УДК 656.073

Симакина А.Е.,
студент,
6 курс, специальность «Таможенное дело»
Юридический институт Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых
Россия, г. Владимир
Научный руководитель: Аксенов И.А.

ОСНОВНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ДАННЫХ В ЕДИНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ ТАМОЖЕННЫХ ОРГАНОВ (ЕАИС ТО)

Аннотация: *В статье рассматривается автоматизация процессов в сфере таможенного дела России на базе ЕАИС ТО. Анализируются проблемы информационной безопасности системы. Описываются направления их решения.*

Ключевые слова: *информационная безопасность, таможенная сфера, угрозы, киберугрозы, цифровизация, ЕАИС ТО, уязвимости, импортозамещение.*

Simakina A.E.,
student,
6th year, specialty «Customs Affairs»
Law Institute of Vladimir State University named after Alexander Grigorievich and Nikolai Grigorievich Stoletov
Russia, Vladimir
Supervisor: Aksenov I.A.

MAIN PROBLEMS OF DATA PROTECTION IN THE UNIFIED AUTOMATED INFORMATION SYSTEM OF CUSTOMS AUTHORITIES (UAIS TO)

Annotation: *This article examines the automation of customs processes in Russia using the Unified Automated Information System (UAIS) for customs. It analyzes the system's information security issues and describes possible solutions.*

Keywords: *information security, customs, threats, cyberthreats, digitalization, UAIS for customs, vulnerabilities, import substitution.*

Автоматизация бизнес-процессов в сфере таможенного дела в России осуществляется за счет компонентов Единой автоматизированной информационной системы таможенных органов (далее - ЕАИС ТО). Это распределенная многоуровневая система, структура которой соответствует организационно-штатной схеме таможенных органов Российской Федерации [1]. Современная ЕАИС ТО (рисунок 1) объединяет средства вычислительной техники, программное обеспечение, программно-информационные продукты, базы данных, инструменты защиты информации, а также сетевое и телекоммуникационное оборудование и каналы передачи данных.

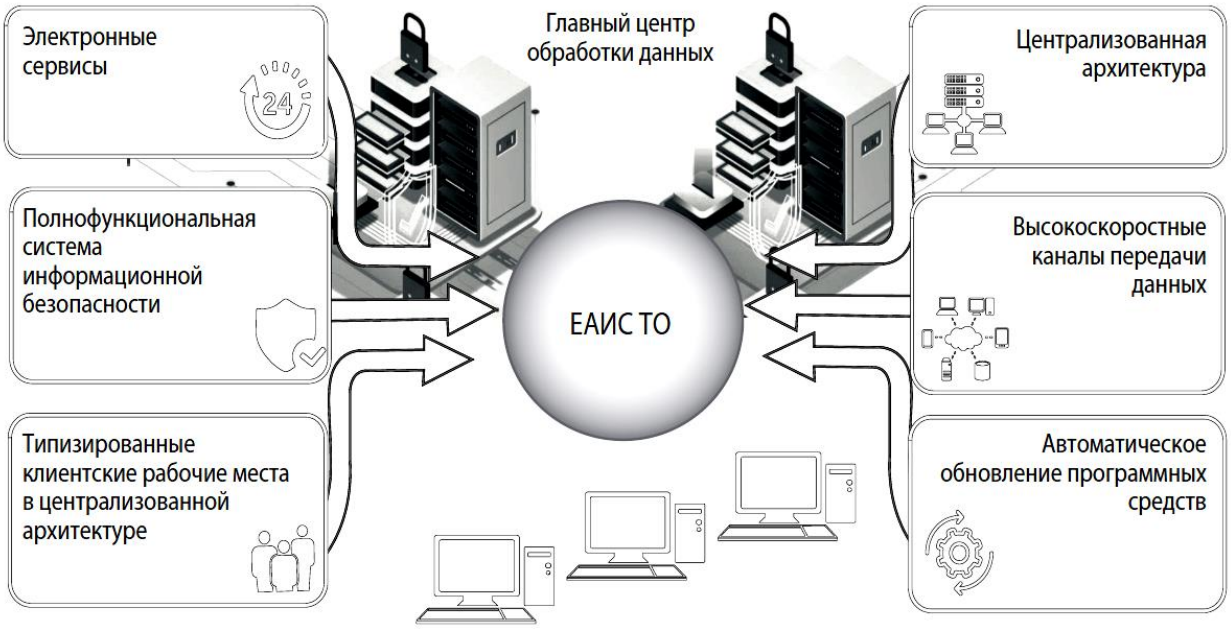

Рисунок 1. Структура ЕАИС ТО

Сегодня система включает свыше 70 информационных ресурсов, задействованных через примерно 2 тыс. каналов передачи данных, и ежедневно обрабатывает около 35 млн электронных сообщений в режиме реального времени [1]. Ее структура соотносится с организационно-штатной схемой таможенных органов РФ и состоит из функциональных сегментов горизонтального и вертикального уровней.

Совершенствование ЕАИС в части обеспечения информационной безопасности ведется на протяжении длительного времени. Реализация целей Стратегии 2030 потребовала существенных вложений в обновление информационных мощностей таможенных органов [3]. Был осуществлен перенос и модернизация баз данных, внедрялись современные решения для автоматизации и цифровизации. При этом, ЕАИС ТО как элемент важной информационной инфраструктуры Российской Федерации сталкивается с рядом проблем, которые требуют глубокого анализа и выработки научно обоснованных решений.

