УДК 343

Н. М. Саулов,
курсант 1-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Т. И. Вишневская,
начальник кафедры правовых дисциплин
факультета повышения квалификации и переподготовки кадров
Могилевского института МВД,
кандидат юридических наук

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цифровые технологии стремительно развиваются и проникают практически во все сферы нашей жизни. Они изменяют способы взаимодействия людей, облегчают рутинные задачи, улучшают качество образования, здравоохранения, коммуникаций и других областей.

Использование смартфонов, развитие облачных технологий, «Интернета вещей», искусственного интеллекта и многие другие инновации ускоряют цифровую трансформацию общества. Эти изменения создают новые возможности для бизнеса, науки, культуры и улучшают качество жизни людей в целом.

Однако вместе с преимуществами цифровизации возникают и новые вызовы, такие как проблемы защиты конфиденциальности данных, цифровое неравенство, угрозы кибербезопасности. Поэтому важно развивать инфраструктуру и законы, которые обеспечили бы безопасное и эффективное использование цифровых технологий во имя благополучия общества. Среди актуальных и проблемных вопросов в данной сфере, требующих решения, следует отметить следующие:

− идентификация и анализ угроз (как оперативно выявлять потенциальные киберугрозы и проводить анализ их характеристик для предотвращения атак);

− сотрудничество с другими службами безопасности (как эффективно сотрудничать с правоохранительными органами и другими службами безопасности для обмена информацией и координации действий);

− разработка и использование технологий противодействия (какие новые технологии могут помочь в предупредительной деятельности, например, использование искусственного интеллекта для анализа данных);

− законодательство и правовые аспекты (какие нормы права регулируют деятельность в сфере информационной безопасности);

− обучение и подготовка специалистов (как обеспечить высокий уровень подготовки сотрудников, чтобы они могли эффективно выполнять задачи по обеспечению информационной безопасности).

Обеспечение информационной безопасности государства представляет собой сложную задачу, требующую комплексного подхода. Целесообразно выделить ряд перспективных подходов, которые помогут в противодействии преступности цифрового мира: обучение и подготовка персонала, использование шифрования и защиты данных, управление доступом, мониторинг и обнаружение угроз, соблюдение законодательства, регулярное обновление систем и процедур, сотрудничество с другими службами безопасности [1].

Предупредительная деятельность по обеспечению информационной безопасности — это комплекс мероприятий, направленных на предотвращение угроз и рисков в области информационной безопасности. Эта деятельность может включать в себя следующие аспекты.

В первую очередь это анализ рисков, он включает в себя оценку и анализ потенциальных угроз, уязвимостей и возможных последствий для информационных систем и данных. На основе этого анализа разрабатываются стратегии и планы по предотвращению угроз.

После этого следует разработка политики безопасности, а именно установление правил, процедур и мер по обеспечению безопасности информации. Политика безопасности определяет стандарты и требования, которые должны соблюдаться для защиты данных.

И в завершение — обучение и осведомление персонала. Проведение обучающих программ и тренингов для сотрудников по правилам безопасности информации, обнаружению угроз и защите от них. Эффективное обучение персонала играет важную роль в предупреждении инцидентов в области информационной безопасности.

Многие субъекты хозяйствования, компании, предприятия отказываются от хранения информации на серверах и транспортируют ее в облако, где чаще всего располагается информация, обрабатываемая при работе программных продуктов для менеджмента, банковских и CRM-систем. Нередко, особенно при размещении в облачных системах персональных данных, возникает вопрос об их защищенности в соответствии с требованиями законодательства и возможности несанкционированного доступа к информации [2, с. 340].

Обезопасить облачные хранилища данных очень важно, особенно учитывая все угрозы кибербезопасности. Сделать это можно при помощи следующих способов: шифрование данных (это гарантирует, что данные остаются защищенными даже в случае несанкционированного доступа); многофакторная аутентификация (это поможет предотвратить несанкционированный доступ

к вашим данным); регулярное резервное копирование данных (регулярное создание резервных копий данных в облачном хранилище для обеспечения возможности восстановления в случае утраты или повреждения данных); мониторинг и аудит безопасности (мониторинг за активностью в облачном хранилище и регулярные аудиты безопасности для выявления уязвимостей и незаконного доступа); управление доступом (ограничение доступа к данным, необходимым только пользователям, и управление правами доступа с помощью ролей и политики безопасности); обновление программного обеспечения (регулярное обновление программного обеспечения и патчи безопасности облачного хранилища для предотвращения угрозы безопасности).

Обеспечение информационной безопасности государства представляет собой сложную задачу, требующую комплексного подхода. Модификация преступности требует совершенствования форм и методов по ее противодействию. Прогрессивное развитие предупредительной деятельности — залог успеха в борьбе с новыми криминальными вызовами и угрозами, устойчивого правопорядка и благополучия в обществе. Рассмотренные выше направления помогут создать надежную основу для обеспечения информационной безопасности государства.

1. Николаев О. Э. Угрозы информационной безопасности при осуществлении оперативно-розыскной деятельности и основные пути их отражения [Электронный ресурс] // Тр. Акад. упр. МВД России. 2020. № 3 (55). URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-pri-osuschestvlenii-operativno-rozysknoy-deyatelnosti-i-osnovnye-puti-ih-otrazheniya (дата обращения: 03.06.2024). Перейти к источнику Вернуться к статье

2. Клещева Ю. С., Баленко М. С. Проблемы обеспечения информационной безопасности в контексте цифровизации экономики // Современные тенденции и перспективы агропромышленного и транспортного комплексов России : сб. ст. по материалам междунар. конф., Новосибирск, 21 июня 2021 г. / Кубан. гос. ун-т ; редкол.: Е. Б Денисенко, В. В Цынгуева. Новосибирск, 2021. С. 330–342. Вернуться к статье