УДК 930.25: 616.98:578

КИБЕРПРЕСТУПНОСТЬ В ЭПОХУ ЦИФРОВИЗАЦИИ: РИСКИ, УГРОЗЫ И МЕРЫ ЗАЩИТЫ

Я. Л. Кислейко

студентка, Гродненский государственный университет имени Янки Купалы, г. Гродно, Беларусь, yanakisleiko@gmail.com

Научный руководитель: **М. В. Солодуха**

магистр экономических наук, старший преподаватель, Гродненский государственный университет имени Янки Купалы, г. Гродно, Беларусь, soloduha_mv@grsu.by

В рамках доклада будут рассмотрены основные виды киберугроз, методы их предотвращения, а также последствия атак на информационные системы для бизнеса и государства. Также будет проанализировано текущее состояние законодательства в области кибербезопасности и предложены рекомендации по усилению защиты информации и противодействию киберугрозам.

Ключевые слова: экономическая безопасность; киберугрозы; киберпреступность; цифровизация; цифровая экономика; информационная безопасность.

CYBERCRIME IN THE ERA OF DIGITALIZATION: RISKS, THREATS AND PROTECTION MEASURES

Y. L. Kisleiko

student, Yanka Kupala State University of Grodno, Grodno, Belarus, yanakisleiko@gmail.com

Supervisor: **M. V. Soloduha**

master of economic sciences, senior lecturer, Yanka Kupala State University, Grodno, Belarus, soloduha_mv@grsu.by

The report will consider the main types of cyber threats, methods of their prevention, as well as the consequences of attacks on information systems for business and the state. The current state of cybersecurity legislation will also be analyzed and recommendations on strengthening information protection and countering cyber threats will be proposed.

Keywords: economic security; cyber threats; cybercrime; digitalization; digital economy; information security.

В современной цифровой экономике предприятия и частные лица неизбежно сталкиваются с растущими рисками для цифровой безопасности и защиты личной информации. Сетевой мир предоставляет новые возможности для транснациональной киберпреступности. Автоматизированный анализ поисковых запросов пользователей, данные с персональных «умных» устройств, транзакции по банковским картам, электронная почта и мессенджеры формируют обширную базу информации о личности, которая может быть похищена и использована в корыстных целях.

В контексте кибербезопасности особое внимание следует уделить недостаточному освещению этой темы в отечественном законодательстве. В частности, в Государственной программе развития цифровой экономики и информационного общества на 2021–2025 гг. вопросы борьбы с киберпреступлениями и повышения кибербезопасности отсутствуют год [2].

Однако статистика демонстрирует ухудшение криминогенной обстановки в сфере высоких технологий. Так, с 2016 по 2020 год количество выявленных киберпреступлений увеличилось в 9,3 раза – с 2471 до 25 575. При этом наиболее распространенные способы совершения киберпреступлений в кредитно-финансовой сфере:

– фишинг (подделка сайтов, аккаунтов);

– вишинг (телефонное мошенничество с применением методов социальной инженерии);

– взлом учетных записей пользователей с использованием вредоносных программ [3].

Рост киберпреступности в Беларуси обусловлен рядом факторов, которые способствуют увеличению уровня уязвимости информационной инфраструктуры страны, потенциальным ущербом для экономики и бизнеса, а также угрозой для личной безопасности граждан. Эти факторы включают:

− распространение безналичных расчетов;

− увеличение количества устройств, совершающих финансовые транзакции;

− рост числа пользователей электронных платежных систем;

− увеличение числа абонентов сотовой связи, держателей банковских карт и интернет-пользователей;

− расширение виртуального пространства и увеличение сегмента рынка, связанного с ним [4].

