УДК 656.073

АНАЛИЗ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ РОССИИ

Сакович С.И.

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

ANALYSIS OF INFORMATION SECURITY ISSUES OF THE CUSTOMS BODIES OF RUSSIA

Sakovich S.I.

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

Аннотация

В статье описаны основные принципы построения системы информационной безопасности. Рассмотрены основные проблемы, возникающие в процессе ее функционирования.

Ключевые слова: информация, информационные технологии, информационная безопасность, таможенный контроль, таможенное администрирование.

Abstract

The article describes the basic principles of building an information security system. The main problems arising in the process of its functioning are considered.

Keywords: information, information technology, information security, customs control, customs administration.

Для таможенных органов Российской Федерации основной целью создание системы электронной таможни [1], в связи с этим возрастает потребность в сотрудниках, являющихся специалистами в области функционирования информационных систем.

Одним из главных элементов работоспособности любой организации является наличие оптимальной структуры. Сфера таможенного дела не является исключением. В современных условиях важнейшими элементами организации таможенного дела являются выбор оптимальной структуры таможенной службы и численности её подразделений. Вопросы, связанные с комплектованием служб и отделов, обеспечивающих поддержку информационных технологий возникли давно.

Некоторые специалисты считают, для оптимального обеспечения информационной безопасности достаточно использовать современные средства защиты. Такое мнение имеет право на существование. Ведь результат работы технических средств защиты более нагляден и осязаем. К тому же с такими средствами приходится работать практически ежедневно как сотрудникам профильных отделов, так и не специалистам в области защиты. Яркий пример, антивирусные программы или парольная защита.

Процесс информатизации тесно связан с таможенным делом [2]. В связи с этим необходимо создавать современные центры обработки данных, которые будут отвечать требованиям мировой торговли, обладающие высокой степенью технической защиты.

Стоит отметить, что помимо технических средств защиты неоценимый вклад в дело вносят организационные и правовые меры. Тем не менее, их вклад чаще всего оценивается как менее видимый [3]. К правовому регулированию данной проблематики необходимо отнести нормативно-правовые акты, устанавливающие порядок отношений в сфере информационной безопасности таможенной деятельности Российской Федерации. К организационным аспектам информационной безопасности относится создание качественной организационно-штатной структуры подразделений обеспечения информационной безопасности, а также режим работы с информацией и информационными ресурсами.

Таким образом, технические, правовые и организационные средства образуют единую систему информационной безопасности таможенной деятельности.

Внедрение инновационных технологий в процесс обеспечения информационной

безопасности таможенного дела обусловлено несколькими взаимосвязанными факторами [4].

В развитии информационных технологий и их широком применении на мировом рынке важную роль призвана сыграть активизация инновационной деятельности, высокая роль которой связана со значительной перегруппировка факторов и источников, определяющих экономическое развитие. Экономисты утверждают – экономический рост определяется использованием результатов научных и технических достижений. Подтверждением этому является курс государства на инновационную политику, разработку механизмов поддержки приоритетных инновационных программ и проектов.

В контексте инновационной политики Россия, как и многие государства, стоит перед необходимостью рационального вложения финансовых средств в научные исследования и разработки, преследуя цель получения необходимых благ для экономики страны и перевод ее на качественно новый уровень.

Организация информационно-правового обеспечения защиты информации в таможенном деле, предусматривает внедрение в практику таможенной службы современных информационных технологий. Речь особенно идет о таких технологиях, которые позволяют выполнять функции управления, вырабатывать управленческие решения.

Информатизация управленческой деятельности позволяет повышать научную обоснованность принятия управленческих решений, придавать им такие свойства, как оперативность и актуальность их принятия, адресность, целенаправленность.

Общее понятие «информационные технологии» по своему содержанию означает систему средств и методов работы с информацией для получения информации нового качества о состоянии объекта, процесса или явления, а применительно к заявленной теме – под информационными технологиями следует понимать автоматизированную систему средств использующих определенную совокупность методов сбора, обработки (анализа), оценки и защиты социально-правовой информации в процессе выработки проектов управленческих решений.

