стало более точным и обоснованным. Тем самым ускоряются комплексные процессы общественной жизни как в моногосударственном, так и в глобальном масштабах.

Современные технологии облегчают жизнь людей путем автоматизации рутинных процессов, которые отнимают самый важный и драгоценный человеческий ресурс – время. Появляются новые возможности для образования и освоения культурных ценностей, творчества и межэтнического обмена, личностной и коллективной коммуникации, духовного и физического развития.

Вместе с тем, цифровой мир – это не только новый уровень свободы, но и новые вызовы. Бездуховность, социальная апатия, игровая зависимость, киберпреступность и другие «подводные камни» цифрового мира способны перечеркнуть позитивные тенденции социального прогресса на основе цифровых технологий.

В этой связи назрела необходимость в формировании не только цифровой грамотности (пользовательских навыков), но и своеобразной «цифровой морали» – набора качеств и установок пользователя, которые сохранят и защитят гуманистическую основу личности.

Список использованных источников

1. Фадеева, И. П. Социальные последствия развития цифровой экономики в современной России / И. П. Фадеев // Молодой ученый. – 2023. – № 51 (498). – С. 106–108.

УДК 681.518.5

СЦЕНАРНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Хамаза А. С., асп.
Российский университет транспорта, г. Москва, Российская Федерация

Критическая инфраструктура транспорта представляет собой комплекс жизненно важных объектов, включающий системы управления движением, энергоснабжения, информационно-телекоммуникационные системы, объекты транспортной инфраструктуры и транспортные средства. В условиях цифровизации повышается эффективность управления этими объектами, но одновременно возрастают риски информационной безопасности.

Специфика транспортной отрасли заключается в необходимости обеспечивать безопасность территориально распределенных систем, устаревшего оборудования и программного обеспечения, а также систем реального времени, что требует существенных инвестиций и адаптации стандартных средств защиты.

Для эффективного управления рисками информационной безопасности предлагается использовать методологию сценарного анализа угроз. Ее преимущества заключаются в учете взаимосвязей между компонентами инфраструктуры, детальном моделировании действий нарушителя, возможности анализа комплексных атак, наглядности и простоте формирования сценариев, а также возможности определения наиболее критичных

угроз для выработки оптимальных защитных мер.

Предлагаемый подход включает идентификацию критически важных активов, анализ и оценку рисков, разработку комплекса организационно-технических мер защиты, а также непрерывный мониторинг эффективности принятых мер. Особое внимание уделяется внедрению современных средств защиты информации, обучению персонала, разработке регламентов реагирования на инциденты и взаимодействию с регуляторами.

Применение сценарного подхода позволяет провести углубленный анализ рисков с учетом специфики транспортной инфраструктуры и реализовать более эффективную стратегию защиты по сравнению с общими методами. Однако его внедрение требует высокой квалификации специалистов, наличия детальных данных о защищаемых системах и интеграции с другими методами анализа рисков.

Список использованных источников

1. Банк данных угроз информационной безопасности [Электронный ресурс] // ФСТЭК России : [сайт]. – Режим доступа: https://bdu.fstec.ru/threat. – Дата доступа: 25.02.2025.
2. Риски ИБ в промышленных компаниях [Электронный ресурс] // Positive Technologies : [сайт]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ics-risks-2021. – Дата доступа: 25.02.2025.
3. Самые громкие кибер-атаки на критические инфраструктуры [Электронный ресурс] // SecurityLab.ru : [сайт]. – Режим доступа: https://www.securitylab.ru/blog/company/ PandaSecurityRus/326371.php. – Дата доступа: 15.02.2025.
4. Positive Technologies: технологическая сеть 75 % промышленных компаний открыта для хакерских атак [Электронный ресурс] // Positive Technologies : [сайт]. – Режим доступа: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-tekhnologicheskaya-set-75-promyshlennyh-kompanij-otkryta-dlya-hakerskih-atak/. – Дата доступа: 20.02.2025.
5. Зависляк, И. В. Политика информационной безопасности на предприятии / И. В. Зависляк, Т. В. Кувылина // Международный научно-исследовательский журнал. – 2020. – № 6 – 1 (96). – С. 61–63.
6. Гневанов, М. В. Информационная безопасность ERP-систем / М. В. Гневанов, Р. Г. Баранов // Московский экономический журнал. – 2021. – № 2. – С. 15–20.
7. Кузнецов, А. А. Методы и средства обеспечения безопасности информации на транспорте / А. А. Кузнецов, С. П. Евсеев, О. Г. Король. – Харьков : Изд-во ХНАДУ, 2018.– 212 с.