ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ В ТАМОЖЕННОМ ДЕЛЕ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Козлов В. В.

Ионин В. С. – канд.техн.наук,доцент

В статье рассматриваются результаты исследования, целью которого является усовершенствование системы безопасности таможенных органов путем обеспечения информационной безопасности с использованием инновационных методов, а так же предлагается возможное решение для достижения поставленной цели.

Особенностью регулирования информационного обеспечения административного расследования в таможенной сфере является то, что при проведении административного расследования приходится иметь дело с особым видом информации: таможенной информацией, содержащейся в таможенных документах. Так, согласно Таможенному Кодексу Республики Беларусь (ТК РБ), таможенные документы - это документы, составляемые исключительно в таможенных целях. Они характеризуются особой формой представления информации (товарные декларации, инвойсы, декларация таможенной стоимости и др.), содержанием (содержат сведения, необходимые для выполнения таможенных процедур), способом и порядком представления, утвержденным ведомственными нормативными актами, а также субъектами, уполномоченными на их представление (перевозчики, декларанты и другие участники внешней экономической деятельности, список которых установлен ТК РБ, государственными органами и другими сторонними организациями, в том числе международными, по запросам таможенных органов). Для таможенных документов установлен особый порядок хранения и движения, который закреплен в инструкциях, рекомендациях, регламентах и технологических схемах, действующих в таможенной сфере [1].

Цель исследования – повышение качества административного расследования в таможенном деле за счет модернизации системы безопасности таможенных органов инновационными методами.

Угрозами безопасности информационных и средств, и систем таможенных органов могут являться:

– нарушения технологии обработки информации ограниченного доступа, обрабатываемой в таможенных органах;

– нарушение законных ограничений на распространение информации ограниченного доступа, обрабатываемой в таможенных органах;

– противоправные сбор и использование информации ограниченного доступа, обрабатываемой в таможенных органах;

– компрометация ключей и средств криптографической защиты информации;

– перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации или ее подмена;

– несанкционированный доступ к информации, находящейся в базах данных таможенных органов;

– внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

– разработка и распространение программ (компьютерных вирусов), нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

– воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

– утечка информации по техническим каналам;

– внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения таможенных органов;

– уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

– использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии автоматизированных систем таможенных органов [2].

Меры по защите компьютерной информации можно подразделить на следующие виды:

– правовые меры (дисциплинарные, гражданско-правовые, уголовно-правовые);

– административные меры (средства физической защиты (например, блокирование некоторых функций технических средств, таких как порт USB);

– программные средства защиты информации (например, антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);

– организационные меры защиты (доступ в помещения, разработка стратегий безопасности организации и т.д.) [3].

Для достижения поставленной цели предлагается внедрить Архитектуру безопасности автоматизированной информационной системы. Данная архитектура определяет практические пути реализации важнейших направлений и принципов обеспечения информационной безопасности таможенных органов, а также структуру, основные системотехнические решения, методы, механизмы и средства построения этой системы.

При разработке архитектуры информационной безопасности таможенных органов можно использовать разработанную компанией IBM методику создания архитектуры защищенных решений (IBM Method for Architecting Secure Solutions — MASS), основывающуюся на положениях национального и международного стандарта, известного под названием "Общие критерии", ГОСТ Р ИСО/МЭК 15408-2002 (ISO/IEC 15408:1999) "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий".

Методика MASS успешно реализована во многих крупных проектах по всему миру, в том числе и в проектах, выполненных в интересах таможенных органов ряда зарубежных стран. Использование методики MASS гарантирует достижение высокого качества решений по обеспечению информационной безопасности на всех стадиях проектных работ. Она позволяет определять основные угрозы и уязвимости на каждом организационном уровне проектируемой информационной системы, а также предлагать рациональные решения по их устранению и комплексному обеспечению информационной безопасности.

Общей целью разработки архитектуры информационной безопасности ЕАИС таможенных органов являлось достижение автоматически возобновляемого и развивающегося процесса управления информационной безопасностью, который является методическим, организационным и технологическим базисом для непрерывного развития и совершенствования архитектуры информационной безопасности ЕАИС таможенных органов.

В процессе разработки архитектуры информационной безопасности таможенных органов необходимо учесть следующие системные принципы:

– преемственность по отношению к существующей системе обеспечения информационной безопасности;

– системность и комплексность построения системы обеспечения информационной безопасности;

– унифицированность принципов, методов и технических решений по обеспечению информационной безопасности на всех уровнях иерархии информационной системы таможенных органов;

– интегрированность системы обеспечения информационной безопасности;

– эшелонирование системы обеспечения информационной безопасности на всех этапах доступа к информации;

– использование модульного подхода;

– обеспечение информационной безопасности автоматизированных систем таможенных органов на уровне архитектуры сети, сетевых протоколов и оборудования;

– соответствие национальным и международным стандартам в области информационной безопасности.

Введение подобного инструмента поможет достичь следующих целей:

– структуризация основных угроз и оценка рисков информационной безопасности;

– определить модель нарушителя и классификации нарушителей;

– определить рекомендации по минимизации возможных угроз и рисков в области информационной безопасности;

– создать требования национальных и международных стандартов в области информационной безопасности.

Список использованных источников:

1. Постановление № 11 государственного Таможенного комитета Республики Беларусь «О технических средствах таможенного контроля и порядке их применения» от 3 мая 2018 г. Приложение №1..

2. Специфика правового регулирования информационной безопасности таможенных органов: материалы 60 науч. конф. специалистов таможенного дела, Москва, 17-18 мая 2017 г. - Н. М. Кожуханов [и др.]. – Москва. – 8 с.

3. Информационные технологии и управление: материалы 49 науч. конф. аспирантов, магистрантов и студентов, Минск, 6–10 мая 2013 г. / Белорус. гос. ун-т информатики и радиоэлектроники; редкол: Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2013. – 103 с.