4 [2024]
ISBN 978-5-901722-87-9
ТРАНСПОРТ. ГОРИЗОНТЫ РАЗВИТИЯ

УДК 656.61.052

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ЦИФРОВИЗАЦИИ ТРАНСПОРТНОЙ ОТРАСЛИ

Кобзев Артем Александрович[1], студент
e-mail: p.plan@rambler.ru
Волков Андрей Анатольевич[1], доцент
e-mail: welbot@rambler.ru

[1] Каспийский институт морского и речного транспорта им. генерал-адмирала Ф.М. Апраксина – филиал Волжского государственного университета водного транспорта, Астрахань, Россия

Аннотация: В современных условиях вопросы информационной безопасности играют ключевую роль при цифровизации транспортной отрасли. Угрозы, которые могут нарушить нормальное функционирование транспортного комплекса, включают в себя антропогенные риски и риски внешнего вмешательства, такие как нарушение требований безопасности на транспорте, коррупционные риски, проблемы в профессиональной подготовке и многие другие. В статье авторы рассматривают проблему обеспечения транспортной безопасности в России в условиях роста цифровизации транспортной отрасли. Цифровизация широко распространилась среди компаний в различных сферах деятельности, и важно развивать меры по обеспечению безопасности в этом новом цифровом пространстве.

Ключевые слова: безопасность судоходства, киберриски, цифровизация транспорта, автономное судоходство.

INFORMATION SECURITY IN THE DIGITALIZATION OF THE TRANSPORT INDUSTRY

Kobzev Artyom Alexandrovich[1], Student
e-mail: p.plan@rambler.ru
Volkov Andrei Anatolievich[1], Associate Professor
e-mail: welbot@rambler.ru

[1] Caspian Institute of Sea and River Transport. Admiral General F.M. Apraksina – branch of the Volga State University of Water Transport, Astrakhan, Russia.

Abstract. In modern conditions, information security issues play a key role in the digitalization of the transport industry. Threats that can disrupt the normal functioning of the transport complex include anthropogenic risks and risks of external interference, such as violations of transport safety requirements, corruption risks, problems in vocational training and many others. In the article, the authors consider the problem of ensuring transport security in Russia in the context of the growing digitalization of the transport industry. Digitalization has spread widely among companies in various fields of activity, and it is important to develop security measures in this new digital space.

Keywords: safety of navigation, cyber risks, digitalization of transport, autonomous navigation.

Цифровизация, внедрение искусственного интеллекта, применение нанотехнологий, трехмерная визуализация – все это уже стало реальностью нашего времени. Беспилотные аппараты, электромобили, дроны, интеллектуальные оповещения и навигационные системы, модули машинного зрения, позволяющие распознавать пешеходов – все это успешно интегрируется в современный мир.

Проблема кибербезопасности в транспортной отрасли, особенно в морском секторе, действительно становится все более острой с распространением цифровых технологий. Уязвимости, связанные с использованием новых технологий, беспроводных средств связи и автоматизированных систем, делают судоходные компании привлекательными целями для кибератак. Недостаток обновления стандартов и правил, а также нехватка информированности в области кибербезопасности, только усугубляют эту проблему [1].

Отсутствие достаточного числа квалифицированных специалистов по кибербезопасности является серьезным ограничивающим фактором для защиты транспортных компаний от киберугроз. Эффективная защита от кибератак требует наличия обученного персонала, способного грамотно реагировать на угрозы и обеспечивать безопасность цифровых систем.

Факт того, что кибератаки в сфере транспорта и логистики стали происходить с учащением, говорит о необходимости принятия срочных мер по укреплению кибербезопасности в этом секторе. Масштабные и частые кибератаки могут нанести серьезный ущерб как самим компаниям, так и всей инфраструктуре транспортной отрасли, что подчеркивает важность разработки и внедрения комплексных мер по защите от киберугроз.

