ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(НИУ «БелГУ»)

ИНСТИТУТ УПРАВЛЕНИЯ

КАФЕДРА СОЦИАЛЬНЫХ ТЕХНОЛОГИЙ

Организация выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни

Дипломная работа
студента очной формы обучения, группы 05001305
специальности 38.05.02 Таможенное дело
Туман Сергея Евгеньевича

Научный руководитель
кандидат экономических наук,
доцент Шевченко Н.В.

БЕЛГОРОД 2018

ВВЕДЕНИЕ

Актуальность темы дипломного исследования. Проблема информационной безопасности и защиты информации в таможенных органах является одной из важнейших проблем современности. Еще несколько лет назад задачи защиты информации решались, в основном, с помощью различных организационных мер, таких как выполнение режимных мероприятий, использование средств охраны и сигнализации и т. д., а также программных средств разграничения доступа.

На сегодняшний день, информация рассматривается как один из наиболее ценных продуктов человеческой жизнедеятельности, а информационные ресурсы и информационные технологии, которыми располагает государство, определяют его стратегический потенциал и влияние в мире, поэтому безопасность информации — это одно из основных направлений обеспечения безопасности таможенных органов, реализующих функции по защите экономических интересов Российской Федерации.

Актуальность проблемы безопасности информации и технической защиты информации в современных условиях характеризуется следующими факторами:

1. Повышение количества пользователей сферы использования персональных компьютеров, повсеместным распространением информационно-управляющих систем, сетевых технологий, развитием локальных и глобальных компьютерных сетей;

2. Повышением степени доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности;

3. Привлечение все большего числа людей в информационный процесс, стремительным возрастанием их потребностей в информации, наличием стремительного обмена информацией между участниками этого процесса;

4. Концентрацией больших объёмов информации различного назначения и принадлежности на электронных носителях;

5. Совершенствование способов количественного и качественного доступа пользователей к информационным ресурсам;

6. Возникновением новых возможных каналов несанкционированного доступа к информации, а также разнообразием видов угроз.

Таким образом, актуальность темы дипломного исследования обусловлена необходимостью совершенствования требований информационной безопасности и технической защиты информации в структурных подразделениях таможни.

Степень разработанности темы. Теоретические и практические основы организации информационной безопасности и технической защиты информации в структурных подразделениях таможни стали объектами исследования ряда ученых. Ведущая роль в разработке теоретических и практических проблем в этой области принадлежит таким ученым как: Л.А. Жигун, К.Б Калиновский, Е.О. Любкина, Т.Г. Николаева, И.В. Овчинский, Д.О. Старкова, Д.А. Турчин[1].

Труды этих ученых внесли существенный вклад в развитие методологических и методических таможенного дела. Однако, несмотря на повышенный интерес ученых к информационной безопасности и технической защиты информации в структурных подразделениях таможни в существующих работах недостаточно исследованы.

---

[1] Жигун Л.А. Информационная безопасность в структурных подразделениях таможни // Вестник Российской таможенной академии. 2015. № 3; Калиновский К.Б. Критерии оценки безопасности информационных технологий. М., 2016; Любкина Е.О. Техническая защита информации в таможенных органах // Вестник МГОУ. 2016. № 4; Николаева Т.Г. Основы инженерно-технической защиты информации // Вестник Санкт-Петербургского университета МВД России. 2016. № 2; Овчинский И.В. Организационные, технологические и координационные функции службы защиты информации // Вестник Нижегородского государственного университета. 2017. № 3; Старкова Д.О. Основы таможенного дела. М., 2016; Турчинский Д.А. Основы защиты информации // Таможенный вестник. 2017. № 2.

В качестве **проблемы** исследования выступает противоречие между необходимостью совершенствования требований информационной безопасности и технической защиты информации, и недостаточной разработанностью практических рекомендаций по оптимизации данного процесса в структурных подразделениях таможни.

Объектом дипломного исследования является система информационного обеспечения деятельности структурных подразделений таможни.

Предмет исследования - требования информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни.

Цель дипломной работы является разработка рекомендаций по совершенствованию требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни.

Задачи дипломного исследования:

1) Изучить теоретические основы информационной безопасности и технической защиты информации в структурных подразделениях таможни.
2) Рассмотреть нормативно-правовое обеспечение информационной безопасности и технической защиты информации в структурных подразделениях таможни.
3) Проанализировать практику организации выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни.
4) Предложить направления совершенствования требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни.

Теоретической и методологической основой исследования выступают основные положения системного подхода, изложенного в исследованиях О.В. Березиной, Б.Н. Габричидзе,

Н.Г. Дорониной, В.А. Жбанкова, Е.А. Логиновой, И.В. Овчинского, А.Л. Полыхина, А.Е. Федюнина и позволившего рассмотреть информационную безопасность и техническую защиту информации в структурных подразделениях таможни как систему, изменяющуюся в результате взаимодействия отдельных элементов с внешней средой[1].

При проведении исследования были использованы такие научные методы, как анализ, синтез, сравнение, наблюдение, аналогия, а также методы сравнительного анализа. Исследование опирается на методологический принцип единства теории и практики, а также системный, процессный и другие подходы. В аналитической части работы использованы прикладные экономико-статистические методы.

Эмпирической базой исследования послужили федеральные нормативно-правовые акты, указы президента РФ, приказы Федеральной таможенной службы, а также статистические данные Белгородской таможни[2].

Научно – практическая значимость исследования: заключается в том, что основные положения и выводы представленного исследования уточняют позиции организации требований информационной безопасности и

---

[1] Березина О.В. Информационное обеспечение в таможенных органах // Молодой ученый. 2015. № 9; Габричидзе Б.Н. Таможенная служба Российской Федерации. М., 2017; Доронина Н.Г. Об информации, информатизации и защите информации в таможенных органах Российской Федерации // Пробелы в российском законодательстве. 2016. № 5; Жбанков В.А. Организация выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях таможни. М., 2017; Логинова Е.А. Безопасность информационных технологий // Вестник Нижегородской академии МВД России. 2017. № 21; Полыхин А.Л. Специальные требования и рекомендации по технической защите конфиденциальной информации // Вестник МГОУ. 2017. № 1.

[2] О таможенном регулировании в Российской Федерации : федер. закон от 27 ноября 2010 года № 311-ФЗ (ред. от 28 декабря 2017 года) // Российская газета. – 2010. – № 269. − 29 ноября; Об утверждении Положения по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах Российской Федерации : приказ от 7 ноября 2010 г. № 1866 // Российская газета. – 2010. – 4 января; Об утверждении Положения и состава Совета по обеспечению информационной безопасности Управления : приказ от 7 августа 2010 г. № 480 (ред. от 14.05.2013) // Российская газета. – 2012. – 7 октября.

технической защиты информации в структурных подразделениях таможни. Результаты данного исследования способны повысить эффективность информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни.

Структура дипломной работы. Работа состоит из введения, двух разделов, четырех параграфов, заключения, списка источников и литературы, приложений.

ГЛАВА I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОРГАНИЗАЦИИ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ ТАМОЖНИ

1.1. Сущность и содержание требований информационной безопасности и технической защиты информации в структурных подразделениях таможни

В современном обществе в связи с бурной информатизацией всё более актуальной становится проблема защиты информации.

Частные организации, государственные предприятия и отдельные категории граждан владеют информацией, которая является ценной не только для них, но и для злоумышленников, конкурентов или зарубежных разведчиков. Неважно, в каком виде сохраняется данная информация и по каким каналам осуществляется ее передача, потому что на всех этапах должна функционировать техническая защита информации.

Информация – это любые сведения, передаваемые и применяемые, сохраняемые различными источниками[1].

По мнению В.И. Козлова: «Информационная безопасность – это защищенность информации и соответствующей инфраструктуры от случайных или преднамеренных воздействий сопровождающихся нанесением ущерба владельцам или пользователям информации»[2].

А.Г. Маркушин писал: «Информационная безопасность – это обеспечение конфиденциальности, целостности и доступности информации»[3].

Обеспечение безопасности информации — на данный момент является крайней необходимостью и одним из ключевых направлений обеспечения

---

[1] Опарина Н.Н. Защита информации в таможенных органах // Государственное управление. 2015. № 48. С. 42.

[2] Козлов В.И. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных // Юридический мир. 2016. № 9. С. 99.

[3] Маркушин А.Г. Безопасность информационных технологий. М., 2015. С. 79.

безопасности таможенных органов, основной функцией которых, является защита экономических интересов Российской Федерации.

В силу специфики деятельности подразделений таможенных органов обеспечение их информационной безопасности является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства.

Структурные подразделения таможни – это отделы и им подобные подразделения. Ими, как правило, являются: отдел организации борьбы с контрабандой и административными таможенными правонарушениями; отдел обеспечения операций таможенного контроля; отдел организации таможенного контроля; отдел контроля доставки; отдел технических средств таможенного контроля и связи; отдел таможенных исследований и экспертиз; отдел подакцизных товаров и финансовых гарантий; отдел таможенных платежей; отдел таможенных расследований и т.д.

Должностные лица таможенных органов владеют значительным объемом информационных ресурсов, информационных технологий, информационных систем, осуществляют ведение статистики внешней торговли, получают и используют при осуществлении таможенного контроля персональные данные лиц, которые перемещающих товары и транспортные средства через таможенную границу, имеют доступ к коммерческой тайне участников внешнеэкономической деятельности в процессе осуществления таможенных операций.

Информационные системы таможенных органов – это упорядоченная совокупность информационных технологий и информационных ресурсов, с применением средств связи и вычислительной техники, обеспечивающие эффективную реализацию процедур таможенного контроля и таможенного оформления[1].

---

[1] Евтеева А.А. Информационные ресурсы таможенных органов // Вестник Российской таможенной академии. 2017. № 3. С. 67.

В связи с внедрением в деятельность таможенных органов электронного декларирования активно развиваются информационные системы таможенных органов. Они взаимодействуют и интегрируют с информационными системами участников внешнеэкономической деятельности, других организаций и государственных органов, которые предназначены для представления сведений в электронной форме, с сетями общего пользования.

Угроза информационной безопасности – это целенаправленное действие, которое повышает уязвимость накапливаемой, хранимой и обрабатываемой информации и приводит к ее случайному или предумышленному изменению или уничтожению[1].

