***Качалов Вадим Юрьевич***
канд. социол. наук, доцент
***Саппарова Карина Евгеньевна***
студентка
Казанский кооперативный институт (филиал)
АНОО ВО ЦС РФ «Российский университет кооперации»
г. Казань, Республика Татарстан

# ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

***Аннотация****: статья посвящена теме вопросов обеспечения информационной безопасности таможенных органов Российской Федерации. Авторами также рассмотрено правовое обеспечение и причины борьбы с угрозами информационной безопасности.*

***Ключевые слова****: безопасность, информационная безопасность, персональные данные, государственная тайна, обмен информацией.*

Структура экономической безопасности Российской Федерации многогранна, отчасти она обеспечивается деятельностью таможенных органов таможенной службы ФТС России. Причиной тому является взаимодействие таможенных органов и иных государственных органов власти, граждан и организаций с доступом к коммерческой и государственной тайне, а также таможенные органы имеют доступ к персональным данным сторон различных внешнеэкономических сделок. Поэтому развитие информационных технологий и взаимодействие государственных органов власти и таможенных органов говорят о том, что необходимо совершенствовать данное направление в целях обеспечения экономической безопасности и развития стратегических направлений Российской Федерации.

ФТС России, как и многие другие государственные органы, имеют доступ к государственной тайне и к персональным данным участников внешнеторговых экономических сделок. Так, одной из задач ФТС России, согласно законо-

дательству Российской Федерации, является гарантия конфиденциальности и защиты полученной информации, а также сохранение её целостности [1, с. 54].

Постоянное совершенствование и изменения автоматизированных программ, которыми пользуются ФТС России, является одной из причин для постоянного анализа информационной безопасности таможенных органов.

Совершенствование работы баз данных, с которыми работает ФТС России, говорит о том, что им необходимо постоянно отражать любые угрозы.

Данная задача решается с помощью введения процедуры наблюдения и осуществления контроля за всеми аспектами деятельности таможенных органов, с того самого момента, как данные поступают в систему таможенных органов Российской Федерации до того момента, когда они подлежат утилизации или же когда нет необходимости обращения к ним. Также контроль должен осуществляться именно в те сроки, которые установлены законодательством и внутренними регламентами ФТС России

При правильной разработке и правильном применении программ, а также обеспечение их безопасности сводит риски угроз к нулю. Следовательно, никаких утечек данных и государственной тайны быть не должно. В любом случае данные действия должны соответствовать законодательству Российской Федерации и быть правомерными.

Причиной тому служит тот факт, что информация на сегодняшний день является одним из самых ценных продуктов, поэтому защита государственной тайны и персональных данных граждан и организаций – одно из приоритетных направлений в деятельности многих органов государственной власти, в том числе и Федеральной таможенной службы России. В данном случае защита информации включает в себя два направления. Это непосредственно защита самой информации и её содержание. Вторым направлением является защита информации от возможных изменений, даже и уничтожения. В данном случае безопасность информационного обеспечения Федеральной таможенной службы России базируется на 2 основных принципах. Первым принципом является защита информации базы данных, которые находятся в ведении Федеральной та-

моженной службы. Вторым принципом является защита той системы, которая обрабатывает, собирает их, группирует и хранит, а также к данному принципу относится защита сотрудников, которые обслуживают информационные ресурсы и базы данных.

Данные принципы реализуют органы контроля со стороны Федеральной таможенной службы [1, с. 53].

Вышеуказанные вопросы законодательно регламентированы международными договорами Российской Федерации, закреплены в Конституции Российской Федерации и федеральных законах, а также обеспечены указами Президента РФ и постановлениями Правительства Российской Федерации. Многие вопросы непосредственного регулирования информационной безопасности в таможенных органах регламентированы внутренними административными регламентами.

Стоит отметить, что на данный момент разработана Концепция обеспечения информационной безопасности таможенных органов, однако там не уделено должного внимание вопросам внутренней безопасности. В Концепции раскрываются цели, задачи, функции защиты информации, а также компетенции и полномочия сотрудников [2, с. 24].

В данной Концепции также установлены договоренности с органами исполнительной власти. Но на сегодня ещё не со всеми органами и их ведомствами удалось наладить информационный обмен и защищенность информации, что говорит о том, что Концепция требует дальнейшей доработки. Так, с некоторыми органами власти не согласованы регламент и порядок обмена информацией.

Одним из приоритетных направлений разработки новых положений Концепции является направление по устранению отсутствия единых форм и форматов взаимодействия между органами государственной власти и таможенными органами. Отсутствие таких форм и форматов привело к увеличению сроков обработки информации и вопросам их защиты. Следующая проблема, имеющую необходимость устранения, является техническая неготовность органов

власти предоставлять актуальную информацию, которая нужна для принятия соответствующих решений. Следовательно, это говорит ещё раз о том, что назрела необходимость в формировании новых возможностей для развития информационной безопасности таможенных органов, а также разработке механизма взаимодействия ФТС России с иными органами государства и с другими странами. Также необходимо разработать единую систему регламентов и положений по обеспечению безопасности информации и о защите сотрудников, которые с ней работают для всех органов государственной власти.

Причиной тому служат статистические данные, в которых говорится о том, что на государственные органы власти и их системы баз данных постоянно происходят вирусные атаки [2, с. 22].

В целом же с помощью нарушений самой системы обеспечения безопасности в неё могут быть внесены опасные вирусы, которые вредят аппаратным и программным обеспечениям службы, а также допускают возможность создания и рассылки вредоносных писем.

Выполнение мероприятий, которые намечены в целях совершенствования концепции и на повышение степени информационной безопасности таможенных органов являются средством для достижения того состояния, при котором нанести ущерб информационным отношениям становится крайне сложно. Несомненно, что здесь большое значение в области информационной безопасности принадлежит новейшим техническим разработкам и цифровым технологиям.

Но также стоит отдать должное и тому, что сами организационные меры должны быть приняты соответствующим образом. Такими мерами могут быть контроль, надзор, проверка сотрудников и повышение их квалификации. Полноценная информационная безопасность при работе в таможенных органах может быть достигнута только при комплексном подходе.

***Список литературы***

1. Погодина Н.А. Информационная безопасность в деятельности таможенных органов / Н.А. Погодина // Информационная безопасность регионов. – 2021. – №2. – С. 53–54.

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