Инциденты, подобные кибератакам на Transnet и ColonialPipeline, подчеркивают серьезность проблемы кибербезопасности в транспортной отрасли. Такие атаки не только нарушают операции компаний, но и могут привести к значительным экономическим потерям и нарушению поставок важных товаров и услуг.

Для предотвращения подобных инцидентов и обеспечения безопасности важно развивать кибербезопасность в транспортной отрасли путем внедрения современных технологий защиты, обучения персонала и активного мониторинга потенциальных угроз. Компании должны принимать кибербезопасность как приоритетную задачу и инвестировать в необходимые меры для защиты своих цифровых систем и данных.

Да, безопасность данных в транспортной отрасли становится все более критической в связи с растущими возможностями хакеров и киберпреступников. Угрозы, связанные с кибератаками на суда, портовые терминалы и навигационные системы, имеют потенциал нанести серьезный ущерб как самим компаниям, так и клиентам.

Уязвимость кибератак на навигационные системы кораблей, такие как GPS, AIS и ECDIS, может привести к опасным ситуациям в море, включая изменение маршрутов судов, помехи во взаимодействии с другими судами и даже возможные столкновения. Контроль над системами управления горючим, управляющими системами и балластными системами также может быть использован для причинения серьезных последствий.

Профилактика и защита от подобных киберугроз требует комплексного подхода, включающего в себя усиление сетевой безопасности, постоянный мониторинг и обновление систем, а также обучение персонала по повышению осведомленности о кибербезопасности. Регулярные аудиты безопасности и применение современных методов шифрования и защиты данных могут снизить риск несанкционированного доступа и минимизировать возможные угрозы для транспортной отрасли.

Действительно, все большее количество устройств, подключенных к сети, делает их более уязвимыми для кибератак. Морские и нефтяные отрасли, объединяющие корабли и

нефтяные вышки с компьютерными сетями, становятся объектом серьезных угроз со стороны хакеров. Например, пираты у побережья Сомали и в других зонах пиратства могут использовать онлайн-навигацию с помощью AIS, ECDIS и радиолокаторов для выбора целей нападений.

Кибербезопасность играет сейчас ключевую роль, поскольку все больше оборудования как на судах, так и в компаниях становится электронным. Это увеличивает риски кибератак. Существует множество способов проникновения в сеть, начиная от простых вирусов в электронной почте и заканчивая целенаправленными атаками для получения доступа к ценной информации. Учитывая огромные денежные суммы, с которыми взаимодействуют компании в этой отрасли, привлечение внимания киберпреступников становится неизбежным, что требует улучшения систем безопасности.

Международная морская организация (IMO) играет важную роль в обеспечении безопасности на море и защите окружающей среды в международных водах. Резолюция MSC.428(98), принятая Комитетом по безопасности на море IMO, связанная с управлением морскими киберрисками, является важным шагом в направлении обеспечения безопасности судоходных компаний от киберугроз.

Проблема морской кибербезопасности действительно требует серьезного внимания, поскольку атаки на сервера могут иметь серьезные последствия для судоходных компаний и безопасности на море в целом. Важно, чтобы компании были открытыми относительно кибератак, чтобы можно было обменяться информацией и произвести анализ уязвимостей [2].

В России действительно принимается специальное законодательство по противодействию киберугрозам, что способствует укреплению кибербезопасности в морской отрасли. Федеральный закон "О безопасности критической информационной инфраструктуры РФ" играет значительную роль в этом процессе.

Резолюция IMO MSC.428(98) является важным инструментом для снижения и контроля киберрисков в судоходных компаниях. Ее целью является обеспечение того, чтобы киберриски должным образом учитывались в системах управления безопасностью компаний, что поможет снизить вероятность успешных кибератак и улучшить общую кибербезопасность в морской отрасли.

1) идентификация – это определение задач и обязанностей экипажа и персонала компании по управлению и контролю за киберрисками. Выявление систем, ресурсов, данных и функциональных возможностей, которые могут представлять собой опасность, как для судна, так и для компании в случаи сбоя или взлома третьими лицами.

