ресурсам, программное обеспечение, парольную защиту. Физический кон-

троль направлен на защиту собственно рабочего места. Все эти мероприятия направлены на нормальное функционирование организации, внутреннюю безопасность. Таким образом, действия, направленные на повышение уровня информационной безопасности, отвечают за нахождение, оценивание и минимизацию рисков влияния на информационные технологии и системы.

Нормативно вопросы выполнения положений информационной безопасности в Российской Федерации закрепляются Международными договорами РФ, Конституцией РФ, Федеральными законами РФ, Указами Президента РФ, Постановлениями Правительства РФ и иными правовыми актами. Существует еще ряд законов, действие которых непосредственно не направленно на регулирование отношений в области информационной безопасности, но включающие в себя отдельные статьи, посвященные информации, ее защите.

Одним из основных документов, посвященных вопросам безопасности информации является «Доктрина информационной безопасности Российской Федерации» [3]. В этом документе описаны способы, объекты, а также процедуры, необходимые для обеспечения информационной безопасности. Однако, следует отметить, что изучаемый вопрос безопасности информации данным набором правовых актов не ограничивается. Защита информации требует системного и комплексного подхода, так как представляет собой сложный комплекс мероприятий, подразумевающих большой круг различных процедур и явлений, связанных с противодействием угрозам безопасности.

Информационные комплексы, используемые таможенной службой, представляют собой сложные системы, объединяющие центральные и региональные базы данных и телекоммуникационные сети, гарантирующие качественное выполнение всех видов деятельности таможенной службы. Данные системы постоянно модернизируются и развиваются вместе с развитием таможенных органов. Развитие систем наглядно прослеживается в процессе интеграции взаимодействия с информационными системами участников ВЭД, около таможенных структур, государственных органов.

Защита информации в таможенных органах разделяется два направления. С одной стороны, мероприятия по информационной безопасности таможенных органов выполняется для достижения национальной безопасности. С другой, определенные процедуры направлены для обеспечения своего естественного функционирования.

Острота проблемы отражена в приказе, которым утверждена «Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020 года» [4]. Данная Концепция определяет штатную структуру и основные задачи. Необходимо также указать, что, опираясь на Стратегию национальной безопасности и Доктрину информационной безопасности в Концепции уделено внимание лишь защите информации в целях защиты национальных интересов, при этом упущенным остается уровень внутренней безопасности.

В положении «Стратегии развития таможенной службы Российской Федерации до 2020 года» в разделе 8 «Совершенствование информационно-технического обеспечения» установлено, что повышение уровня безопасности информационных ресурсов, увеличение форм и способов по обеспечению защиты информации, в том числе при организации защищенного обмена информацией с федеральными органами исполнительной власти – это одна из главных задач, получение ответа на которую будет способствовать совершенствованию информационно-технического обеспечения деятельности таможенных органов [5].

Взаимодействие в сфере обмена информацией между ФТС России и иными органами власти разделяется на три основных направления. Первое направление – обмен информацией, проводимый в рамках протоколов об информационном взаимодействии. Этот вариант предполагает обмен юридически значимыми документами в электронном виде. В данном обмене участвуют также сведения, содержащие информацию с ограниченным доступом, но не отнесенные к государственной тайне. Второе – обмен информацией в рамках реализации норм закона о предоставлении государственных и муниципальных услуг служит для исполнения и контроля электронных регламентов. Третий вид обмена направлен на выполнение функций контроля, совершаемых таможенными органами.

Уже сегодня таможенной службой установлены договоренности с различными органами исполнительной власти и иными ведомствами. Обмен информацией с одними

уже налажен и активно используется, с другими продолжаются работы по определению технических условий, описывающих процесс информационного взаимодействия для дальнейшей практической реализации обмена в соответствии с заключенными соглашениями. Одним из динамичных информационных обменов ФТС России осуществляет с Федеральной налоговой службой России [6].

Электронный информационный обмен между ведомствами осуществляется несколькими способами. Среди них, с применением защищенных выделенных каналов связи, электронной почты, а также съемных носителей информации.

