УДК 338.46

ЭКОСИСТЕМА КИБЕРБЕЗОПАСНОСТИ КАК КЛЮЧЕВОЙ ЭЛЕМЕНТ УСТОЙЧИВОГО РАЗВИТИЯ ТАМОЖЕННЫХ ОРГАНОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

CYBERSECURITY ECOSYSTEM AS A KEY ELEMENT OF SUSTAINABLE DEVELOPMENT OF THE CUSTOMS AUTHORITIES OF THE RUSSIAN FEDERATION

Ionina M.V.
St. Petersburg named after V.B. Bobkov Branch of the Russian Customs Academy

Аннотация
В условиях цифровизации деятельности таможенных органов особую остроту приобрели вопросы, связанные с обеспечением информационной безопасности и защиты таможенной информации, составляющей коммерческую или налоговую тайну. Нарастающее с каждым годом количество попыток деструктивного воздействия на информационные системы таможенных органов ставит под угрозу возможность совершения внешнеторговых операций, что негативным образом может сказаться на экономической безопасности нашей страны. Выстраивание эффективной архитектуры информационной безопасности по типу экосистемы (экосистемного подхода), будет являться важнейшим фактором для безопасности и бесперебойности функционирования информационных систем таможенных органов.

Ключевые слова: цифровизация, кибербезопасность, экосистема информационной безопасности, таможенные органы.

Abstract
In the context of digitalization of the activities of customs authorities, issues related to information security and protection of customs information constituting a commercial or tax secret have become particularly acute. The increasing number of attempts of destructive influence on the information systems of customs authorities every year threatens the possibility of foreign trade operations, which can negatively affect the economic security of our country. Building an effective information security architecture according to the type of ecosystem (ecosystem approach) will be the most important factor for the security and smooth functioning of customs information systems.

Keywords: digitalization, cybersecurity, information security ecosystem, customs authorities.

Ссылка для цитирования: Ионина М.В. Экосистема кибербезопасности как ключевой элемент устойчивого развития таможенных органов Российской Федерации // Бюллетень инновационных технологий. – 2023. – Т. 7. – № 4 (28). – С. 38-41. – EDN FWXWOB.

Российская Федерация (РФ) находится в условиях изменчивой общественно-политической обстановки, а также в условиях санкций, введенных в отношении нее от недружественных стран: 6 пакетов американских и 11 пакетов западноевропейских были введены с марта 2022 года с целью нарушить работу финансовых институтов, дестабилизировать деятельность правительства, осложнить работу предприятий. Введенные санкции также были направлены на разрушение внешнеторговой сферы России, включая систему международных расчетов, функционирование транспортно-логистических цепочек, блокировку каналов российского экспорта с целью отрезать страну от рынков современной высокотехнологической продукции, что повлияло на уход иностранных вендоров с рынка информационных технологий РФ.

Западные санкции содействовали «глобальному развороту» российской внешней торговли на Восток и Юг, открывая новые транспортные коридоры. Активно развиваются новые направления товаропотоков по

стратегически значимым логистическим коридорам «Север – Юг» и «Запад – Восток». Уход иностранных вендоров стал стимулом для активного развития отечественной отрасли информационных технологий. Продолжается курс, взятый на цифровизацию, которая способствует решению задач по адаптации всей внешнеторговой сферы России к работе в новых условиях. На сегодня оцифрованы практически все основные таможенные процедуры. Это позволило существенно увеличить скорость совершения операций, обеспечить качество и эффективность таможенного контроля и выполнить одну из основных задач, стоящих перед таможенными органами (ТО) – обеспечить полноту и своевременность поступления таможенных платежей в федеральный бюджет [1]. Об этом свидетельствуют статистические данные: на октябрь 2023 года ТО РФ собрано более 5 триллионов рублей.

В последнее время «особую остроту приобрели вопросы информационной безопасности (ИБ) и защиты таможенной информации, составляющей коммерческую или налоговую тайну. С начала СВО зафиксировано более 1,5 тысяч попыток деструктивного воздействия на информационные системы ТО. В том числе и предпринятая в апреле 2023 года наиболее масштабная попытка парализовать работу информационных систем ТО и заблокировать возможность совершения внешнеторговых операций» [2].

