МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра таможенного, административного и финансового права

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ТАМОЖЕННЫХ ОРГАНАХ

АВТОРЕФЕРАТ ДИПЛОМНОЙ РАБОТЫ

Студента5курса 552 группы
специальности 38.05.02 «Таможенное дело»
юридического факультета СГУ им. Н.Г.Чернышевского
Ким Романа Алексеевича

Научный руководитель
доцент, к.ю.н., доцент Т.Г.Касаева

Зав. кафедрой
таможенного, административного
и финансового права, к.ю.н. С.А. Овсянников

Саратов 2023

Во введении обоснована актуальность выбранной темы.

В свете научно-технического прогресса, ускоряющейся глобализации и информатизации общества, возрастают риски нарушения информационной безопасности, в том числе и в сфере таможенных органов. Для эффективной защиты национальной безопасности и безупречной работы своей системы, таким органам необходимо бороться с различными информационными угрозами.

Таможенным органам приходится сталкиваться с новыми видами угроз информационной безопасности, что требует изменения методов их противодействия. Вместо традиционных физических и радиоэлектронных методов нарушения безопасности появляются новые информационные методы, что приводит к качественной трансформации стратегий борьбы с угрозами в данной сфере.

В настоящее время отсутствует эффективная система профилактики и предотвращения нарушений информационной безопасности в таможенных органах. Ранее существовавшие формы борьбы и профилактики основывались на законодательстве и криптографической базе. Однако в современных условиях, когда угрозы информационной безопасности в основном имеют информационный характер, традиционная система профилактики неэффективна. Следует также отметить, что актуальность и значимость проблемы обеспечения информационной безопасности закреплена в списке приоритетных задач таможенных органов и в Стратегии развития таможенной службы РФ до 2030 г.

Степень разработанности проблемы. В современных условиях вопросы информационной безопасности нашли отражение в трудах таких ученых как В.И. Кузнецов, В.Н. Лопатин, И.А. Михальченко, С.А. Модестов, В.И. Мухин, В.К. Новиков, А.И. Палий, Т.А Полякова, М.М. Рассолов, В.В. Ратиев, а также других авторов, которые посвящали свои работы данной тематике.

Объектом исследования являются общественные отношения, возникающие в процессе обеспечения информационной безопасности таможенных органов РФ.

Предметом исследования являются нормы, которые регулируют обеспечение информационной безопасности таможенных органов РФ.

Цель выпускной квалификационной работы – разработать эффективную модель обеспечения информационной безопасности таможенных органов.

Для раскрытия темы исследования определены следующие основные задачи:

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

– уточнить сущность и значение и информационной безопасности в области таможенного дела;

– исследовать особенности информационной безопасности в рамках ЕАЭС;

– охарактеризовать основные угрозы обеспечения информационной безопасности таможенных органов;

– выявить особенности электронной цифровой подписи как основного способа противодействия правонарушениям в системе информационной безопасности;

– охарактеризовать электронное декларирование как практическую основу эффективной модели выявления нарушителя информационной безопасности в системе таможенных органов РФ;

– обозначить основу информационной безопасности в системе таможенных органов в виде электронного правительства;

– выделить модель потенциального нарушителя как профилактическую основу эффективной модели выявления нарушителя информационной безопасности в системе таможенных органов РФ.

Теоретико-методологической основой работы являются труды отечественных и зарубежных ученых, раскрывающие различные аспекты обеспечения информационной безопасности таможенных органов РФ.

Нормативно - правовая база исследования включает в себя: международные правовые акты, федеральное законодательство, нормативные акты по вопросам деятельности таможенной службы, Федеральной таможенной службы Российской Федерации, Таможенного Союза ЕАЭС.

В данной работе 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).

Структура работы отражает порядок исследования и решение поставленных задач. Выпускная квалификационная работа состоит из введения, трех глав, заключения, списка используемых источников.

В первойглаведипломной работы «Информация и информационная безопасность в современной системе таможенных органов РФ»рассматривается информация как объект правонарушения, а также сущность и значение информационной безопасности в таможенном деле и ее особенности в рамках ЕАЭС.

