УДК 004.056

КИБЕРУГРОЗЫ КАК НАПАСТЬ XXI ВЕКА

Скоробогатов И.Е. – студент 2 курса факультета инженерии и цифровых технологий
Научный руководитель – Грицкевич Р.А., старший преподаватель кафедры физической культуры и спорта
ФГБОУ ВО «Морской государственный университет имени адмирала Г.И. Невельского»

Ключевые слова: *киберугрозы, кибератаки, кибербезопасность, цифровизация, киберпреступления, программирование.*

Работа посвящена разбору киберугроз для различных сфер деятельности как в России, так и в мире в целом. Исследование показало, что кибератаки – одна из опаснейших угроз современности и будущего.

Введение. Одной из проблем в современном мире является вопрос кибербезопасности. И с каждым годом влияние данной проблемы на наше общество усиливается. Грамотно разработанная стратегия защиты от киберугроз позволит не только обеспечить интересы каждого из нас, но и гарантировать национальную безопасность.

Ежегодно количество кибератак возрастает в разы. Только за прошедшие три года число уникальных инцидентов возросло более чем на 50%. Совершенствуются существующие системы программного обеспечения, и создаются новые, наименее уязвимые к угрозам кибербезопасности. Однако, проведя анализ статистических данных, можно сделать вывод, что развитие навыков субъектов, занимающихся противоправной вредоносной деятельностью происходит значительно быстрее.

Рассматривая цели киберпреступников, можно увидеть, что более 30% выбирают в качестве «добычи» персональные данные, поскольку именно они открывают для злоумышленников новые

возможности получения «рычагов давления» и баснословных денежных средств.

Часто объектами кибератак становятся не только коммерческие организации, но и государственные и муниципальные предприятия, медицинские организации. Проблема состоит в том, что данные государственных органов и учреждений содержат охраняемую законом тайну. В данном случае под угрозой находятся не только интересы личности, но и безопасность всего государства, настолько значителен масштаб урона, который наносят киберпреступники [1].

Атака промышленных организаций влечет за собой не только множество исков от пострадавших пользователей, падение акций, но и прекращение существования данных предприятий. Злоумышленники, в большинстве своём, остаются неизвестными, и весь урон ложится на ту компанию, которая пострадала от вышеназванных преступлений. Иногда субъекты, совершившие кибератаку раскрывают своё сообщество, но только преследуя личные цели, такие, как повышение авторитета своей «организации» и наведение ещё большей смуты.

К категориям тяжких и особо тяжких преступлений, совершенных против Российской Федерации, и её граждан относится почти половина от общего количества. Раскрываемость же данных преступлений не превышает 25% от числа совершенных атак.

Прогрессирующая цифровизация экономики коснулась и морской отрасли. Большая часть судов в своей деятельности использует электронную навигацию. Увеличивается количество судов и уменьшается состав команд, так как именно современные технологии позволяют значительно снизить расходы. Обновление систем с помощью Интернета происходит не только на суше, но и во время плавания в территориальных водах России и за их пределами. Значительное число кибератак совершается на системы администрирования и системы связи. Системы управления двигателями, доступа и обслуживания пассажиров на большинстве судов действуют с использованием автоматических программ, что повышает их уязвимость перед киберпреступниками. Тот факт, что практически все системы, обеспечивающие судно автоматизированы может привести не только к потерям денежных средств, но и самого дорогого – человеческих жизней [2].

Необходимость принятия мер по защите остро стоит не только на национальном, но и на международном уровне. За последнее десятилетие наблюдается огромное количество инцидентов, приведших к выходу из строя пассажирских и промышленных судов, погрузочно-разгрузочных терминалов, буровых установок, и даже нефтяных вышек.

Заключение. Международные организации приняли множество актов, призывающих администрации вести учёт рисков кибератак. Одним из них является резолюция, принятая Комитетом безопасности на море ИМО в 2017 году.

Серьезной проблемой кибератаки считает и Российская Федерация, которая в последние годы все чаще подвергается данным правонарушениям. В 2017 году был принят Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации"[3], который регулирует отношения в области безопасности информационной инфраструктуры РФ, в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак. Под компьютерной атакой понимается целенаправленное воздействие программных средств в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Библиографический список:

1. Згоба А.И., Маркелов Д.В., Смирнов П. И. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. 2014. №5 (8). URL: https://cyberleninka.ru/article/n/kiberbezopasnost-ugrozy-vyzovy-resheniya (дата обращения: 05.02.2025).

2. Аверкиев А.А., Камбулов Д.А. КИБЕРБЕЗОПАСНОСТЬ ВИДЫ И МЕТОДЫ // StudNet. 2022. №1. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-vidy-i-metody (дата обращения: 06.02.2025).

3. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция) // СПС «КонсультантПлюс». — URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 04.02.2025).

CYBER THREATS AS AN ATTACK OF THE 21ST CENTURY

Skorobogatov I.E.
Scientific supervisor – Gritskevich R.A.
Maritime State University named after Admiral G.I. Nevelskoy

Keywords: *cyber threats, cyber attacks, cybersecurity, digitalization, cybercrime, programming.*

The work is devoted to the analysis of cyber threats for various fields of activity both in Russia and in the world as a whole. The study showed that cyber attacks are one of the most dangerous threats of our time.