Итак, под угрозой безопасности информации понимается событие или действие, которое может привести к искажению или разрушению, также незаконному использованию информационных ресурсов, включая обрабатываемую, передаваемую, хранимую информацию, аппаратные и программные средства. В случаях, когда ценность информации теряется при ее хранении или распространении, то возникает угроза нарушения конфиденциальности информации. Если происходит изменение или уничтожение информации с потерей ее ценности, то возникает угроза нарушения целостности информации. Если информация не была вовремя передана указанному пользователю, то уровень ее ценности снижается и со временем полностью обесценивается, тем самым угроза оперативности использования или доступности информации.

Таким образом, можно выделить угрозы информационного обеспечения таможенных органов Российской Федерации:

---

[1] Кудаев П.П. Технические средства и методы защиты информации // Молодой ученый. 2017. № 12. С. 58.

– монополизация рынка информации таможенных органов Российской Федерации российскими или иностранными информационными структурами;

– нехватка высококвалифицированных кадров, а также отсутствие системы формирования и реализации государственной информационной политики таможенного дела[1].

Основными угрозами, наносящими ущерб развитию и формированию российской информационной индустрии, которая включает: средства информатизации, связи и телекоммуникации, способствующие обеспечению потребностей таможенных органов Российской Федерации в ее продукции, а также обеспечение сохранности и накопления эффективного использования российских информационных ресурсов таможенного дела могут быть:

– импорт средств вычислительной техники, телекоммуникации, программного обеспечения, связи и защиты информации, при наличии российских образцов, идентичных характеристик с зарубежными аналогами;

– устранение с российского рынка производителей средств вычислительной техники, телекоммуникации, связи, защиты информации и программного обеспечения[2].

Угрозами безопасности информации в информационных автоматизированных системах таможенных органов Российской Федерации являются:

–нарушение технологий информационной обработки ограничительного доступа в таможенных органах Российской Федерации;

–нарушение ограничений распространения информации ограничительного доступа, которая обрабатывается в таможенных органах Российской Федерации;

---

[1] Демичев А.А. Прогнозирование угроз автоматизированным системам управления // Современная наука. 2017. № 3. С. 19.

[2] Федюнин А.Е. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации // Молодой ученый. 2015. №1. С. 33.

– незаконный использование информации ограничительного доступа и ее сбор, обрабатывающей в таможенных органах Российской Федерации;

–порча средств и ключей криптографической защиты информации;

–подмена или перехват информации в ведомственной интегрированной телекоммуникационной сети ЕАИС таможенных органов или передаваемой при информационном взаимодействии Федеральной таможенной службы Российской Федерации с таможенными администрациями иностранных государств, федеральными органами исполнительной власти Российской Федерации, международными организациями, участниками внешнеэкономической деятельности, организациями банковской сферы;

– незаконный доступ к информации, которая находится в базах данных таможенных органов Российской Федерации[1].

По своей общей направленности угрозы информационной безопасности таможенных органов подразделяются на следующие виды:

1. угрозы конституционным правам и свободам человека и гражданина в информационной сфере деятельности таможенных органов;

2. угрозы информационному обеспечению государственной политики в области таможенного дела;

3. угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей таможенных органов в ее продукции, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов в области таможенного дела;

4. угрозы безопасности информационных и телекоммуникационных средств и систем таможенных органов[2].

Сотрудники и должностные лица таможенных органов владеют большим количеством конфиденциальной информации, (государственная

---

[1] Калиновский К.Б. Критерии оценки безопасности информационных технологий. М., 2016. С. 27.

[2] Есина А.С. Угрозы информационной безопасности Российской Федерации (в контексте таможенных интересов) // Оперативник. 2016. № 4. С. 102.

тайна, персональные данные, коммерческая тайна, профессиональная или служебная тайна). Искажение, незаконное использование или хищение такой информации в итоге ведут к тяжелым последствиям.

Поэтому необходимо обеспечивать безопасность информационных систем, ресурсов, где она хранится и обрабатывается, а также помещений и подразделений, где она распространяется, сотрудников, осуществляющих доступ к информации ограничительного доступа.

Современное состояние и острота проблемы обеспечения информационной безопасности в таможенных органах России во многом были предопределены темпами автоматизации и внедрения средств вычислительной техники.

Выделяет основные составляющие национальных интересов Российской Федерации в информационной сфере:

1) соблюдение конституционных прав и свобод гражданина и человека в области использования, распространения и получения таможенной информации, а также информации о документах и сведениях, которые были получены в ходе осуществления уголовного судопроизводства, оперативно-розыскной деятельности и административного судопроизводства;

2) информационное обеспечение государственной политики Российской Федерации, которое связано с распространением достоверной информации до международной и российской общественности, информации о государственной политике Российской Федерации с обеспечением доступа граждан к открытым государственным информационным ресурсам в сфере таможенного дела;

3) содействие развитию современных информационных технологий российской информационной индустрии, в том числе индустрии информатизации и средств, связи и телекоммуникации, обеспечение потребностей российского рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение сохранности и накопления, эффективного использования российских информационных ресурсов,

находящихся в ведении Федеральной таможенной службы Российской Федерации;

4) защита информационных ресурсов таможенных органов Российской Федерации от незаконного доступа, обеспечение безопасности телекоммуникационных и информационных систем как уже развернутых, так и создаваемых в интересах таможенных органов Российской Федерации[1].

Следует отметить, что за нарушение правовых норм безопасности информации в таможенных органах, применяются различные виды ответственности: уголовная, гражданско-правовая, дисциплинарная, административная. Это обуславливается спецификой совершаемого правонарушения. Применяемые меры ответственности носят широкий спектр, начиная от выговора, административного штрафа и заканчивая лишением свободы[2].

В современном мире наблюдается тенденция огромного потока увеличения информации. Научно технический прогресс и эволюция общества в целом способствуют этому процессу. Соответственно, перед обществом ставится проблема обеспечения информационной безопасности, что необходимо для устойчивого развития и благосостояния. Таможенная служба не исключение. Она располагает огромными информационными ресурсами, которым также требуется защита. Но на таможенных органах лежит часть ответственности за национальную безопасность страны, поэтому надежное обеспечение информационной безопасности весомая часть достижения этой цели.

Условно обеспечение информационной безопасности таможенных органов можно разделить на два типа:

---

[1] Овчинский И.В. Организационные, технологические и координационные функции службы защиты информации // Вестник Нижегородского государственного университета. 2017. № 3. С. 115.

[2] Орехов Е.В. Информационной безопасности и технической защиты информации в структурных подразделениях таможни // Вестник МГОУ. 2016. № 3. С. 21−22.

1. это обеспечение информационной безопасности для цели обеспечения национальной безопасности (экономической, социальной, территориальной и.т.д.);

2. обеспечение информационной безопасности для целей своего нормального функционирования (эффективность управления, взаимодействия)[1].

На основании этих направлений можно выделить виды информации, которые могут быть потенциальными объектами правонарушений. Их можно условно разделить на внешние и внутренние виды информации. Для их защиты существует особая институциональная система, которая структурирована в соответствии с институтами ФТС.

В соответствии со структурой таможенных органов Российской Федерации на федеральном уровне за информационное обеспечение и безопасность отвечает Центральное информационно техническое таможенное управление (ЦИТТУ), на уровне региона – Информационно техническая служба, на уровне таможни и таможенных постов действует инспектор информационно технической службы. Порядок иерархии представлен на рисунке 1.

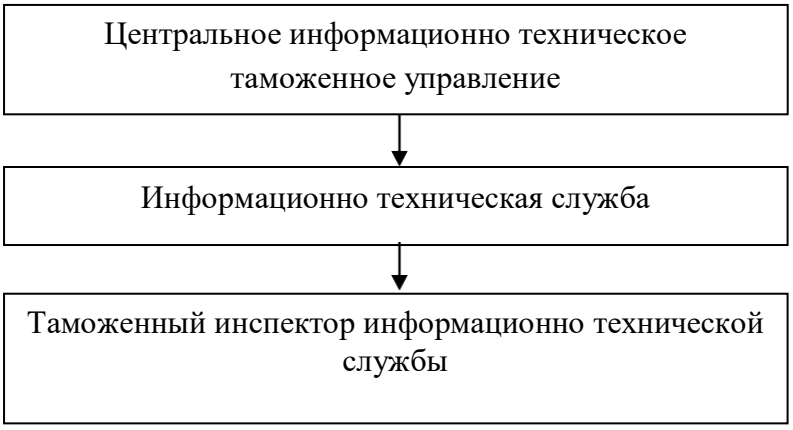

Рис.1. Структура информационного обеспечения безопасности таможенных органов

[1] Строгович М. С. Руководство по защите информации её утечки по техническим каналам // Таможенный вестник. 2017. № 4. С. 22.

Что касается взаимодействия между службами на уровне региона или таможен, то они происходят исходя из положений и внутренних должностных обязанностей. Информационно техническая служба организует передачу необходимой информации и обеспечивает ее безопасность между взаимодействующими подразделениями таможенной службы. Но как показывает практика на сегодняшний день все еще остается проблемы.

Основными требованиями информационной безопасности структурных подразделений таможни являются:

1. Доступность – возможность в приемлемое время получить требуемую информационную услугу;

2. Целостность – непротиворечивость информации и ее актуальность, а также её защищённость от разрушения и несанкционированного изменения;

3. Конфиденциальность – защита от несанкционированного доступа к информации.

С практической точки зрения абсолютной защищённости не существует. Важно соотношение ущерба от нарушения информационной безопасности и стоимости мер по её обеспечению.

Техническая защита информации — это совокупность мероприятий и технических средств по их использованию в целях защиты конфиденциальной информации[1].

Техническая защита информации характеризуется комплексом мероприятий по предотвращению утечки информации по техническим каналам, предупреждению преднамеренных программно-технических воздействий, защита от несанкционированного доступа к ней.

Мероприятия по информационной защите являются составной частью научной, производственной и управленческой деятельности, и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

---

[1] Мухин И.И. Основы защиты информации в таможенных органах. М. 2015. 150 с.

Во всех органах государственной власти и на предприятиях, которые владеют информацией, содержащей сведения, отнесенные к государственной или служебной тайне, информационная защита в средствах и системах информатизации и связи является основной частью работ по их эксплуатации и созданию.