2) защита – это реализация процедур и мер контроля рисков, планирование действий на случай кибератаки, а также сбоя, с целью предотвращения и минерализации ущерба.

3) обнаружение – это разработка и принятие мер для своевременного обнаружения кибер опасности.

4) реагирование – это разработка и выполнение мер и планов по обеспечению отказоустойчивости и восстановление систем, жизненно не обходимых для функционирования судна или компании.

5) восстановление – это оценка ущерба и идентификация мер по резервному дублированию и восстановлению необходимых для эксплуатации судна и компании киберсистем [3].

Действительно, информационная защита является критически важным аспектом в судоходной отрасли в современном мире. Учитывая все новые технологии и цифровые инновации, необходимо обеспечить надежную защиту данных на судах и в портовых зонах. Принципы целостности, конфиденциальности и доступности информации играют ключевую роль в обеспечении безопасности информационных систем в морской отрасли.

Подготовка кибератак на суда и порты становится все более актуальной проблемой, так как киберугрозы могут представлять серьезную угрозу как для материальных ценностей,

так и для жизней людей. Возможность кибератак на суда, перевозящие большую часть мировых грузов, вызывает серьезные опасения относительно безопасности и неприкосновенности транспортных потоков.

Международная морская организация (IMO) действительно играет ключевую роль в разработке стандартов и рекомендаций по обеспечению кибербезопасности в морской индустрии. Она регулярно обновляет свои нормативные акты и руководства, чтобы справиться с вызовами цифровой безопасности в сфере мореплавания. Необходимо постоянное совершенствование мер по защите информации и обучение кадров, чтобы минимизировать риски кибератак и обеспечить безопасность морских операций.

В заключение хотел бы сказать, что судоходство не стоит на месте. судоходство не стоит на месте и постоянно развивается с появлением новых технологий. Электронные карты, РЛС и другие современные устройства действительно значительно улучшили безопасность навигации, обеспечивая моряков современными средствами для более точного и надежного плавания.

Однако, с развитием электроники и цифровых систем появляются новые угрозы в виде кибератак. Защита информации и кибербезопасность становятся все более важными аспектами для морской отрасли. Вместе с тем, разработка более сложных и совершенных методов защиты данных и информационных систем позволяет справляться с этими угрозами.

Важно, что развитие беспилотных технологий в управлении судами также представляет новые вызовы и возможные угрозы для безопасности. Понимание этих рисков и разработка соответствующих мер безопасности являются приоритетными задачами для индустрии. Управление судном дистанционно требует не только передовых технологий, но и надежных систем защиты от потенциальных киберугроз [4].

Будущее судоходства, безусловно, связано с инновационными технологиями, но важно не забывать о обеспечении их безопасности и защите от возможных угроз. Развитие и применение современных методов защиты данных и информационных систем позволит морской отрасли эффективно справляться с вызовами цифровой эпохи и обеспечивать безопасность на море.

Список литературы:

1. Naser Abdel Raheem Al Ali. Cyber security in marine transport: opportunities and legal challenges. – URL: http://www.researchgate.net/publication/357264721_Cyber_security_in_marine_transport_opportunities_and_legal_challenges (дата обращения: 01.03.2024)

2. Kimberly Tam. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. – URL: https://www.researchgate.net/publication/327332564_Maritime_cybersecurity_policy_the_scope_and_impact_of_evolving_technology_on_international_shipping. (дата обращения: 05.03.2024)

3. Резолюция IMO MSC.428(98). – URL: http://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf (дата обращения: 01.02.2024)

4. Nikolaos Kampantais. Legal and regulatory implications of the unmanned ship operation. – URL: http://www.researchgate.net/publication/324978865_Legal_and_regulatory_implications_of_the_unmanned_ship_operation (дата обращения: 05.03.2024)