Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение
высшего образования

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт социально – гуманитарных технологий
Направление подготовки «Таможенное дело»
Кафедра истории и философии науки и техники

ДИПЛОМНАЯ РАБОТА

Тема работы
Обеспечение информационной безопасности Таможенных органов РФ

УДК 339.543:004.056

Студент

Группа	**ФИО**	**Подпись**	**Дата**
О-1191	Гайченко Владислав Сергеевич		

Руководитель

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент кафедры ИФНТ	Штанько Марина Александровна	Кандидат философских наук		

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Зав. кафедрой истории и философии науки и техники	Трубникова Наталья Валерьевна	Д.и.н., профессор		

Томск – 2017

Планируемые результаты обучения по ООП

Код результата	Результат обучения (выпускник должен быть готов)	Требования ФГОС, критериев и/или заинтересованных сторон
	Профессиональные компетенции	
Р1	Постоянно повышать уровень профессиональных знаний и компетенций, находить, анализировать и применять необходимую информацию для решения профессиональных задач, владеть навыками использования компьютерной техники, информационных технологий и систем, проводить научные исследования, внедрять научные и инновационные методы и проекты в сфере профессиональной деятельности	Требования ФГОС (ОК -5, 6, ПК-4, 5) Требования заинтересованных работодателей: Томская таможня, Томский таможенный пост
Р2	Контролировать соблюдение участниками ВЭД таможенного, валютного законодательства РФ, достоверность классификации товаров, сведений о происхождении товара, установленных запретов и ограничений при таможенных перемещениях, заявленную таможенную стоимость перемещаемых товаров, правильность исчисления, полноты и своевременности уплаты таможенных платежей, пошлин, взимания пени, процентов, задолженности при осуществлении таможенных операций	Требования ФГОС (ПК-7, 10, 11, 14, 15, 16, 17) Требования заинтересованных работодателей: Томская таможня, Томский таможенный пост
Р3	Владеть навыками применения форм, технологий, средств таможенного контроля товаров, эксплуатации соответствующего современного оборудования и приборов; применять правила интерпретации ТН ВЭД, методы определения таможенной стоимости перемещаемых товаров, выявления фальсифицированного и контрафактного товара	Требования ФГОС (ПК-8, 9, 10, 12, 19) Требования заинтересованных работодателей: Томская таможня, Томский таможенный пост
Р4	Применять навыки заполнения и контроля деклараций и др. таможенной документации, использования в таможенном деле информационных технологий, статистических данных, анализа и прогнозирования поступления таможенных поступлений финансово-хозяйственной деятельности участников ВЭД,	Требования ФГОС (ПК-13,14, 37, 38, 41, 44) Требования заинтересованных работодателей: Томская таможня, Томский таможенный пост
Р5	Выявлять и противодействовать административным злоупотреблениям, правонарушениям, и преступлениям в сфере таможенного дела, совершать для этого юридически значимые действия	Требования ФГОС (ПК - 23, 24, 25, 27, 28) Требования заинтересованных работодателей: Томская таможня, Томский таможенный пост
Р6	Управлять деятельностью таможенных органов и структур, персоналом в таможенных органах, качеством, результативностью и рисками в области профессиональной деятельности, прогнозировать и планировать личную и коллективную профессиональную деятельность; владеть приемами применения СУР в профессиональной деятельности, понимать место ТО в системе госуправления	Требования ФГОС (ПК-29 – 33, 20, 36) Требования заинтересованных работодателей: Томская таможня, Томский таможенный пост
Р7	Применять профессиональные знания для организации и содействия внешнеэкономической деятельности государственных органов, предприятий, фирм, связанной с таможенным перемещением и оформлением; информировать и консультировать участников ВЭД в области таможенного дела, состояния и развития российской и мировой экономики, потенциала таможенных территорий	Требования ФГОС (ПК-4,5, 38, 39, 42) Требования заинтересованных работодателей: Томская таможня, Томский таможенный пост

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт социально-гуманитарных технологий
Направление подготовки (специальность) Таможенное дело
Кафедра истории и философии науки и техники

УТВЕРЖДАЮ:
Зав. кафедрой

_____
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Дипломного проекта

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	ФИО
О-1191	**Гайченко Владислав Сергеевич**

Тема работы:

Обеспечение информационной безопасности Таможенных органов РФ	
Утверждена приказом директора (дата, номер)	

Срок сдачи студентом выполненной работы: Июнь 2017 г.	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе ***(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. д.).***	Объектом исследования является информационная безопасность Таможенных органов РФ. Режим работы – непрерывный. Особых требованию к процессу исследования нет.
Перечень подлежащих исследованию, проектированию и разработке вопросов ***(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).***	Постановка цели и задачи исследования. Выявления предмета и объекта, составление плана работы. Исследованию подлежат нормативные правовые документы обеспечивающие информационную безопасность Таможенных органов. Анализ научной литературы и научных публикаций по вопросу деятельности таможенных органов в сфере обеспечения информационной безопасности государства.

	Виды и формы Таможенной информации. Угрозы обеспечения информационной безопасности Таможенных органов. Методы, способы нарушения информационной безопасности Таможенных органов, исследование профилактики правонарушений.
Перечень графического материала ***(с точным указанием обязательных чертежей)***	Отсутствуют

Консультанты по разделам выпускной квалификационной работы

(с указанием разделов)

Раздел	Консультант
1 Информация и информационная безопасность в современной системе Таможенных органов.	**Штанько М.А.**
2 Способы нарушения информационной безопасности Таможенных органов.	**Штанько М.А.**
3.Практические, институциональные и профилактические основы формирования модели потенциального нарушителя информационной безопасности.	**Штанько М.А.**

Названия разделов, которые должны быть написаны на русском и иностранном языках: Все разделы дипломной работы пишутся на русском языке.

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	**25.10.2016**

Задание выдал руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
доцент кафедры ИФНТ	**Штанько Марина Александровна**	кандидат философских наук		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
О-1191	**Гайченко Владислав Сергеевич**		

Реферат

Выпускная квалификационная работа «Обеспечение информационной безопасности Таможенных органов РФ» 89 с, 61 источник.

Ключевые слова: Информационная безопасность, Национальная безопасность, информационная система, правонарушения, Единая автоматизированная информационная система, электронная цифровая подпись.

Объектом исследования в дипломной работе является информационная безопасность Таможенных органов РФ.

Целью работы является выявление потенциальных угроз и рисков обеспечения информационной безопасности Таможенных органов и предложение путей их решения.

В данном научном исследовании использованы такие методы как анализ (выявление сущностных характеристик системы информационной безопасности и методов ее нарушения), классификация (способствует упорядочиванию видов, типов и форм информационной безопасности), описание (составление целостных формулировок, актуальных для темы научного исследования), моделирование (позволяет сформировать целостную модель системы информационной безопасности) и системный подход (направлен на выявление специфических связей между структурными элементами системы Таможенных органов РФ)

В результате исследования полученные выводы позволяют определить угрозы информационной безопасности Таможенных органов, их виды и методы реализации возможных правонарушений.

Областью применения является сфера информационной безопасности Таможенных органов РФ.

Значимость заключается в Создание эффективной модели потенциального нарушителя информационной безопасности Таможенных органов РФ.

Graduation qualification work "Ensuring Information Security of the Customs Authorities of the Russian Federation" 89 s, 61 source.

Key words: Information security, National security, information system, offenses, Unified automated information system, electronic digital signature.

The object of research in the thesis is the information security of the Customs Authorities of the Russian Federation.

The purpose of the work is to identify potential threats and risks to ensure the information security of the Customs authorities and suggest ways to address them.

In this scientific research, methods such as analysis (identification of essential characteristics of the information security system and methods of its violation), classification (contributes to the ordering of types, types and forms of information security), description (compilation of holistic formulations relevant to the topic of scientific research), modeling (Allows to form an integral model of the information security system) and a systematic approach (aimed at identifying specific links between the structural elements of the si The Customs Authorities of the Russian Federation)

As a result of the research, the findings allow us to identify threats to the information security of the Customs authorities, their types and methods of implementing possible offenses.

The sphere of application is the sphere of information security of the Customs Authorities of the Russian Federation.

The significance lies in the creation of an effective model of a potential infringer of information security of the Customs authorities of the Russian Federation.

Список условных сокращений

1. ВТО – Всемирная торговая организация
2. ВЭД – Внешняя экономическая деятельность
3. ГОСТ - Межгосударственный стандарт
4. ГНИВЦ – Главный научный информационно-вычислительный центр
5. ЕАИС – Единая автоматизированная информационная система
6. ЕАЭС – Евразийский экономический союз
7. НТП – Научно-технический прогресс
8. ПО – Программное обеспечение
9. ТКТС – Таможенный кодекс Таможенного союза
10. ТН ВЭД ТС – Товарная номенклатура внешней экономической деятельности Таможенного союза
11. ФЗ – Федеральный закон
12. ФТС РФ Федеральная таможенная служба Российской Федерации
13. ЦВК – Центральный вычислительный комплекс
14. ЧС – Чрезвычайные ситуации
15. ЭД – Электронное декларирование товаров и транспортных средств
16. ЭЦП – Электронная цифровая подпись

Оглавление

Введение

Актуальность. В современных условиях научно - технического прогресса, ускорения темпов мировой глобализации и информатизации общества увеличиваются и угрозы обеспечения информационной безопасности, в том числе, и в Таможенных органах. Данным структурам необходимо эффективно противодействовать различным информационным угрозам для обеспечения национальной безопасности страны и для качественного функционирования собственной системы. Из информации таможенной службы о правоохранительной деятельности таможенных органов Российской Федерации за 2015 и 2016 года видно, что правонарушения в сфере информационной безопасности (электронного декларирования) увеличились. Происходит качественная трансформация видов угроз информационной безопасности Таможенных органов и методов борьбы с ними. Подобные изменения проявляются, главным образом, в том, что на смену традиционным физическим и радиоэлектронным методам приходят новые информационные методы нарушения информационной безопасности Таможенных органов. Кроме того на сегодняшний день почти отсутствует эффективная система профилактики предотвращения нарушений в области информационной безопасности Таможенных органов, так как существовавшие ранее формы противодействия были основаны на законодательной и криптографической базе. В современных условиях преобладания информационных методов нарушения информационной безопасности традиционная система профилактики перестает быть эффективной.

Следует также отметить, что значимость и актуальность проблемы обеспечения информационной безопасности закреплена в списке приоритетных задач Таможенных органов и в Стратегии развития Таможенной службы до 2020 г. Именно п.8 настоящей Стратегии включает в себя следующую задачу: «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, актуальность темы данной исследовательской работы трудно недооценить.

Степень теоретической разработанности проблемы. При написании данной научной работы использовал различные источники, которые условно можно разделить на несколько групп.

К первой группе относятся источники нормативно - правовой базы такие как: Конституция РФ, ТК ТС, Стратегия развития ФТС до 2020 года, Положения правительства, ФЗ, доктрины регулирующие порядок обеспечения информационной безопасности в Российской Федерации. Такого рода материалы были необходимы для анализа правовой составляющей проблемы информационной безопасности в Таможенных органах современной РФ.

Ко второй группе относится научная литература, которая посвящена основным характеристикам информационной безопасности как проблеме в мире в целом, и в системе Таможенных органов в частности. Это работы таких авторов как А.Г. Ревин, В.И. Лапин – учебное пособие по информационному праву, Шушков Г.М., Сергеев И.В. - концептуальные основы информационной безопасности Российской Федерации. Так же во внимание были взяты статистические данные с официального сайта ФТС РФ.

Третью группу источников составляют работы, позволяющие проанализировать существующие способы нарушения информационной безопасности и основные меры борьбы с ними. Такие авторы, как Малюк А.А. «Угрозы информации и информационные угрозы. Подготовка кадров в области информационной безопасности», Жбанкова В.А. «Обеспечение экономической безопасности правоохранительными подразделениями таможенных органов», информация с Интернет портала Электронной цифровой подписи в РФ дают подробное описание имеющимся на

сегодняшний день возможностям противодействия методам незаконного получения таможенной информации.

Еще одна группа – четвертая, включает в себя специальную литературу, позволяющую проанализировать плюсы и минусы электронного декларирования, институциональной системы Таможенных органов и профилактических мер, направленных на обеспечение информационной безопасности. К этой группе можно отнести работы таких авторов, как Высотина О.А., Гончарова К.А «Электронное декларирование».

В особую группу, считаем необходимым выделить справочно-методические материалы о устройстве технических средств защиты информации таможенных органов и их электронных систем, а также источники, которые позволили выявить сущность модели и особенностей ее формулирования. Это работы таких авторов, как Шаньгин В.Ф. «Защита информации в сети — анализ технологий и синтез решений», Лопатин В.Н. «Информационная безопасность России».

На основании всего вышесказанного, можно сделать вывод о том, что основная часть научных изысканий по теме «Информационное обеспечение безопасности Таможенных органов» посвящена анализу собственно информационной безопасности и способам ее обеспечения, которые основаны на особенностях уже совершенных правонарушений в этой области. Думается, что принципиальное значение имела такая модель обеспечения информационной безопасности Таможенных органов, которая была бы основана на преобладании превентивных (предупреждающих, упреждающих) мер (способов).

Таким образом, **цель** данного научного исследования – разработать эффективную модель обеспечения информационной безопасности Таможенных органов. Для достижения поставленной цели необходимо решить следующие **задачи**:

1. проанализировать значение и сущность информации как объекта обеспечения информационной безопасности в современном мире;

2. охарактеризовать основные способы нарушения информационной безопасности;
3. изучить особенности применения методов нарушения информационной безопасности Таможенных органов на базе Единой автоматизированной информационной системы;
4. выявить особенности обеспечения информационной безопасности Таможенных органов в рамках Таможенного союза и определить основные виды информации которые могут быть объектом потенциального нарушения;
5. охарактеризовать электронное декларирование как практическую основу эффективной модели выявления нарушителя информационной безопасности в системе Таможенных органов РФ
6. охарактеризовать институциональную основу эффективной модели выявления нарушителя информационной безопасности в системе Таможенных органов РФ
7. выделить модель потенциального нарушителя как профилактическую основу эффективной модели выявления нарушителя информационной безопасности в системе Таможенных органов РФ.

Объектом данного исследования является информационная безопасность Таможенных органов РФ.

Предметом исследования являются способы обеспечения информационной безопасности Таможенных органов РФ.

В данном научном исследовании будут использованы такие **методы** как анализ (выявление сущностных характеристик системы информационной безопасности и методов ее нарушения), классификация (способствует упорядочиванию видов, типов и форм информационной безопасности, способов ее нарушения и предотвращения), описание (составление целостных формулировок, актуальных для темы научного исследования), моделирование (позволяет сформировать целостную модель системы информационной безопасности) и системный подход (направлен на

выявление специфических связей между структурными элементами системы Таможенных органов РФ)

В структурном отношении работа состоит из введения, трех глав, заключения и списка литературы.

Научная новизна данной работы основана на разработки нового способа профилактики таможенного нарушения в области информационной безопасности. На основании проведенного анализа имеющихся материалов об основных видах правонарушениях в системе информационной безопасности Таможенных органов, а так же на основании их целей и задач, можно смоделировать возможного правонарушителя. Соответственно это позволит контролировать деятельность такого рода потенциальных нарушителей и предупреждать возможные правонарушения.

Практическая значимость данной дипломной работы заключается в том, что ее материалы могут быть использованы таможенной службой для разработки способов профилактики правонарушений в области обеспечения информационной безопасности Таможенных органов РФ. Данную модель, возможно, внедрить в Систему управления рисками Таможенных органов путем доработки профилей рисков. Внедрение данной модели в систему таможенных органов поможет повысить обеспечение информационной безопасности Таможенных органов РФ, что в свою очередь положительно скажется на национальном благосостоянии страны.