Требования по защите информации в средствах и системах информатизации и связи определяются заказчиками во взаимосвязи с разработчиками на стадии согласования и подготовки решений, директив и приказов, программ и планов работ, тактико-технических заданий, связанных с проведением исследований, модернизацию, эксплуатацию и реализацию на основе стандартов, методических и нормативно-технических документов, которые утверждаются Комитетом Российской Федерации по стандартизации, метрологии и сертификации, Государственной технической комиссией при Президенте Российской Федерации и другими органами государственной власти в соответствии с их компетенцией. Данные требования согласовываются с подразделениями по защите информации.

Организация информационной защиты в средствах и системах связи и информатизации возлагается на руководителей предприятий, органов государственной власти, разработчиков и заказчиков средств и систем связи и информатизации, руководителей подразделений, которые эксплуатируют эти средства и системы, в свою очередь, ответственность за обеспечение информационной защиты – непосредственно возлагается на пользователя, использующего данную информацию.

В целях обеспечения защиты информации в средствах и системах связи и информатизации защите подлежат:

1) информационные ресурсы, которые содержат сведения, отнесенные к служебной и государственной тайне, представленные в виде носителей на оптической и магнитной основе, информативных массивов и баз данных, информативных физических полей;

2) Средства и системы информатизации (информационно-вычислительные комплексы, сети и системы), программные средства (системы управления базами данных, операционные системы, другое прикладное и общесистемное программное обеспечение), технические средства передачи. обработки и приема информации (звукоусиления, звукозаписи, звуковоспроизведения, телевизионные и переговорные устройства, средства изготовления, тиражирования документов и другие технические средства обработки смысловой, графической и буквенно-цифровой информации), автоматизированные системы управления, системы связи и передачи данных, использующиеся для обработки информации, которая содержит сведения, отнесенные к служебной или государственной тайне;

3) технические системы и средства, не обрабатывающие информацию, но размещенные в помещениях, где вращается информация, которая содержит сведения, отнесенные к служебной или государственной тайне, а также сами помещения, которые предназначены для ведения секретных переговоров[1].

Эффективной защита информации считается тогда, когда принимаемые меры соответствуют установленным нормам и требованиям.

Несоответствие установленным нормам и требованиям по защите информации является нарушением.

Нарушения по степени важности можно разделить на три категории:

1. невыполнение норм и требованиям информационной защиты, в результате чего имеется реальная возможность ее утечки по техническим каналам;

2. невыполнение требований информационной защиты, в результате чего создаются условия к ее утечки по техническим каналам;

---

[1] Жбанков В. А. Организация выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях таможни. М., 2017. С. 145.

3. невыполнение других требований информационной защиты.

Таким образом, обеспечение безопасности информации является важнейшей необходимостью и одним из ключевых направлений обеспечения безопасности таможенных органов, которые реализуют функции по защите экономических интересов Российской Федерации. Таможенные органы располагают большими информационными ресурсами, специфическими информационными технологиями, информационными системами, используют при осуществлении таможенного контроля персональные данные лиц, которые перемещают товары, имеют доступ к коммерческой тайне участников внешнеэкономической деятельности в процессе применения таможенных операций, поэтому информационная безопасность на сегодняшний день является одной из основных составляющих национальной безопасности страны.

1.2. Нормативно-правовое обеспечение информационной безопасности и технической защиты информации в структурных подразделениях таможни

В условиях развития и внедрения информационно-телекоммуникационных технологий во все сферы жизнедеятельности общества, человека, и государства в целом, решение вопросов обеспечения безопасности информации технической защиты информации в Российской Федерации, государственных органов является одним из ключевых.

Информационная безопасность и техническая защита информации в структурных подразделениях таможенных органов, можно понимать, как состояние защищённости национальных интересов государства в сфере информатизации таможенных органов[1].

Правовой режим безопасности информации таможенных органов – это установленный нормами права особый порядок нормативно - правового регулирования общественных отношений, которые складываются в сфере обеспечения безопасности информации в структурных подразделениях таможенных органов, осуществляемый при помощи многочисленных правовых средств и направленный на создание состояния защищённости интересов участников информационных правоотношений[2].

С точки зрения правового регулирования информационно-аналитическая деятельность выступает в двух аспектах - как специфический вид оперативно-служебной деятельности таможенных органов и как деятельность в сфере обращения информации. В этой связи, правовую основу информационно-аналитической деятельности составляют:

— нормативно-правовые акты, регулирующие оперативно-служебную деятельность оперативных подразделений таможенных органов;

---

[1] Козлов В.И. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных // Юридический мир. 2016. № 9. С. 99.

[2] Турчин Д.А. Основы защиты информации // Таможенный вестник. 2017. № 2. С. 25−29.

— нормативно-правовые акты, регулирующие отношения в сфере информации, использования компьютерных программ и банков данных.

Нормативно-правовое обеспечение безопасности информации в структурных подразделениях таможенных органов включает в себя совокупность законов и подзаконных актов Российской Федерации, а также международных нормативных правовых актов, утверждённых в их исполнении государственных стандартов и технических регламентов.

В настоящее время Федеральной таможенной службой Российской Федерации подписано 32 соглашения с федеральными органами исполнительной власти и другими ведомствами (Банк России, Федеральное Казначейство и др.) Из них только с 18 министерствами и ведомствами (Минтранс России, Росрыболовство, ФНС России, Росфинмониторинг, Минсельхоз России, Росстат, ФАС России, Минпромторг России, Минэкономразвития России, Роспотребнадзор, Росздравнадзор, Ростехрегулирование, Роспатент, Минздравсоцразвития России, ФСТЭК, Банк России, Федеральное Казначейство) организован непосредственный обмен информацией. С некоторыми ведомствами ведутся переговоры по согласованию технических условий информационного взаимодействия для дальнейшей практической реализации обмена в соответствии с заключенными соглашениями. Наиболее активный информационный обмен ФТС России осуществляет с ФНС России, Минпромторгом России, Роспотребнадзором, Росздравнадзором, Ростехрегулирование, а также с Банком России и Федеральным Казначейством.

Содержание национальных интересов Российской Федерации раскрывается в Доктрине безопасности информации и Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года (далее - Концепция). Концепция выделяет четыре составляющих национальных интересов Российской Федерации в информационной сфере:

1. соблюдение конституционных прав и свобод гражданина и человека в области получения и использования таможенной информации, а также информации о сведениях и доказательствах, которые получены в процессе оперативно-розыскной деятельности, административного и уголовного судопроизводства;

2. информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации с обеспечением доступа граждан к открытым государственным информационным ресурсам в сфере таможенного дела;

3. содействие развитию современных информационных технологий отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов, находящихся в ведении Федеральной таможенной службы Российской Федерации.

4. защита информационных ресурсов таможенных органов Российской Федерации от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как уже действующих, так и создаваемых в интересах таможенных органов Российской Федерации[1].

Целью обеспечения безопасности информации в структурных подразделениях таможни является защита национальных интересов страны в сфере информатизации при осуществлении таможенными органами своих функций по разработке государственной политики и нормативно-правового регулирования, надзора и контроля в сфере таможенного дела, а также

[1] О Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года [Текст] : приказ ФТС России от 13 декабря 2010 года № 2401 // Российская газета. – 2010. – 15 января.

реализация функций валютного контроля и специфических функций по борьбе с контрабандой и иными правонарушениями, возникающими в таможенной сфере.

Сейчас речь идёт об общих, концептуальных началах в данном направлении деятельности, т.е. при помощи определенных мер защиты поддерживается и обеспечивается защищенность национальных интересов, под которыми следует понимать управленческие меры, которые направленны на обеспечение безопасности информации: административные регулирующие документы (распоряжения, приказы и инструкции Федеральной таможенной службы Российской Федерации); дополнительные программы и аппаратные устройства, главной их целью является предотвращение преступлений и правонарушений.

Концепция обеспечения информационной безопасности таможенных органов Российской Федерации выделяет следующие нормативные правовые акты ФТС России, участвующие в регулировании обеспечения информационной безопасности и технической защиты информации в таможенных органах:

1. Собственно Концепция обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года, утвержденная приказом ФТС России №2401 от 13 декабря 2010 года[1].

Данный нормативно - правовой акт характеризует место и роль обеспечения безопасности информации в сфере таможенного дела, а также в обеспечении национальных интересов страны в сфере информатизации с помощью формулировки определения, что можно считать безопасностью информации в структурных подразделениях таможни, характеристикой задач национальных интересов Российской Федерации в сфере информационной деятельности таможенных органов, анализом объектов обеспечения

[1] О Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года [Текст] : приказ ФТС России от 13 декабря 2010 года № 2401 // Российская газета. – 2010. – 15 января.

безопасности информации таможенной службы. В содержании концепции описывается современное состояние безопасности информации в структурных подразделениях таможенных органов Российской Федерации, раскрываются основные принципы и стратегия обеспечения безопасности информации в таможенных органах. Данный документ выделяет основные направления и задачи обеспечения информационной безопасности таможенных органов на период до 2020 года. Отдельный раздел концепции посвящён организации контроля за состоянием обеспечения информационной безопасности таможенных органов.

2. Положение о Совете по обеспечению информационной безопасности таможенных органов Российской Федерации, утверждённое приказом ФТС России №1027 от 22 августа 2011 года[1].

Совет по обеспечению информационной безопасности таможенных органов Российской Федерации имеет функцию постоянно действующей технической комиссии по защите государственной тайны.

Положение раскрывает назначение, цели и задачи, стоящие перед данным органом, раскрывает его структурные особенности и т.п.

3. Положение по проведению функциональных проверок таможенных органов Российской Федерации по вопросам организации и состояния обеспечения информационной безопасности и технической защиты информации, утвержденное приказом ФТС России №19 от 19 января 2009 года[2].

Целевой установкой данного нормативного правового акта является регламентация проведения функциональных проверок таможенных органов Российской Федерации по вопросам организации и состояния обеспечения

---

[1] Об утверждении Положения о Совете по обеспечению информационной безопасности таможенных органов Российской Федерации : приказ ФТС России от 22 августа 2011 г. № 1702 // Российская газета. — 2011. — № 36. — 15 сентября.

[2] Об утверждении Положения о проведении функциональных проверок таможенных органов Российской Федерации по вопросам организации и состояния обеспечения информационной безопасности и технической защиты информации : Приказ ФТС России от 19 января 2009 г. № 19 // Российская газета. — 2009. — № 17. — 16 февраля.

информационной безопасности и технической защиты информации, которая включает в себя органы, осуществляющие проверку и т.п.

