*УДК: 164.07*

# ЗАЩИТА ИНФОРМАЦИИ В ЛОГИСТИКЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

**М. А. Стельмашек**

*студент факультета инновационных технологий, Гродненский государственный университет имени Янки Купалы, г. Гродно, Беларусь, e-mail: markstelmasek@gmail.com*

Научный руководитель: **Ю. В. Крупенко**

*кандидат экономических наук, доцент, доцент кафедры логистики и методов управления, Гродненский государственный университет имени Янки Купалы, г. Гродно, Беларусь, e-mail: Julia_kul@list.ru*

Цифровая трансформация ощутимо повысит качество услуг в секторе логистики. Но внедрение инновационных технологий также повышает уязвимость информации в логистических системах. Кибератаки оказывают значительное финансовое воздействие на бизнес. В этой статье рассматриваются причины и методы повышения кибербезопасности в логистике. Представлен опыт повышающий кибербезопасность в логистике а также управление цепочками поставок. Разработаны мероприятия, обеспечивающие защиту информации в логистике.

***Ключевые слова:*** логистика; цифровизация; кибербезопасность; защита информации.

# INFORMATION PROTECTION IN LOGISTICS IN THE CONDITIONS OF DIGITALIZATION

*Student of the Faculty of Innovative Technologies of Mechanical Engineering at Yanka Kupala State University of Grodno, Grodno, Belarus, e-mail: markstelmasek@gmail.com .*

Supervisor: **Yu. V. Krupenko**

*PhD in Economics, Associate Professor of the Department of Logistics and Management Methods, Yanka Kupala State University of Grodno, Grodno, Belarus, e-mail: Julia_kul@list.ru*

Digital transformation will significantly improve the quality of services in the logistics sector. But the introduction of innovative technologies also increases the vulnerability of information in logistics systems. Cyberattacks have a significant financial impact on businesses.. This article discusses the reasons and methods for improving cybersecurity in logistics. The experience improving cybersecurity in logistics and supply

chain management is presented. Measures have been developed to ensure the protection of information in logistics.

***Keywords:*** logistics; digitalization; cybersecurity; information protection.

Логистика (от греческого слова logistics – искусство мышления и расчета) – это наука об управлении и оптимизации потоков товаров, финансов, информации и услуг, которая основана на использовании современных технологий и самых передовых экономических решений для внутренней интеграции. логистика. Она учитывает внешние материальные потоки и направлена на конечный результат.

Цифровизация широко используется в транспортно-логистическом секторе (ТИЛ) и представляет собой глобальную тенденцию в логистике, поскольку она улучшает весь технологический цикл в отрасли. Это упрощает и ускоряет процессы и положительно влияет на качество выполняемых задач. Многие логистические процессы могут быть автоматизированы с помощью различных программ и сервисов. Например: создание и изменение задач. Документооборот между торговыми партнерами. Подбор оптимальных маршрутов. Расчет рентабельности перевозки грузов. Анализ сбытовой деятельности компании. Проведение взаиморасчетов с торговыми партнерами. Прогноз технического обслуживания транспортного средства на основе эксплуатационных данных. Отслеживание движения транспортного средства.

Ярким примером автоматизации логистической деятельности является торговая платформа. Большинство процессов, связанных с получением товаров и отправкой заказов, автоматизированы. Это гарантирует, что поставки осуществляются в режиме реального времени и что товар поступает к клиенту как можно быстрее.

Это привело к небывалому увеличения эффективности и расширению канала получения доходов. Это положительный аспект. Негативной стороной является то, что переход к цифровым технологиям выявил ряд проблем, которые делают компании (ТИЛ) очень уязвимыми для кибератак. Это затрагивает все отрасли промышленности, включая судоходство, железнодорожные перевозки, грузовые автомобили, логистику и доставку посылок. Это может иметь дорогостоящие, разрушительные и финансово ответственные последствия, особенно когда личные данные клиентов попадают в руки хакеров.

Кроме того, хакеры пытаются похитить информацию, хранящихся в сетях, что необходимо для модернизации и развития индустрии (ТИЛ), чтобы обеспечить более эффективное и качественное обслуживание клиентов. Эти сети предоставляют цифровые улучшения, такие как автоматизированный заказ, отслеживание груза и доступ к информации об

учетной записи. Хотя эти преимущества очень ценны для клиентов, они также требуют хранения больших объемов личных данных через онлайн-платформы, мобильные приложения и другие мобильные устройства, которые представляют одними из наиболее небезопасных каналов из-за отсутствия строгих протоколов кибербезопасности. Пользователи растущего количества мобильных устройств производят все больше контента, который удобно хранить в облаках [2]. Транспорт и логистика имеют ряд слабых мест. Во-первых, операционные технологии (ОТ), новые каналы связи, напрямую связанные с цифровой экосистемой компаний (ТИЛ), и растущее применение беспроводных каналов делают компании предпочтительной мишенью для хакеров. Во-вторых, правила и стандарты в области ИТ устарели, а осведомленность о кибербезопасности недостаточна. И, наконец, и, пожалуй, самым важным фактором является нехватка квалифицированного персонала, который мог бы обеспечить защиту.

