УДК 004.056(476)

КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

А.Н. Труханович, 2 курс
Научный руководитель – **О.В. Володько**, к.э.н., доцент
Полесский государственный университет

В современном мире, где технологии развиваются с огромной скоростью, обеспечение защиты данных и цифровых сетей стало приоритетной задачей, превратив кибербезопасность в ключевую область. Всеобщая цифровизация и автоматизация производства открывают новые возможности, однако одновременно создают и слабые места, подверженные усилению кибератак. Эти атаки могут быть разными по своей природе и требуют от правительств не только использования новейших технологий, но и создания комплексного подхода к обеспечению безопасности в цифровой среде.

В соответствии с указом № 40 "О кибербезопасности", который был подписан президентом Республики Беларусь Александром Лукашенко 14 февраля 2023 года, определяется правовая основа создания и функционирования национальной системы обеспечения кибербезопасности, предусматривающей формирование комплексного многоуровневого механизма противодействия кибератакам на государственные органы и организации, критическую информационную инфраструктуру [1].

Исходя из различных подходов к определению понятия кибербезопасность можно отметить, что: кибербезопасность — сфера деятельности, занимающаяся защитой компьютерных систем, сетей, программ и данных от киберугроз, включая хакерские атаки, вирусы, вредоносное про-

граммное обеспечение и другие цифровые угрозы. Ее целью является обеспечение конфиденциальности, целостности и доступности информации, а также предотвращение нанесения ущерба компьютерным системам и пользователям [2, 4].

На данный момент выделяют следующее киберугрозы в Республике Беларусь:

— количество атак локальными вредоносными файлами, распространяющимися через съемные носители в виде зашифрованных документов или в составе сложных инсталляторов, выросло на 12 %.

— число атак с использованием шпионских программ – на 34 %.

— использование зловредного программного обеспечения для скрытого удаленного управления устройствами подскочило сразу на 36 %.

Исходя из данных таблицы 1, которая представлена ниже, мы можем наглядно рассмотреть атаки, угрозы и уязвимости цифровой трансформации. Важно отметить, что наибольший процент значимости угроз составляют полиморфные атаки – 85%, а наименьший – возрастание времени простоя ИТ-системы, который составляет 23%.

Таблица – Атаки, угрозы и уязвимости цифровой трансформации

Атаки, угрозы и уязвимости цифровой трансформации (ЦТ)	Значимость угроз (%)	Рекомендации по обнаружению и предотвращению атак, ликвидацию угроз и уязвимостей ЦТ
Полиморфные атаки	85	Внедрение SIEM-систем и систем мониторинга на базе систем ИИ и глубокого машинного обучения Deep learning
Угрозы технологии Dev Ops	81	Перейти на более безопасную технологию Dev Sec Ops
Уязвимости «слепых» зонинфраструктуры ИТ-системы	70	Принять меры для придания прозрачности инфраструктур ИТ-систем, подлежащих ЦТ
Рост атакующего потенциала киберпреступников	68	Широкое внедрение систем автоматизации и интеграции ИБ инфраструктур ИТ-систем, подлежащих ЦТ
Широкое использование протокола SSL	57	Для снижения доли фишинговых атак следует перейти на EVSSL
Угрозы и уязвимости интернета вещей	47	Использование технологий Блокчейн для управления аунтефикацией, обеспечения неделимости информации и работоспособности ИТ-сервисов
Расширение пространства реализации угроз	34	Использование проактивных методов защиты информации
Незащищенность клиентских данных	28	Использование криптографических методов защиты информации
Возрастание времени простоя ИТ-системы	23	Комплексное решение вопросов безопасности для обеспечения непрерывности бизнес-процессов компании

Примечание – Источник [3, с. 47]

Важно выделить следующие достижения по кибербезопасности: за 11 месяцев 2024 года в Республике Беларусь защитные технологии заблокировали миллионы попыток белорусских пользователей перейти на фишинговые страницы.

Также можно отметить следующие рекомендации от каких-либо киберугроз:

— необходимо скачивать программы только из официальных источников или с сайтов разработчиков;

— внимательно изучать отзывы перед установкой, чтобы снизить риск столкнуться с вредоносным программным обеспечением [4].

