УДК 004.056

КИБЕРБЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ В ЭПОХУ ЦИФРОВИЗАЦИИ

Дюкова В.А., студентка 3 курса факультета управления и права
Научный руководитель - Репина О.М.,к.э.н., доцент
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола, Россия

Ключевые слова: *цифровизация, кибербезопасность, информационные системы, государственное управление, методы информационной безопасности.*

Сейчас опасность существует не только реальная, но и виртуальная. Хакерские атаки теперь нацелены и на государство, а с появлением электронных госуслуг интерес ко взлому официальных ресурсов и аккаунтов граждан возрос, повышая необходимость улучшения кибербезопасности.

Именно повышение качества кибербезопасности являлось одним из приоритетов в 2024 году. Одним из вызовов для государства стала нехватка профессионалов в этой области, ведь как таковой в университетах «кибербезопасность» лишь одна из дисциплин и не всегда полно изучаемая. Огромную роль сыграло развитие генеративного искусственного интеллекта, чьи способности могут не только совершать вредоносные действия, в обход человеческой внимательности и подготовке, но и также обеспечивать безопасность благодаря анализу аномалий и автоматических реакций на изменения[1]. На основе ИИ преступники могут успешно совершать фишинговые атаки, DDoS-атаки, наносить вред устройствам пользователей и совершать удалённые подключения.

Целью работы является характеристика существующих угроз кибербезопасности для государственных учреждений, изучениетекущих мер защиты и предложение рекомендаций по их улучшению.

За прошедший год в России было совершено около 765 тысяч киберпреступлений, 8% атак пришлось на фишинговые письма якобы от госорганов, 15% это атаки на государственный сектор, что на 5% больше показателя 2023 года [1].Мотивы таких атак зачастую носят политический и идеологический характер в связи со сложившейся мировой обстановкой, а также желание завладеть или удалить важную информацию. Одними из самых запоминающихся преступлений в 2024 году стала фишинговая рассылка в конце апреля, нацеленная на сотрудников крупных российских промышленных и финтех-компаний, также в апреле 2024 года зафиксировано большое количество DDoS-атак на все электронные сервисы «Единой России», что связывают с проведением “Диктанта Победы”, под предлогом предложения крупных пособий, мошенники начали выманивать персональные данные граждан [2].

С 2017 года введён в работу реестр и категории объектов критической информационной инфраструктуры, установлены требования по обеспечению их безопасности, взаимодействию этих систем с иными государственными системами[3]. Задачи по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации были возложены на ФСБ России, введены новые статьи, подразумевающие административную и уголовную ответственность за нарушения требований безопасности и неправомерное воздействие на инфраструктуру. К концу 2025 года Минцифры совместно с ФСБ и Федеральной службой по техническому и экспортному контролю разработает и предоставит госучреждениям рекомендации по нейтрализации уязвимостей ГИС[4]. На данный момент эффективно используются следующие мероприятия по предотвращению кибератак [5]:

1. Регулярные аудиты информационной безопасности
2. Системы контроля и управления доступом
3. Системы предотвращения утечек
4. Средства защиты от вредоносного ПО
5. Защита от DDoS-атак
6. Системы обнаружения и предотвращения вторжений

7. Системы анализа событий информационной безопасности и др.

Для повышения безопасности государственных учрежденийвозможно рассмотрение следующих мероприятий, которые помогут не только оперативно реагировать, но и предугадывать кибератаки:

1. Продолжение развития должного уровня кибербезопасности в регионах. Цифровая трансформация происходит успешно, тем не менее на региональном уровне её качество сильно разнится. Хакеры пользуются этими слабостями и совершают атаки на плохо защищённые сервера и устройства.

2. Обучение кибербезопасности в учебных заведениях всех уровней. Общество быстро развивается и сейчас просто необходимо начинать защиту государства в первую очередь с осведомления граждан, ведь некоторые атаки и взломы происходят из-за неосведомлённости граждан о существующих опасностях.

3. Использование ИИ. Следует продолжать внедрять и грамотно работать над нейросетями, так как именно они способны мгновенно среагировать на внедрение извне, предугадать или предупредить о попытках взлома. Сейчас искусственный интеллект также используется и хакерами, шифруя вредоносные программы и взламывая аккаунты и базы данных через уязвимые места.

4. Сотрудничество с частным сектором. Сюда можно отнести установление партнерств между государственными органами и частными компаниями для обмена информацией о киберугрозах. Разработка совместных инициатив по защите критической инфраструктуры и обмену лучшими практиками.

Взлом информации в государственном секторе может поставить под угрозу не только выполнение критически важных задач, конфиденциальность данных граждан, но и безопасность страны в целом. Для защиты государства и его граждан разработан целый перечень законов и мероприятий, работает национальный координационный центр по компьютерным инцидентам и Система ГосСОПКА**.**

Библиографический список:

1. Исследование российского ландшафта угроз за 2024 год / [Электронный ресурс] // Хабр : [сайт]. — URL: https://habr.com/ru/news/880130/ (дата обращения: 09.02.2025).

2. 5 крупнейших тенденций кибербезопасности в 2024 году, к которым все должны быть готовы уже сейчас / [Электронный ресурс] // CNewsMarket: [сайт]. — URL: https://cnews.ru/link/n589454 (дата обращения: 09.02.2025).

3. Крупные кибератаки и утечки первой половины 2024 года в России / [Электронный ресурс] // Cortel: [сайт]. — URL: https://blog.cortel.cloud/2024/05/23/krupnye-kiberataki-i-utechki-pervoj-poloviny-2024-goda-v-rossii/ (дата обращения: 13.02.2025).

4. Как в России обеспечивают защиту государственных информационных систем от хакеров / [Электронный ресурс] // Государственная дума Федерального Собрания: [сайт] – URL: http://duma.gov.ru/news/51685/ (дата обращения: 10.02.2025)

5. Требования к защите информации в государственных информсистемах / [Электронный ресурс] // TADVISER: [сайт]. — URL: https://www.tadviser.ru/a/474955 (дата обращения: 10.02.2025).

6. Информационная безопасность в государственных учреждениях / [Электронный ресурс] // ЕВРААС: [сайт]. — URL: https://www.evraas.ru/industries/government/ (дата обращения: 09.02.2025).

CYBERSECURITY OF GOVERNMENT AGENCIES IN THE AGE OF DIGITALIZATION

Valeria A.D.
Scientific supervisor –Repina O.M.
Volga State University of Technology, Yoshkar-Ola, Russia

Keywords: *digitalization, cybersecurity, information systems, public administration, information security methods.*

Now the danger is not only real, but also virtual. Hacker attacks are now targeting the state, and with the advent of electronic public services, interest in hacking official resources and accounts of citizens has increased, increasing the need to improve cybersecurity.