В настоящее время проблемы защиты данных в ЕАИС ТО проявляются в двух основных направлениях, которые являются взаимосвзянными:

1. Использование зарубежного ПО.

2. Угрозы кибербезопасности.

Рассмотрим подробнее данные проблемы.

Сегодня как никогда за последние годы встал вопрос импортозамещения. Назрела необходимость в тотальной защите отечественных баз данных и систем от внешних атак и угроз. Зависимость от зарубежных решений создает потенциальные уязвимости. Так, санкционные ограничения нарушили работоспособность важных компонентов ЕАИС ТО, а отсутствие полного контроля над кодом повышает риски наличия скрытых закладок или недекларированных возможностей.

В рамках курса на импортозамещение ФТС России планомерно переводит свое информационно-программное обеспечение ЕАИС ТО на отечественную систему управления базами данных (СУБД). По многим

программным модулям этот процесс уже завершен. Технологическая интеграция ЕАИС ТО требует обеспечения совместимости данных и их бесшовного взаимодействия с действующими платформами обработки информации. Для решения этой проблемы в Твери построили Главный центр обработки данных ФТС России (ГЦОД). Он призван автоматизировать таможенные операции по всей стране в режиме реального времени. Именно это решение позволило устранить зависимость от зарубежного ПО. С точки зрения информационной безопасности ГЦОД выполняет функцию централизованного контролируемого узла, где возможно обеспечить соблюдение единых стандартов защиты и мониторинга событий безопасности.

Информационно-коммуникационные системы и инфраструктура ЕАИС ТО нуждаются в надежной защите от киберугроз, которые несут как прямой ущерб, так и несанкционированный доступ. Угрозы кибербезопасности могут привести к утечкам информации в Даркнет (Darknet), к использованию злоумышленниками технологий цифровых двойников (Digital twins) и дипфэйков (Deepfake), перехвату косвенных данных - излучений от аппаратуры и так далее. Наиболее частым видом атак в последние годы стали DDoS-атаки (Distributed Denial of Service, или «отказ в обслуживании»). Они предполагают скоординированную отправку одновременно огромного числа запросов к информационным ресурсам, из-за чего система перегружается и обычные пользователи лишаются доступа к сервисам. Проще говоря, система зависает

Эксперты в области ИТ сегодня выделяют свыше 100 разновидностей киберугроз. Для всех них разработаны классификации и методики оценки рисков. Однако порой злоумышленник обладает компетенциями уровня разработчика, что представляет особую опасность. В таких случаях защитные механизмы оказываются неэффективными. Это подчеркивает необходимость перехода от реактивных мер защиты к проактивным стратегиям. К такими стратегиям относится моделирование угроз, прогнозирование векторов атак и внедрение адаптивных систем обнаружения вторжений.

Для решения проблемы кибербезопасности требуется внедрение передовых защитных технологий, организации защищенных каналов связи, а также качественной подготовки квалифицированных ИТ-специалистов. Также важно в таможенных органах создать условия, которые снижают риски утечек данных из ЕАИС ТО. В качестве одного из перспективных инструментов защиты информации в таможенной сфере ряд экспертов рассматривает технологию блокчейн.

«Блокчейн представляет собой децентрализованную цепочку хранения информации, где каждый блок цепи может быть расположен на любом сервере без привязки к территориальным границам» [4, с. 32]. Участники конкретных таможенных операций получают доступ к единой распределенной базе данных. Криптографическая защита гарантирует неизменность зафиксированных операций. Это снижает риски кибератак и проведения мошеннических действий с информацией. При этом, внесение изменений в систему строго регламентировано. Так, новые данные принимаются только после того, как все участники цепочки подтвердят согласие на обновления. С позиций информационной безопасности основными преимуществами блокчейна являются прозрачность операций, устойчивость к фальсификациям и возможность аудита каждой транзакции.

В заключении следует особо подчеркнуть, что в контексте цифровой трансформации таможенных органов необходимо стремиться к созданию общего стандарта информационной безопасности в ЕАИС ТО, который будет отвечать новейшим тенденциям Стратегии-2030. В условиях стратегических перспектив акцент следует ставить на создании эффективной с точки зрения информационной безопасности системы управления и защиты информации в ЕАИС ТО, как одного из основных элементов критической инфраструктуры таможенных органов. Реализация данной задачи предполагает формирование многоуровневой системы защиты, которая объединяет технологические, организационные и нормативно-правовые меры, а также непрерывный мониторинг и адаптацию к постоянно меняющимся киберугрозам.

Литература:

1. Приказ ФТС России от 17.06.2010 №1154 (ред. от 28.07.2017) «Об утверждении Положения о Единой автоматизированной информационной системе таможенных органов» [Электронный ресурс]. URL: Справочная правовая система «КонсультантПлюс» http://consultant.ru (дата обращения 24.03.2026);

2. Абрамов А.С. Роль Единой автоматизированной информационной системы таможенных органов в архитектуре «интеллектуального» пункта пропуска // Вестник Российской таможенной академии. – 2024. – №1(66). – С. 45-55;

3. Распоряжение Правительства РФ от 23.05.2020 №1388-р (ред. от 12.07.2024) «Стратегия развития таможенной службы Российской Федерации до 2030 года» // Собрание законодательства РФ, 01.06.2020, №22, ст. 3572;

4. Ионина М.В. Информационная безопасность таможенных органов в условиях цифровой трансформации // Ученые записки Санкт-Петербургского имени В.Б. Бобкова филиала Российской таможенной академии. – 2023. – № 1(85). – С. 30-33.