УДК 339.543

КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ТАМОЖЕННЫХ ОРГАНОВ

Тихонова Анна Николаевна, аспирант
Потапова Наталья Васильевна, заведующий кафедрой БУАиА, к.э.н., доцент
Брестский государственный технический университет
Tikhonova Anna Nikolaevna, graduate student, ann16tt@gmail.com
N.V. Potapova, Head of the Department of BUAA, PhD in Economics, Associate Professor
Brest State Technical University, pnatv2026@yandex.by

Аннотация. В статье рассмотрены современные технологии защиты персональных данных, проведен анализ положения страны в Глобальном индексе кибербезопасности, а также предложены рекомендации по повышению уровня кибербезопасности информационных систем таможенных органов.

Ключевые слова: информационные системы, кибербезопасность, персональные данные, таможенные органы.

Переход к электронным формам взаимодействия таможенных органов с другими государственными органами, участниками внешнеэкономической деятельности, цифровизация процессов, а также внедрение интеграционных систем вызывает необходимость повышения уровня обеспечения кибер-безопасности [1]. Актуальность данной темы обусловлена активным исполь-зованием современных технологий при обмене информацией, в результате чего возрастает риск киберугроз и утечек конфиденциальных данных. Целью статьи являются: определить технологии и классифицировать меры, используемые таможенными органами для защиты персональных данных, а также разработать рекомендации для повышения уровня кибербезопасности информационных систем таможенных органов.

В первую очередь следует рассмотреть актуальные угрозы для информа-ционной безопасности таможенных систем. Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем [2, с. 43]. Как правило, в таможенной сфере угрозы направлены на несанкционированное получение информации, что возможно при наличии внутренних угроз (злоупотребление полномочиями должностными лицами, человеческий фактор), внешних угроз (взломы систем, атаки хакеров) и технических уязвимостей (устаревшее программное обеспечение, ошибки конфигурации программ). В таких условиях кибербезопасность играет важнейшую роль в обеспечении конфиденциальности, целостности и доступности информа-ционных систем. Любое нарушение может привести к существенному репутационному ущербу, финансовым издержкам, перебоям во внешне-экономической деятельности предприятий [3].

Основой нормативно-правовой базы в области информационных технологий таможенных органов выступает Таможенный кодекс ЕАЭС, который устанавливает общие принципы обработки и защиты данных [4]. При этом следует отметить, что в рамках ЕАЭС отсутствует единое специализированное законодательство по защите персональных данных, иными словами, данный вопрос регулируется национальным законодательством государств-членов ЕАЭС. Так, В Республике Беларусь защита персональных данных в таможенных органах регламентируется Законом Республики Беларусь от 07.05.2021 г. № 99-З «О защите персональных данных». Государственный таможенный комитет Республики Беларусь выступает оператором, осу-ществляющим обработку персональных данных в соответствии с положениями данного Закона. Кроме того, важную роль играет Национальный центр защиты персональных данных Республики Беларусь, который является уполномоченным органом по защите прав субъектов персональных данных. Основной задачей Национального центра защиты персональных данных является принятие мер по защите прав субъектов персональных данных при обработке их персональных данных [2].

Рассмотрим технологии защиты персональных данных, используемые таможенными органами. Для обеспечения кибербезопасности широко применяются методы криптографической защиты информации, суть которых заключается в том, что данные, отправляемые на хранение, или сообщения, готовые для передачи, зашифровываются и тем самым преобразуются в шифрограмму или закрытый текст. Только санкционированный пользователь может получить доступ к исходной информации, применяя процесс дешифрования. Криптографическая защита данных является основой кибербезопасности в таможенных органах, поскольку она защищает информацию от несанкционированного доступа и модификации. Для этого используются специальные алгоритмы шифрования, активирующиеся с помощью уникального шифровального ключа, который может быть представлен в виде числа или битовой последовательности. Существуют два основных типа криптографического шифрования: симметричное шифрование и асимметричное шифрование. Симметричное шифрование применяется в классической криптографии и предполагает использование всего лишь одного ключа для шифрования и дешифрования данных [5].