Глава 1. Информация и информационная безопасность в современной системе Таможенных органов

1.1 Значение и сущность информационной безопасности

Обеспечение информационной безопасности таможенных органов Российской Федерации регулируется различными правовыми актами, которые в совокупности определяют порядок данной деятельности. Информационно-правовая база в РФ в области информатизации и обеспечении информационной безопасности на сегодняшний день состоит из[1]:

- Федеральных законов;
- Положений Конституции;
- Указов президента РФ;
- Распоряжений правительства РФ;
- Подзаконных актов;
- Должностных приказов и распоряжений, и.т.д.

Основные права и свободы граждан Российской Федерации в сфере информатизации определяет ст. 23 Конституции РФ, а конкретно право тайны переписки, телефонных, почтовых, телеграфных и иных переговоров, право на неприкосновенность личной, частной, семейной жизни. Статья 42 Конституции РФ дает гражданину право на получение актуальной и достоверной информации о состоянии жизни и окружающей среды. Права граждан РФ регулируются и Уголовным кодексом РФ. Данные статьи в той или иной мере регулируют вопрос обеспечений информационной безопасности Таможенных органов России:

- Статья 137. Нарушение неприкосновенности частной жизни.
- Статья 138. Нарушение тайны переписки, почтовых, телеграфных и других сообщений, телефонных переговоров.

[1] Консультант плюс Правовая поддержка [Электронный ресурс] / Официальный сайт компании «КонсультантПлюс» // http://www.consultant.ru

- Статья 140. Отказ в предоставлении гражданину РФ информации.

- Статья 155. Разглашение тайны о усыновлении или удочерении.

- Статья 183. Незаконное получение сведений, а также их разглашения, которые составляют банковскую или коммерческую тайну.

- Статья 272. Незаконный доступ к компьютерным данным.

- Статья 273. Распространение, создание или использование вредоносных программных средств для Электронных вычислительных машин.

- Статья 274. Нарушение правил эксплуатации Электронных вычислительных машин, их систем или сетей.

В основополагающих документах регулирующих общественную жизнь граждан России, таких как Конституция РФ, Уголовный кодекс РФ, и др., указаны статьи, на которые ссылаются таможенные органы РФ при обеспечении информационной безопасности. Но в них есть определенные недостатки. Они являются общими, и могут затянуть процесс разбирательства в специфических случаях. Для этих ситуаций как показывает практика проще проработать отдельные документы и положения чем каждый раз вносить изменения в Конституцию РФ.

Для своевременного решения возможных проблем в сфере регулирования правовой деятельности по вопросам информационной безопасности, Правительством РФ разрабатываются определенные стратегии и доктрины.

Документ, содержащий в себе основные принципы, цели и задачи для обеспечения информационной безопасности РФ – «Доктрина информационной безопасности Российской Федерации». Утверждена президентом РФ от 9.09.2000 года.

Этот документ на многие годы определяет политику государства в области обеспечения информационной безопасности РФ. Определяет порядок и цели обеспечения улучшения методологического, правового, организационного и научно-технического обеспечения информационной

безопасности РФ. Прорабатывает различные программы обеспечения информационной безопасности РФ.

Данная доктрина способствует развитию Концепции национальной безопасности Российской Федерации, относящейся к информационной деятельности. Так спустя два года, в январе 2002, Правительством РФ была принята целевая федеральная программа под названием «Электронная Россия», на срок 8 лет (2002 – 2010 годы). Программа основывалась на:

- Характеристики проблемы
- Выработкой целей, задач, этапов и методов решения.
- Выработка механизмов реализации программы.
- Оценка проделанной работы.

После успешного завершения данной программы, ей на смену был выработан следующий этап. Это целевая государственная программа Российской Федерации «Информационное общество» сроком с 2011 года по 2020 год.

Ответственность за выполнение данной концепции лежит на министре связи и массовых коммуникаций Российской Федерации. Цель реализации данной программы выработать способы взаимодействия государства с обществом в информационной среде, а так же проработать различные административно правовые акты, которые будут регулировать данный процесс. Стоит отметить что «Информационное общество», как программа, разрабатывалась на основе различных международных документов и соглашений (Декларации о построении всемирного общества, положения окианавской хартии, и др.), а также с учетом внешней политики страны и интересов различных международных субъектов. Это позволяет делать прогнозы об упрощении процедуры интеграции информационного общества в систему международных отношений.

На сегодняшний день политика в области обеспечении информационной безопасности таможенных органов РФ определяется

«Стратегией развития таможенной службы до 2020 года». Это основной вектор политики таможенной службы на ближайшее время.

Конкретными инструментами правового регулирования определенных процессов информационной безопасности являются Федеральные законы. Они максимально подробно регламентируют определенную процедуру, с максимальной проработкой данного процесса. Следующие Федеральные законы регулируют правовую деятельность обеспечения информационной безопасности таможенных органов:

1. ФЗ №149 от 27 июля 2006 «Об информации, информационных технологиях и защите информации».
2. ФЗ №63 от 10 июля 2012 «Об электронной подписи, электронной цифровой печати»

С точки зрения рассмотрения вопроса со стороны обеспечения информационной безопасности, информационно технической политики государства о правового обеспечении стоит обратить внимание на Решение президента РФ и Правительства РФ.

1. Стратегия развития информационного общества РФ (Утверждено президентом РФ от 7.02.2008).
2. «Концепция формирования электронного правительства в РФ до 2020 года» (утверждено правительством РФ от 6.05.2008)
3. Федеральная целевая программа «Электронная Россия» (Утверждено правительством РФ от 28.01.2002)

На сегодняшний день перед таможенными органами стоит задача унификации и объединения правовых инструментов не только в рамках правового поля РФ, но и Таможенного союза. У Российской таможни уже сделаны несколько шагов в данном направлении. Например, РФ в 2010 году присоединилась к Киотской конвенции об упрощении и гармонизации таможенных процедур. В ней закреплена возможность подавать декларацию на товары в электронном виде и использовать информационные технические средства при необходимости. Российская федерация, придерживаясь данных

принципов, упрощает процедуру возможной интеграции таможенных органов с субъектами мировой торговли. Ведь на данный момент проблемой обеспечения информационной безопасности таможенных органов с правовой стороны можно выделить как ее отсутствие в Таможенном союзе. Нет наднационального законодательства, которое бы регулировало данный процесс.

Определяя тип информации, который может быть объектом потенциального правонарушения необходимо провести анализ понятия термина информационная безопасность.

Термин «Информационная безопасность» — это состояние сохранности и защищённости информационных ресурсов государства, прав и свобод личности и общества в информационной среде[2]. Ее можно разделить на два вида: Информационно-техническая безопасность и информационно-психологическая безопасность. В первом случае берется под внимание искусственно созданный человеком мир, например, технологии и.т.д. Во втором – сам человек и мир живой природы.

Следует отметить, что точную дату появления термина «Информационная безопасность» никто не может сказать, так как оно уходит далеко в прошлое. Это связанно с тем, что даже на ранних этапах развития человечества существовала потребность людей в защите. Вместе с тем можно выделить основные исторические этапы формирования информационной безопасности[3]. Основанием для данной классификации является специфика средств защиты информации. По мере их развития – развивается и система информационной безопасности.

Первый этап - начальный. В период до 1916 года для обеспечения информационной безопасности использовались средства коммуникации данного периода времени. Основной задачей было защита сведений о фактах,

[2] Понятия информационной безопасности и угрозы национальной безопасности в информационной сфере [Электронный ресурс] / М.А. Лапина, А.Г. Ревин // http://jurisprudence.club/informatsionnoe-pravo_703/ponyatiya-informatsionnoy-bezopasnosti-ugrozyi.html

[3] Этапы развития информационной безопасности [Электронный ресурс] / Программирование и визуализация// http://life-prog.ru/1_46301_etapi-razvitiya-informatsionnoy-bezopasnosti.html

событиях, местонахождении и т. д, которые имели жизненной значение для человека или общества.

Второй этап - технический. С 1916 года, когда начались активно использоваться технические средства электро и радиосвязи, начинается второй этап развития информационной безопасности, на котором защита осуществляется при помощи данных средств.

Третий этап – акустиколокационный, который берет свое начало с 1935 года. Обусловлено это появлением гидроакустических и радиолокационных средств связи. Основой информационной безопасности в данный период времени было организационно-техническое регулирование мер на повышение эффективности радиосвязи.

На четвертом вычислительном этапе, который начался с 1946 года с появлением первых Электронно-вычислительных машин (ЭВМ) начинаются проблемы информационной безопасности в области ограничения доступа к ЭВМ.

Пятый этап – сетевой, начинается с 1965 год. В этот период были созданы первые информационно локальные сети. Проблема безопасности также, как и на прошлом этапе имела решения с ограничением доступа к сетевым ресурсам.

Шестой этап - мобильный. Использование сверхкоммуникальных мобильных устройств началось в 1973 году. Для обеспечения информационной безопасности с беспроводными сетями передачи данных потребовались новые подходы, так как угроза стала более серьезной. В этот период начинает появляться такая угроза как Хакерство. Хакер – это сообщество людей, цель которых нанесение ущерба информационной безопасности государству, организации и отдельным людям. В этот период государство признает информационный ресурс одним из важнейших и ставит задачу обеспечения его безопасности на уровне национальной. Так же формируется отрасль международной правовой системы Информационное право.

На седьмом глобализационном этапе, который берет свое начало с 1985 года, начинают создаваться глобальные информационные сети. Помимо всего выше в этот период используются космические средства обеспечения информационной безопасности. Исходя из прогноза международных аналитических компаний следует, что последующие этапы информационной безопасности будут связаны с развитием научно технического процесса в мире и с движением мировой глобализации[4].

Проанализировав данные этапы, можно сделать вывод, что на развитие информационной безопасности оказали существенное влияние такие факторы как необходимость защиты жизненно важных сведений о человеке и обществе, развитие НТП и процессы глобализации общества.

В любой отрасли системы, как и в таможенной службе, для описания технологии информационной безопасности выстраивается политика информационной безопасности. То есть направление деятельности таможенных органов ориентированное на защиту национальных интересов страны способом обеспечения информационной безопасности. Термин политики информационной безопасности говорит о совокупности задокументированных правил и процедур, практических и теоретических принципах руководства информационной безопасностью, которых придерживается организация в своей деятельности[5]. Другими словами, это распределение различных средств с учетом прогноза для поддержания контроля безопасности.

Политика информационной безопасности включает в себя несколько направлений защиты информационной системы: управление системой защиты информации, защита объектов информационной системы, защита каналов связи, избежание электромагнитных излучений и чрезвычайных ситуаций.

---

[4] Информационный взрыв продолжается [Электронный ресурс] / Идеи и практики автоматизации // https://www.pcweek.ru/idea/article/detail.php?ID=123306

[5] Политика информационной безопасности [Электронный ресурс] / Компания «Альтернативные решения» // http://www.arinteg.ru/articles/politika-informatsionnoy-bezopasnosti-27713.html

Политика информационной безопасности по каждому из вышесказанных направлений, должна описывать следующие этапы создания средств защиты информации[6]:

1. Точное определение Технических и информационных ресурсов, которые подлежат защите;
2. Выявление всех возможных каналов утечки информации и потенциально возможных угроз;
3. Оценка всех выявленных каналов утечки информации и потенциально возможных угроз;
4. Определение требований к системе защиты;
5. Соответствующий выбор определенных средств защиты информации;
6. Внедрение в использование выбранных мер и средств защиты информации;
7. Осуществление контроля за управление системы защиты и ее целостности.

Политика информационной безопасности имеет ряд задокументированных требований к информационной системе. Исходя из национального стандарта РФ «О методах обеспечения информационной безопасности» документы подразделяют по уровню детализации процессов защиты информации. В свою очередь эти документы можно разделить на три уровня: верхний, средний, нижний[7].

Верхний уровень документов политики информационной безопасности отражают действия определенной организации в области защиты информации, а также ее стремления соответствовать требованиям в этой же

[6] ГОСТ Р ИСО/МЭК 13335-1-2006 Библиографическая ссылка. Национальный стандарт РФ. М., 2006. 22 с. (Методы и средства обеспечения безопасности)
[7] ИСО/МЭК 17799, ИСО/МЭК 13335-4 Библиографическая ссылка. Национальный стандарт РФ. М., 2006. П. 2. (Термины и определения)

области на государственном и международном уровне. Это такие документы как концепции, технические стандарты, регламенты управления и.т.д[8].

Документы среднего уровня политики информационной безопасности это отдельный аспект информационной безопасности. Зачастую это требования и порядки действий на создания средств обеспечения информационной безопасности. Например, это обеспечение информационной безопасности бизнес процессов и организация конкретных направлений защиты информации. Также стоит сказать, что все документы среднего уровня создаются в виде внутренних документов организаций и как правило они конфиденциальны.

Что касается нижнего уровня политики информационной безопасности, так это документы, касающиеся руководства эксплуатации, регламентом работ различных руководств сервисов информационной безопасности.

Стоит сказать несколько слов и о организационной защите объектов информатизации. Это взаимоотношений исполнителей и регламентация производственной деятельности на правовой основе, которое исключает либо затрудняет незаконное овладение секретной информацией и появлением внешних и внутренних угроз. Виды деятельности, которые обеспечивает организационная защиты, можно разбить на несколько пунктов:

1. Организация режима, охраны, работа с документами, с кадрами;
2. Использование технических средств обеспечения информационной безопасности и аналитическую деятельность для выявления внешних и внутренних угроз;

К организационным мероприятиям можно отнести:

1. Организация режима и охраны, цель которых исключения проникновения на территорию посторонних лиц;
2. Организация работы с сотрудниками, целью которой является подбор персонала, его проверкой, обучениям правил работы с секретной

[8] Формирование политики информационной безопасности [Электронный ресурс] / Менеджмент в сфере информационной безопасности // http://rfcmd.ru/sphider/docs/InfoSec/GOST-R_ISO_IEC_13335-1-2006.htm

информацией и ознакомление с мерами ответственности за нарушение правил защиты информации;

3. Организация работы с документами и различной информацией. Сюда также включается порядок использование секретных документов и носителей, их отчетность, хранение и порядок уничтожения.

4. Организация использования технических средств обработки, сбора и хранения секретной информации;

5. Организации работы относительно анализа внутренних и внешних угроз, а также разработка мер по их преодолению;

6. Организации работы проведения контроля и проверок персонала, которые имеют доступ к секретной информации.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, которое заключается на обеспечение безопасности информации в конкретных условиях.

Таким образом, можно сделать вывод о том, что таможенные органы делают акцент на защите прав и свобод государства и общества, в рамках информационной безопасности. Здесь стоит даже сказать, что она приобретает большую значимость, так как ее обеспечение является национальной задачей.

1.2 Информация как объект правонарушения в системе Таможенных органов

В современном мире наблюдается тенденция огромного потока увеличения информации. Научно технический прогресс и эволюция общества в целом от части 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[9]:

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

- обеспечение информационной безопасности для целей своего нормального функционирования(эффективность управления, взаимодействия).

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.

Таможенная служба Российской Федерации является одной из крупных таможенных служб мира. Численность сотрудников составляет около 70ти тысяч человек. Также включает в себя 11 региональных таможенных управлений, 136 таможен, 708 таможенных постов, и это не включая таких служб как экспертные лаборатории, учебные заведения вычислительные центры и многих других служб находящихся под ведомством ФТС[10]. Все звенья системы являются федеральными и не подчиняются органам государственной власти субъектов РФ, органам местного самоуправления и общественным объединениям. Каждый

[9] Обеспечение информационной безопасности таможенных органов РФ [Электронный ресурс] / Таможенный брокер // http://brokert.ru/material/informacionnaya-bezopasnost-tamozhennyh-organov

[10] Система таможенных органов России: основные функции и принципы их взаимодействия [Электронный ресурс] / Таможенное дело // http://studme.org/159701227784/ekonomika/sistema_tamozhennyh_organov_rossii_osnovnye_funktsii_printsipy_vzaimodeystviya

нижестоящий таможенный орган подчинен по вертикали только вышестоящим таможенным органам, контролирующим его деятельность.