Информационные технологии являются составным элементом – технологии управленческой деятельности. Как научная дисциплина технология управления нацелена на исследование и разработку правил эффективного управления с целью достижения высоких результатов, являющихся критерием качества.

Качество применения информационных технологий устанавливается четкой организацией следующих этапов сбора информации: разработка программы действий; подбор и подготовка исполнителей; создание условий для их работы.

Для эффективной защиты информации главным является точная проработка правового аспекта [5]. Здесь необходимо разграничить информационные объекты, законодательно определить правовой режим каждого из них.

Правовой режим информации как объекта правового регулирования должен рассматриваться с позиций ее доступности. В этом контексте можно определить общедоступную информацию (открытую информацию), конфиденциальную информацию (информацию ограниченного доступа) и информацию, составляющую государственную тайну (закрытую информацию).

В практической деятельности сотрудникам таможенных органов приходится взаимодействовать с информацией всех типов. И тут под особым контролем находится защита конфиденциальной информации. При этом нужно понимать, что безопасность информации является лишь составной частью информационной безопасности.

В увеличение объема использования информационных технологий в таможенных органах вносит весомый вклад их применение для противодействия угрозам безопасности. Необходимо уточнить, что усиление спроса на подобные технологии обусловливается ростом информатизации общества и как следствие повышение количества внешних и внутренних угроз, а также развитием технических средств защиты информации.

Эффективность управленческой деятельности таможенных органов зависит от различных факторов. Главным, конечно же, является умение сформулировать принципы работы с информационными ресурсами, а также создать условия для их безусловной защиты от нерегламентированного доступа.

Важным вектором дальнейшего развития системы таможенного администрирования [6], совершенствования механизмов таможенного оформления и контроля, повышения прозрачности таможенных процедур

является автоматизация таможенных технологий и оперативного управления таможенной деятельностью, обеспечивающая решение нескольких комплексных задач. К таким задачам относятся сбор, обработка, хранение, а также мониторинг рабочей информации о состоянии процессов таможенного оформления и контроля, планирование деятельности таможенных органов и оценка качества их работы, построение и распространение в автоматизированном режиме по всей таможенной службе управляющей информации, касающейся всех направлений работы.

Суть автоматизации таможенных технологий заключается в минимизации человеческого влияния при принятии решений, передавая эти полномочия информационно-техническим средствам, объединенным в систему оперативного управления таможенной деятельностью.

В этом ключе появляется необходимость подготовки специалистов широкого профиля, которые будут одинаково компетентны в технических, правовых и организационных вопросах.

На сегодняшний день, в правовом обеспечении информационной безопасности в таможенной сфере существуют некоторые разночтения. В связи с этим определенные нормативные акты требуют корректировки. Существует необходимость приведения действующей правовой базы к единому знаменателю. А именно, оптимизация правовых режимов информационной безопасности, закрепление принципов построения алгоритма принятия управленческих решений, для максимально эффективного обеспечения информационной безопасности в таможенных органах.

Набором основополагающих принципов для обеспечения информационной безопасности можно считать невозможность обхода средств защиты и перехода в открытое состояние, наличие многоуровневой защиты, широкий спектр используемых защитных средств, усиление слабой стороны, делегирование полномочий, сокращение прав, а также простота и управляемость системы.

Принцип невозможности обхода средств защиты заключается в том, что все без исключения входящие и исходящие потоки информации должны проходить через средства защиты информации. В штатном режиме работы и при возникновении критических ситуаций, система защиты не должна открывать доступ к содержимому неограниченному кругу лиц. Информация должна быть либо защищена, либо заблокирована.

