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.

СОВРЕМЕННЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТАМОЖЕННОЙ СФЕРЕ

Аннотация: *В статье анализируются современные угрозы информационной безопасности в таможенной сфере Российской Федерации в условиях цифровой трансформации государственных институтов. Исследуются основные типы угроз. Рассматриваются их источники и способы реализации.*

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

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.

CONTEMPORARY THREATS TO INFORMATION SECURITY IN THE CUSTOMS SPHERE

Annotation: *This article analyzes current information security threats in the Russian customs sector amid the digital transformation of government institutions. The main types of threats are explored, their sources and methods of implementation are considered.*

Keywords: *information security, customs, threats, cyber threats, digitalization, Unified Automated Information System of the Customs Union, vulnerabilities.*

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. В условиях цифровой трансформации государственных институтов ее роль неуклонно возрастает, поскольку информационные потоки становятся базовым ресурсом управления и принятия решений.

Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость постоянно увеличивается. Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [1, с. 89].

Современное состояние и острота проблемы обеспечения информационной безопасности в таможенных органах России во многом были предопределены темпами автоматизации и внедрения средств вычислительной техники. Интенсивная цифровизация таможенных процессов создала новые уязвимости, которые могут быть использованы злоумышленниками для дестабилизации работы ведомства/

По мнению К.А. Турянской, потенциальные угрозы информационной безопасности можно классифицировать по ряду признаков:

- характер возникновения (природные и техногенные угрозы);

- степень намеренности (умышленные или случайные действия);

- непосредственный источник (внутренние или внешние субъекты);

- местоположение источников (локальные или трансграничные);

- фазы доступа пользователей (на этапе ввода данных, передачи, хранения или обработки) [2, с.153].

Лаврищева Т. С., не углубляясь в вопросы типологизации, путем анализа научных источников выделяет следующие наиболее актуальные угрозы в контексте современных геополитических вызовов:

1. Угрозы, связанные с использованием иностранного ПО. В условиях санкций возрастает риск блокировки протоколов, отзыва лицензий, внедрения скрытых уязвимостей в зарубежных программных продуктах. Например, прекращение поддержки коммерческих решений может парализовать ключевые процессы таможенного контроля, если не предусмотрены альтернативные отечественные аналоги.

2. Рост количества и изощренности кибератак. Распространение APT-угроз (Advanced Persistent Threats - целевых продолжительных атак) и спонсирование хакерских групп национальными государствами создают риски для устойчивости таможенных информационных систем. Такие атаки часто нацелены на кражу конфиденциальных данных (например, сведений о грузопотоках) или на вывод из строя критически важных сервисов.

3. Сближение киберпреступности и традиционной преступной деятельности. Незаконный оборот товаров, контрабанда и коррупция все чаще сопровождаются кибератаками. Например, подделкой электронных документов, взломом систем декларирования, перехватом каналов связи. Особую опасность представляют транснациональные преступные группы, использующие кибервозможности для обхода таможенных процедур [1, с.90].

Лаврищева Т. С. также указывает, что эволюция угроз в сфере информационной безопасности в таможенном деле характеризуется непрерывным циклом инноваций и адаптации. Злоумышленники постоянно совершенствуют методы атак, используя:

- социальную инженерию (фишинг, поддельные сайты для кражи учетных данных);

- эксплойты нулевого дня (уязвимости, неизвестные разработчикам ПО);

- ботнеты и DDoS-атаки для перегрузки информационных систем;

- криптографические атаки для взлома защищенных каналов передачи данных [1, с.90].

Согласно данным Федеральной службы по техническому и экспортному контролю (ФСТЭК России) в банке данных угроз безопасности информации зарегистрировано более 200 видов угроз и более 45 тыс. уязвимостей информационной безопасности [3]. Такая статистика подчеркивает масштабность проблемы и необходимость постоянного мониторинга угроз.