В соответствии с данной структурой 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 с верху вниз построен следующим образом[11]:

1.Центральное информационно техническое таможенное управление.

2.Информационно техническая служба

3. Таможенный инспектор информационно технической службы.

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. Например, правоохранительная деятельность. Зачастую бывает, что необходимая при обмене информация теряется, не соответствует требованиям, является неактуальной, а также ее могут воспользоваться незаконно. И вместо того чтобы таможенным органам работать совместно для предотвращения или пресечения правонарушений. Они вынуждены, занимается сбором информации, что влияет на эффективность их работы.

Такая проблема существует не только по вопросам правоохранительной деятельности, во внимание берется любое информационное взаимодействие.

[11] Структура таможенных органов Российской Федерации [электронный ресурс] / Альта Софт: Онлайн справочник // https://www.alta.ru/tam/struct/

Одной из причин вышесказанной проблемы может считаться недостаточное обустройство таможенных органов техническими средствами связи и автоматизированными системами. Хотя, исходя из стратегии развития таможенной службы, на данную причину сделан акцент, и до 2020 года планируют вывести систему информационно технического обеспечения и обустройства таможенной службы на новый уровень. Но научно-технический прогресс не стоит на месте, и соответственно цели, поставленные таможенной службой в 2012 году уже сегодня перестают быть актуальными. Не стоит также забывать о большой разнице в уровне инфраструктурно-технического развития регионов. В качестве примеров можно привести, например Московские таможенные посты и Томские таможенные посты. В техническом оснащении таможенных постов большая разница, это соответственно влияет на эффективность передачи и обеспечения информации.

Таким образом, можно сделать вывод о том, что к внешнему виду относится вся информация для обеспечения национальной безопасности страны. Это может быть любая информация, например, из таможенной декларации, статистических сборников, СМИ и др., которая будет угрозой экономической, социальной, территориальной обстановкой в стране. К внутренним видам относятся информация необходимая для качественного функционирования самой таможенной службой. Это может быть данные служебных переписок, информация внутренних распоряжений, любая информация, которая сможет повлиять на работу таможенных органов.

1.3 Особенности информационной безопасности в рамках Таможенного союза

Обеспечение информационной безопасности в рамках Таможенного союза является задачей обеспечения национальной безопасности страны. В настоящее время организация информационной безопасности не строится на

наднациональным контролем в Таможенном союзе. Каждая страна участница обеспечивает его на своей территории в соответствии со своим законодательством. В связи с этим необходимо четкое взаимодействие таможенных органов Таможенного союза для формирования единых принципов и критериев защиты информации Таможенных органов.

Для определения видов информации являющиеся объектом потенциального нарушения информационной безопасности таможенных органов в рамках Таможенного союза необходимо выявить:

1. Цели взаимодействия;
2. Тип информации перемещающийся;
3. Порядок передачи данных.

Исходя из статьи 124 Таможенного кодекса Таможенного союза таможенные органы используют обмен информации для задач связанных с контролем перемещаемых товаров, соблюдением законодательство стран участниц Таможенного союза[12]. В данной статье прописано законодательно, что обмен информации для обеспечения таможенного контроля после выпуска товаров, является задачей всех стран.

Еще одной нормативной составляющей этого процесса является соглашение о взаимной помощи между таможенными службами Таможенного союза[13]. В данном соглашении прописан порядок и метод обмена информацией. Она осуществляется путем электронной или письменной формой передачи данных, которые формируются с помощью запросов участников Таможенного союза, либо по собственной инициативе в рамках взаимопомощи. Также обмену подлежат документы и необходимые нормативные акты, которые требуются для производства дел.

Таможенные службы стран участников Таможенного союза, а конкретно России, Белоруссии и Казахстана, вместе принимают состав

[12] ТК ТС, Статья 124. Обмен информацией между таможенными органами
[13] Приказ Федеральной таможенной службы от 9 декабря 2011 г. № 2490 “Об утверждении Инструкции о порядке подготовки и исполнения международных запросов, не относящихся к делам об административных правонарушениях и не связанных с проведением оперативных проверок”

данных, который необходим для информационного обмена. Кроме того ведется работа в рамках стандартизации технических средств и порядка обмена информации. Формируют следующие сведения для документального запроса[14]:

1. Несоответствие сведений о товарах и транспортных средств;
2. Информация о возможном нарушении таможенного законодательства, какого либо участника Таможенного союза;
3. При применении таможенным органом страны участника Таможенного союза таможенного контроля.

Таможенными органами может быть сформирован запрос, не исходя из данного списка, а при наличии других законных оснований.

Для получения необходимой информации таможенные органы формируют запрос в письменном виде, и относят на подпись своему начальнику. Разрешается пользоваться при формировании запросов электронной почтой с защищённым каналом связи. Однако для отчетности все равно таможенным службам необходим посменный запрос, который позднее отправляется почтой.

В пункте третьем статьи 6 Соглашения о взаимной помощи подробно расписаны сведения, которые должны быть отражены в формируемом запросе. Сам запрос должен быть рассмотрен в течение одного месяца с момента его получения. Если существует необходимость более короткого срока, то участники таможенного союза имеют право договорится о них в устном порядке. Точно также они договариваются если срока не хватает для предоставления информации. Если таможенный орган не имеет необходимых запрашиваемому сведений, то он имеет право на их получение в соответствии со своим законодательством. Важным моментом данной

[14] Соглашение о взаимной административной помощи
таможенных органов государств-членов таможенного союза от 21 мая 2010 г.

процедуры является то, что взаимодействие между таможенными службами налажено на устном уровне, что не позволяет затормозить процесс проверки.

Запрашиваемый таможенный орган в ответ на запрос, предоставляет следующие сведения[15]:

1. Документы и сведения, которые были запрошены;
2. Данные о проведении таможенного контроля и всех необходимых мероприятий;
3. Любые документы и сведения, с помощью которых могут быть принято решения запрашиваемым.

Существуют также и основания отказа таможенным органам в предоставления информации. Этот вопрос регулируется восьмой статьей соглашения о взаимной помощи.

В первую очередь во внимания берут данные, которые могут способствовать нарушению законодательства страны участника Таможенного союза. Например, таможенная служба России запрашивает у таможенной службы Белоруссии сведения, которые могут быть поводом нарушения законодательства одной из стран участниц Таможенного союза, в том числе и Российского. Естественно, что Белоруссия отклонит данный запрос.

Развитие взаимоотношений между странами участниками Таможенного союза в области обмена информацией закреплено в соглашении о требовании к обмену данными, от 10.05.2010. В нем установлено, что не вся информация может подлежать обмену. Особые ограничения введены к данным касающимся государственных тайн. К ним могут относиться любые сведения как налоговые, банковские так и государственные. Разумеется, что информация такого рода может перемещаться, в случаи гарантии запрашиваемого ее защите. Запрашиваемые таможенные органы обязуются, сохранять полученные им данные, не

[15] Соглашение о взаимной административной помощи таможенных органов государств-членов таможенного союза от 21 мая 2010 г.

передавать их третьим лицам, если на то не существует согласия государства предоставившего ее в письменном виде.

Обязанности таможенных органов и различных государственных органов[16]:

1. Обеспечивать бесперебойность предоставления необходимой информации;

2. Своевременное обеспечение запрашиваемого органа о невозможности предоставления необходимых данных.

В случаи прегрешения предоставления информации таможенным органам странам участникам Таможенного союза, предоставлявший орган обязан проинформировать их не ранее шести месяцев. Данное уведомления передается в письменном виде со всеми необходимыми подписями и печатями.

В рамках взаимодействия таможенных служб Таможенного союза существует соглашение о обмене предварительной информации. Его суть направлена на сокращения таможенных рисков в случаи несоблюдения таможенного законодательства, а так же унификация таможенных операций и повышение качества таможенного контроля. Заинтересованным лицам предоставляется порядок передачи таможенным органам Таможенного союза предварительной информации о[17]:

1. Товарах и транспортных средствах;
2. Время прибытия и место прибытия товаров;
3. Информацию о пассажирах;
4. Иная информация, интересующая таможенные органы Таможенного союза.

Для удобства предоставления необходимых данных таможенная служба пользуется специальными техническими средствами и

[16] Федеральный закон от 27.11.2010 N 311-ФЗ (ред. от 28.12.2016) "О таможенном регулировании в Российской Федерации"
[17] Соглашения «О представлении и об обмене предварительной информацией о товарах и транспортных средствах, перемещаемых через таможенную границу таможенного союза» 0т 27 ноября 2009 г.

информационными технологиями. Это предусмотрено статьей 124 Таможенного кодекса Таможенного союза и седьмой главой Киотской конвенции, которая тоже предусматривает информационный обмен в рамках развития внешней торговли[18]. Исходя из этих положений комиссией Таможенного союза было принято решение о создании соглашения об обмене информации для аналитических функций таможенных органов.

Организация информационного обеспечения безопасности в рамках взаимодействия между таможенными службами Таможенного союза построена эффективным способом. Организация информационного обеспечения Таможенных органов строится не на наднациональном уровне, поэтому необходимость взаимодействия просто необходима. Еще более важным моментом при взаимодействии таможенных служб Таможенного союза считается то, что при запросе необходимых данных все службы прекрасно понимают цели и важность данных запросов. Работа налажена практически в устном формате, и зачастую письменные документы необходимы лишь для отчетности.

Проанализировав порядок передачи информации в рамках Таможенного союза, были выявлены типы информации, являющиеся потенциально возможными объектами таможенных правонарушений. Это любые данные о возможном нарушении таможенного законодательства, какого либо участника Таможенного союза, сведения таможенной статистики Таможенного союза и о применении таможенного контроля. Это наиболее, с точки зрения угрозы обеспечения информационной безопасности Таможенных органов, важные виды информации которые могут быть объектом правонарушения.

[18] Международная конвенция от 18 мая 1973 года «Об упрощении и гармонизации таможенных процедур»

1.4 Информационная безопасность Таможенных органов РФ в системе международного сотрудничества

Еще одной угрозой для информационной безопасности Таможенных органов РФ является информационный обмен с иностранными государствами. Правовой базой обеспечения такого рода безопасности можно назвать Киотскую конвенцию и Таможенный кодекс Таможенного союза. Киотская конвенция предполагает информационный обмен между таможенными службами иностранных государств как основу унификации и гармонизации таможенный процедур[19].

Таможенный кодекс Таможенного союза описывает порядок информационного обмена между таможенными органами иностранных государств и стран участниц Таможенного союза, тем самым давая возможность регулировать данную процедуру на национальном уровне. Способом же такого взаимодействия является заключение международных договоров.

По информации Федеральной таможенной службы РФ на первую половину 2016 года было разработано и подписано 19 международных актов. В их число входит[20]:

- 5 меморандумов;
- 10 Международных договоров;
- два плана и программа взаимодействия с более чем 11ти странами.

На сегодняшний день ведется работа по предотвращению правонарушений при перемещении товаров и транспортных средств воздушным транспортом. Данные договора разрабатываются на

[19]Международная конвенция от 18 мая 1973 года «Об упрощении и гармонизации таможенных процедур»
[20]Итоговый доклад о результатах и основных направлениях деятельности ФТС России в 2016 году [Электронный ресурс] / ФТС РФ: Официальный сайт // http://www.customs.ru/index.php?option=com_content&view=article&id=24865:-2016-&catid=475:2015-03-12-09-57-15&Itemid=2588

межведомственном уровне с такими странами как Германия, Франция и Япония[21].

К тому же на данный момент уже существуют проработанные договора по вопросам информационного обмена предварительной информации о товарах и транспортных средств, требующие согласования сторон.

Как видно обеспечение информационной безопасности таможенных органов РФ регулируется совокупностью различных правовых актах основными, которых являются международные договора. Их работа направлена на различную деятельность например получение предварительной информации о товаре, совместная работа по предупреждению возможных нарушений законодательств. То есть их деятельность направлена на соблюдения внутренних законодательств и унификацию таможенных процедур.

Еще одним инструментом в обеспечении информационной целостности в процессе взаимодействия иностранных государств является представитель таможенной службы РФ за рубежом[22]. Он необходим для эффективного осуществления международных отношений Федеральной таможенной службы России. Данные представители являются сотрудниками ФТС России. Их штатная численность за рубежом варьируется от одного человека до нескольких десятков. Это зависит в первую очередь от уровня взаимодействия иностранного государства с таможенной службой России, от значимости интересов их интересов, а также от количества международных договоров, подписанных между двумя странами. В качестве примера приведу два разных Таможенных представительства в таких странах как Латвия и Белоруссия. Торговое взаимоотношение между Российской федераций и Латвией находится не на высоком уровне. В связи с этим фактором

[21] Международное сотрудничество Российской Федерации в области таможенного дела [Электронный ресурс] / Таможенное право // http://lib.sale/tamojennoe-pravo-uchebnik/mejdunarodnoe-sotrudnichestvo-rossiyskoy-34122.html

[22]Общая информация о представителях таможенной службы Российской Федерации за рубежом [Электронный ресурс] / ФТС РФ: Официальный сайт // http://www.customs.ru/index.php?option=com_content&view=article&id=22293:2015-12-15-06-49-51&catid=179:2011-03-25-06-42-48&Itemid=2088

представитель Таможенной службы РФ имеет возможность эффективно работать и взаимодействовать не только с таможенной службой Латвии, но и с другими вблизи лежащими странами, такими как Эстония и Литва. Тем самым один представитель Таможенной службы РФ эффективно выполняет свои задачи в данном регионе. Что касается в Республике Беларусь торговые отношения между нашими странами на достаточно высоком уровне, в соответствии с этим Таможенное представительство насчитывает численность около нескольких десятков человек. Ко всему прочему, несмотря на Таможенное представительство в Минске, их сотрудники рационально распределены по таким городам как Гомель, Брест, Витебск, Гродно.

Таможенные представительства РФ выполняют огромный спектр задач в том числе и обеспечение информационной безопасности таможенных органов. Основной целью считается представлений национальных интересов России и исполнение поручений руководства Федеральной таможенной службы РФ.

Если попробовать проанализировать данную цель, то мы сможем выделить ее составляющие подцели, которые в свою очередь, будучи охарактеризованными, укажет нам на инструменты обеспечения информационной безопасности таможенных органов РФ.

1. Налаживание контактов, организация сотрудничества и взаимодействия с таможенными органами данной страны.

В данном случаи имеется в виду организация работы и подготовка необходимых документов и соглашений. Здесь отчетливо видно как прорабатывается порядок передачи информации и закрепляется в правовом и практическом поле. Представитель Таможенной службы РФ налаживает связь с таможенной службой иностранного государства, договариваясь о процедуре и порядке связи, и обговаривают данные, которые будут переданы друг другу. Это очень важный момент организации взаимодействия, таможенные органы разных стран находясь на расстоянии друг с другом, с

помощью представителя Таможенной службы имеют возможность проводить связь без посредников не боясь за сохранность информации.

2. Второй подцелью организации работы представителя Таможенных органов РФ является, сбор и анализ актуальной информации о состоянии таможенной ситуации в данной стране.

Здесь представитель Таможенных органов РФ изучает имеющуюся обстановку в стране в плане правовой системы, возможного изменения законодательства. Исследуется таможенный опыт данной страны, возможности и технологии. Вся проводимая работа снабжает ФТС РФ необходимой актуальной информацией от надежного источника.