Его основной задачей является выявление нарушений в проверяемой сфере.

4. Приказ ФТС России от 30.10.2006 г. №1062 «Об обеспечении безопасности информации при информационном взаимодействии таможенных органов с участниками внешнеэкономической деятельности и сетями общего пользования» издан в целях совершенствования обеспечения безопасности информации при декларировании товаров путем заявления таможенным органам сведений в электронной форме»[1].

5. Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи» регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами[2].

Суть Федерального закона сводится к следующим положениям.

Принципами использования электронной подписи являются:

1. право участников электронного взаимодействия использовать электронной подписи любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

---

[1] Об обеспечении безопасности информации при информационном взаимодействии таможенных органов с участниками внешнеэкономической деятельности и сетями общего пользования : Приказ ФТС России от 30.10.2006 г. №1062 (ред. 07.10.2010) // Российская газета. — 2010. — № 11. — 19 ноября.

[2] Об электронной подписи : федер. закон от 06.04.2011 г. № 63-ФЗ (ред. 23.06.2016) // Собр. законодательства Рос. Федерации. — 2016. — № 23.

2. возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, при использовании конкретных видов электронной подписи;

3. недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронной подписи создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронной подписи в информационной системе.

Среди основополагающих актов российского законодательства об информационной безопасности важное место занимает Федеральный закон «О безопасности», Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О коммерческой тайне», Федеральный закон «О персональных данных», Федеральный закон «Об электронной подписи»[1].

Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует правовые отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; при создании и использовании информационных технологий и средств их

---

[1] О безопасности : федер. закон от 28.12.2010 № 390-ФЗ // Российская газета. – 2010. – 18 ноября; Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 года № 149-ФЗ (ред. 23.04.2018) // Собр. законодательства Рос. Федерации. – 2018. – 20 марта; О коммерческой тайне : федер. закон от 29 июля 2004 года № 98-ФЗ (ред.18.04.2018) // Собр. законодательства Рос. Федерации. – 2018. – 17 мая; О персональных данных : федер. закон от 27 июля 2006 года № 152-ФЗ (ред.29.07.2017) // Собр. законодательства Рос. Федерации. – 2017. – 27 августа; Об электронной цифровой подписи : федер. закон от 06.04.2011 № 63-ФЗ (ред.31.12.2017) // Собр. законодательства Рос. Федерации. – 2017. – 29 января.

обеспечения; при защите информации, прав субъектов информационных отношений, участвующих в информационных процессах и информатизации[1].

Федеральный закон «О безопасности» позволяет использовать соответствующий понятийный аппарат для определения безопасности, объектов безопасности, угроз безопасности в сфере информационно-аналитической деятельности правоохранительных подразделений таможенных органов, а также позиционировать таможенные органы и их правоохранительные подразделения, как органы, участвующие в обеспечении государственной, экономической, экологической безопасности[2].

Федеральный закон «Об электронной подписи» регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами[3].

Суть Федерального закона сводится к следующим положениям.

Принципами использования электронной подписи являются:

1. право участников электронного взаимодействия использовать электронной подписи любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2. возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии

---

[1] Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 года № 149-ФЗ (ред. 23.04.2018) // Собр. законодательства Рос. Федерации. – 2018. – 20 марта.

[2] О безопасности : федер. закон от 28.12.2010 № 390-ФЗ // Российская газета. – 2010. – 18 ноября.

[3] Об электронной подписи : федер. закон от 06.04.2011 г. № 63-ФЗ (ред. 31.12.2017) // Собр. законодательства Рос. Федерации. — 2017. — 29 января.

и (или) технических средств, при использовании конкретных видов электронной подписи;

3. недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронной подписи создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронной подписи в информационной системе.

Следует отметить, что за нарушение правовых норм, регулирующих информационную безопасность таможенных органов, положены различные виды ответственности:

– дисциплинарная,

– гражданско-правовая,

– административная,

– уголовная.

Это обусловлено спецификой совершаемого правонарушения. Соответственно, применяемые меры ответственности носят достаточно широкий спектр, начиная от выговора, административного штрафа и оканчивая лишением свободы.

Таким образом, можно сделать следующие выводы:

1. Информационная безопасность таможенных органов является современной необходимостью и одним из ключевых направлений обеспечения безопасности таможенных органов, реализующих функции по защите экономических интересов Российской Федерации. Таможенные органы владеют большими информационными системами и ресурсами, специфическими информационными технологиями, ведут статистику внешней торговли, получают и используют при осуществлении таможенного контроля персональные данные лиц, которые перемещают товары, имеют доступ к коммерческой тайне участников внешнеэкономической деятельности в процессе применения таможенных операций.

2. Основой информационной безопасность таможенных органов является именно Единая автоматизированная информационная система. Это обусловлено многими факторами. Например, сильная интеграция во всех направлениях работы таможенных органов, довольно длинная история и хороши опыт функционирования системы. Разумеется, еще не достигнута конечная цель в разработке ЕАИС, еще многое предстоит сделать, но также можно сказать, что уже многое сделано и система показывает свою жизнеспособность и способность обеспечить информационную безопасность не только в рамках таможенных органов РФ, но и в рамках Таможенного союза. На ЕАИС возможно применения всех методов нарушения безопасности информации. Исходя из этого, можно сделать вывод, что Единая автоматизированная информационная система таможенных органов является основным объектом таможенного нарушения в сфере обеспечения безопасности информации.

3. На основе проведенного анализа нормативно-правовых актов, были сделаны выводы, что несмотря на активную ведомственную позицию Федеральной таможенной службы Российской Федерации в области правового сопровождения внедрения новых информационных технологий и средств обеспечения безопасности информации остаются некоторые проблемы, которые требуют совершенствования.

ГЛАВА II. ПРАКТИКА ОРГАНИЗАЦИИ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ БЕЛГОРОДСКОЙ ТАМОЖНИ

2.1. Анализ организации выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни

В Российской Федерации, как и во всем мире, информация о таможенном оформлении и торговых сделках относятся к числу конфиденциальной, поэтому государство относит информационную безопасность и техническую защиту информации к одному из важнейших компонентов государственной безопасности.

Защите подлежит любая документированная информация, составляющая государственную тайну, а также конфиденциальная информация, предоставляемая организациям, учреждениям и таможенным органам Российской Федерации.

Осуществление мер по реализации безопасности информации и технической защиты информации является главным видом деятельности должностных лиц таможенных органов. Таможенные органы на всех уровнях взаимодействия и подразделения должны обеспечивать своевременную защиту информации в соответствии с должностными обязанностями и в пределах своей компетенции[1].

На сегодняшний день Белгородская таможня считается одной из самых крупных в Центральном регионе Российской Федерации. Зона деятельности таможни граница с Украиной протягивается на 540,9 км проходит через Сумскую, Харьковскую, а также Луганскую области. Таможня состоит из - 11 таможенных постов, 8 автомобильных, 7 железнодорожных пунктов пропуска и воздушный пункт пропуска – аэропорт международного значения в Белгороде. Из 8 автомобильных пунктов пропуска, функционирующих в

[1] Гармаев Ю. П. Информационные системы, информационные технологии и средства их обеспечения, используемые таможенными органами. М., 2016. С. 211.

регионе деятельности Белгородской таможни, 4 являются многосторонними – Грайворон, Ровеньки, Шебекино, Нехотеевка. Многосторонний автомобильный пункт пропуска Нехотеевка расположен на одной из важнейших автомагистралей, соединяющих центральную часть России с Республикой Крым, и является крупнейшим автомобильным пунктом пропуска в Европе.

Организационная структура Белгородской таможни включает в себя 57 подразделений. Приложение 1.

Организацией выполнения требований информационной безопасности и технической защиты информации в Белгородской таможне занимается отделение информационной безопасности и технической защиты информации.

Отделение информационной безопасности и технической защиты информации (далее – Отделение) является структурным подразделением информационно-технической службы (далее – ИТС) таможни.

Организационное, методическое руководство и контроль деятельности Отделения осуществляет подразделение информационной безопасности и технической защиты информации РТУ, а в части выполнения задач и функций, возложенных на Отделение, – начальник таможни или первый заместитель начальника таможни по таможенному контролю, начальник ИТС таможни.

Отделение возглавляет начальник Отделения, который подчиняется непосредственно начальнику ИТС таможни, а в части выполнения задач и функций, возложенных на Отделение начальнику таможни или первому заместителю начальника таможни по таможенному контролю.

Основными задачами отделения является:

1. Осуществление в таможне и подчиненных таможенных постах единой научно-технической политики, проводимой в таможенных органах, по вопросам обеспечения информационной безопасности и технической защиты информации.

2. Организация и контроль эксплуатации, технического обслуживания и ремонта систем и средств защиты информации в таможне и подчиненных таможенных постах.

3. Защита информации в автоматизированных информационных системах и локальных сетях таможни от несанкционированного доступа.

4. Защита информации при подключении к открытым глобальным вычислительным сетям и при взаимодействии с внешними абонентами.

5. Защита информационно-вычислительных ресурсов таможни от заражения программными вирусами.

6. Организация эксплуатации подсистемы межсетевого экранирования.

7. Организация эксплуатации подсистемы криптографической защиты информации, не содержащей сведения, составляющие государственную тайну, передаваемую между таможенными органами.

8. Организация эксплуатации персональных средств идентификации и аутентификации в таможне.

9. Организация эксплуатации пункта удаленной регистрации таможни.

10. Контроль за соблюдением требований по защите информации от утечки информации по техническим каналам на объектах информатизации таможни и подчиненных таможенных постов.

Организация защиты информации в Белгородской таможне включает в себя средства защиты информации, к которым относятся: подсистема антивирусной защиты информации; межсетевое экранирование; подсистема обнаружения компьютерных атак; подсистема криптографической защиты информации и поддержки механизмов электронной подписи, система защиты информации от несанкционированного доступа в процессе ее хранения и обработки.

Подразделения Белгородской таможни можно условно объединить по направлениям деятельности, каждое из которых в свою очередь взаимодействует с отделением по информационной безопасности и технической защите информации:

– организационно-управленческое;

– кадровое направление;

– финансово-экономическое;

– направление таможенного оформления.

Анализируя организацию выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни, необходимо остановиться на направлении таможенного оформления, так как главной задачей информационной безопасности и технической защиты информации является управление информацией внутри таможенной системы, с целью повышения эффективности деятельности по совершению таможенных операций и проведению таможенного контроля, создания благоприятных условий для участников внешнеэкономической деятельности и при этом максимальное выявление нарушений таможенного законодательства.