Автором отмечается, что таможенная служба имеет обширные информационные ресурсы, которые также требуют защиты. Также на таможенных органах лежит часть ответственности за обеспечение национальной безопасности страны, поэтому надежное обеспечение информационной безопасности является значимым элементом достижения

этой цели. Обеспечение информационной безопасности таможенных органов может быть условно разделено на два типа: первый заключается в обеспечении информационной безопасности для достижения национальной безопасности (экономической, социальной, территориальной и т. д.), а второй - в обеспечении безопасности информации для своего обычного функционирования (эффективности управления, взаимодействия).

Охрана информационной безопасности в рамках ЕАЭС считается задачей, неотъемлемой для обеспечения национальной безопасности страны. В текущий момент обеспечение информационной безопасности не осуществляется на уровне наднационального контроля. Каждая страна-участница ЕАЭС обеспечивает национальную безопасность на своей территории в соответствии со своим законодательством. В связи с этим необходимо грамотное взаимодействие между таможенными органами ЕАЭС, чтобы создать единые принципы и критерии защиты информации таможенных органов. Для выявления объектов потенциальных нарушений информационной безопасности таможенных органов в рамках ЕАЭС, необходимо определить цели взаимодействия, типы информации, которые передаются, и порядок передачи этих данных.

Для обеспечения информационной безопасности таможенных органов необходимо приводить передаваемую информацию к унифицированному стандарту и технологии передачи данных. При международном взаимодействии таможенных органов были выявлены виды информации, которые могут стать объектом правонарушения, включая данные о международных перевозках, информацию об участниках ВЭД, информацию о процедуре предварительного информирования, а также сведения о международных договорах и соглашениях. Важность этих видов информации связана с потенциальной угрозой для информационной безопасности таможенных органов.

Таким образом, в данной главе рассмотрена актуальность и значимость информационной безопасности для таможенных органов, обозначена

информация как объект правонарушения в системе таможенных органов. Также рассмотрены особенности информационной безопасности в рамках ЕАЭС.

Во второй главе«Способы и средства противодействия посягательствам на информационную безопасность в системе таможенных органов РФ» описываются угрозы информационной безопасности таможенных органов, методы незаконного получения таможенной информации, а также электронная цифровая подпись как основной способ противодействия правонарушениям.

Для выявления методов нарушения информационной безопасности таможенных органов необходимо проанализировать все возможные виды угроз для информационной безопасности этих органов. Процесс обеспечения информационной безопасности таможенных органов является комплексным и многогранным. Деятельность этого процесса определяет большое количество факторов, которые с течением времени изменяются либо дополняются новыми. Формирование определенных факторов наиболее сильно влияет на современную ситуацию. Эти факторы могут включать политические процессы, экономические условия в стране, а также развитие внешнеторговых отношений. На обеспечение информационной безопасности таможенных органов это влияние проявляется особенно ярко, поскольку указанные процессы создают благоприятные условия для потенциальных нарушителей.

Основой информационной безопасности таможенных органов является именно ЕАИС. Это обусловлено многими факторами. Например, сильная интеграция во всех направлениях работы таможенных органов, довольно длинная история и хороший 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 ЕАЭС. В ЕАИС возможно применение всех методов нарушения информационной безопасности, что делает ее основным объектом таможенных правонарушений в области информационной безопасности.

Таким образом, можно выделить пять основных методов нарушения информационной безопасности таможенных органов: физические, радиоэлектронные, информационные, программно-математические и организационно-правовые. Эти методы образуют основу для выделения основных видов правонарушений в сфере таможенной информационной безопасности.