Эксперты в сфере кибербезопасности прогнозируют рост кибератак, направленных на государственные учреждения, что может привести к негативным последствиям от дефейса сайтов до разрушения информационной инфраструктуры. В условиях постоянного изменение ландшафта угроз целью преступников является негативное влияние на критическую информационную инфраструктуру, что вызывает аварии, перебои в деятельности с последующей остановкой важнейших технологических и бизнес-процессов организаций, также утечка конфиденциальной информации в том числе и персональных данных. Все это наносит существенный экономический ущерб организациям и государству в целом.

Современные реалии повысили важность обеспечения информационной безопасности и киберустойчивости компаний, государственных структур и отраслей экономики. Внимание государства к обеспечению информационной безопасности в последние годы многократно возросло. Этому свидетельствует ряд принятых нормативных документов:

- Указ Президента РФ от 30.03.2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». С учетом проводимой в Российской Федерации политики импортозамещения взят курс на постепенный отказ от зарубежных технологий для обеспечения технологической безопасности и независимости объектов критической информационной инфраструктуры, переход на отечественное программное обеспечение [3].

- Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации». Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак [4].

- С 1 сентября 2022 года вступили в силу новые требования Федерального закона № 152 «О персональных данных». Они обязывают компании в течение суток уведомлять ФСБ и Роскомнадзор о произошедших утечках персональных данных. Новая норма об уведомлении распространяется на 8 миллионов предприятий — от органов власти и компаний первого эшелона до индивидуальных предпринимателей [5].

- Согласно Указу Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с 1 января 2025 года органам (организациям) запрещается использовать средства защиты информации, происходящие из недружественных государств, либо производителями которых являются организации, находящиеся под их юрисдикцией, прямо или косвенно подконтрольные им либо аффилированные с ними [6]. Данный указ направлен на радикальное повышение защищенности от кибератак ключевых предприятий страны. Под действие этого указа попал более широкий круг организаций, чем, например, под действие Федерального закона № 187«О безопасности критической информационной инфраструктуры Российской Федерации», а в вопросы

обеспечения ИБ теперь вовлекаются первые лица компаний, ответственные за кибербезопасность, а также отдельной службы по ИБ. Помимо этого, Президент РФ В.В. Путин поручил Правительству РФ рассмотреть вопросы об установлении оборотных штрафов в отношении компаний, допускающих утечку персональных данных, усилении ответственности за их незаконный оборот и иные нарушения законодательства в области персональных данных [7].

Возрастающее количество утечек конфиденциальной информации с одной стороны и оборотные штрафы с другой, вероятно, станут стимулом для российских предприятий и организации пересмотреть свою архитектуру защиты данных, а также выстроить систему управления инцидентами для своевременного уведомления о них. Требование об уведомлении в течение 24 часов, независимо от праздников и выходных, – это серьезный вызов даже для опытных в управлении кибербезопасностью организаций [8].

Нехватка квалифицированных кадров в сфере защиты информационной безопасности может стать драйвером для создания сервисной модели и автоматизации процессов защиты ИБ. Актуальный запрос на практическую кибербезопасность будет, с одной стороны, стимулировать развитие рынка компаний (провайдеров), которым делегировано управление средствами защиты информации, а с другой — формировать запрос на появление технологий с высокой автоматизацией противодействия киберугрозам, когда роль оператора продуктов ИБ будет все больше замещаться технологиями автоматического противодействия атакам [9].

Важнейшими приоритетами в работе ФТС России является обеспечение безопасности и бесперебойности функционирования информационных систем ТО. Таким образом, для повышения уровня защиты таможенной информации и противодействию угрозам экономической безопасности России, по мнению временно исполняющего обязанности руководителя ФТС России Р.В. Давыдова, необходимо: «рассмотреть вопрос перехода от регламентной передаче информации из таможенных баз данных к работе по запросам с обоснованием необходимости получения соответствующей информации в условиях взаимодействия с ведомствами и организациями (действует 98 соглашений об информационном взаимодействии); в рамках статьи 183 Уголовного Кодекса РФ повысить ответственность за незаконное получение, использование или распространение таможенной информации составляющей коммерческую или налоговую тайну» [2].