Защита информации в данном направлении определяет порядок обеспечения безопасности информации, передаваемой между декларантами и таможенными органами при заявлении сведений о товарах и транспортных средствах в электронной форме, необходимых для таможенного оформления и таможенного контроля, а также обеспечивает надежную защиту данных.

Использование электронного декларирования стало одним из важнейших направлений на пути к упрощению таможенных операций и процедур, позволяет сэкономить время участников внешнеэкономической деятельности, а также процесс таможенного оформления сделать наиболее прозрачным и меньше реагирующим на влияние разных субъективных факторов. В свою очередь, сама процедура электронного декларирования позволила участникам внешнеэкономической деятельности очень быстро почувствовать все ее преимущества.

Так, по данным Федеральной таможенной службы, в настоящее время более 90% деклараций на товары подаётся в электронном виде большинством (свыше 85%) участников внешнеэкономической деятельности[1].

Одним из средств обеспечения защиты информации является использование электронной цифровой подписи (далее-ЭЦП). Использование систем электронного документооборота с применением ЭЦП существенно ускоряет проведение многочисленных коммерческих операций, сокращает объемы бумажной бухгалтерской документации, экономит время сотрудников и расходы, связанные с заключением договоров, оформлением платежных документов с предоставлением отчетности в контролирующие органы, получением справок от различных госучреждений.

Таблица 1

Количество, выпущенных электронных цифровых подписей за 2015-2017 гг.

Год	Кол-во ЭЦП
2015	570
2016	635
2017	687

На протяжении 3-х лет, мы наблюдаем увеличение количества, выпускаемых электронных цифровых подписей, это говорит о том, что данный вид документооборота очень востребован, он значительно ускоряет процесс таможенного оформления и таможенного контроля товаров и транспортных средств.

Но в связи с тем, что электронное декларирование все более широко используется в электронном виде, возрастает риск поймать вирус в ту или иную программу, используемую таможенным органам.

[1] Шумилова А. Ю. Основные итоги деятельности Белгородской таможни // Таможенный вестник. 2016. № 3. С. 35.

Таблица 2

Количество вирус атак в Белгородской таможне за 2015-2017 гг.

Год	Кол-во вирусных атак
2015	499
2016	742
2017	1 124

Анализируя данные за 2015-2017 годы, можно сделать вывод, что количество вирусных атак только увеличивается, это обусловлено постоянным развитием информационных технологий. Также хотелось бы отметить, что возможен риск появления нештатных ситуаций. Работа таможенных органов по защите информации за исследуемый период значительно улучшилась. Количество нештатных ситуаций сократилось более чем в два раза. На сегодняшний день в Белгородской таможне проводятся проверки по работе и предотвращению появления нештатных ситуациях.

Для предотвращения угрозы утечки информации необходимо усилить систему защиты электронного декларирования и установить надежную антивирусную программу.

Существуют такие антивирусные программы как: Антивирус Касперского, NOD32, Dr. Web. Белгородская таможня пользуется единой надежной антивирусной системой Касперского, которая установлена на каждом персональном компьютере Белгородской таможни.

Так, в 2017 году в соответствии с утвержденным планом мероприятий по переводу информационных систем таможни на сертифицированные по требованиям безопасности информационные системы была произведена установка операционной системы Windows 7 на 54 автоматизированные системы доступа к сети «Интернет».

Проводится еженедельная профилактика состояния средств антивирусной защиты информации.

Постоянно осуществляется консультирование должностных лиц таможенных постов отвечающих за информационно-техническую работу по вопросам эксплуатации электронных подписей, проверки соблюдения установленных норм информационной безопасности.

Для формирования и ведения бюджетной сметы, лимитов бюджетных обязательств и управления закупками должностные лица отдела бухгалтерского учета и финансового мониторинга, и отдела тылового обеспечения были подключены к государственной интегрированной информационной системе управления общественными финансами «Электронный бюджет».

Для обеспечения информационной безопасности таможенных органов была создана Единая автоматизированная информационная система (ЕАИС). Начальным этапом этого процесса является создания автоматизированных систем управления, основанный на управлении процессами экономических и математических методов с помощью вычислительной техники. На сегодняшний день ЕАИС полностью выполняет такие задачи как хранение информации, ее обработка, автоматизированный ввод, формирование документов и отчетов для таможенных органов[1].

Единая автоматизированная информационная система является важной частью таможенной инфраструктуры. Задачей ЕАИС является автоматизирование процессов детальности таможенных органов и информационное взаимодействие таможенных органов друг с другом и с внешними субъектами.

На сегодняшний день Федеральная таможенная служба, в том числе и Белгородская таможня активно пользуется ЕАИС, и можно сказать, что она полностью включена в работу. Однако, как и все иные системы, Единая автоматизированная информационная система сталкивается в процессе времени с определенными сложностями и необходимостью идти в ногу со

[1] Черныш А. Я. Организация и современные методы защиты информации. М., 2017. С. 76.

временем. К тому же таможенные органы никогда не забывают о приоритете задач связанные с унификацией системы. Для выхода системы на определенно новый уровень может быть осуществлена с помощью решения задачей связанной с модернизацией Центрального вычислительного комплекса (ЦВК), с помощью создания аналогичный комплексов для регионов и их собственной автоматизированной базы данных.

Транспортная система Единой автоматизированной информационной системы и ее компоненты, которые участвуют в процессе таможенного оформления и контроля расположены в региональных таможенных управлениях, а также в таможнях и таможенных постах. В них формируют платежные документы, архивы, статистическая информация, которая передается в центральное управление системы. Такой обмен информации носит асинхронный характер, то есть программа создает файл с данными, отправляет его в директорию для отправки, а сама продолжает работу. Эта процедура не требует подтверждения о доставке электронного документа в тот же момент. По данному виду деятельности системы можно выделить все пять методов нарушения информационной безопасности. В процессе обмена данными присутствует метод Радиоэлектронный и Информационный. В процессе формирования документов – Физический и Программно-целевой. В процессе обработки ЕАИС данных присутствует Программно-математический метод[1].

Основой информационной безопасность таможенных органов является именно Единая автоматизированная информационная система. Это обусловлено многими факторами. Например, сильная интеграция во всех направлениях работы таможенных органов, довольно длинная история и хороши опыт функционирования системы. Разумеется, еще не достигнута конечная цель в разработке ЕАИС, еще многое предстоит сделать, но также можно сказать, что уже многое сделано и система показывает свою

[1] Кудаев П. П. Технические средства и методы защиты информации // Молодой ученый. 2017. № 12. С. 58.

жизнеспособность и способность обеспечить информационную безопасность не только в рамках таможенных органов РФ, но и в рамках Таможенного союза[1].

На ЕАИС возможно применения всех методов нарушения информационной безопасности. Исходя из этого, можно сделать вывод, что Единая автоматизированная информационная система таможенных органов является основным объектом таможенного нарушения в сфере обеспечения информационной безопасности.

Таким образом, анализируя организацию выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни, можно сделать следующие выводы:

Во–первых, в настоящее время Белгородская таможня считается одной из крупнейших в Центральном регионе России. Организацией выполнения требований информационной безопасности и технической защиты информации в Белгородской таможне занимается отделение информационной безопасности и технической защиты информации. Отделение информационной безопасности и технической защиты информации является структурным подразделением информационно-технической службы таможни.

Во–вторых, наряду с положительными моментами, связанными с организацией выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможне, было выявлено ряд проблем, которые требуют решения. К таковым можно отнести: несовершенство нормативно-правовой базы, регулирующей информационную безопасность и техническую защиту информации в структурных подразделениях таможни, отсутствие методов

[1] Полыхин А. Л. Специальные требования и рекомендации по технической защите конфиденциальной информации // Вестник МГОУ. 2017. № 1. С. 67−73.

оценки эффективности средств и систем безопасности информации и их сертификации, а также отставание российских информационных технологий, которые вынуждают идти по пути закупок небезопасной импортной техники, в результате чего возникает вероятность незаконного доступа к базам данных таможенных органов Российской Федерации, также возрастает огромная зависимость от иностранных производителей телекоммуникационной техники, информационной продукции и компьютеров.

В–третьих, обеспечение безопасности информации — это современная проблема и одно из приоритетных направлений реализации мер по безопасности таможенных органов, которые реализуют функции по защите экономических интересов Российской Федерации в пределах своей компетенции. Ведь таможенные органы владеют большими информационными ресурсами и системами, а также информационными технологиями, формируют статистику внешней торговли, получают и используют при осуществлении таможенного контроля персональные данные физических и юридических лиц, которые перемещают товары и транспортные средства, также они имеют доступ к коммерческой тайне участников ВЭД в процессе осуществления таможенных процедур. Вот почему информационная безопасность на сегодняшний день является одной из основных направлений национальной безопасности страны.

2.2. Направления совершенствования требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни

В настоящее время актуальной проблемой стало обеспечение безопасности информации. На данный момент произошло повышение роли информационных ресурсов, информации, а также информационных технологий, в виду этого обстоятельства, вопросы безопасности информации выходят на первый план в системе обеспечения безопасности физических лиц, организаций и государства в целом. Стремительные темпы развития информационных технологий и возрастание угроз вынуждают постоянно совершенствовать систему обеспечения безопасности информации и технической защиты информации в структурных подразделениях таможни[1].

Информационная защита на сегодняшний момент как никогда актуальна. Необходимость защиты информации связана, прежде всего, с тем, что обеспечение безопасности информации в деятельности таможенных органов играет важнейшую роль в обеспечении национальной безопасности Российской Федерации в целом.

Обеспечение безопасности информации — является одним из главных направлений обеспечения собственной безопасности любой организации, которая оказывает значительное влияние на ее эффективное функционирование, защиту сотрудников, внутренней информации, систем и подразделений.

Деятельность таможенных органов основывается на использовании большого количества информации, которая носит конфиденциальный характер (коммерческая тайна, государственная тайна, персональные данные, профессиональная и служебная тайна). Искажение, хищение, незаконное использование такой информации в следствие ведут к негативным последствиям. Поэтому необходимо обеспечивать не только

[1] Федюнин А.Е. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации // Молодой ученый. 2015. №1. С. 33.