3. Обеспечение экономической безопасности и национальных интересов Российской Федерации.

Представители Таможенных органов РФ проводят анализ внешнеторговых отношений между Россией и иностранной страной, выделяют возможные проблемы и пути их решений в данной области. Также он учувствует в правоохранительной работе по предотвращению нарушений таможенного законодательства двух стран, путем координации действий, курирования и мониторинга.

4. Представитель Таможенной службы координирует деятельность участников ВЭД, активно сотрудничает с ними. При необходимости оказывает им помощь исходя из своей компетенции.

Разбираясь в сути данной подцели можно сделать вывод, что представитель Таможенной службы РФ сильно интегрируется в деловую и административную деятельность иностранной страны. Соответственно данные представительства вынуждены адаптироваться к определенным условиям. Необходимо брать во внимание такие условия как менталитет страны, национальный язык и отличительные особенности законодательной системы. В качестве примера можно привести особенности в некоторых странах. Например, в Японии из-за частой смены должностных лиц представителям Таможенных органов РФ приходится постоянно выстраивать

новые связи взаимодействий. Что касается стран Евросоюза, например Бельгии, то необходимость о сотрудничестве рассматривается над национально, Еврокомиссией. Бельгия имеет право заключать договора и различные соглашения только с разрешения Еврокомиссии либо на определенные полномочия. В соответствии представителю Таможенных органов РФ приходится выстраивать работу по взаимодействию с данной страной ссылаясь на Еврокомиссию. Также для примера можно привести всем знакомое Евразийское экономическое содружество. В данном регионе представители Таможенной службы РФ почти не сталкиваются с языковым барьером. К тому же здесь максимально упрощенно таможенное законодательство[23].

При передаче информации из-за пределов Российской Федерации, стоит обращать внимание на два фактора:

- Содержание информации, кем и когда передана;

- Принцип и технология передачи.

В данных факторах отображается сущность порядка передачи информации.

При взаимодействии таможенных органов РФ с иностранными государствами перед ней становятся огромное количество визовой в обеспечении информационной безопасности. Из-за огромного разнообразия административных, правовых и национальных различий разных стран порой тяжело контролировать обеспечений информационной безопасности. В Российской Федерации на сегодняшний день правовой поле регулирующая данную деятельность, представители таможенных служб за рубежом выполняют некую роль информационного посредника. На дальнейшую перспективу с уверенностью можно сказать, что данных инструментов будет не достаточно для обеспечения информационной безопасности Таможенных

[23] Контакты представительств (представителей) таможенной службы за рубежом [Электронный ресурс] / ФТС РФ: Официальный сайт // http://www.customs.ru/index.php?option=com_content&view=article&id=22294:2015-12-15-06-56-45&catid=179:2011-03-25-06-42-48&Itemid=2088

органов РФ. Необходимо будет привести передаваемую информацию к унифицированному стандарту и технологии передачи данных.

При взаимодействии Таможенных органов с иностранными государствами были выявлены следующие виды информации, являющиеся объектом правонарушения. Это данные о международных перевозках, информация о участниках ВЭД, данные о процедуре предварительного информирования, и сведения международных договоров и соглашений. Данные виды являются наиболее важными с точки зрения потенциальной угрозы информационной безопасности таможенных органов.

Глава 2. Способы нарушения информационной безопасности

2.1 Угрозы обеспечения информационной безопасности таможенных органов

Для выявления методов нарушения информационной безопасности таможенных органов необходимо проанализировать все возможные виды угроз информационной безопасности таможенных органов.

Обеспечение информационной безопасности таможенных органов это многогранный процесс. Его деятельность определяют огромное количество факторов, которые с течением времени изменяются либо дополняться новыми.

Современная ситуация больше всего влияет на формирование определенных факторов. Такие процессы как экономическая ситуация в стране, политические процессы, развитие внешне торговых отношений все это в первую очередь влияет на обеспечение информационной безопасности таможенных органов, так как данные процессы создают благоприятные условия для потенциальных нарушителей. К тому же, как показывает статистика правонарушений, при этом существуют факторы, которые являются следствием текущего состояния информационной безопасности ТО, например[24]:

1. Создание Таможенного союза между странами Россия, Белоруссия и Казахстан;
2. Увеличение международных связей России в области сотрудничества в таможенной сфере;
3. Недостаточное инвестирование средств в систему защиты информации (разработка ПО, закупка необходимого оборудование, создание технических средств защиты информации, и др.);

[24] Показатели правоохранительной деятельности таможенных органов Российской Федерации за 2015 год [Электронный ресурс] / ФТС РФ: Официальный сайт // http://www.customs.ru/index.php?option=com_content&view=article&id=22498:-2015-&catid=55:2011-01-24-16-40-26&Itemid=1958

4. Текущая политическая и экономическая обстановка в Российской Федерации (санкции, замедление темпов развития экономики);

5. Отсутствие отечественного комплекса производства средств защиты информации в области таможенного дела;

6. Высокая доля импорта иностранного программного обеспечения и технических средств в области защиты информации;

7. Увеличения объемов таможенной информации и каналов ее передачи;

8. Увеличение прецедентов и правонарушений в области обеспечения информационной безопасности таможенных органов и финансово кредитной сфере;

9. Увеличение вирусных атак, компьютерных преступлений, и др.

Обобщая данный перечень факторов можно выделить основной - это рост мировой глобализации в сфере торговых отношений.

Угрозы информационной безопасности это различные действия, которые причиняют вред использованию, обработке или хранению информации. Более того, к угрозам информационной безопасности относится случайное или умышленной уничтожение, изменение необходимой информации. При обеспечении информационной безопасности таможенных органов России существуют следующие виды угроз, которые можно разделить на главные группы[25]:

- Деятельность человека. Основной источник угроз. При прямом или непрямом воздействии на необходимую информацию.

- Техногенные факторы. Угрозы, связанные с неисправностями и отказами в работе технических средств информатизации.

- Действия непреодолимой силы. Различные чрезвычайные ситуации, такие как наводнения, пожары, стихийные бедствия, катастрофе и др., которые могут уничтожить или нанести вред необходимой информации.

[25] Виды угроз информационной безопасности [Электронный ресурс] / Системы информационной безопасности // http://www.arinteg.ru/articles/ugrozy-informatsionnoy-bezopasnosti-27123.html

Сами источники угроз в свою очередь делятся на внутренние и внешние. Угрозы внутреннего характера вытекают из разработчиков системы ЕАИС, пользователей и обслуживающего персонала данной системы и других ее субъектов. Все они имеют определенный контакт с таможенной информацией и различными сведениями системы и формируют следующие источники внутренних угроз обеспечения информационной безопасности таможенных органов:

- нарушение закона в деятельности экономических и политических структур в области использования, формирования и распространения таможенной информации;

- Нарушения роботы различных государственных органов, приводящие к нарушению деятельности таможенных органов;

- нарушение порядка обработки, сбора и передачи информации Единой автоматизированной информационной системой Федеральных таможенных органов России;

- преднамеренные или непреднамеренные ошибки должностных лиц таможенных органов РФ связанные с порчей информации;

- отказы и поломки технических средств.

К внешним угрозам относятся все субъекты не входящие в систему ЕАИС, субъектов, не имеющих непосредственный контакт с таможенной информацией, а также стихийные бедствия и чрезвычайные ситуации. Источники данных угроз следующие[26]:

- Деятельность спецслужб разведки иностранных государств;

- Недружественная политика со стороны иностранных государств в области информатизации и распространения информации;

- деятельность различных иностранных структур и организаций направленная против национальных интересов Российской Федерации;

[26] Угрозы информации и информационные угрозы. Подготовка кадров в области информационной безопасности / А.А. Малюк// Московский государственный инженерно-физический институт – 2006 г.

- различная преступная деятельность отдельных лиц и международных группировок направленная против национальных интересов Российской Федерации;

- катастрофы и стихийные бедствия.

Угрозы обеспечения информационной безопасности таможенных органов реализуются возможными методами нарушения информационной безопасности. Таких методов можно выделить пять[27]. Физические, радиоэлектронные, информационные, программно-математические и организационно-правовые. Необходимо их разобрать по порядку.

1. Физические.

- Хищение и уничтожение средств связи, защиты и обработки информации. Умышленное нанесение на них неисправностей.

- Хищение и уничтожение носителей информации в электронном или ином виде.

- Хищение или уничтожение ключей, кодов доступа других средств от защиты несанкционированного доступа к информации.

- Физическое воздействие на пользователей и обслуживающий персонал системы ЕАИС в целях получения доступа к информации.

- Диверсии и теракты по отношению информационной инфраструктуре.

2. Радиоэлектронные

- Перехват информационных данных в сети интернет и линии связи.

- Перехват информационных данных в внутренних каналах ее утечки.

- Замена, навязывание ложных информационных данных в сети интернет и линий связи.

- Внедрение устройства – перехватчика данных.

- Подавление информационных данных путем различных генераторов электромагнитной энергии.

3. Информационные.

[27] Способы нарушения информационной безопасности таможенных органов Российской Федерации [Электронный ресурс] / Правовая консультация // http://www.zakonprost.ru/content/base/part/491871

- Незаконный сбор, хранение, распространение и использование информации.

- Нарушение секретности информации.

- Противозаконное хранение, копирование, уничтожение информационных данных и программ.

- Различные манипуляционные действия с информацией (искажение информации, ее скрытие, дезинформация).

- Нарушение оперативности обмена информационными данными.

- Хищение информационных данных.

- Нарушение технологии информационного обмена и обработки информации.

4. Программно-математические.

- Создание и внедрение в информационную систему ЕАИС вредоносных программ (вирусов).

- Создание программ вирусов для компрометации системы защиты информации.

5. Организационно-правовые.

- Невыполнений законодательства в области обеспечения информационной безопасности таможенных органов РФ.

- Оборудование таможенных органов устаревшими и неактуальными средствами обеспечения информационной безопасности.

На сегодняшний день наиболее уязвимыми местами информационной безопасности таможенных органов России являются информационные угрозы. Связанно это с процессами мировой глобализации, развитием НТП и недостаточным опытом борьбы с данным видом угроз.

Огромное количество угроз обеспечению информационной безопасности таможенных органов РФ делают данный процесс актуальным и приоритетным в работе Таможенных органов и правительства РФ. Приведённая выше структура возможных угроз дает возможность прогнозировать возможные проблемы в определённых направлениях.

Определение факторов с сочетанием угроз дают нам возможность дальнейшего анализа в области обеспечения информационной безопасности.

Таким образом, с учетом всего выше сказанного, можно выделить пять основных методов правонарушения информационной безопасности таможенных органов, это Физические, радиоэлектронные, информационные, программно-математические и организационно-правовые. Данные методы являются основой для выделения основных видов Таможенных правонарушений в области информационной безопасности.

2.2 Трансформация методов незаконного получения таможенной информации

В процессе эволюции процесса информатизации общества и государства происходят изменения методов получения необходимой информации, которая может быть использована в противозаконных целях. Изучая процесс информатизации, необходимо определить причины появления методов нарушения информационной безопасности таможенных органов в процессе развития информатизации.

Эффективность работы коллективов, организаций отдельных людей в условиях современного общества зависит от их информированности. К тому же им приходится обрабатывать огромный объем информации. Так как информатизация это научно-технический и социально-экономический процесс, при котором создаются более оптимальные условия, способные удовлетворить информационную необходимость следующих элементов органов государственной власти, органов местного самоуправления, общественных объединений и всех граждан, для соблюдения их прав и свобод, то можно сделать вывод о том, что это процесс обеспечения благосостояния страны.

Если обратится к истории развития процесса информатизации, то мы увидим в ней четыре этапа.

Этап 1. Речевой. Появление речи, а в дальнейшем письменности. С данного этапа информация получает способность к хранению и передаче ее будущим поколениям.

Этап 2. Письменный. С появлением печатного станка появляется новый толчок в развитии информатизации общества. Массовое производство книг и печатной продукции дает возможность передавать данные более широкому кругу людей.

Этап 3. Индустриальный. Он ознаменуется с развитием телеграфа, радио, телефонной связи, а в дальнейшем и телевиденья. Процесс информатизации становится быстрым, актуальным, и позволяет охватывать огромные расстояния.

Этап 4. Информационный. Он происходит в настоящее время. Начало берет от создания Электронных вычислительных машин, информационных компьютерных сетей, связи интернет, развитием информационного общества и индустрии.

Окончание данного процесса предугадать сложно, и скорее всего, нереально. Каким будет следующий этап - покажет время и развитие научно технического процесса. Но чтобы проанализировать влияние данного этапа развития информатизации на общество, необходимо его проанализировать и рассмотреть с разных сторон.

Изучив данные этапы эволюции процесса информатизации можно применить к ним определенные методы нарушения информационной безопасности. Например, к Речевому и посменному этапу подойдёт Физический метод, где нарушение будет происходить путем хищения, уничтожения и изменения информации непосредственно человеком. К индустриальному этапу подойдет радиоэлектронный метод нарушения информационной безопасности, где характерны нарушения вида радиоэлектронного перехвата, уничтожения и изменения информации. Информационному этапу подходит одноименный метод - Информационный.

Ему характерны различные виды нарушений от нарушения секретности в сети интернета до формирования ложной технологии переработки данных.

Процесс перехода информационного развития общества с третьего на четвертый этап, а другими словами с индустриального на информационный, проявляется в определенных факторах[28], а именно преобладание и частичное перераспределение трудовых ресурсов на информационные услуги и продукты с материального производства. Помимо интеграции информатизации в обществе она охватывает остальные социальные сферы жизнедеятельности человека (культуру, политику, экономику, образование, и.т.д.). также происходит изменение в финансово расчетной системе взаимоотношений в обществе. Появляются электронные деньги, которые постепенно начинают вытеснять бумажные, металлические и другие традиционные валюты.

С наступлением информационной эрой развития человечества мир изменился и продолжает меняться. В связи с этим появляются новые угрозы и новые методы нарушения, которые в том числе и охватывают таможенную службу.

Что касается причиной наступления информационной эрой то, безусловно, основой всего является развитие научно технического прогресса. Именно скорость развития НТП молниеносно внедряет информатизацию в наш мир.

Некоторые процессы развития информатизации происходят незаметно. Например, за счет развития НТП увеличивается развитие интеллектуальной деятельности человека. Вследствие чего происходят изменение в мировом секторе экономике. Где преобладающее большинство трудовых ресурсов занято в сфере услуг, информатизации и творчестве. Опыт развитых стран мира наглядно показывает нам как высокие технологии совместно с движением процесса информатизации общества стали основой их

[28] Информатизация общества. Основные этапы развития вычислительной техники / В.З. Аладьев // Издательский дом «Флинт» 2009г.

экономического, социального и культурного развития. Достоинствами данного подхода является общий доступ всех граждан к информации и развитие информационной инфраструктуры. Российской Федерации, разумеется, стоит ориентироваться на их опыт. Если проанализировать развитие отечественной информационной инфраструктуры вместе с развитием информационного общества и НТП, то мы увидим весьма низкие показатели[29]. Это негативно сказывается на экономическом росте нашей страны, в том числе на деятельности таможенной службы. Отсюда можно выделать одну из приоритетных целей, это развитие и реализация отечественного потенциала в области высоких технологий, информатизации и культурной составляющей общества для выхода экономики на уровень конкурентоспособной с развитыми странами мира.