Подводя итог по данной главе, можно отметить пять основных методов правонарушения информационной безопасности таможенных органов, которые являются основой для выделения основных видов таможенных правонарушений в области информационной безопасности. Стоит отметить, что современный этап развития информатизации общества и таможенной службы подвержен в большей мере информационному методу нарушения информационной безопасности таможенных органов, это связанно с тем, что они являются наиболее эффективными в настоящее время. Также определено, что ЕАИС таможенных органов является основным объектом таможенного нарушения в сфере обеспечения информационной безопасности. И стоит отметить электронную цифровую подпись, которая является эффективным методом обеспечения информационной безопасности таможенных органов на сегодняшний день.

В третьей главе«Направления совершенствования информационной безопасности в таможенных органах РФ» дается описание направлений совершенствования информационной безопасности в таможенных органах, таких как электронное декларирование, электронное правительство, а также модель потенциального нарушителя как основа профилактики правонарушений информационной безопасности.

На практике, электронное декларирование товаров стало важным фактором упрощения и ускорения проведения таможенных процедур,

таможенного контроля. Разумеется, существуют еще и определенные проблемы, которые решаются и будут решаться, в том числе и по вопросам информационной безопасности. Процесс информатизации таможенных органов и интеграции в электронное правительство на сегодняшний день отмечается достаточно хорошими достижениями. Также, при формировании модели потенциального нарушителя информационной безопасности важно учитывать 3 составляющих, это цель использования похищаемой информации, вид похищаемой информации и метод, при помощи которого эта информация была похищена. Эти элементы необходимо соотносить с классификацией нарушителей информационной безопасности для того, чтобы более конкретно определить вид нарушителя информационной безопасности таможенных органов.

Заключение работы отражает основные выводы автора, сделанные в ходе всего дипломного исследования.

Была представлена эффективная модель потенциального правонарушителя информационной безопасности таможенных органов, основанная на анализе информации о наиболее распространенных нарушениях в этой области, а также на изучении целей и задач этих правонарушителей.

В ходе исследования были обнаружены различные виды угроз и целей по отношению к информации, которые были учтены при написании данной работы.

Данные, полученные при изучении концепции информационной безопасности, могут быть классифицированы на два вида: внутреннюю и внешнюю информацию. Внешним видом является любая информация, которая может представлять угрозу экономическому, социальному и территориальному благополучию страны и требует защиты для обеспечения национальной безопасности. К такой информации относятся данные из таможенных деклараций, статистических отчетов, СМИ и т.д. Внутренние виды включают данные, необходимые для эффективной работы таможенных

служб, такие как данные переписок, внутренних указаний и любая другая информация, которая может оказать влияние на работу таможенных органов.

Современные угрозы информационной безопасности, связанные с глобализацией, прогрессом в науке и технологиях, а также недостаточным опытом борьбы с этими угрозами, являются наиболее уязвимыми местами для таможенных органов Российской Федерации в настоящее время.

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. Основу определения основных видов таможенных правонарушений в области информационной безопасности составляют определенные методы. Они могут использоваться для различных целей и принципов, в зависимости от потребностей потенциальных нарушителей. Среди них выделяются коррупция и уклонение от уплаты таможенных сборов и налогов, которые являются самыми распространенными целями нарушения информационной безопасности, согласно статистике таможенных правонарушений на данный момент.

Для обеспечения безопасности информации таможенных органов Российской Федерации каждый тип данных рассматривается в контексте потенциального нарушителя, который является основой модели. При определении этой модели учитываются такие факторы, как цели и задачи практической деятельности субъекта, его круг партнеров, возможный шпионаж, любопытство, вандализм и другие, которые могут оказать влияние на безопасность информации.

Анализ основных видов правонарушений в системе информационной безопасности таможенных органов, а также их целей и задач, позволяет создать модель потенциального нарушителя информационной безопасности.

Это обеспечивает контроль над деятельностью таких потенциальных нарушителей и помогает предотвратить возможные нарушения закона.

Подводя итог, следует отметить научную значимость данной работы. Разработка эффективной модели потенциального нарушителя информационной безопасности таможенных органов позволит улучшить процесс профилактики правонарушений в области обеспечения информационной безопасности в таможенной сфере. Это направлено на повышение эффективности работы таможенных институтов и обеспечение лучшей защиты информации от внешних угроз.