информационную безопасность, но и защиту информационных систем и информационных ресурсов, а также место где они обрабатываются и хранится, помещения, где они распространяются, подразделения и сотрудники, которые обладают доступом к информационным ресурсам ограниченного доступа[1].

В настоящее время особую актуальность приобрели вопросы обеспечения безопасности информации на единой территории Евразийского экономического союза. Объединение в ЕАЭС создало новые обстоятельства, где появились общие сферы деятельности, требующие согласования между странами, в том числе в информационной области.

Очевидно, что информационная безопасность в таможенных органах охватывает широкий спектр задач, от которых зависит эффективность работы как таможенных органов, так и взаимодействующих с ними организаций и ведомств.

В этих условиях выполнение мероприятий по обеспечению безопасности информации является видом основной деятельности таможенных органов Российской Федерации. Информационная безопасность разделяется на две части: безопасность основной части (смысла информации) и защищенность информации от внешних воздействий либо уничтожения. В деятельности таможенных органов Российской Федерации по обеспечению безопасности информации можно выделить несколько направлений.

Во-первых, это информационная защита, обрабатываемая автоматизированными системами (например, антивирусная защита). Во-вторых, это защита данных, которые передаются между подразделениями таможенных органов. В-третьих, это использование средств защиты от несанкционированного доступа. В-четвертых, это использование систем электронного документооборота и электронной цифровой подписи. В-пятых,

[1] Барихин А.Б. Защита информации в информационных технологиях. М., 2015. 44 с.

обеспечение безопасности при осуществлении международного информационного обмена[1].

Информационная защита на сегодняшний момент как никогда актуальна. Необходимость защиты информации связана, прежде всего, с тем, что обеспечение безопасности информации в деятельности таможенных органов играет важнейшую роль в обеспечении национальной безопасности Российской Федерации в целом.

Обеспечение безопасности информации — является одним из главных направлений обеспечения собственной безопасности любой организации, которая оказывает значительное влияние на ее эффективное функционирование, защиту сотрудников, внутренней информации, систем и подразделений.

Деятельность таможенных органов основывается на использовании большого количества информации, которая носит конфиденциальный характер (коммерческая тайна, государственная тайна, персональные данные, профессиональная и служебная тайна). Искажение, хищение, незаконное использование такой информации в следствие ведут к негативным последствиям. Поэтому необходимо обеспечивать не только информационную безопасность, но и защиту информационных систем и информационных ресурсов, а также место где они обрабатываются и хранится, помещения, где они распространяются, подразделения и сотрудники, которые обладают доступом к информационным ресурсам ограниченного доступа[2].

Таким образом, для совершенствования информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни, необходимо:

---

[1] Александрова А.С. Информационное обеспечение таможенных органов // Ученые записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии. 2015. № 5 (40). С. 254.

[2] Барихин А.Б. Защита информации в информационных технологиях. М., 2015. 44 с.

1. Совершенствование нормативно – правовой базы обеспечения информационной безопасности и технической защиты информации в структурных подразделениях таможни, с учётом современных динамично изменяющихся угроз и на основе анализа возможных рисков.

Данное направление можно реализовать по двум направлениям. Первое направление связано с доработкой и конкретизацией базовых действующих нормативно-методических документов; второе направление – с разработкой совокупности новых документов, регламентирующих и конкретизирующих комплексное решение всех вопросов обеспечения информационной безопасности и технической защиты информации в структурных подразделениях таможни.

2. Совершенствование информационно-технического обеспечения системы управления рисками на основе разработки новых методологических подходов, а также разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности и технической защиты информации.

Целевыми индикаторами указанного направления является:

— доля средств вычислительной техники со сроками эксплуатации и их характеристиками, которые будут достаточны для беспрерывного функционирования информационных систем в составе единой автоматизированной информационной системы таможенных органов, в общем количестве средств вычислительной техники, эксплуатируемых в таможенных органах Российской Федерации;

— отношение количества телекоммуникационных каналов ведомственной интегрированной телекоммуникационной сети Федеральной таможенной службы, имеющих пропускную способность 2 Мбит/с и более, к общему количеству телекоммуникационных каналов.

3. Развитие ведомственной интегрированной телекоммуникационной сети Федеральной таможенной службы, в том числе для обеспечения

доставки актуальной информации, содержащейся в единой автоматизированной информационной системе таможенных органов, в режиме времени, близком к реальному, на всех уровнях системы таможенных органов, а также повышение уровня защищенности информационных ресурсов, расширение спектра мер по обеспечению информационной безопасности, в том числе при организации защищенного обмена информацией с федеральными органами исполнительной власти.

Таким образом, административно-правовое обеспечение информационной безопасности в таможенных органах, развиваясь в различных направлениях, должно исходить, прежде всего, из норм и принципов правового регулирования в рассматриваемой области и в общем виде может быть представлено следующим образом:

1) участие Федеральной таможенной службы Российской Федерации в правотворчестве с учетом интересов всех категорий субъектов информационной безопасности;

2) устранение пробельности правовых актов, противоречий между нормами федерального и таможенного законодательства, а также нормами международного права;

3) закрепление правовых гарантий презумпции открытости информации, затрагивающей конкретные права и интересы, в целях реализации конституционных прав на получение информации и установление соответствующих ограничений;

4) развитие системы обеспечения информационной безопасности таможенных органов путём совершенствования норм, регулирующих ответственность за правонарушения в информационной сфере;

5) изменение и совершенствование системы обучения, подготовки и переподготовки должностных лиц таможенных органов по вопросам обеспечения информационной безопасности;

6) развитие современных информационных таможенных технологий, обеспечение накопления, сохранности и эффективного использования информационных ресурсов таможенных органов.

В осуществлении целей, способствующих развитию внешнеэкономической деятельности, а также меры, направленные на минимизацию издержек участников внешнеэкономической деятельности и государства в целом, связанных с совершением таможенных операций и процедур, а также способствующих повышению эффективности таможенного администрирования необходимо проводить комплексную работу по развитию информационно-технического обеспечения таможенных органов. Развитие и реализация мер, направленных на повышение эффективности информационно-технического обеспечения таможенных органов осуществляется с учетом мировых тенденций и стандартов развития таможенных органов.

Эффективность информационной безопасности в системе таможенных органов зависит от наличия комплекса профилактических мер направленных на предотвращение правонарушений. Для предохранения утечки важной таможенной информации можно выделить следующие формы профилактической защиты на основании концепции обеспечения информационной безопасности таможенных органов: законодательные, физические, управление доступом, криптографическое закрытие.

К законодательным формам обеспечения защиты таможенной информации относят должностные инструкции, внутренние нормативно правовые документы, правила и порядок использование таможенной информации, а также соблюдение ответственности за возможные нарушения данных правил.

Они создают нормативно правовое поле в рамках обеспечения безопасности информации таможенных органов[1].

[1] Логинова Е.А. Безопасность информационных технологий // Вестник Нижегородской академии МВД России. 2017. № 21. С. 12.

Физическая защита информации представляет собой ограничение доступа нарушителе к объектам информационной инфраструктуры. Организовывается данная мера путем введения системы пропусков, допусками секретности, заграждением территории и др. стоит отметить, что данный способ защищает таможенную информацию только от нарушителей из вне системы. Риски, связанные с возможными нарушителями внутри системы (с правом доступа), в данной форме не учитываются.

Таким образом, создание положительного образа таможенных органов будет происходить путем информационной деятельности через средства СМИ и посредством активного взаимодействия общественных объединений и государства. Сложившийся инфраструктурный и институциональный потенциал, сформированный на таможенных, инновационных и информационных технологиях и соответствующий практике ведущих таможенных администраций зарубежных стран, будет положен в фундамент устойчивого развития таможенной службы Российской Федерации.

Целью обеспечения безопасности информации таможенных органов является защита интересов государства в информационной сфере при осуществлении таможенными органами функций по выработке государственной политики и нормативному правовому регулированию, контролю и надзору в области таможенного дела, а также функций агента валютного контроля и специальных функций по борьбе с контрабандой, иными преступлениями и административными правонарушениями.

Выделяют принципы обеспечения безопасности информации и технической защиты информации в таможенных органах:

1. Комплексность и системность, которая включает:

– обеспечение безопасности информационных ресурсов начиная с ее конфиденциальности, на всех этапах их преобразования и использования, во всех режимах функционирования технических средств, при взаимодействии с другими информационными системами;

– обеспечение полная защиты информации от различных угроз возможными методами, средствам и мероприятиями;

– способность системы самосовершенствованию в соответствии с изменениями условий функционирования.

2. Своевременность, которая носит предупредительный характер обеспечения безопасности информации, также включает выделение задач по планомерной информационной защите и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ЕАИС таможенных органов в целом и ее системы защиты информации в частности, на основе анализа и прогнозирования состояния мирового рынка, технических, программных средств и информационных технологий, угроз безопасности информации, а также разработку эффективных мер предупреждения посягательств на законные интересы государства.

3. Законность, характеризуется разработкой системы информационной защиты согласно законодательству Российской Федерации в области защиты информации и информатизации, правовых актов по безопасности информации, которые утверждаются федеральными органами исполнительной власти в пределах своей компетенции, с применением определенных методов выявления и пресечения правонарушений в области информации. Принятые стандарты безопасности информации не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством Российской Федерации случаях к информации конкретных оппонентов ЕАИС таможенных органов.

4. Научно-техническая реализуемость и обоснованность. Предлагаемые программные и технические средства, информационные технологии, средства и меры защиты информации должны соответствовать установленным нормам и требованиям по безопасности информации, должны быть реализованы на современном уровне развития техники и науки, должны быть научно и технически обоснованы с точки зрения заданного уровня безопасности информации.

5. Экономическая целесообразность. Анализ возможных затрат и возникновения ущерба. Предполагает адекватность уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, несанкционированный доступ, потери, искажения. Реализуемые меры и средства обеспечения безопасности информационных ресурсов не должны снижать уровень экономических показателей работы ЕАИС таможенных органов, в которой эта информация варьируется.

6. Профессионализм и специализация. Основывается на привлечении к внедрению и разработке средств и мер защиты информации организаций специализирующихся в этой области, информационных ресурсов, которые наиболее подготовлены к данному виду деятельности по обеспечению безопасности, которые имеют опыт работы и государственную лицензию на право оказания услуг в области информатизации, а также эксплуатация данных средств и мер должна осуществляться высококвалифицированными специалистами.