Методы асимметричного шифрования предполагают шифрование при наличии двух ключей – секретного (закрытого) и публичного (открытого). Особенность таких методов заключается в одностороннем характере применения ключей. Такой подход обеспечивает более высокий уровень безопасности, поскольку в случае если открытый ключ станет известен злоумышленникам, они не смогут расшифровать данные без доступа к закрытому ключу. Так, например, применение электронной цифровой подписи основано на асимметричном шифровании, когда секретным ключом

шифруется подпись при ее формировании, а открытый ключ позволяет убедиться, что документ заверен именно владельцем закрытого ключа, что подтверждает подлинность подписи. Правовые условия использования электронной цифровой подписи в электронных документах регламентирует Закон Республики Беларусь от 28.12.2009 г. № 113-З «Об электронном документе и электронной цифровой подписи».

Помимо криптографических методов, таможенные органы Республики Беларусь также применяют комплекс дополнительных технологий для защиты персональных данных. В информационных системах широко используется многофакторная аутентификация, а также ролевая модель доступа, согласно которой доступ к данным предоставляется только уполномоченным должностным лицам таможенных органов [6]. Поскольку в таких масштабных системах невозможно назначать права каждому сотруднику индивидуально, доступ распределяется по ролям, которые соответствуют должностным обязанностям.

Также к дополнительным мерам защиты относятся автоматизированные системы логирования и аудита, которые фиксируют все действия пользователей с данными, тем самым позволяя своевременно выявлять подозрительную активность. Для защиты сетевой инфраструктуры используются межсетевые экраны, сегментация сети на изолированные зоны по уровням конфиденциальности и антивирусные системы. Для защиты периметра и фильтрации трафика используются межсетевые экраны, которые пропускают только разрешенные запросы и блокируют подозрительную активность или несанкционированные попытки доступа.

Меры по защите персональных данных традиционно делятся на три взаимодополняющие группы: технические, правовые и организационные. Под техническими мерами понимаются мероприятия, направленные на осуществление технической и криптографической защиты персональных данных [2, с. 9]. Правовые меры включают обязательную разработку и утверждение политики обработки персональных данных с четким указанием целей обработки, сроков хранения и порядка уничтожения информации. Организационные меры направлены на разграничение доступа к информации по кругу лиц и характеру информации.

В связи с этим показательным инструментом в оценке уровня информационной безопасности является Глобальный индекс кибербезо-пасности (GCI), который отражает уровень киберзащищенности государств и усилия, которые прилагает страна для улучшения этого показателя. Среди критериев выделяют правовое, техническое, организационное поля, а также потенциал развития и сотрудничество [2, с. 32]. По методологии данного рейтинга страны распределяются по пяти уровням в зависимости от общей суммы баллов по каждому критерию (каждый из критериев дает 20 баллов, максимальная общая сумма – 100 баллов). Так, в 2024 году Республика Беларусь была включена в третью группу стран и набрала 61,53 балла, что является заметным прогрессом по сравнению с предыдущим результатом, составившим в 2020 году 50,57 балла [2]. Республика Беларусь улучшила позиции благодаря сотрудничеству, развитию правовой базы и организационных структур, но все еще отстает в технических мерах и мерах, связанных с потенциальным развитием, по сравнению с лидерами рейтинга.

Существующие традиционные средства защиты информации, такие как межсетевые экраны, криптографическое шифрование и многофакторная аутентификация, хотя и обеспечивают необходимый базовый уровень безо-пасности, в современных условиях уже не всегда достаточны для противодействия сложным и постоянно эволюционирующим киберугрозам [5]. В информационных системах таможенных органов Республики Беларусь и других государств-членов ЕАЭС уязвимости могут быть использованы для мошеннических действий, включая кражу персональных данных, подделку электронных документов и несанкционированный доступ к сведениям о внешнеэкономической деятельности предприятий.

Для построения действительно надежной и устойчивой модели кибербезопасности традиционные меры должны органично дополняться современными технологиями и подходами [7]. Рассмотрим основные направления повышения уровня киберзащищенности в таможенных органах Республики Беларусь:

1. Внедрение модели «нулевого доверия», в которой каждый запрос на доступ к данным, независимо от источника, проходит полноценную верификацию по нескольким параметрам (идентификация пользователя, устройство, контекст запроса, время и поведение). Проверка осуществляется на каждом этапе доступа пользователя к ресурсам. В таможенных органах такая модель позво-

лит минимизировать риски беспрепятственного перемещения злоумышленника внутри сети и существенно повысить защиту информационных систем.