В Российской Федерации уже реализуются целый ряд программ по развитию информационного общества России. На официальном сайте Федеральных таможенных органов РФ выложен отчет о реализации Программы «Модернизация информационной системы Таможенных органов России»[30]. Программа была запущенна поле подписания соглашения между Международным банком реконструкции и развития и Российской федерацией. Временной период программы составил 31.10.2003-30.06.2013гг. Цель данной программы основывалась на выведение отечественной таможенной системы на мировой уровень конкурентоспособности с развитыми странами мира и ее глобальную интеграцию в всемирную торговую систему. Реализовывался данный проект путем укомплектования таможенной службы современными информационными технологиями, развитием сотрудничества в области совместной разработки информационных и автоматизированных систем. Закупкой необходимого программного обеспечения. Проработкой нормативной правовой базы,

[29] Признаки информационного общества [Электронный ресурс] / Проблемы информатизации образования // https://sites.google.com/site/probinobrz/problemy-informatizacii-obrazovania-1/priznaki-informacionnogo-obsestva
[30] Итоги Реализации проекта «Модернизация информационной системы Таможенных органов» [Электронный ресурс] // ФТС РФ: Официальный сайт http://www.customs.ru/index.php?Itemid=1871&id=18644&option=com_content&view=article

регулирующая таможенную деятельность в области информационного взаимодействия со всеми участниками мирового рынка. Разработкой методов и форм для дальнейшего развития законодательной базы. Созданием обширных связей в области дальнейшего взаимодействия и сотрудничества в данной отрасли. Таможенные органы России завершили данный проект успешно, так как были достигнуты все поставленные перед ними цели.

Из незавершенных программ можно выделить «Проект развития информационного общества РФ на период с 2011 по 2020 годы»[31]. ФТС России непосредственного участия в данной программе не принимает, но, разумеется, ее реализация скажется на их развитии. Программа ставит перед собой цель развития гражданского общества путем внедрения в их жизнь информационных технологий с увеличение качества жизни. Но здесь для таможенных органов могут возникнуть определенные риски при ее реализации. Например, неактуальная проблема качества жизни населения. Уровень информатизации общества в России, безусловно, является проблемой на сегодняшний день, но ее не стоит делать приоритетной. Довольно длительные временные рамки. Научно технический прогресс, возможно, пойдет совершенно другим направлением от задач программы. Нерациональное распределение финансовых средств. А также несбалансированность целей и задач с программами развития таможенных органов, в том числе и в области информатизации.

Расходы на данную программу колоссальные – около 123 миллиардов рублей в каждый год программы. Сами разработчики утверждают, что после реализации «информационного общества России» наша страна войдет десятку стран по развитию информационной продукции и технологий. Также высокие показатели будут достигнуты в социальной сфере, культурной, политической. На сегодняшний день никто не решается делать прогнозы о

[31] Государственная программа «Информационное общество» (2011–2020 годы) [Электронный ресурс] / Минкомсвязь России: Официальный сайт // http://minsvyaz.ru/ru/activity/programs/1/

данной работе. Остается не так много времени до конца реализации программы кода ее смогу уже проанализировать и сделать выводы.

Основным направлением развития ФТС России в области информатизации и информационного обеспечения информации Таможенных органов является «Стратегия развития Федеральной таможенной службы России до 2020 года»[32]. Это основная программа таможенных органов, описывая их дальнейшее направление на ближайшее будущее.

Приоритеты развития выстроены исходя из международных стандартов и общепринятых направлений в сфере информатизации, для противостоянию вызовам процесса мировой глобализации торговых отношений[33]. Таможенные органы Российской Федерации к 2020 году планируют выйти на высокий уровень по нескольким направлениям:

- создание информационных технологий, комплексов обработки данных в рамках ЕАИС;

- развитие атоматизации деятельности таможенных органов;

- развите внутренный сети связи, через ЕАИС. Унификация ее работы во всех регионах страны;

- выход на более новый уровень качества в области информационно-технического обеспечения ФТС России;

- дальнейшая разработка и их унификация технологий таких процессов как электронное декларирование, управление рисками, предварительное информирование, и.т.д;

-совершенствование системы взаимодействия ФТС России с участниками ВЭД, органами исполнительной власти, координирующими органами, с Таможенным союзом, и.т.д;

- повышение информационной защищенности таможенных органов при процедуре таможенный транзит;

[32] Стратегия развития Федеральной таможенной службы России до 2020 года [Электронный ресурс] / ФТС РФ: Официальный сайт // http://customs.ru/index.php?option=com_content&view=article&id=17220&Itemid=2375

[33] Стандартизация в области информационных технологий [Электронный ресурс] / XI Международный семинар по стандартизации // http://normdocs.ru/page.jsp?pk=node_1157453970729

- повышения взаимодействия таможенных органов России с таможенными органами стран-участниц Таможенного союза путем развития ЕАИС;

- обеспечение информационной безопасности Таможенных органов РФ с помощью улучшения взаимодействия с органами исполнительной власти.

Данные направления выбраны приоритетными, исходя из целей и задач стратегии.

Прогнозы о выполнении данных задач делать преждевременно, хотя можно предугадать что показатель, связанный с поставками иностранного оборудования и программного обеспечения может быть выполнен не полностью[34]. Связанно это, прежде всего из-за событий вокруг антироссийских санкций. Соединенные штаты Америки и Европейский союз, у которых наша страна закупала необходимое таможенным органам оборудование, ввели нам запрет на их покупку. Также на выполнение задач стратегии развития ФТС может повлиять экономическая ситуация в России, резко снизившаяся за последние годы. В любом случаи нам стоит дождаться 2020 года и делать выводы, а пока это всего лишь прогнозы.

Стратегия развития информационной системы таможенных органов России, является совокупностью различных направлений, документов программ, доктрин. Таможенные органы на сегодняшний день сталкиваются с огромным количеством задач в данной области, которые им необходимо выполнить в очень короткий промежуток времени. Помимо всего прочего на процесс реализации целей влияет совокупность различных факторов, таких как НТП, социальна, политическая, культурное состояние общества, и.т.д. какие-то из них помогают в реализации целей, какие-то наоборот создаю помехи. Поэтому таможенным органам необходимо правильно расставлять приоритеты, мыслить на долгосрочную перспективу и брать на себя

[34] Разработка в сфере информационно-коммуникационных технологий в таможенных органах [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://www.customs.ru/index.php?option=com_content&view=article&id=22977:-31-2016-&catid=26:2011-01-24-14-45-21&Itemid=1830

посильные задачи. Если учитывать все данные факторы то любые программы и стратегии, направленные не только на обеспечение информационной безопасности таможенных органов РФ будут выполнены на 100%.

Подводя итог можно сделать вывод о том, что современный этап развития информатизации общества и таможенной службы подвержен в большей мере Информационному методу нарушения информационной безопасности таможенных органов. Их доминирование объясняется тем что они являются наиболее эффективными в настоящее время.

2.3 Применение методов нарушения информационной безопасности таможенных органов на базе Единой автоматизированной информационной системы

Для эффективного анализа методов нарушения информационной безопасности таможенных органов следует рассмотреть их на примере Единой автоматизированной информационной системы Таможенной службы (ЕАИС).

Для обеспечения информационной безопасности таможенных органов РФ в современных условиях была создана в России, а в последующем и в Таможенном союзе 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[35].

Единая автоматизированная информационная система является важной частью таможенной инфраструктуры. Совокупные составляющие это

[35] Единая автоматизированная информационная система (ЕАИС) ФТС России [Электронный ресурс] / Сущность экономической безопасности РФ // http://studopedia.info/2-52279.html

информационно вычислительные центры региональных таможенных служб, телекоммуникационные сети, различные программы и базы данных. Задачей ЕАИС является автоматизирование процессов детальности таможенных органов и информационное взаимодействие таможенных органов друг с другом и с внешними субъектами.

История создания Единой автоматизированной информационной системы берет свое начало еще с Советского периода. Первым шагом являлось постановлении Министров Советского союза от 15 октября 1988 года, под номером 203 о создании Главного научно-информационного вычислительного центра (ГНИВЦ), которое последующем стало фундаментом для создания ЕАИС. В начале 90х годов прошлого века ГНИВЦ был передан в систему таможенных органов России. После этого момента Единая автоматизированная информационная система принимается к рассмотрению именно как таможенный инструмент реализации и регулирования ее процессов[36].

Основные документы, которые закрепили статус ЕАИС в системе таможенных органов, был приказ главного таможенного комитета России, от 19 марта 2004 года «Об утверждении общего порядка разработки и модернизации программных средств ЕАИС ГТК России». [37]

Единая автоматизированная информационная система на данный момент включает всю территорию России, все региональные вычислительные центры и доступ к системам стран участниц таможенного союза. Это очень объемный охват территорий, так как не стоит забывать, что у каждой таможни существуют собственный информационные сети и базы данных которые тоже включаются в ЕАИС. Также, так как таможенные органы не посредственно имеют отношение к национальной безопасности

[36] Приказ ФТС РФ от 19 марта 2004 года «Об утверждении общего порядка разработки и модернизации программных средств ЕАИС ГТК России» http://customs.ru/index.php?option=com_content&view=article&id=21732:2015-09-30-10-04-42&catid=40:2011-01-24-15-02-45

[37]Приказ ФТС РФ от 13 марта 2015 года №423 «Об утверждении Положения по организации процессов жизненного цикла информационно-программных средств в таможенных органах»

страны то Единая автоматизированная информационная система имеет обмен данными между правоохранительной системой и налоговой службой страны.

Как и у всех систем у Единой автоматизированной информационной системы существует свои задачи в развитии автоматизации таможенных органов. Проанализировать их возможно, если изучить развитие данной системы, которое необходимо на три этапа.

Первым этапов в развитии Единой автоматизированной информационной системы являлось оформление бизнес процессов и описания действий, которые на рабочем месте выполняли инспектора таможенной службы. После этого начался процесс автоматизирования действий, которые выполняли таможенные служащие. На этом этапе произошли довольно большие кадровые изменения стали создаваться автоматизированные рабочие места взамен старых.

Вторым очень важным этапом является развитие и внедрение программ и технологий, на которых базируется ЕАИС. За основу были взяты новые информационные программные средства и операционные системы, такие как Novell, Windows, Oracle и другие. В связи с этим в дальнейшем у этого процесса появились свои проблемы. Так как все программные средства в основном были не отечественного производства, что заставило ФТС задуматься о политической независимости Единой автоматизированной информационной системы. К тому же программные средства были разные и в ЕАИС начались различные не состыковки в роботе системы. Этот этап был самым трудоемким и кропотливым, так как все время уходило на стандартизацию и унификацию программных продуктов для нормальной работы функционирования системы. В настоящее время проводится доработка программных средств обеспечения ЕАИС, а в вопросе связанным с замещением на отечественные программные средства, так и нет решения.

Все действия, связанные со стандартизацией Единой автоматизированной информационной системой, плавно переходят в третий

этап, который работы уже направлены на развитие и модернизацию, системное проектирование и внедрение их в работу.

На сегодняшний день Федеральная таможенная служба 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 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.

Эксперты в области таможенного дела давно работают над задачей организации системы, и уже пришли к некоторым решениям[38]:

1. Осуществить упорядоченной хранения таможенных документов и данных в электронной среде;
2. Организовать удаленный доступ пользователям к информационным данным системы, и обеспечить защиту на основе WEB технологий;
3. Создать удобную структуру хранения данных в ЕАИС;
4. Централизовать управлений в системе;
5. Реализовать в режиме автоматизации процедуры управления рисками;
6. Автоматизировать режим контроля после выпуска товара.

Таможенные органы постоянно модернизируют данные направления и выводят данные задачи на новый уровень, тем самым обеспечиваю еще более упрощенную работу в системе связанную с получением или хранением информацией и ее защищённостью.

[38] Информационные системы в экономике / В.Н. Ясенев, О.В. Ясенев // Москва – 2016г.

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.

Информация, которая обрабатывается в ЕАИС подразделяется по способу ее формирования:

1. Электронные данные, которые были созданы с помощью специальных программных комплексов, реализующих информационные таможенные технологии;

2. Электронные данные, которые созданы с помощью стандартных средств общего пользования, например, электронные таблицы, текстовые редакторы и другие.

3. Электронные данные, которые созданы неопределенными программными средствами.

Также можно подразделить поток информации в ЕАИС и другой категорией[39]:

[39] Характеристика информационных процессов [Электронный ресурс] / Центр управления финансами // http://center-yf.ru/data/stat/Harakteristika-informacionnyh-processov.php

1. Исходные данные для формирования и загрузки баз данных таможенной информации.

2. Оперативная информация таможенных органов.

3. Нормативно справочная.

4. Информация о транзите

5. Отчетная

6. Служебная переписка таможенных органов.

Объясняя требования к существующей классификации необходимо обратить внимание на то что, оперативная информация должна быть доставлена в самый ранний срок. Как правило, к этой категории относят такие данные оперативного управления как ориентировки, или данные которые входят в функционирование ЕАИС.

Что касается регламента, так это отчеты таможенных органов, которые соответствуют определенным приказам таможенных органов и форм статистический отчетов. Самый отличительный фактор этой классификации, это определенная периодичность формирования данных. Здесь не берется основное внимание на ее оперативность, как в прошлой категории. Зато ее приоритетом является полная достоверность и полнота данных.

Про нормативно справочную информацию совсем мало особенностей. Ее задача одновременно вступать в действие во всех таможенных органах.

Также в федеральном таможенном управлении создали особый классификатор, который помогает таможенным органам оценить работу системы[40]:

1. Достоверность формируемой таможенной статистики;

2. Взимание всех таможенных сборов в бюджет государства;

3. Улучшение эффективности работы, связанной с проведением таможенных операций, путем оптимизаций технологий;

4. Ускорение и упрощение процесса таможенного контроля;

[40] Информационные технологии в таможенном деле / Учебное пособие: В 2 ч. Часть 1 // Владивосток: ВФ РТА, 2003. – 265

5. Оперативное решение задач таможенной службы;

6. Сокращение финансовых и временных затрат на поисковые, информационные и аналитические работы системы;

7. Обеспечения должного уровня защиты и безопасности и ограничения доступа к определенным данным системы;

8. Уменьшение времени к адаптации системы к изменению нормативно правовой базы;

9. Полное оснащение резервами системы (информация, программная часть, коммуникации сети).

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 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.

2.4 Электронная цифровая подпись как основной способ противодействия правонарушениям в системе информационной безопасности

Электронная цифровая подпись (ЭЦП) в процессе электронного декларирования в последнее время завоевали у участников внешней экономической деятельности статус надежного инструмента обеспечения

информационной безопасности. Но, как и любого эффективного метода у нее существуют свои плюсы и минусы. Для определения эффективности его противодействия методам правонарушения таможенной информации необходимо провести анализ механизма ЭЦП.

На сегодняшний день Электронная цифровая подпись применяется не только в ВЭД, она охватывает различные сферы взаимодействия общества, где с развитием Научно-технического прогресса бумажные формы подписей сменяются электронными. Это заключение сделок, покупки в интернете, взаимодействие с банковскими организациями и.т.д[41].

Анализируя техническую составляющую метода ЭЦП, необходимо обратить внимание на ФЗ закон «ОБ электронной цифровой подписи от 23 января 2002 года»[42]. В нем говорится, что ЭЦП это набор закрытых ключей и зашифрованных алгоритмов определенного электронного документа. И предназначенный для идентификации пользователя и разрешения доступа к данному документу. Отсюда можно сделать вывод, что Электронная цифровая подпись это набор сложных математических алгоритмов доступа к ответным данным. Для определения эффективности ЭЦП в системе обеспечения информационной безопасности таможенных органов нам необходимо подробно рассмотреть механизм работы системы Электронной цифровой подписи.