7. Координация и взаимодействие, предполагающее при обеспечении безопасности информации таможенных органов взаимодействие с ФСБ России и ФСТЭК России, иными заинтересованными федеральными органами исполнительной власти, а также с предприятиями и организациями, привлекаемыми для выполнения работ по обеспечению безопасности информации таможенных органов.

8. Эффективность контроля и его обязательность, которая предполагает своевременность и обязательность пресечения и выявления угроз, связанных с нарушением системы обеспечения безопасности информации, на основе используемых средств и систем информационной защиты при совершенствовании методов и критериев оценки их эффективности;

9. Непрерывность и преемственность совершенствования. Предполагает постоянное повышение эффективности средств и мер защиты информации на основе преемственности технических и организационных

решений, кадрового аппарата, анализа функционирования системы защиты информации ЕАИС таможенных органов с учетом изменений в средствах и методах перехвата информации, нормативных требований по ее защите, достигнутого зарубежного и российского опыта в этой области[1].

Таким образом, можно сделать следующие выводы:

Во–первых, деятельность таможенной службы Российской Федерации направлена на обеспечение национальной и экономической безопасности государства, актуальным становится вопрос об совершенствовании информационной безопасности и технической защиты информации в таможенных органов, поскольку именно таможенные орган обладают значительным объёмом информации, связанной с осуществлением внешнеэкономической деятельности.

Во–вторых, обеспечение безопасности информации таможенных органов Российской Федерации характеризуется созданием условий, при которых причинение вреда элементам системы информационных отношений (свойствам, инфраструктуре, порядку функционирования субъектов информационных отношений или законным интересам отдельных граждан) в сфере таможенного дела становится очень затруднительным или же невозможным. Информационная защита от возникающих угроз может быть обеспечена лишь при комплексном подходе к обеспечению безопасности информации, представляющем собой организационно-правовую совокупность отдельных элементов, средств, задач, методов, а также мероприятий по обеспечению информационной защиты от несанкционированного доступа или разглашения.

В–третьих, для совершенствования требований информационной безопасности и технической защиты информации в структурных подразделениях Белгородской таможни необходимо: совершенствование

[1] Марченко И. Безопасность информационных технологий в таможенных органах // Государственная власть. 2016. № 14. С. 35.

нормативно – методической базы обеспечения информационной безопасности и технической защиты информации в структурных подразделениях таможни, с учётом современных динамично изменяющихся угроз и на основе анализа возможных рисков; совершенствование информационно-технического обеспечения системы управления рисками на основе разработки новых методологических подходов, а также разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности и технической защиты информации; принятие закона, устанавливающего запрет на использование иностранного продукта при осуществлении своих функций таможенными органами, а также совершенствование единой автоматизированной информационной системы таможенных органов в условиях функционирования Евразийского экономического союза, в целях развития информационного взаимодействия между таможенными органами государств - членов ЕАЭС, с учетом развития интегрированной информационной системы внешней и взаимной торговли. Предложенные направления повысят эффективность деятельности таможенных органов, а также эффективность обеспечения экономической безопасности Российской Федерации в целом.

ЗАКЛЮЧЕНИЕ

В современном мире наблюдается тенденция огромного потока увеличения информации. Научно технический прогресс и эволюция общества в целом отчасти способствуют этому процессу. Соответственно, перед обществом ставится проблема обеспечения информационной безопасности, что необходимо для устойчивого развития и благосостояния. Таможенная служба не является исключением. Она располагает огромными информационными ресурсами, которым также требуется защита. Но на таможенных органах лежит часть ответственности за национальную безопасность страны, поэтому надежное обеспечение информационной безопасности весомая часть достижения этой цели.

Информационная сфера является основным системообразующим фактором жизни государства. Развитие индустрии информационных технологий, масштабы проникновения их в повседневную жизнь и влияние на все сферы деятельности человека настолько велики, что проблема информационной безопасности в современном мире стала первостепенной, а принятие мер, направленных на её обеспечение, в том числе для государственных органов, учреждений и граждан, является жизненной необходимостью.

Обеспечение информационной безопасности на сегодняшний день, является насущной необходимостью и одно из основных направлений обеспечения безопасности таможенных органов, реализующих функции по защите экономических интересов Российской Федерации. Таможенные органы Российской Федерации владеют большими объемом информационных ресурсов, информационных систем, огромным количеством специфических информационных технологий, также осуществляют ведение статистики внешней торговли, получают в свой адрес и используют при проведении таможенного контроля персональные данные физических и юридических лиц, которые перемещают товары и

транспортные средства, имеют доступ к коммерческой тайне участников ВЭД в процессе проведения таможенных процедур.

Национальная безопасность нашей страны во многом зависит от обеспечения безопасности информации.

Безопасность информации – это состояние защищенности информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Под «информационной угрозой» можно понимать действие, которое может привести к уничтожению, несанкционированному или искажению использованию информационных ресурсов, включая хранимую и обрабатываемую, а также передаваемую информацию, аппаратные и программные средства.

В соответствии со структурой таможенных органов на федеральном уровне за информационное обеспечение и безопасность отвечает Центральное информационно техническое таможенное управление (ЦИТТУ), на уровне региона – Информационно техническая служба, на уровне таможни и таможенных постов действует инспектор информационно технической службы.

Таможенные органы используют многочисленные информационные системы и технологии, а также средства их обеспечения, которые ими разрабатываются, производятся или приобретаются в соответствии с законодательством и международными договорами государств-членов Евразийского экономического союза.

Для таможенных целей порядок и условия использования информационных технологий и систем, а также средств их обеспечения и программных технических средств защиты информации, требования к ним при организации информационного взаимодействия, которое основано на электронных методах обмена информации, определяются таможенным

законодательством Евразийского экономического союза и законодательством государств-членов ЕАЭС.

Для реализации целей взаимодействия таможенных органов на таможенной территории Евразийского экономического союза создаются интегрированные информационные технологии и системы.

Информационная защита прав субъектов, которые участвуют в информационных процессах и информатизации, регулируется в порядке, установленном законодательством государств-членов Евразийского экономического союза.

Степень защиты информации, обеспечиваемая программно - техническим средством защиты информации, должна соответствовать категории информации. Соответствие уровня защиты информации определенной категории обеспечивается таможенными органами, в ведении которых находятся информационные ресурсы.

Обмен информационными ресурсами между таможенными органами осуществляется в соответствии с международными договорами государств-членов Евразийского экономического союза.

Таможенные органы участвуют в международном обмене информацией с таможенными органами иностранных других государств, а также международными и иными организациями в порядке и на условиях, которые определяется законодательством государств-членов Евразийского экономического союза.

Структура нормативно-правовой базы обеспечения информационной безопасности таможенных органов включает в себя:

– законодательство Российской Федерации;

– правовые акты по обеспечению информационной безопасности таможенных органов в целом;

– правовые акты по обеспечению информационной безопасности в центральном аппарате ФТС России;

– правовые акты по обеспечению информационной безопасности таможенных органов уровня федерального округа (регионального таможенного управления);

– правовые акты по обеспечению информационной безопасности в иных таможенных органах.

Анализируя требования информационной безопасности и технической защиты информации в структурных подразделениях таможни, был выявлен ряд проблем, которые требуют решения. К таковым проблемам, можно отнести:

– несовершенство нормативно-правовой базы, регулирующей информационную безопасность и техническую защиту информации в таможенных органах;

– отсутствие критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации;

– отставание отечественных информационных технологий вынуждает идти по пути закупок незащищенной импортной техники, в результате чего повышается вероятность несанкционированного доступа к базам данных таможенных органов Российской Федерации, а также возрастает зависимость от иностранных производителей компьютерной и телекоммуникационной техники и информационной продукции.

Для решения указанных проблем, были предложены направления совершенствования требований информационной безопасности и технической защиты информации в структурных подразделениях таможни.

1. Совершенствование нормативно – методической базы обеспечения информационной безопасности и технической защиты информации в структурных подразделениях таможни, с учётом современных динамично изменяющихся угроз и на основе анализа возможных рисков.

2. Совершенствование информационно-технического обеспечения системы управления рисками на основе разработки новых методологических

подходов, а также разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности и технической защиты информации.

3. Принятие закона, устанавливающего запрет на использование иностранного продукта при осуществлении своих функций таможенными органами, а также совершенствование единой автоматизированной информационной системы таможенных органов в условиях функционирования Евразийского экономического союза, в целях развития информационного взаимодействия между таможенными органами государств - членов ЕАЭС, с учетом развития интегрированной информационной системы внешней и взаимной торговли.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ [Текст] (ред. от 19.02.2018) // Собр. законодательства Рос. Федерации. − 1997. − № 1.

2. О безопасности [Текст] : федер. закон от 28.12.2010 № 390-ФЗ // Российская газета. – 2010. – 18 ноября.

3. О коммерческой тайне [Текст] : федер. закон от 29 июля 2004 года № 98-ФЗ (ред.18.04.2018) // Собр. законодательства Рос. Федерации. – 2018. – 17 мая.

4. О персональных данных [Текст] : федер. закон от 27 июля 2006 года № 152-ФЗ (ред.29.07.2017) // Собр. законодательства Рос. Федерации. – 2017. – 27 августа.

5. О таможенном регулировании в Российской Федерации [Текст] : федер. закон от 27 ноября 2010 г. № 311-ФЗ (ред. от 28.12.2017) // Российская газета. – 2010. – № 269. − 29 ноября.

6. Об информации, информационных технологиях и о защите информации [Текст] : федер. закон от 27 июля 2006 года № 149-ФЗ (ред. 23.04.2018) // Собр. законодательства Рос. Федерации. – 2018. – 20 марта;

7. Об электронной подписи [Текст] : федер. закон от 06.04.2011 г. № 63-ФЗ (ред. 23.06.2016) // Собр. законодательства Рос. Федерации. — 2016. — № 23.

8. О Концепции обеспечения информационной безопасности таможенных органов Российской Федерации на период до 2020 года [Текст] : приказ ФТС России от 13 декабря 2010 г. № 2401 // Российская газета. — 2010. — № 36. — 7 января.

9. Об обеспечении безопасности информации при информационном взаимодействии таможенных органов с участниками внешнеэкономической деятельности и сетями общего пользования [Текст] : приказ ФТС России от

30.10.2006 г. №1062 (ред. 07.10.2010) // Российская газета. — 2010. — № 11. — 19 ноября.