Автоматизация механизмов таможенного администрирования, процессов совершения таможенных операций и проведения таможенного контроля с использованием информационных систем является приоритетным направлением развития таможенного обеспечения РФ, что определяет повышенные требования по формированию доверия к их функционированию. При деструктивном воздействии на информационно-технические средства и объекты ТО их эффективное функционирование невозможно.

Источники угроз информационной безопасности таможенного обеспечения РФ можно разделить на три группы: техногенные, стихийные и антропогенные (рисунок 1). Техногенные угрозы связаны с отказами оборудования, сбоями программного обеспечения, нарушениями работы сетей. Стихийные угрозы включают природные катастрофы, способные вывести из строя серверные центры или линии связи. Антропогенные угрозы это наиболее многочисленная и опасная категория, охватывающая умышленные действия внешних злоумышленников, внутренние нарушения, социально-политические факторы и пр.

Рисунок 1. Источники угроз информационной безопасности таможенного обеспечения

К способам нарушения информационной безопасности таможенного обеспечения РФ, реализующим угрозы безопасности информации, относят:

- использование в противоправных целях санкционированными пользователями информационных систем штатно предоставляемых сервисов (например, утечка данных через легальные каналы доступа);

- использование нештатного программного обеспечения (вредоносные скрипты, несанкционированные утилиты);

- разработка и применение вредоносного программного обеспечения (вирусы, трояны, шифровальщики);

- несанкционированное изменение конфигурации штатного программного обеспечения (модификация алгоритмов проверки деклараций);

- подбор и перехват парольной и иной аутентификационной информации (фишинг, кейлоггеры, взлом паролей);

- использование уязвимостей протоколов сетевого взаимодействия (атаки типа Man-in-the-Middle, подмена DNS);

- использование недостатков в реализации организационных мер защиты информации (например, отсутствие регулярного аудита прав доступа,

несоблюдение регламентов смены паролей, слабая подготовка персонала к выявлению фишинговых атак);

- перехват передаваемой информации (возможен при недостаточной криптографической защите каналов связи);

- реализация попыток неправомерных, в том числе деструктивных, действий из информационно-телекоммуникационных сетей и систем, имеющих подключение к ЕАИС ТО [4, с.128].

В условиях роста и эволюции вызовов в сфере информационной безопасности система защиты должна быть гибкой, многофакторной и подстраивающейся под изменчивый ландшафт киберугроз, подобно экосистеме, которая реагирует на вызовы как единое целое, сохраняя стабильное состояние и устойчивость функционирования.

Таким образом, угрозы информационной безопасности в таможенной сфере представляют собой многоаспектный комплекс рисков, способных нарушить конфиденциальность, целостность и доступность критически важных данных. Их основными характеристиками являются многообразие методов реализации, целенаправленность, потенциальный масштаб ущерба для экономической безопасности государства и постоянная эволюция в ответ на развитие технологий. Эффективное противодействие таким угрозам требует комплексного подхода, объединяющего технические средства защиты, организационные меры и совершенствование нормативно-правовой базы, что позволит обеспечить устойчивую работу таможенных органов и защиту национальных интересов в цифровой среде.

Использованные источники:

1. Лаврищева, Т. С. Информационная безопасность в таможенном деле / Т. С. Лаврищева // Образование и наука без границ: социально-гуманитарные науки. – 2024. – № 22. – С. 88-91;

2. Турянская, К. А. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной

безопасности объектов различного вида и класса / К. А. Турянская // Международный журнал гуманитарных и естественных наук. – 2024. – № 2-2(89). – С. 151-155.

3. Официальный сайт Федеральной службы по техническому и экспортному контролю. – [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat (дата обращения: 20.03.2026);

4. Ионина, М. В. Предпосылки создания цифровой экосистемы информационной безопасности таможенных органов Российской Федерации / М. В. Ионина // Вестник Российской таможенной академии. – 2024. – № 1(66). – С. 125-133.