И еще одним направлением в борьбе с киберугрозами является построение архитектуры ИБ способной обеспечить комплексную защиту информационной инфраструктуры ТО. Смена парадигмы ИБ, переход к результативной защите, основанной на решении ряда разноплановых задач кибербезопасности с помощью тесной взаимосвязи различных технологий и выстроенных между ними процессов, может развиваться по трем направлениям:

- сервисная модель ИБ, предполагающая оказание услуг кибербезопасности (всех или только некоторых) внешним поставщиком (провайдером), который обладает квалифицированным персоналом и реализует все необходимые, а также предусмотренные законодательством функции;

- «автоматизация рутинных задач за счет использования специализированного ПО (например, системы класса SOAR6) или отдельных модулей и функций в существующем ПО (например, SIEM7, NDR8 или WAF9), позволяющих решить большинство задач ИБ силами существующих специалистов, а также использование уникальных средств защиты, основанных на применении ML-технологий, способных предотвращать хакерские атаки и требующих для этого буквально одного-двух экспертов ИБ» [8].

- выстраивание собственной экосистемы ИБ - эталонной архитектуры с набором интегрированных между собой элементов (решений, не дублирующих функции друг друга, а лишь дополняющих их), чем и отличается, в первую очередь, от отдельных разрозненных решений. Экосистема ИБ — это комплекс технологий, компонентов и сервисов, объединённых пользовательскими задачами. Он позволит организации решать вопросы, связанные с защитой ИБ на стыке технологий и продуктов, что обеспечивает комплексное управление процессами ИБ.

Развитие экосистемной архитектуры в сфере информационной безопасности было определено вызовами нового времени. В ситуации постоянного роста количе-

ства и уровня киберугроз организации «нуждаются в комплексном и стратегически продуманном подходе к построению центров мониторинга информационной безопасности (Security Operation Center, SOC) и обеспечению эффективной защиты». Такой подход основан на решении ряда разноплановых задач кибербезопасности с помощью тесной взаимосвязи различных технологий и выстроенных между ними процессов [10].

Таким образом, экосистема ИБ является наиболее перспективным направлением в выстраивании эффективной защиты ИБ ТО и может в полной мере отвечать задачам по цифровизации ТО согласно Стратегии развития таможенной службы РФ до 2030 года [11]. ТО вносят существенный вклад в обеспечение экономической безопасности РФ. Возможно, в будущем это будет вклад в защиту цифровой экономики и обеспечение экономической кибербезопасности.

Список литературы

1. Мантусов В.Б., Афонин Д.Н., Афонин П.Н., Данько Д.Ю. Цифровой фактический контроль: тренд современности; Российская таможенная академия, Санкт-Петербургский имени В. Б. Бобкова филиал. – Санкт-Петербург: Российская таможенная академия, 2019. – 200 с. – ISBN 978-5-9590-1113-0. – EDN FERUEO.
2. Официальный сайт Президента России [Электронный ресурс]. – URL: http://www.kremlin.ru.
3. Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // СПС «Консультант Плюс». URL: www.consultant.ru.
4. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция) [Электронный ресурс] // СПС «Консультант Плюс». – URL: www.consultant.ru.
5. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) [Электронный ресурс] // СПС «Консультант Плюс». – URL: www.consultant.ru.
6. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [Электронный ресурс] // СПС «Консультант Плюс». – URL: www.consultant.ru.
7. Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека (утв. Президентом РФ 12.01.2023 № Пр-19) [Электронный ресурс] // СПС «Консультант Плюс». – URL: www.consultant.ru.
8. Официальный сайт компании «Positive Technologies» [Электронный ресурс] // URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id5 (дата обращения: 05.09.2023).
9. Афонин Д.Н. Возможности, перспективы и проблемы виртуализации в Федеральной таможенной службе России // Бюллетень инновационных технологий. – 2020. – Т. 4, № 2(14). – С. 52-55. – EDN HMKSVT.
10. Интернет-портал по информационной безопасности в сети [Электронный ресурс] // URL: safe-surf.ru/specialists/article/5309/687698/.
11. Распоряжение Правительства РФ от 23.05.2020 № 1388-р «О Стратегии развития таможенной службы Российской Федерации до 2030 года».

Поступила в редакцию 12.10.2023

Сведения об авторе:

Ионина Марина Владимировна – старший научный сотрудник научно-исследовательского отдела Санкт-Петербургского имени В.Б. Бобкова филиала Российской таможенной академии, e-mail: ioninaspb@mail.ru

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