Центральное информационно-техническое таможенное управление в основном весь информационный обмен, происходящий на федеральном уровне, пропускает через себя. ФТС России выполняет все возложенные на нее обязательства по передаче информации федеральным органам исполнительной власти, которые предусмотрены соглашениями об информационном обмене. Тем не менее, существует ряд проблемных точек, на которых необходимо заострить внимание.

1. Отсутствие необходимого уровня развития отдельных систем органов исполнительной власти влечет за собой отсутствие единых требований к форматам, предоставляемой информации, способов ее передачи, регламентов взаимодействия.

2. Отдельные органы власти не готовы к предоставлению информации, с требуемой степенью актуальности, необходимую для исполнения ФТС своих функций.

3. Административные преграды, повышенные сроки утверждения с органами исполнительной власти технических условий, необходимых для проведения информационного обмена в рамках реализации соглашений об информационном взаимодействии.

Таким образом, существует необходимость совершенствования механизмов межведомственного взаимодействия в целях повышения качества и эффективности при реализации функций, закрепленных за таможенными органами Российской Федерации.

Для государственных структур задача защиты информации всегда являлась актуальной. С совершенствованием механизмов организации кибератак она вышла на принципиально новый уровень. Отсюда следует задача по защите информации и информационных систем от вирусных атак. В целях качественного построения системы антивирусной защиты действует приказ ФТС России от 28.05.2007 № 660 «О системе антивирусной защиты информации в таможенных органах Российской Федерации» [7]. Данным приказом введено в действие положение об антивирусной защите в таможенных органах. Здесь подробно описана структура системы по борьбе с вирусной активностью, порядок оснащения программными и аппаратными средствами защиты таможенных органов, а также схема эксплуатации данной системы и распределение обязанностей между сотрудниками. Данная система позволяет предотвращать факты заражения компьютерными вирусами, а также нежелательными программами вычислительных ресурсов автоматизированных систем таможенных органов.

Система антивирусной защиты включает несколько участников. Главное управление информационных технологий ФТС России – отвечает за общее управление. Сюда входят функции по проработке документальной стороны защиты информации, проектированию процедур по защите, оснащению структурных подразделений, мониторинг функционирования систем защиты, постановка и сопровождение эксплуатации системы, а также организация проверок по выявленным случаям заражения систем обработки информации. Руководитель службы, отвечающей за формы и средства информационной безопасности и технической защиты, осуществляет управление мероприятиями, направленными на информационную защиту в таможенном органе. Руководители структурных подразделений несут персональную ответственность за выполнение требований информационной безопасности подчиненными должностными лицами.

Выполнение функций по координации антивирусной защиты в структурных подразделениях таможенных органов проводит назначенное приказом должностное лицо – администратор системы защиты. После назначения на роль администратора дополнительные обязанности, закрепленные за должностным лицом, должны быть отражены в должностной инструкции.

Администратор системы несет персональную ответственность за установку и настройку, эксплуатацию средств защиты информации, а также за обновление лицензионных ключей и баз данных средств антивирусной защиты.

Ответственность за соблюдение норм и правил антивирусной защиты при выполнении своих должностных обязанностей на рабочих местах несут пользователи. Согласно приказу пользователям запрещается отключать или использовать средства антивирусной защиты, не рекомендованные для использования в таможенных органах.

Итоги мониторинга защиты от вредоносных программ аккумулируются в результатах отчета по контролю за защитой информации таможенных органов. В отчете полно описаны обнаруженные нарушения, связанные с порчей информации вредоносными программами, причины возникновения и структура вирусов, результаты их деятельности и принятые меры. Как уже было отмечено, на всех автоматизированных рабочих местах, которые используются в таможенных органах, обязательно должны быть установлены программы антивирусного контроля. Безусловно, первоочередно инсталляцию производят на серверы всех типов. Затем установку распространяют на рабочие места всех типов. Средствами защиты от вирусов охватывают все места, которые задействованы в таможенных технологиях, и места, имеющие доступ к информационно-вычислительным сетям общего пользования. Для централизованного управления антивирусными программами, контролем за их работой администратор системы антивирусной защиты в таможенном органе должен располагать программными средствами, которые позволяют удаленно посредством локальной вычислительной сети контролировать составляющие системы антивирусной безопасности различных уровней. Удаленный контроль особенно эффективен, когда в компьютерной сети имеется достаточно большое количество машин, пользователей, или сеть состоит из территориально удаленных друг от друга сегментов.