2. Использование искусственного интеллекта и машинного обучения для выявления аномалий в поведении пользователей и сетевом трафике, предиктивного анализа угроз и автоматического реагирования на них в режиме реального времени.

3. Инвестирование в разработку отечественных и союзных сертифицированных систем защиты информации, в том числе межсетевых экранов нового поколения (NGFW), систем обнаружения и предотвращения вторжений (IDS/IPS), которые будут сертифицированы Оперативно-аналитическим центром при Президенте Республики Беларусь. При этом усилия по развитию отечественной индустрии кибербезопасности могут быть реализованы в форме механизмов стимулирования, таких как гранты и стипендии.

4. Регулярное прохождение аттестации действующих систем защиты информации с целью выявления уязвимостей и несоответствий установленным требованиям по защите информации, а также подтверждения соответствия системы защиты информации нормативным требованиям безопасности.

5. Создание рабочей группы ЕЭК по вопросам кибербезопасности для выработки общих стандартов в сфере оборота данных в рамках ЕАЭС. Необходимо определение четких подходов к разделению данных, какими данными целесообразно обмениваться в рамках интеграционных процессов, а какую информацию следует хранить исключительно на стороне государства-члена ЕАЭС.

Таким образом, кибербезопасность и защита персональных данных в таможенных органах Республики Беларусь приобретают сегодня стратегическое значение, поскольку таможня является одним из ключевых звеньев обеспечения национальной безопасности и обрабатывает огромные массивы конфиденциальных информации.

В условиях активной цифровой трансформации таможенных органов надежная киберзащита превращается из технической задачи в обязательное условие эффективного и безопасного функционирования всей таможенной инфраструктуры. Именно поэтому обеспечение высокого уровня кибербезопасности и защита персональных данных выступают важнейшим фактором устойчивого развития внешней торговли, сохранения конкурентоспособности страны и укрепления доверия со стороны участников внешнеэкономической деятельности.

Список использованных источников

1. Отраслевые финансы : учебно-методическое пособие для студентов специальности 1-25 01 04 Финансы и кредит / Т.Н. Лобан, М.П. Самоховец, М.И. Бухтик, А.В. Киевич. – Пинск : Полесский государственный университет, 2018. – 67 с. – EDN: HJQCIV.

2. Национальный центр защиты персональных данных [Электронный ресурс]. – Режим доступа: https://cpd.by/o-centre/. – Дата доступа: 09.04.2026.

3. Галкина М.Н., Киевич А.В. Проблемы обеспечения информационной и экономической безопасности государства / М.Н. Галкина, А.В. Киевич // Экономика и банки. 2021. № 1. С. 65-76.

4. Киевич А.В., Король О.В. Евразийский экономический союз: итоги деятельности за год / А.В. Киевич, О.В. Король // «Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серыя 5. Эканоміка. Сацыялогія. Біялогія». – 2016. – Том 6. – № 2. – С. 69-76.

5. Ковалевская, Ю.Д. Цифровая трансформация управления рисками в таможне при внедрении искусственного интеллекта таможенными службами / Ю.Д. Ковалевская, Н.В. Потапова // Устойчивое развитие экономики : состояние, проблемы, перспективы : сборник трудов XIX междунар. науч.–практ. конф., Пинск, 25 апреля 2025 г. / Полесский государственный университет [и др.], редкол.: В. И. Дунай, И. Э. Бученков, И. А. Пригодич. – Пинск : ПолесГУ, 2025. – С. 218-220.

6. Ливенский В.М., Лисовский М.И., Янковский И.А. Тенденции развития сетевых форм организации цифровой экономики в РБ / В.М. Ливенский, М.И. Лисовский, И.А. Янковский // Современные аспекты экономики. 2021. № 3 (283). С. 26-32.

7. Потапова Н.В., Четырбок Н.П. Роль малого бизнеса в экономике Республики Беларусь / Н.В. Потапова, Н.П. Четырбок // Современные аспекты экономики. 2021. № 4 (284). С. 23-29.