Под многоуровневой защитой подразумевается усиление защиты с использованием нескольких форм и методов. Например, первоначально защитой служат физические свойства (решетки, двери, замки). Затем используются программно-технические средства, идентификация и аутентификация, разграничение прав доступа. Также обязательно использование систем протоколирования и аудита действий. Протоколирование и аудит – лишает возможности уязвимостям остаться незамеченными. Широкий спектр защитных средств предполагает использование средств с различными принципами действия, что заметно усложняет процесс их взлома или обхода, так как потребуют специфических знаний и умений.

В любой системе защиты необходимо определить самое уязвимое, слабое место. Проблема уязвимости может носить технический (программа, техническое средство) или нетехнический (человеческий фактор) характер. Знание природы проблемы уязвимости позволяет укрепить систему защиты.

Делегирование полномочий или распределение прав доступа (ролей, ответственности) позволяет избежать нарушения или остановки критически важного для таможенного органа процесса. Делегирование полномочий предотвращает злонамеренные или непрофессиональные действия. Этому также способствует принцип сокращения прав. Рекомендуется выделять только те права, которые необходимы и достаточны для выполнения должностными лицами служебных обязанностей

Принцип простоты и управляемости позволяет проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

Информатизация таможенных процессов требует вовлечения компетентных специалистов, которые смогли бы обеспечивать все информационные операции. Таможенные информационные технологии становятся все более совершенными в техническом смысле и требуют большего внимания в обслуживании, что, возможно, влечет за собой увеличение штатной численности специалистов, обеспечивающих их функционирование и защиту.

Еще один аргумент в пользу увеличения числа сотрудников подразделений информационной безопасности и технической защиты информации таможенных органов – выполнение таможенных операций в должном объеме невозможно без использования информационных технологий, их модернизации.

Стоит также отметить, что, увеличивая количество специалистов подразделений информационной безопасности и технической защиты информации таможенных органов нельзя забывать о необходимости повышения их профессиональных навыков. Их уровень умений, знаний и навыков должен выходить за рамки одной специализации. Таким специалистам кроме технических знаний, требуются и знания организационного и правового аспекта информационных процессов, проводимых в таможенных органах.

Список литературы

1. Шашаев А.Е. Перспективные направления долгосрочного развития информационно-технического обеспечения Федеральной таможенной службы / сборник материалов международной научно-практической конференции 7-8 апреля 2011года «Единое окно», обмен данными, межведомственное и государственно-частное сотрудничество при упрощении процедур торговли. М. 2011. 229 с.

2. Павлова Я.В. Информационные технологии в таможенном деле // Бюллетень инновационных технологий. 2019. Т. 3. № 2 (10). С. 56-59.

3. Кожуханов Н. М. Проблемы разграничения правовых категорий в сфере обеспечения информационной безопасности деятельности таможенных органов // Юриспруденция. 2010. №2. URL: https://cyberleninka.ru/article/n/problemy-razgranicheniya-pravovyh-kategoriy-v-sfere-obespecheniya-informatsionnoy-bezopasnosti-deyatelnosti-tamozhennyh-organov (дата обращения: 09.11.2019).

4. Аксенов И.А. Информационные технологии в таможенном деле: учебное пособие. СПБ: Свое издательство, 2016. 90 с.

5. Цидилина И. А. Проблемы правового регулирования информационной безопасности таможенного администрирования в Российской Федерации // Информационная безопасность регионов. 2012. №2. URL: https://cyberleninka.ru/article/n/problemy-pravovogo-regulirovaniya-informatsionnoy-bezopasnosti-tamozhennogo-administrirovaniya-v-rossiyskoy-federatsii (дата обращения: 09.11.2019).

6. Павлова Я.В. Проблемы использования информационных технологий в таможенных органах // Бюллетень инновационных технологий. 2019. Т. 3. № 3 (11). С. 31-34.

Поступила в редакцию 09.11.2019

Сведения об авторе:

Сакович Сергей Иванович – заместитель декана по учебной работе факультета таможенного дела, доцент кафедры информатики и информационных таможенных технологий Санкт-Петербургского филиала Российской таможенной академии, кандидат технических наук, e- mail: ssakovich15@gmail.com

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