Система функционирования ЭЦП основана методе «открытых и закрытых ключей»[43]. Закрытый ключ это зашифрованный пароль, как правило, небольшой длиной, находящийся отдельно от всей информационной системы. Как правило, это электронные носители (флэш-карты, дискеты, CD-диски, и др.). Закрытый ключ работает только в паре с открытым. Открытый ключ это сертификат о зашифрованном пароле закрытого ключа. Находится он непосредственно в базе данных системы. Его

[41] Виды электронной подписи [Электронный ресурс] / Единый портал ЭЦП в РФ // http://www.iecp.ru/ep
[42] ФЗ закон «ОБ электронной цифровой подписи от 23 января 2002 года».
[43] Выдача ключей Электронной Подписи [Электронный ресурс] / Единый портал ЭЦП в РФ // http://www.icentr.ru/center.html

алгоритм намного длиннее, так как включает в себя закрытые ключи всех пользователей системы. Система доступа работает при подключении пользователем закрытого ключа. После чего идет передача информации о закрытом коде в базу данных системы, идентификация пользователя. Техническим языком это означает, что открытый ключ сверяет протоколы доступа с алгоритмами присоединившегося закрытого ключа, в случаи совпадений – разрешает доступ.

Процесс обмена данными ключей происходит не только для осуществления входа в систему. Он также необходим для установлении личности пользователя, и процедурах подтверждения действий в процессе работы с системой.

Для исключения риска возможных подделок ключа, протокол открытых ключей отправляют в Удостоверяющий центр занимающийся их достоверностью. В нем обеспечивается надежное хранение ключей, исключаются возможные варианты его расшифровки и подделки. Главная функция Удостоверяющего центра это обработка данных полученных с открытых и закрытых ключах, их хранение в процессе работы. Важной особенностью обеспечения информационной безопасности таможенных органов является то что в процессе работы пользователя информация с ключей не находиться на одном и том же удостоверяющем центре а постоянно перемещается, тем самым усложняя задачу нарушителю ее расшифровки. Можно с уверенностью сказать, что на данных Удостоверяющих центрах лежит огромная ответственность за обеспечение информационной безопасности всей системы ЭЦП.

«Федеральный Закон об ЭЦП» на законодательном уровне ставит электронную подпись на один уровень с традиционной бумажной. Развитие Электронной цифровой подписи в России как правовой институт начинается со сферы банковских операций. И это абсолютно логично. Банковское кредитное дело требует для организованной работы огромное количество юридических подписанных документов. В связи с эти необходимо пускать

основной поток документа оборота через электронные сети связи и контролировать е правовую основу с помощью ЭЦП.

Организация нормативно правовой базы на первых этапах функционирования Электронной цифровой подписи на территории РФ принадлежит Центральному Банку России. Этот государственный орган принял больше всего нормативных документов регулирующая деятельность ЭЦП.

Электронная цифровая подпись в процессе обеспечения информационной безопасности таможенных органов широко встречается в процедуре Электронного декларирования товаров и транспортных средств. Процедура электронного декларирования в России осуществляется с помощью специальных программ, доступом к которым осуществляется с помощью ЭЦП[44]. Данная форма защиты призвана обеспечивать максимальную информационную безопасность. Но на деле не всегда это положительно.

С введением таможенной службы обязательного электронного декларирования все участники ВЭД России стали приобретать ЭЦП. Унифицировав систему торговли с одной стороны, снизив коррупционную составляющую, увеличились риски с процессом расшифровки кодов. Так как число ЭЦП увеличилось то и соответственно увеличился риск его расшифровки. Так же я был непосредственным свидетелем во время прохождения мной производственной практики ошибок системы Электронной цифровой подписи.

Преддипломная производственная практика была пройдена мной городе Томске, в научно производственной фирме «Микран», в отделе материально технического обеспечения. В соответствии с целями моей преддипломной практикой я производил анализ надежности системы и информационной безопасности электронного декларирования под

[44] Электронное декларирование через Интернет [Электронный ресурс] / ТКС: Все о таможни // http://www.tks.ru/ed2prosto.shtml

руководством штатного сотрудника фирмы, специалистом по ВЭД. Моим руководителем мне было продемонстрированы как при отправке электронной декларации на проверку в таможенную службу, с помощью ЭЦП, данные из декларации были похищены конкурентами фирмы. Декларация не пришла в таможенную службу, а оказалась в общем доступе в интернете. ЭЦП подтвердил данное действие. В чем причина данного сбоя еще предстоит установить. Таможенные органы по данному факту в свою очередь начали проверку. Проанализировав данный прецедент я пришёл к выводу, что ЭЦП на сегодняшний день является хорошим защитником информации, но не совершенна. Необходимо усовершенствовать шифровальные функции Электронной цифровой подписи, так как при данном прецеденте был применен в основном Радиоэлектронный метод нарушения информационной безопасности таможенных органов, а конкретно, перехват информационных данных в сети интернет и линиях связи.

Подведя итоги, можно отметить, что Электронная цифровая подпись на сегодняшний день является эффективным методом обеспечения информационной безопасности таможенных органов. Однако в нем присутствуют определенные недостатки, а конкретно в области радиоэлектронного шифрования данных. Радиоэлектронный метод правонарушения информационной безопасности таможенных органов будет преобладать в правонарушениях связанных с Электронной цифровой подписью.

Глава 3. Эффективная модель системы информационной безопасности в Таможенных органах

3.1 Электронное декларирование как практическая основа информационной безопасности в системе Таможенных органов

Цели, для которых может быть использована необходимая информация, зависят от потребностей каждого субъекта информационного взаимодействия. В информационном взаимодействии с таможенной службой учувствуют огромное количество субъектов, которых можно разделить на две отрасли: внутренние и внешние[45]. К внутренним субъектам относятся участники ВЭД, отечественные банки и финансовые организации, государственные органы, и.т.д. Другими словами это все субъекты, которые находятся на территории Российской Федерации и функционируют в ее правовом поле. К внешним – иностранные таможенные службы, банковские организация, различные международные компании. Также к внешним участникам относится Таможенный союз, так как вопрос обеспечения информационной безопасности регулируется на национальном уровне.

Анализ потребностей различных субъектов информационного взаимодействия с таможенной службой выделил следующие цели:

Для участников ВЭД.

1. Уклонения уплаты от таможенных пошлин, сборов, налогов.
2. Нарушение таможенного законодательства для получения различных преференций (экономических, социальных, территориальных и др.);
3. Недобросовестная конкуренция;

Для государственных служащих.

1. Коррупция;
2. Манипулирование другими субъектами (Дезинформация);

[45] Способы нарушения информационной безопасности таможенных органов Российской Федерации [Электронный ресурс] / Правовая консультация // http://www.zakonprost.ru/content/base/part/491871

3. Получение личной выгоды;

Для внешних субъектов информационного взаимодействия.

1. Дестабилизация внутренней обстановки в стране (экономической, политической, социальной);

2. Коммерческая выгода;

Цели и принципы, для которых может быть использована информация может быть огромное множество, также как и потребностей потенциальных нарушителей. Основными же стоит выделить такие, как коррупция и уклонение от уплаты таможенных сборов и налогов. Как показывает статистика таможенных правонарушений на сегодняшний день это самые популярные цели нарушения информационной безопасности, для устранения которых может быть использовано электронное декларирование.

Эффективная степень организованности в практической деятельности обеспечения информационной безопасности в системе Таможенных органах отчетлива, видна на процедуре электронного декларирования.

Электронное декларирование товаров и транспортных средств (ЭД) является одним из основных объектов инструментов обеспечения информационной безопасности таможенных органов.

Для того чтобы нам понять, какие виды таможенного правонарушения чаще всего используются в процедуре ЭД, стоит понять особенность самого электронного декларирования что оно означает и чем отличается от обычной декларации.

Собственно, сам термин электронного декларирования говорит нам что это технологи, которая позволяет удаленно подавать декларацию на товары в таможенные органы при этом ее оформление осуществляется через сети Интернет[46]. Прейдя к электронной форме декларирования товаров заметно упростилось взаимодействие между таможенной службой и участниками ВЭД. При этом за счет развития научно технического прогресса стали

[46] Подключение к системе электронного декларирования [Электронные ресурсы] / Передовые технологии// https://www.sztls.ru/services/elecdecl/

активно применятся телекоммуникационные средства, в связи с чем исключается необходимость личной встречи участника ВЭД с таможней.

В России электронное декларирование введено относительно недавно. Его история берет свое начало с 2002 года, когда был принят закон об электронной цифровой подписи. И в этом же году была оформлена первая декларация в России с использованием технологии электронного декларирования. Эксперимент был проведен в Москве на Каширском таможенном посту, который входит в состав южной таможни Центрального таможенного управления. Спустя два года первая система электронного декларирования начала действовать также в Москве на Чертановском таможенном посту. Далее все последующие годы технология электронного декларирования распространялась по всей стране. Процесс распространения был очень медленным, так как был весьма затратным.

Крупная экспансия технологии электронного декларирования в России начался в 2008 году, после выхода приказа ФТС о возможности пользоваться при передаче данных сети интернет, ведомственной сетью таможни. Эти требования расширили круг абонентов. Так же позднее в этом году уже были выпущены первые грузовые декларации, использовавшие технологию ЭД. А к 2010 году все таможенные посты были оборудованы для приема данных деклараций.

Существуют данные статистике об использовании электронного декларирования, которые я хотел бы привести в данной работе. На 2010 год доле электронных деклараций из общего объема составила 52%, а уже в 2011 году эта цифра была 61%[47].

С 1 января 2014 года в России осуществлён переход на обязательное электронное декларирование.

[47] Интервью начальника Главного управления организации таможенного оформления и таможенного контроля (ГУОТОиТК) Дмитрия НЕКРАСОВА журналу «Таможня» № 12-13, 2011 «Таможенный союз: пути и решения» [Электронный ресурс] / ФТС РФ: Официальный сайт // http://www.customs.ru/index.php?option=com_content&view=article&id=14332:----------lr--12-13-2011-l----r&catid=26:2011-01-24-14-45-21&Itemid=1830&Itemid=

Электронное декларирование подразумевает внедрение электронного документооборота и последующую его реализацию между органами исполнительной власти и хозяйствующими субъектами при предоставлении таможенной документации. К тому же внедрение опытных проектов, связанных с использование механизма Электронной цифровой подписи (ЭЦП).

Не все документы могут быть подтверждены ЭЦП. В соответствии с Федеральным законом «Об информации, информатизации и защите информации»[48] законная сила электронной цифровой подписи признается только при наличии лицензионных программ и технических средств, которые обеспечиваю ее идентификацию. В связи с этим можно сделать вывод что коррупция, как цель таможенного правонарушения сводится к минимуму. Но тем ни менее цели неуплаты таможенных пошлин приобретают новые методы их реализации. Например, Радиоэлектронный.

Для более полного понимания сущности электронного декларирования, можно выделить цели ее реализации:

1. Унификация процедур Таможенного оформления и контроля;
2. Сведение к минимуму личного контакта между Таможенными органами и участником ВЭД;
3. Выполнение таможенных процедур, связанных с режимом удаленного доступа;
4. Унификации порядка и процедуры уплаты таможенных платежей;
5. Снижение затрат необходимых на таможенное оформление;
6. Замена бумажного документа электронным.

При электронной форме декларировании товара происходит автоматическая обработка данных заявляемых декларантом в центральной базе данных. Она проходит проверку на уровне региональных таможенных

[48] Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

управлениях. Данное взаимодействии возможно при подключении рабочего места декларанта к Единой автоматизированной информационной системе (ЕАИС). По данному каналу связи и происходит информационный обмен данными. Такое взаимодействие при использовании программного средства декларанта и системы ЕАИС происходит только на начальных и заключительных этапах таможенного оформления. Сама основа таможенного оформления осуществляется штатными программными средствами с взаимодействием систем таможенного оформления и контроля. На завершающем этапе электронная декларация отправляется в программное средство ЭД. Там она будет оформлена в электронном и текстовом документе.

Существует и ряд проблем, которые препятствуют развитию на начальных этапах технологии электронного декларирования: отсутствие доступа декларанта к системе в связи с затратами, и нестандартизированность программ использованных декларантом и таможенными органами. В первое время программы контроля таможенных органов и программы заполнения декларации – декларанта, занималась интеграцией.

Что касается программного обеспечения – в системе предварительного информирования существуют четыре портала:

1. Грузоотправитель;
2. Граница;
3. Декларант;
4. Инспектор.

На практике в электронной декларации задействовано всего лишь два: «Декларант» и «Инспектор». Поэтому пока что система предварительного информирования неприменима. То есть нельзя получить сведения о товаре путем изучения транспортными и коммерческими документами в электронной форме. Иначе декларант смог бы подготовить нужный комплект документов для подачи в таможенную службы, еще не дожидаясь прибытия

груза в таможню. Под действующим законом декларант отправляет в таможенный орган минимум документов составляющий совокупность документов сделки. В комплекс СДС входят:

1. Грузовая таможенная декларация;
2. Декларация транспортного средства;
3. Опись документов.

Разумеется, что таможенный инспектор в случаи возникновения необходимости может запросить и дополнительные документы (контракт, инвойс, TIR и другие).

Электронное декларирование обеспечивает простоту оформления и необходимую прозрачность действий, но тем ни менее она ставит таможенные органы и участника внешней экономической сделки в непростую ситуацию. Они зависят от надежности и бесперебойности программы и системы в целом. Так же необходимым является условие совмещение программ с налоговой службой и банковскими программами. Это необходимо для возврата Налога на добавленную стоимость и учета паспорта сделки.

Электронное декларирование товаров было создано Всемирной торговой организацией (ВТО) с 2010 года[49]. ЭД и предварительное информирование это составляющие введение новых стандартов, которые внедряются прежде всего для обеспечения безопасности внешнеторговых операций и содействию торговли.

Практический процесс декларирования товаров с применением электронных программных средств реализуется путем нескольких шагов:

1. Участник ВЭД при перемещении товаров через границу отправляет декларанту необходимые документы.
2. Исходя и з полученных сведений участником ВЭД, декларант формирует декларацию и отправляет ее на проверку в таможню.

[49] Электронное таможенное декларирование [Электронный ресурс] / Таможенный брокер «КВТ» // http://www.kvtservice.su/services/ed/

3. Таможенный инспектор проверяет сведения, которые заявлены в электронной декларации и проложенных с ней пакете документов. Также он производит все необходимые формальности, связанные с таможенным оформлением. При необходимости уточняет сведения у декларанта, отправляя ему запрос в электронной форме.

4. После того как груз прибывает в таможню назначения таможенный инспектор проводит процедуру закрытия доставки товаров и выпускает ДТ.

Как показала практика, электронное декларирование товаров стало важным фактором упрощения и ускорения проведения таможенных процедур, таможенного контроля. Таможенные органы к моменту введения обязательного ЭД смогли провести оснащение и обустройство постов для обеспечения безопасности. Разумеется, существуют еще и определенные проблемы, которые решаются и будут решаться, в том числе и по вопросам информационной безопасности.

Основными целями таможенных правонарушений в области электронного декларирования являются неуплата таможенных пошлин. Реализуется она зачастую путем изменения таможенной стоимости товара, количества грузовых мест и др. данные ЭД которые могут повлиять на сумму таможенной пошлины. На сегодняшний день это основная цель незаконного получения таможенной информации в области электронного декларирования.

3.2 Институциональная основа информационной безопасности в системе Таможенных органов

Эффективность информационной безопасности таможенных органов зависит от наличия институтов, соотносимых по своей сущности с информационной безопасности системы в Таможенных органах. Данным институтом является Электронное правительство РФ.

Электронное правительство призвано обеспечить информационную безопасность государства, в том числе и таможенной службы, то есть противодействовать различным целям нарушения информационной безопасности. Для определения эффективности данного процесса необходимо изучить работу данной системы.