10. Об утверждении Положения по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена в таможенных органах Российской Федерации [Текст] : приказ от 7 ноября 2010 г. № 1866 // Российская газета. – 2010. – 4 января.

11. Об утверждении Положения о проведении функциональных проверок таможенных органов Российской Федерации по вопросам организации и состояния обеспечения информационной безопасности и технической защиты информации [Текст] : приказ ФТС России от 19 января 2009 г. № 19 // Российская газета. — 2009. — № 17. — 16 февраля.

12. Об утверждении Положения о Совете по обеспечению информационной безопасности таможенных органов Российской Федерации [Текст] : приказ ФТС России от 22 августа 2011 г. № 1702 // Российская газета. — 2011. — № 36. — 15 сентября.

13. Об утверждении Положения и состава Совета по обеспечению информационной безопасности Управления [Текст] : приказ от 7 августа 2010 г. № 480 (ред. от 14.05.2013) // Российская газета. – 2012. – 7 октября.

14. Об обеспечении безопасности информации при информационном взаимодействии таможенных органов с участниками внешнеэкономической деятельности и сетями общего пользования [Текст] : приказ ФТС России от 30.10.2006 г. №1062 (ред. 07.10.2010) // Российская газета. — 2010. — № 11. — 19 ноября.

15. Положение о проведении функциональных проверок таможенных органов Российской Федерации по вопросам организации и состояния обеспечения информационной безопасности и технической защиты информации [Текст] : приказ ФТС России от 19 января 2009 г. № 19 // Российская газета. — 2009. — № 17. — 16 февраля.

16. Положение о Совете по обеспечению информационной безопасности таможенных органов Российской Федерации [Текст] : приказ ФТС России от 22 августа 2011 г. № 1702 // Российская газета. — 2011. — № 36. — 15 сентября.

17. Авдонин, В. А. Административно-правовые аспекты обеспечения информационной безопасности таможенных органов Российской Федерации [Текст] : автореф. дис. … канд. юрид. наук / В. А. Авдонин. – Люберцы, 2015. – 30 с.

18. Александрова, А. С. Информационное обеспечение таможенных органов [Текст] / А. С. Александрова // Ученые записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии. – 2015. – № 5 (40). – С. 254.

1. Андреев, А. Ф. Развитие информационных таможенных технологий [Текст] / А. Ф. Андреев, В. В. Макрусев. – М. : РИО РТА, 2016. – 176 с.

2. Архипов, М. А. Обеспечение информационной безопасности таможенных органов Российской Федерации [Текст] / М. А. Архипов // Инновационная экономика. − 2016. − № 2. – С. 105.

3. Асланов, М. А. Применение информационных технологий в деятельности таможенных органов [Текст] / М. А. Асланов // Экономико-юридический журнал. − 2017. − № 2. – С. 115.

4. Бабаян, К. А. Информационное обеспечение управления в таможенной системе. Автореф. дис. … канд. юрид. наук [Текст] / К. А. Бабаян. – Люберцы, 2015. – 27 с.

5. Барамзин, С. В. Информационные ресурсы таможенных органов [Текст] : монография / С. В. Барамзин. – 2-е изд., перераб. – М. : Изд-во Российской таможенной академии, 2016. – 142 с.

6. Барихин, А. Б. Защита информации в информационных технологиях [Текст] / А. Б. Барихин. − М. : Изд-во РАГС, 2015. – 44 с.

7. Бахрах, Д. Н. Развитие информационных таможенных технологий [Текст] / Д. Н. Бахрах. Вестник МГОУ. – 2016. – № 2. – С. 119.

8. Березина, О. В. Информационное обеспечение в таможенных органах [Текст] / О. В. Березина // Молодой ученый. – 2015. – №9. – С. 349.

9. Беспалько, В. Г. Таможенное право [Текст] В. Г. Беспалько : монография. – М. : РИО РТА, 2015. – 250 с.

10. Блинова, О. А. К вопросам о внедрении принципа «Единого окна» и совершенствовании информационных таможенных технологий в ТС [Текст] / О. А. Блинова // Таможенный вестник. – 2016. – № 13-1. – С. 164-166.

11. Габричидзе, Б. Н. Таможенная служба Российской Федерации [Текст] / Б. Н. Габричидзе . – М. : ИНФРА-М, 2017. – 433 с.

12. Гармаев, Ю. П. Информационные системы, информационные технологии и средства их обеспечения, используемые таможенными органами [Текст] / Ю. П. Гармаев. – Иркутск : Изд-во ИЮИ ГП РФ, 2016. – 211 с.

13. Губин, А. В. Развитие теории оценки результатов деятельности таможенных органов : монография [Текст] / А. В. Губин. – М. : Изд-во РТА, 2017. – 120 с.

14. Демичев, А. А. Прогнозирование угроз автоматизированным системам управления [Текст] / А. А. Демичев // Современная наука. − 2017. − № 3. − С. 19.

15. Дианова, В. Ю. Развитие таможенной инфраструктуры [Текст] : монография / В. Ю. Дианова, В. В. Макрусев, О. В. Маркина. – М.: Изд-во РТА, 2016. – 250 с.

16. Доронина, Н. Г. Об информации, информатизации и защите информации в таможенных органах Российской Федерации [Текст] / Н. Г. Доронина // Пробелы в российском законодательстве. − 2016. − № 5. – С. 114.

17. Дударец, М. А. Информационное обеспечение управления в таможенной системе. Автореф. дис. … канд. юрид. наук [Текст] / М. А. Дударец. – Люберцы, 2016. – 90 с.

18. Евтеева, А. А. Информационные ресурсы таможенных органов [Текст] / А. А. Евтеева // Вестник Российской таможенной академии. − 2017. − № 3. – С. 67.

19. Есина, А. С. Угрозы информационной безопасности Российской Федерации (в контексте таможенных интересов) [Текст] / А. С. Есина // Оперативник. − 2016. − № 4. – С. 102.

20. Жбанков, В. А. Организация выполнения требований информационной безопасности и технической защиты информации в структурных подразделениях таможни [Текст] : монография / В. А. Жбанков. – М. : Изд-во РТА, 2017. – 145 с.

21. Жигун, Л. А. Информационная безопасность в структурных подразделениях таможни [Текст] / Л. А. Жигун // Вестник Российской таможенной академии. – 2015. – № 3. – С. 30-39.

22. Зубач, А. В. Техническая защита информации: монография [Текст] / А. В. Зубач, Е. А. Пятикова, Л. Л. Хомяков. – М. : Изд-во РТА, 2016. – 86 с.

23. Иванов, Г. И. Организация и современные методы защиты информации [Текст] Г. И. Иванов. − М. : Изд-во РАГС, 2015. – 92 с.

24. Калиновский, К. Б. Критерии оценки безопасности информационных технологий. [Текст] / К. Б. Калиновский. − М., 2016. – 27 с.

25. Козлов, В. И. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Текст] В. И. Козлов // Юридический мир. − 2016. − № 9. – С. 99.

26. Кудаев, П. П. Технические средства и методы защиты информации [Текст] / П. П. Кудаев // Молодой ученый. − 2017. − № 12. − С. 58.

27. Логинова, Е. А. Безопасность информационных технологий [Текст] / Е. А. Логинова // Вестник Нижегородской академии МВД России. − 2017. − № 21. – С. 12.

28. Любкина, Е. О. Техническая защита информации в таможенных органах [Текст] / Е. О. Любкина // Вестник МГОУ. − 2016. − № 4. – С. 23.

29. Марченко, И. Безопасность информационных технологий в таможенных органах [Текст] / И. Марченко // Государственная власть. − 2016. − № 14. – С. 35.

30. Маркушин, А. Г. Безопасность информационных технологий [Текст] / А. Г. Маркушин. − М., 2015. − С. 79.

31. Мухин, И. И. Основы защиты информации в таможенных органах [Текст] : монография / И. И. Мухин. М. : Изд-во РТА, 2015. – 150 с.

32. Николаева, Т. Г. Основы инженерно-технической защиты информации [Текст] / Т. Г. Николаева // Вестник Санкт-Петербургского университета МВД России. − 2016. − № 2. − С. 262.

33. Овчинский, И. В. Организационные, технологические и координационные функции службы защиты информации [Текст] / И. В. Овчинский // Вестник Нижегородского государственного университета. − 2017. − № 3. – С. 115.

34. Опарина, Н. Н. Защита информации в таможенных органах [Текст] / Н. Н. Опарина, Е. А. Панова // Государственное управление. − 2015. − № 48. – С. 42.

35. Орехов, Е. В. Информационной безопасности и технической защиты информации в структурных подразделениях таможни [Текст] / Е. В. Орехов // Вестник МГОУ. − 2016. − № 3. – С. 21−22.

36. Парамонов, А. А. Комплексные системы безопасности и защиты информации в таможенных органах [Текст] : монография / А. А. Парамонов. М. : Изд-во РТА, 2016. – 102 с.

37. Полыхин, А. Л. Специальные требования и рекомендации по технической защите конфиденциальной информации [Текст] / А. Л. Полыхин // Вестник МГОУ. − 2017. − № 1. – С. 67−73.

38. Ревенко, Н. И. Правовые и организационные особенности развития Таможенного союза [Текст] / Н. И. Ревенко // Хозяйство и право. − 2017. − № 3. – С. 25.

39. Старкова, Д. О. Основы таможенного дела. [Текст] / Д. О. Старкова. – М. − 2016. – 15 с.

40. Строгович, М. С. Руководство по защите информации её утечки по техническим каналам [Текст] / М. С. Строгович // Таможенный вестник. − 2017. − № 4. − С. 22.

41. Тимошенко, И. В. Экранирование как способ защиты объектов информатизации от утечки информации по техническим каналам [Текст] / И. В. Тимошенко. – М. 2015. – 18 с.

42. Турчин, Д. А. Основы защиты информации [Текст] / Д. А. Турчин // Таможенный вестник. − 2017. − № 2. – С. 25−29.

43. Федюнин, А. Е. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации [Текст] / А. Е. Федюнин // Молодой ученый. – 2015. − №1. – С. 33.

44. Черныш, А. Я. Организация и современные методы защиты информации [Текст] / А. Я. Черныш. М., − 2017. − С. 76.

45. Шумилова, А. Ю. Основные итоги деятельности Белгородской таможни [Текст] / А. Ю. Шумилова // Таможенный вестник. − 2016. − № 3. – С. 35.