Антивирусный центр обязан обеспечивать менеджмент структуры антивирусной защиты. При этом обязательным условием является автоматическое обнаружение новых рабочих станций, включенных в сеть, с последующей установкой антивирусных программ. Также в функции центра входит управление установкой и обновлением лицензионных ключей, антивирусных баз, рассылкой служебных сообщений о возникших проблемах и сбоях. Немаловажной является и возможность лимитирования пользователям прав доступа к настройкам системы антивирусной защиты. При этом для администратора остается возможность удаленного решения возникающих в процессе ее эксплуатации проблем.

Значимыми угрозами безопасности при реализации полномочий Федеральной таможенной службой могут быть сбои в обработке, нарушение запретов и ограничений на распространение, незаконный сбор и применение информации ограниченного доступа. Стоит отметить, что дискредитация ключей и средств криптографической защиты информации, а также ее перехват, декодирование, частичная или полная замена также влекут за собой серьезные последствия. Нежелательные последствия могут также возникнуть при нерегламентированном получении информации, которая находится в базах таможенных органов, внесение в аппаратные и программные объекты изменений, создание и рассылка вредоносных программ.

Выполнение мероприятий, направленных на повышение степени информационной безопасности таможенными органами, заключается в достижении того состояния, при котором нанести ущерб составляющим компонентам информационных отношений становится невыполнимой или труднодостижимой задачей. Несомненно, ведущее значение в области защиты информации принадлежит техническим средствам, но и организационным мерам должна быть отведена существенная роль. Полноценная защита может быть достигнута только при комплексном подходе.

Список литературы

1. Погодина Н. А. Информационная безопасность в деятельности таможенных органов // Информационная безопасность регионов. 2011. №2. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-deyatelnosti-tamozhennyh-organov (дата обращения: 07.11.2019).

2. Барбышева Г.И., Мирзаев Ш.Ф. Обеспечение информационной безопасности таможенных органов РФ //Инновационная экономика: материалы II Международной научной конференции (г. Казань, октябрь 2015 г.) – Казань: Бук, 2015. С. 22 – 24.

3. Указ Президента РФ от 05.12.2016 № 646 «Доктрина информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

4. Приказ ФТС России от 13.12.2010 № 2401 «Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020 года» // www.customs.ru

5. Распоряжение Правительства РФ от 28.12.2012 (редакция от 10.02.2018) № 2575-р «О Стратегии развития таможенной службы Российской Федерации до 2020 года» // СПС «Консультант Плюс».

6. Коренькова В.И. Обеспечение информационной безопасности: таможенный аспект // Ростовский научный журнал. 2017. № 1. URL: http://rostjournal.ru/wp-content/journals/RostovScientificJournal12017.pdf (дата обращения: 07.11.2019).

7. Приказ ФТС России от 28.05.2007 № 660 «О системе антивирусной защиты информации в таможенных органах» // www.customs.ru.

Поступила в редакцию 09.11.2019

Сведения об авторе:
Павлова Яна Валерьевна – доцент кафедры информатики и информационных таможенных технологий Санкт-Петербургского филиала Российской таможенной академии, кандидат технических наук, e- mail: kotf.nspu@mail.ru

Электронный научно-практический журнал "**Бюллетень инновационных технологий**"
(**ISSN 2520-2839**) является сетевым средством массовой информации
регистрационный номер **Эл № ФС77-73203**
по вопросам публикации в Журнале обращайтесь по адресу bitjournal@yandex.ru