Постановкой и контролем за исполнением задач в Таможенной службы России занимается правительство РФ. В современных условиях в работе правительства РФ и управления ФТС РФ внедряются электронные формы управления и взаимодействия системой. Данные формы являются способами взаимодействия с помощью информационных технологий для предоставления государственных услуг. Существует ряд показателей, повышение которых влияет на эффективность формирования электронного правительства[50].

1. Снижение административных издержек при обращении граждан и организаций;
2. Сокращение времени на оказание услуг, повышение их качества, эффективности и доступности;
3. Гармонизация и стандартизация процессов оказания услуг организациям и гражданам;
4. Увеличение институтов гражданского общества в системе государственного управления;
5. Повышение доступности и открытости информации о деятельности государственной службы;
6. Создание условий для проведения полного контроля действий органов государственной власти;
7. Обеспечений информационной безопасности органов государственной власти;

Это основные показатели эффективности работы электронного правительства, которые в свою очередь можно выделить и как цели

[50] Оценка эффективности электронного правительства / Е.М. Балашова // Москва – 2015г.

достижения эффективности их работы. Соответственно для достижения данных целей можно привести ниже список следующих критериев[51]:

1. Развитие обеспечения граждан и государственных органов информационно-техническими средствами связей;
2. Создание правового поля в области электронного взаимодействия государственной службы и граждан;
3. Создание правового поля регулирующую порядок хранения документов и сведений, а также их сбор и обработку.
4. Предоставление гражданам государственной службой услуг и способы обращений через сети Интернет;
5. Создание закрытых, защищенных каналов связей, для безопасного документооборота в электронной сети;
6. Внедрение электронной системы отёчности и планирования для создания системы контроля деятельности государственных органов;

При создании электронного правительства существуют три этапа их формирования. Основаны на предыдущих критериях, таким образом, что учитывая каждый критерий в определенном этапе, была сформирована программа создания электронного правительства.

1й Этап – Публичность. При нем доступность граждан, различных организаций и предприятий к органам государственной власти увеличивается. Реализуется это с помощью информационных технических средств и созданием государственными органами Веб-сайтов Интернет свих служб. На данном этапе государственные органы отображают на своих веб-сайтах формы различных документов, отчетность, законодательные акты, экономические и статистические данные. Этот этап дает возможность гражданам при обращении в органы государственной власти оперативно воспользоваться необходимой им информацией при их дальнейшем взаимодействии.

[51] Электронное правительство. Основные понятия и определения [Электронный ресурс] / Электронная коммерция // http://elcomrevue.ru/elektronnoe-pravitelstvo-osnovnyie-ponyatiya-i-opredeleniya/

2й Этап - Транзакции-онлайн. На данном этапе государственные органы власти создают способы предоставления услуг в электронном виде гражданам в режиме онлайн. К примеру, такие услуги как подача деклараций, регистрация и оформление недвижимости, оформление заявлений, и.т.д. С помощью данного направления государственным органам стало возможно оказывать свои услуги в любое время суток, тем самым увеличить время работы. Также уменьшилась бюрократическая и коррупционная составляющая данных процессов, так как сократился физический контакт гражданина с чиновником.

3й Этап – Участие. При этом этапе создается взаимодействие органов государственной власти и общества. Гражданское общество имеет право участвовать в формировании политике и направлении деятельности той или иной государственной службы, предлагать и отвергать различные идеи. Реализуется данное направление с помощью различных веб-форумов, интерактивных опросов, специальных программ.

К функциям работы электронного правительства выделяют принципы разграничения форм взаимодействия, такие как:

- Между гражданином и государством;
- Между бизнесом и государством;
- Между государственными службами и ветвями власти;
- Между госслужащими и государством

С правовой стороны развитие системы таможенного управления закреплено в Стратегии развития ФТС до 2020 года[52]. Направленно оно в первую очередь на улучшении качества предоставляемых таможенных услуг в рамках таможенного администрирования. Таможенной службе необходимо выполнить непростую задачу, с одной стороны повысить эффективность таможенных услуг путем упрощения процедуры таможенного администрирования, с другой - обеспечивать безопасность, в том числе и

[52] Стратегия развития Федеральной таможенной службы России до 2020 года [Электронный ресурс] / ФТС РФ: Официальный сайт // http://customs.ru/index.php?option=com_content&view=article&id=17220&Itemid=2375

информационную. В ближайшем будущем таможенным органам РФ придётся столкнуться с увеличением потребности на таможенные услуги. Разумеется, им придётся в первую очередь развивать это направление.

Для качественной реализации повышения качества предоставляемых таможенными органами услуг, предлагаю решить следующие задачи:

1. Интеграция системы ЕАИС В систему предоставления таможенными органами услуг;
2. Повышения доступности таможенных услуг в электронной системе;
3. Проработка системы мониторинга и анализа качества таможенных услуг в автоматизированном режиме.

Федеральная таможенная служба России была также интегрирована в систему электронного правительства. Процесс начался в 2005 году с объявлением таможенной службы о «Проекте модернизации информационной системы ТО». Первостепенной задачей перед таможенной службой стояла правовое обеспечение данного процесса – необходимо было унифицировать и совершенствовать различные документы необходимые при работе в информационно технической среде. На сегодняшний день данный процесс естественно нельзя назвать завершенным. Чтобы определить на каком этапе развития в процессе интеграции в электронное правительство находится таможенная служба РФ необходимо разобрать следующие задачи:

1. Проанализировать теоретико-методологическую базу Таможенной службы РФ в процессе интеграции ее в электронное правительство;
2. Доказать обоснованность интеграции Таможенной службы РФ в систему электронного правительства с информационно-технической точки зрения;
3. В качестве доказательства привести возможные перспективы развития процесса интеграции Таможенной службы РФ в систему электронного правительства.

Первым наглядным примером развития ФТС РФ в системе электронного правительства является работа их официального сайта. Весьма емкий аналитический и новостной ресурс. Федеральная таможенная служба РФ предоставляет на данном сайте следующую информацию: Таможенное законодательство (своевременно обновляющееся), различные формы документов, ТН ВЭД ТС, отчеты о различной деятельности таможенных органов, принципы взаимодействия таможенных органов с участниками ВЭД и другими субъектами, и многое другое. Федеральная таможенная служба России через данные веб-сайт оказывает различное консультирование по вопросам, касающимся таможенного дела.

Процесс информатизации таможенных органов и интеграции в электронное правительство на сегодняшний день может похвастаться определенными достижениями. Например, с 2014 года декларирование товаров и транспортных средств окончательно перешло на электронную форму обращения. Как и прогнозировалось раньше, качество предоставляемой услуги существенно повысилось. Практически исчез риск коррупционной составляющей и бюрократизации различных процессов. Физическое взаимодействие таможенных органов с различными субъектами на сегодняшний день сведено к минимуму, что можно с уверенностью назвать успехом в интеграции ФТС РФ в систему электронного правительства. Также это отличный показатель в процессе обеспечении их информационной безопасности. Угрозы существенно уменьшились, но появились совершенно новые со стороны информационно технической поддержки. Если же рассматривать данные процессы со стороны экономического благополучия страны, то плюсов в виде повышения качества таможенных услуг намного больше, чем минусов, таких как угрозы информационной безопасности в электронной среде. К тому же развитие не стоит на месте, и таможенные органы успешно справляются с данными проблемами.

3.3 Модель потенциального нарушителя, как основа профилактики правонарушений информационной безопасности системы Таможенных органов

В качестве основы модели потенциального нарушителя информационной безопасности выступает схема, структура определенного фрагмента. Модель описывает основные характеристики оригинала, абстрагируясь от множества второстепенных его свойств[53].

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 РФ на период до 2010 года: 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[54]. Они создают нормативно правовое поле в рамках обеспечения безопасности информации таможенных органов.

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

[53] Моделирование производственно-инвестиционной деятельности фирмы. М., 2002. С. 8.
[54] Федеральный закон "О службе в таможенных органах Российской Федерации" от 21.07.1997 N 114-ФЗ

из вне системы. Риски, связанные с возможными нарушителями внутри системы (с правом доступа), в данной форме не учитываются.

Форма защиты информации Управление доступом это защита с помощью ограничения и регулирование доступа к техническим системам обработки информации[55]. В таможенных органах, как и в других государственных структурах, действует определенный порядок работы с данными и система доступа. Управление правом доступа к таможенной информации через базы данных несет за собой следующие функции защиты:

- Определение идентификации персонала системы, пользователя, необходимых ресурсов. У каждого объекта системы имеется свой персональный код, логин, пароль и др.

- Установка подлинности объекта и его принадлежности данной системы по предъявляемому им логину-паролю (идентификатору). Данная процедура называется аутентификация.

- Установка и проверка системы на соответствие полномочий пользователя с запрашиваемыми им ресурсами, а также датой, и временем. Данный процесс называется авторизация.

- Разрешение работы пользователю с таможенной информацией только в рамках его полномочий.

- Сохранение и регистрация действий объекта при его работе с данными. Данная процедура называется протокол.

- система защиты данных при несанкционированном проникновении (Например: отказ в запросе, выключение системы, срабатывание сигнализации и др.).

Особое внимание, на наш взгляд необходимо обратить внимание на процедуру установления подлинности пароля. Самый распространённый способ это набор цифр и символов. Оператор подтверждает доступ к системе путем ввода на клавиатуре или иных технических средств ввода данных

[55] Общие сведения об управлении доступом [Электронный ресурс] / «Русский ТехНик»: Проект корпорации Microsoft // https://technet.microsoft.com/ru-ru/library/cc753976(v=ws.11).aspx

определенную последовательность символов, букв или знаков. В случае если введённый пароль соответствует с паролем, хранящимся в данной системе, то оператор получает доступ к той или иной информации. Разумеется, что при определенных типах данных пароль служит, как и для разблокировки данных, так и для ее блокировки.

На сегодняшний день данная система паролей широко используется для защиты информации. Из положительных качеств данного метода можно выделить такие, как:

- простота и дешевизна системы;

- простота в процессе обработки техническим средством;

- быстродействие идентификации

Но существуют также и отрицательные стороны данного типа паролей:

- чрезмерно сложный набор символов и знаков непросто запомнить человеку, поэтому ему приходиться дублировать его на бумажном носители, что порождает определённые риски в системе информационной безопасности.

- человек, исходя из своей психологии, склонен выбирать несложный, неоригинальный пароль. Как правило, выбор останавливается на таких наборах символов как дата рождения, номер квартиры, телефона и иных символов связанные с личной жизнью пользователя.

- при вводе пользователя пароля всегда присутствует риск его обнаружения посторонним лицом находящимся рядом, даже если символы не отображаются на экране.

- пароль в зашифрованном виде всегда находится в системе. Опытный специалист всегда сможет завладеть им через иных пользователей данной системы.

- систему может поразить вирусные программы способные перехватывать, изменять или уничтожать пароли.

Проанализировав положительные и отрицательные качества пароля состоящего из символов, по-видимому, следует ввести следующие

требования к пользователям системы ЕАИС для улучшения качества обеспечения информационной безопасности таможенных органов.

1. Не дублировать пароль на бумажном носителе и других запоминающих устройствах.

2. При построении пароля пользователям избегать информации взятой из его личной жизни (дата рождения, имя собаки, и др.).

3. Чаще производить замену пароля, снижая тем самым риск его расшифровки.

4. Не разглашать свой пароль посторонним лицам.

5. Акцентировать внимание на более сложных построениях паролей, тем самым снижая риск его расшифровки.

При соблюдении данных требований, думается, что качество обеспечения информационной безопасности таможенных органов перейдет на более высокий уровень.

Ко всему вышесказанному, проанализировав показатели правоохранительной деятельности таможенных органов Российской Федерации за 2015 и 2016 года можно сделать вывод о том, что в основном современная практика ориентирована на выявление правонарушителя после совершения правонарушения[56].

Возможный вероятный нарушитель информационной безопасности таможенных органов это субъект, который имеет возможность реализовывать противоправные действия в области информационного обмена с помощью технических средств[57]. Для определения вероятности и степени возможности нарушения безопасности в сфере информационного обмена приводится следующая классификация нарушителей[58]:

[56] Показатели правоохранительной деятельности таможенных органов Российской Федерации за 2016 год [Электронный ресурс] / ФТС РФ: Официальный сайт // http://www.customs.ru/index.php?option=com_content&view=article&id=24719:-2016-&catid=55:2011-01-24-16-40-26

[57] Концепция обеспечения информационной безопасности до 2010 года [Электронный ресурс] / Правовая консультация / http://www.zakonprost.ru/content/base/part/491859

[58] Информационные системы в экономике / В.Н. Ясенев, О.В. Ясенев // Москва – 2016г.

1. Нарушитель или группа нарушителей, которая самостоятельно создаёт потенциальную угрозу, а также ее реализует. Нарушитель является внешним не находящимся в системе ЕАИС.

2. Нарушитель или группа нарушителей, состоящая в системе ЕАИС, с участием вышесказанного нарушителя.

3. Нарушитель или группа нарушителей, состоящая в системе ЕАИС, которые самостоятельно создают потенциальную угрозу, а также реализуют ее.

4. Нарушитель или группа нарушителей, состоящие в системе ЕАИС и с участием внешнего нарушителя, которые самостоятельно создают потенциальную угрозу, а также реализуют ее. Ко всему прочему они работают совместно с специалистами и сложными техническими средствами по захвату информации.

5. Нарушитель или группа нарушителей, состоящие в системе ЕАИС и с участием внешнего нарушителя, которые самостоятельно создают потенциальную угрозу, а также реализуют ее. Помимо специально привлеченных вышесказанных специалистов здесь принимают участие научно технические центры, специализирующие на информационной атаке.

6. Последний шестой тип нарушителя являются спецслужбы иностранных государств. Он включает в себя все вышесказанные способы и методы нарушения. Помимо всего прочего можно отметить такой фактор как внедрение иностранного агента в систему ЕАИС.

Исходя из статистики таможенных правонарушений в области информационной безопасности, шестой тип нарушителя является самым опасным для информационной безопасности таможенных органов. Он, как правило, состоит из высококвалифицированных специалистов оснащенных самыми эффективными техническими средствами воздействия на информацию. Для получения необходимой информации в их арсенале присутствуют все известные методы реализации своей цели.

Для обеспечения информационной безопасности таможенных органов по каждым данным формируется модель потенциального нарушителя. Для определения также учитываются такие факторы как цели и задачи практической деятельности субъекта, круг его партнеров, шпионаж, любопытство, вандализм и др.

На основании анализа имеющихся материалов об основных видах правонарушений в системе информационной безопасности Таможенных органов, а также на основании их целей и задач, возможно, смоделировать потенциального нарушителя информационной безопасности. Это позволит контролировать деятельность такого рода потенциальных нарушителей и предупредить возможные правонарушения.

Чтобы определить более конкретного нарушителя информационной безопасности таможенных органов, необходимо объединить данную классификацию и выявленные нами элементы определения модели нарушителя (тип, методы, цели). Например, видом информации будет таможенная стоимость из таможенной декларации, методом нарушения – перехват данных в сети интернет, цель - монополизация сегмента рынка. Применяя классификацию нарушителей информационной безопасности можно сразу исключить первые три класса, так как у них для реализации угрозы отсутствуют специальные технические средства для реализации данного метода нарушения. Чтобы сузить поиск среди оставшихся классов необходимо более конкретно проанализировать элементы определения модели нарушителя информационной безопасности. Если данных таможенной стоимости имеют потребность отечественные участники ВЭД, то навряд ли здесь задействованы иностранные спецслужбы. Если экономическая выгода нарушителя от полученных данных небольшая, то навряд ли здесь присутствует пятый класс нарушителя с его сложными составляющими элементами, реализация которых требует более высоких затрат. К данному примеру более всего подходит 4й тип нарушителя. У него

присутствуют необходимые мотивы и ресурсы для реализации данного нарушения.