В 2024 году был представлен рейтинг Global Cybersecurity Index 2024. В нем оценивается готовность стран к кибератакам. Его разработкой занимался Международный союз электросвязи при ООН. Уровень кибербезопасности Беларуси был оценен как Tier 3 - Establishing (Tier 5 – низший, Tier 1 – наивысший).

Рейтинг построен на основе 83 показателей, которые объединены в 5 блоков. За каждый из блоков страна получает определенное количество баллов. Баллы Беларуси распределились следующим образом (максимум – 20 баллов в категории).

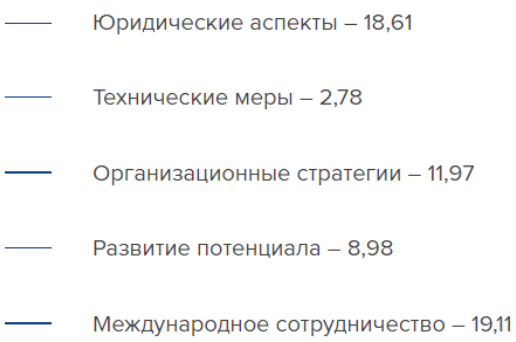

Рисунок 1. – Категории оценивания в Global Cybersecurity Index 2024

Примечание – Источник [5]

Из рисунка 1 мы можем сделать вывод, что в Беларуси хорошо разработаны юридические нормы и развито международное сотрудничество. Однако белорусским организациям серьезно недостает технических мер, потенциала развития и организационных стратегий [5].

На рисунке 2 мы можем наглядно рассмотреть диаграмму, на которой отражается статистика оценки Беларуси в Global Cybersecurity Index 2024.

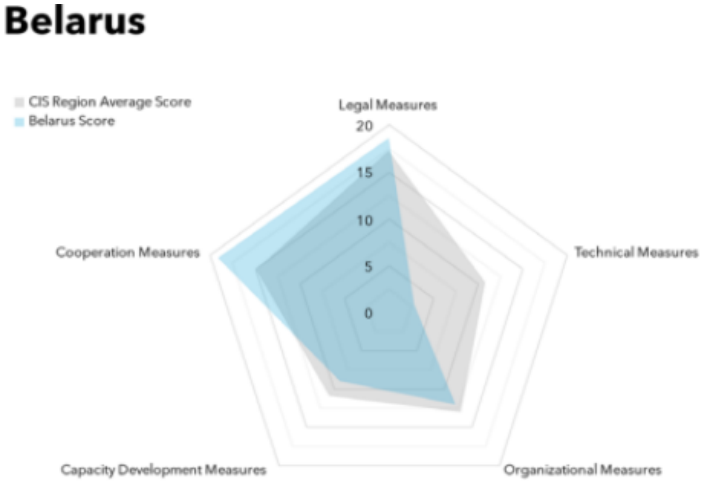

Рисунок 2. – Диаграмма со статистикой оценки Беларуси в Global Cybersecurity Index 2024

Примечание – Источник [5]

Таким образом, на основе всего вышеизложенного, мы можем сделать вывод, что по улучшению и активации кибербезопасности в условиях цифровизации в Республике Беларусь необходимо: объединять усилия общества, правительства и бизнеса в области ответственной за сохранения данных и информации, что позволит сформировать безопасное цифровое пространство, благоприятствующее инновациям и экономическому развитию, что в итоге принесет пользу всему белорусскому обществу.

Список использованных источников

1. Указ № 40 от 14 февраля 2023 г. О кибербезопасности. [Электронный ресурс]. – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g – Дата доступа: 09.04.2025.

2. Что такое кибербезопасность — обеспечение, угрозы. Режим доступа: https://www.banki.ru/wikibank/kiberbezopasnost/ – Дата доступа: 09.04.2025.

3. Артамонов, В. А. Кибербезопасность в условиях цифровой трансформации /В. А. Артамонов, Е.В. Артамонова //Цифровая трансформация. – 2021 – № 4 (17). – С. 42–51.

4. Какие киберугрозы актуальны в Беларуси в 2024 году. Режим доступа: https://normativka.by/lib/news/64139 – Дата доступа: 09.04.2025.

5. Беларусь получила уровень Tier 3 в Global Cybersecurity Index 2024 [Электронный ресурс]. – Режим доступа: https://noventiq.by/about/news/belarus-poluchila-uroven-tier-3-v-global-cybersecurity-index-2024 – Дата доступа: 09.04.2025.