Киберугрозы постоянно развиваются, но основной причиной являются люди. Например, сотрудники, которые не распознают фишинговые электронные письма, могут применяться хакерами в начале атаки. Поскольку более половины утечек данных могут быть напрямую связаны с уязвимостями в организационных процессах и квалификацией или неадекватностью сотрудников, первым шагом в цепочке атак часто является невнимательный сотрудник.

Для защиты от этих атак важно применять строгие меры безопасности, проявлять бдительность в отношении электронной почты и других форм общения, а также обучать сотрудников методам безопасного использования компьютеров [3]. Что еще хуже, во всем мире наблюдается серьезная и растущая нехватка специалистов по кибербезопасности. Вместо того чтобы сделать работу в сфере кибербезопасности более желаемой, например, путем увеличения заработной платы и льгот и поощрения инноваций, многие компании (ТИЛ) рассматривают кибербезопасность как фактор затрат, который должен соответствовать ограниченному бюджету.

Прежде всего, корпоративная культура должна перейти от недостаточного внимания к кибербезопасности к признанию настоятельной необходимости борьбы с угрозами. Во всех секторах укрепление кибербезопасности во всей организации должно быть четким и одним из главных аспектом. Частые тренинги по информированию о кибербезопасности могут помочь развить у сотрудников склонность к риску. Акцент должен быть сделан на мерах, которые каждый сотрудник может предпринять, чтобы защитить себя от хакеров, таких как защита паролем и оповещения о подозрительной активности в корпоративной сети.

Во-вторых, повышенный акцент на управлении киберрисками следует использовать для привлечения специалистов по кибербезопасности из университетов и частного сектора. Компании сообщают, что их

цель - стать лидером в области кибербезопасности. Компании могут привлечь специалистов в области кибербезопасности, сообщив им, что они используют новейшие технологии и заменяют устаревшие системы. Компании могут также рассмотреть возможность обращения за консультацией к беспристрастным поставщикам оборудования, которые не пытаются продать свою технологию.

Актуальные способы применения искусственного интеллекта – это обнаружение мошенничества, вредоносных программ, несанкционированных вторжений. Искусственный интеллект способствует предвидению и предотвращению киберпреступлений, обеспечивает защиту слабо защищённых устройств, требует регулярного обновления паролей [1]. Это из условия обеспечения безопасности бизнеса. Угрозы и поиск губительных файлов, подозрительных IP-адресов или запрещенных действий пользователя выполняются в тот же момент. Таким образом, искусственный интеллект сводит к минимуму участие человека в процессе обеспечения безопасности и вносит свой вклад в кибербезопасность.

Наконец, вам нужно найти сотрудников в технологическом отделе компании, которые активно участвуют в инициативах по кибербезопасности и продемонстрировали ключевые компетенции, необходимые для успешных кандидатов. Обучая и вознаграждая сотрудников, а также создавая специальные стимулы для приобретения необходимых навыков, компании (ТИЛ) могут быстро устранить, по крайней мере, часть пробелов в навыках кибербезопасности.

Основными проблемами безопасности являются недостаточная осведомленность пользователей, участившиеся кибератаки, нехватка специалистов и необходимость постоянного обновления систем безопасности. Решение выше перечисленных проблем требует обучения сотрудников кибербезопасности создания единой системы подготовки и сертификации экспертов. Кроме того, для повышения кибербезопасности необходимо использовать новейшие технологии и методы защиты данных.

**Библиографические ссылки**

1. *Корнев Л. В.* Обеспечение информационной безопасности в условиях цифровизации [Электронный ресурс] // Молодой ученый. 2022. № 12(407). С. 7–11. URL: https://moluch.ru/archive/407/89650/ (дата обращения: 08.10.2023).

2. *Прохоров А. В.* Цифровая трансформация анализ, тренды, мировой опыт издание второе, исправленное и дополненное [Электронный ресурс]. М., 2019. С. 24–27. URL: https://ацим.рф/wp-content/uploads/2021/09/digital_transformation_book.pdf/ (дата обращения: 08.10.2023).

3. *Струнин Д. А.* Кибератаки и их влияние на цифровую экономику [Электронный ресурс] // Молодой ученый. 2023. № 5(452). С. 15–16. URL: https://moluch.ru/archive/452/99590/ (дата обращения: 08.10.2023).