Формирование модели потенциального нарушителя информационной безопасности производится за счет трех составляющих, это цели использования похищаемой информации, вид похищаемой информации и методы, при помощи которых эта информация была похищена. Данные элементы необходимо соотнести с классификацией нарушителей информационной безопасности для определения более конкретного вида нарушителя информационной безопасности таможенных органов.

Заключение

Подводя итог необходимо отметить, что все поставленные задачи для решения цели выпускной квалификационной работы были выполнены. Была описана эффективная модель потенциального правонарушителя информационной безопасности таможенных органов путем анализа полученных материалов об основных видах правонарушений в области информационной безопасности Таможенных органов, а так же на основании их целей и задач. При проведении изучения, анализа, и других методов которые, использовались при написании данной работы, были выявлены виды, угрозы и цели информации.

Виды информации, полученные путем анализа сущности понятия информационная безопасность. Она бывает двух типов – внутренняя и внешняя. К внешнему виду относится вся информация для обеспечения национальной безопасности страны. Это может быть любая информация, например, из таможенной декларации, статистических сборников, СМИ и др., которая будет угрозой экономической, социальной, территориальной обстановкой в стране. К внутренним видам относятся информация необходимая для качественного функционирования самой таможенной службой. Это может быть данные служебных переписок, информация внутренних распоряжений, любая информация, которая сможет повлиять на работу таможенных органов.

На сегодняшний день наиболее уязвимыми местами информационной безопасности таможенных органов России являются информационные угрозы. Связанно это с процессами мировой глобализации, развитием НТП и недостаточным опытом борьбы с данным видом угроз. С учетом поведенного изучения факторов влияющих на информационную безопасность таможенных органов, можно выделить пять основных методов правонарушения информационной безопасности таможенных органов, это Физические, радиоэлектронные, информационные, программно-

математические и организационно-правовые. Данные методы являются основой для выделения основных видов Таможенных правонарушений в области информационной безопасности.

Цели и принципы, для которых может быть использована информация, может быть огромное множество, также как и потребностей потенциальных нарушителей. Основными же, стоит выделить такие, как коррупция и уклонение от уплаты таможенных сборов и налогов. Как показывает статистика таможенных правонарушений на сегодняшний день это самые популярные цели нарушения информационной безопасности.

Для обеспечения информационной безопасности таможенных органов по каждым данным формируется модель потенциального нарушителя. Для определения также учитываются такие факторы как цели и задачи практической деятельности субъекта, круг его партнеров, шпионаж, любопытство, вандализм и др.

На основании анализа имеющихся материалов об основных видах правонарушений в системе информационной безопасности Таможенных органов, а также на основании их целей и задач, возможно, смоделировать потенциального нарушителя информационной безопасности. Это позволит контролировать деятельность такого рода потенциальных нарушителей и предупредить возможные правонарушения.

Подводя итог, стоит упомянуть о научной значимости данной работы. Эффективная модель нарушителя информационной безопасности таможенных органов позволит таможенным институтам улучшить процесс профилактики предупреждения правонарушений в области обеспечения информационной безопасности в таможенной сфере.

Список используемой литературы

1. Понятия информационной безопасности и угрозы национальной безопасности в информационной сфере [Электронный ресурс] / М.А. Лапина, А.Г. Ревин // http://jurisprudence.club/informatsionnoe-pravo_703/ponyatiya-informatsionnoy-bezopasnosti-ugrozyi.html (дата обращения 23.05.2017).

2. Угрозы информации и информационные угрозы. Подготовка кадров в области информационной безопасности / А.А. Малюк// Московский государственный инженерно-физический институт – 2006 г.

3. Информатизация общества. Основные этапы развития вычислительной техники / В.З. Аладьев // Издательский дом «Флинт» 2009г.

4. Информационные системы в экономике / В.Н. Ясенев, О.В. Ясенев // Москва – 2016г.

5. Информационные технологии в таможенном деле / Учебное пособие: В 2 ч. Часть 1 // Владивосток: ВФ РТА, 2003. – 265

6. Электронное декларирование / Высотина О.А., Гончарова К.А // Красноярск, 2012г. С. 18-20

7. Оценка эффективности электронного правительства / Е.М. Балашова // Москва – 2015г.

8. Моделирование производственно-инвестиционной деятельности фирмы. М., 2002. С. 8

9. Разработка правил информационной безопасности / Бармен Скотт // М.: Вильямс, 2002. — 208 с

10. Защита информации в сети — анализ технологий и синтез решений / В.Ф. Шаньгин М // ДМК Пресс, 2004. — 616 с

11. Административно-правовые аспекты обеспечения информационной безопасности таможенных органов Российской Федерации / дисс. канд. юрид. наук. Недосекова Е. С. // Люберцы, 2011. — 260с.

12. Исследование проблем информатизации применения информационных технологий в таможенном деле: отчет о НИР / науч. рук-ль И.И. Никитченко // ФТС России, РТА. Люберцы, 2010.- 136 с.

13. Обеспечение экономической безопасности правоохранительными подразделениями таможенных органов / учебник под общ. ред. В.А. Жбанкова // М.: Изд-во Российской таможенной академии, 2009. - 216 с.

14. Информационная безопасность России / дис. д-ра юрид. наук В.Н. Лопатин // СПб., 2000. - 433 с.

Список используемых источников

1. Конституция РФ, Глава 2 Права и свободы человека и гражданина [Электронный ресурс] / Консультант Плюс // URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения 23.05.2017).

2. Таможенный кодекс Таможенного союза, Статья 124. Обмен информацией между таможенными органами [Электронный ресурс] / Консультант Плюс // URL: http://www.consultant.ru/document/cons_doc_LAW_94890/ (дата обращения 23.05.2017).

3. Договор о Евразийском экономическом союзе [Электронный ресурс]: принят Решением Республики Беларусь, Республики Казахстан и Российской Федерации от 29 мая 2014 г.: (с изм. и доп. от 08.05.2015 г.) // URL: http://www.consultant.ru/document/cons_doc_LAW_170264/ (дата обращение 23.04.2016)

4. Международная конвенция от 18 мая 1973 года «Об упрощении и гармонизации таможенных процедур»

5. Федеральный закон от 27.11.2010 N 311-ФЗ (ред. от 28.12.2016) "О таможенном регулировании в Российской Федерации"

6. ФЗ закон «ОБ электронной цифровой подписи от 23 января 2002 года».

7. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

8. Федеральный закон "О службе в таможенных органах Российской Федерации" от 21.07.1997 N 114-ФЗ

9. Стратегия развития Федеральной таможенной службы России до 2020 года [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://customs.ru/index.php?option=com_content&view=article&id=17220&Itemid=2375 (дата обращения 23.05.2017).

10. Приказ Федеральной таможенной службы от 9 декабря 2011 г. № 2490 “Об утверждении Инструкции о порядке подготовки и исполнения международных запросов, не относящихся к делам об административных правонарушениях и не связанных с проведением оперативных проверок”

11. Соглашение о взаимной административной помощи таможенных органов государств-членов таможенного союза от 21 мая 2010 г.

12. Приказ ФТС РФ от 13 марта 2015 года №423 «Об утверждении Положения по организации процессов жизненного цикла информационно-программных средств в таможенных органах»

13. Приказ ФТС РФ от 19 марта 2004 года «Об утверждении общего порядка разработки и модернизации программных средств ЕАИС ГТК России» [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://customs.ru/index.php?option=com_content&view=article&id=21732:2015-09-30-10-04-42&catid=40:2011-01-24-15-02-45 (дата обращения 23.05.2017).

14. Итоги Реализации проекта «Модернизация информационной системы Таможенных органов» [Электронный ресурс] // ФТС РФ: Официальный сайт URL: http://www.customs.ru/index.php?Itemid=1871&id=18644&option=com_content&view=article (дата обращения 23.05.2017).

15. Государственная программа «Информационное общество» (2011–2020 годы) [Электронный ресурс] / Минкомсвязь России: Официальный сайт // URL: http://minsvyaz.ru/ru/activity/programs/1/ (дата обращения 23.05.2017).

16. Соглашения «О представлении и об обмене предварительной информацией о товарах и транспортных средствах, перемещаемых через таможенную границу таможенного союза» 0т 27 ноября 2009 г.

17. Показатели правоохранительной деятельности таможенных органов Российской Федерации за 2015 год [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://www.customs.ru/index.php?option=com_content&view=article&id=22498:-2015-&catid=55:2011-01-24-16-40-26&Itemid=1958 (дата обращения 23.05.2017).

18. Этапы развития информационной безопасности [Электронный ресурс] / Программирование и визуализация // URL: http://life-prog.ru/1_46301_etapi-razvitiya-informatsionnoy-bezopasnosti.html (дата обращения 23.05.2017).

19. Информационный взрыв продолжается [Электронный ресурс] / Идеи и практики автоматизации // URL: https://www.pcweek.ru/idea/article/detail.php?ID=123306 (дата обращения 23.05.2017).

20. Политика информационной безопасности [Электронный ресурс] / Компания «Альтернативные решения» // URL: http://www.arinteg.ru/articles/politika-informatsionnoy-bezopasnosti-27713.html (дата обращения 23.05.2017).

21. ГОСТ Р ИСО/МЭК 13335-1-2006 Библиографическая ссылка. Национальный стандарт РФ. М., 2006. 22 с. (Методы и средства обеспечения безопасности).

22. ИСО/МЭК 17799, ИСО/МЭК 13335-4 Библиографическая ссылка. Национальный стандарт РФ. М., 2006. П. 2. (Термины и определения).

23. Обеспечение информационной безопасности таможенных органов РФ [Электронный ресурс] / Таможенный брокер // URL: http://brokert.ru/material/informacionnaya-bezopasnost-tamozhennyh-organov (дата обращения 23.05.2017).

24. Система таможенных органов России: основные функции и принципы их взаимодействия [Электронный ресурс] / Таможенное дело // URL: http://studme.org/159701227784/ekonomika/sistema_tamozhennyh_organov_rossii_osnovnye_funktsii_printsipy_vzaimodeystviya (дата обращения 23.05.2017).

25. Структура таможенных органов Российской Федерации [электронный ресурс] / Альта Софт: Онлайн справочник // URL: https://www.alta.ru/tam/struct/ (дата обращения 23.05.2017).

26. Итоговый доклад о результатах и основных направлениях деятельности ФТС России в 2016 году [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://www.customs.ru/index.php?option=com_content&view=article&id=24865:-2016-&catid=475:2015-03-12-09-57-15&Itemid=2588 (дата обращения 23.05.2017).

27. Международное сотрудничество Российской Федерации в области таможенного дела [Электронный ресурс] / Таможенное право // URL: http://lib.sale/tamojennoe-pravo-uchebnik/mejdunarodnoe-sotrudnichestvo-rossiyskoy-34122.html (дата обращения 23.05.2017).

28. Общая информация о представителях таможенной службы Российской Федерации за рубежом [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://www.customs.ru/index.php?option=com_content&view=article&id=22293:2015-12-15-06-49-51&catid=179:2011-03-25-06-42-48&Itemid=2088 (дата обращения 23.05.2017).

29. Контакты представительств (представителей) таможенной службы за рубежом [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://www.customs.ru/index.php?option=com_content&view=article&id=22294:2015-12-15-06-56-45&catid=179:2011-03-25-06-42-48&Itemid=2088 (дата обращения 23.05.2017).

30. Виды угроз информационной безопасности [Электронный ресурс] / Системы информационной безопасности // URL: http://www.arinteg.ru/articles/ugrozy-informatsionnoy-bezopasnosti-27123.html (дата обращения 23.05.2017).

31. Способы нарушения информационной безопасности таможенных органов Российской Федерации [Электронный ресурс] / Правовая консультация // URL: http://www.zakonprost.ru/content/base/part/491871 (дата обращения 23.05.2017).

32. Признаки информационного общества [Электронный ресурс] / Проблемы информатизации образования // URL: https://sites.google.com/site/probinobrz/problemy-informatizacii-obrazovania-1/priznaki-informacionnogo-obsestva (дата обращения 23.05.2017).

33. Стандартизация в области информационных технологий [Электронный ресурс] / XI Международный семинар по стандартизации // URL: http://normdocs.ru/page.jsp?pk=node_1157453970729 (дата обращения 23.05.2017).

34. Единая автоматизированная информационная система (ЕАИС) ФТС России [Электронный ресурс] / Сущность экономической безопасности РФ // URL: http://studopedia.info/2-52279.html (дата обращения 23.05.2017).

35. Характеристика информационных процессов [Электронный ресурс] / Центр управления финансами // URL: http://center-yf.ru/data/stat/Harakteristika-informacionnyh-processov.php (дата обращения 23.05.2017).

36. Виды электронной подписи [Электронный ресурс] / Единый портал ЭЦП в РФ // URL: http://www.iecp.ru/ep (дата обращения 23.05.2017).

37. Выдача ключей Электронной Подписи [Электронный ресурс] / Единый портал ЭЦП в РФ // URL: http://www.icentr.ru/center.html (дата обращения 23.05.2017).

38. Электронное декларирование через Интернет [Электронный ресурс] / ТКС: Все о таможни // URL: http://www.tks.ru/ed2prosto.shtml (дата обращения 23.05.2017).

39. Подключение к системе электронного декларирования [Электронные ресурсы] / Передовые технологии// URL: https://www.sztls.ru/services/elecdecl/ (дата обращения 23.05.2017).

40. Интервью начальника Главного управления организации таможенного оформления и таможенного контроля (ГУОТОиТК) Дмитрия НЕКРАСОВА журналу «Таможня» № 12-13, 2011 «Таможенный союз: пути и решения» [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://www.customs.ru/index.php?option=com_content&view=article&id=14332:----------lr--12-13-2011-l----r&catid=26:2011-01-24-14-45-21&Itemid=1830&Itemid= (дата обращения 23.05.2017).

41. Разработка в сфере информационно-коммуникационных технологий в таможенных органах [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://www.customs.ru/index.php?option=com_content&view=article&id=22977:-31-2016-&catid=26:2011-01-24-14-45-21&Itemid=1830 (дата обращения 23.05.2017).

42. Электронное таможенное декларирование [Электронный ресурс] / Таможенный брокер «КВТ» // URL: http://www.kvtservice.su/services/ed/ (дата обращения 23.05.2017).

43. Электронное правительство. Основные понятия и определения [Электронный ресурс] / Электронная коммерция // URL: http://elcomrevue.ru/elektronnoe-pravitelstvo-osnovnyie-ponyatiya-i-opredeleniya/ (дата обращения 23.05.2017).

44. Общие сведения об управлении доступом [Электронный ресурс] / «Русский ТехНик»: Проект корпорации Microsoft // URL: https://technet.microsoft.com/ru-ru/library/cc753976(v=ws.11).aspx (дата обращения 23.05.2017).

45. Показатели правоохранительной деятельности таможенных органов Российской Федерации за 2016 год [Электронный ресурс] / ФТС РФ: Официальный сайт // URL: http://www.customs.ru/index.php?option=com_content&view=article&id=24719:-2016-&catid=55:2011-01-24-16-40-26 (дата обращения 23.05.2017).

46. Концепция обеспечения информационной безопасности до 2010 года [Электронный ресурс] / Правовая консультация / URL: http://www.zakonprost.ru/content/base/part/491859 (дата обращения 23.05.2017).

47. Формирование политики информационной безопасности [Электронный ресурс] / Менеджмент в сфере информационной безопасности // URL: http://rfcmd.ru/sphider/docs/InfoSec/GOST-R_ISO_IEC_13335-1-2006.htm (дата обращения 23.05.2017).