Киберпреступники используют различные методы для совершения противоправных действий, которые влияют на компьютерные системы, сети, устройства и данные. К этим методом относятся:

− фишинговые атаки: Отправка электронных писем или сообщений с вредоносными ссылками или вложениями, которые крадут личную информацию или устанавливают вредоносное ПО;

− вредоносное ПО: Программы, предназначенные для повреждения данных, кражи информации или прерывания работы системы;

− кибервымогательство: Блокировка доступа к данным или системам и требование выкупа за восстановление доступа;

− кража личных данных: Похищение личной информации, такой как номера социального страхования, данные банковского счета и медицинские записи;

− кибершпионаж: Незаконное получение информации о конкурентах, правительственных организациях или частных лицах;

− отмывание денег: Использование киберпреступлений для сокрытия незаконно полученных средств.

Все вышеперечисленные действия могут иметь серьезные последствия для жертв:

− финансовые потери: Кража денег, повреждение или потеря данных;

− потеря репутации: Урон репутации компании или организации;

− потеря доверия клиентов: Утечка конфиденциальной информации, подорвавшая доверие клиентов;

− юридические последствия: Нарушение законов о защите данных и конфиденциальности;

− психологические проблемы: Стресс, беспокойство и депрессия, вызванные киберпреступлениями.

Для защиты от киберпреступности сами пользователи, как частные лица, так и представители организаций могут принимать следующие индивидуальные меры защиты:

− регулярное обновление программного обеспечения: Установка последних обновлений безопасности для устранения уязвимостей;

− использование надежных паролей: Создание сложных и уникальных паролей и их регулярная смена;

− использование двухфакторной аутентификации: Обеспечение дополнительного уровня безопасности, требующего подтверждения входа не только паролем, но и дополнительным фактором, например, кодом с SMS;

− осторожность с открытием вложений и переходом по ссылкам в электронных письмах: Внимательная проверка отправителя и содержания сообщений, избежание открытия вложений или перехода по ссылкам из подозрительных источников;

− осторожность при совершении финансовых операций в Интернете: Использование надежных веб-сайтов, проверка сертификата SSL и других признаков безопасности;

− использование антивирусного программного обеспечения: Установка и регулярное обновление антивирусного программного обеспечения для защиты от вредоносных программ;

− резервное копирование данных: Регулярное резервное копирование важных данных в случае заражения вредоносным ПО или других кибератак;

− повышение осведомленности о кибербезопасности: Проведение тренингов и информационных кампаний для сотрудников и широкой общественности для повышения осведомленности о киберугрозах.

Кроме индивидуальных мер защиты, на государство и компании также возложена ответственность за обеспечение кибербезопасности. Государство занимается разработкой и реализацией законов и регулирующих документов в сфере кибербезопасности, повышением осведомленности о киберугрозах, сотрудничеством с правоохранительными органами для борьбы с киберпреступностью. Компании, в свою очередь, инвестируют в системы кибербезопасности, внедряют политики и процедуры, просвещение сотрудников и партнеров о киберрисках, сотрудничают с правоохранительными органами для расследования киберпреступлений.

Борьба с киберпреступностью требует международного сотрудничества, поскольку киберпреступники часто действуют за пределами юрисдикции одной страны. Сотрудничество включает обмен информацией о киберугрозах, согласованный подход к расследованию киберпреступлений и взаимную правовую помощь [1].

Технологии кибербезопасности постоянно развиваются, чтобы не отставать от меняющихся тактик киберпреступников. К перспективным направлениям, которые способствуют улучшению общей кибергигиены и повышению осведомленности пользователей о методах защиты от киберугроз. относятся:

− искусственный интеллект (ИИ): Использование ИИ для обнаружения и реагирования на киберугрозы, а также прогнозирования и предотвращения кибератак;

− технологии блокчейн: Использование децентрализованных систем для обеспечения безопасности данных и транзакций;

− квантовые вычисления: Создание усовершенствованных методов криптографии для обеспечения безопасности данных и систем от атак с использованием квантовых компьютеров;

− поведенческая аналитика: Использование данных о поведении пользователей для обнаружения аномалий и предотвращения мошенничества и киберпреступлений.

Перспективные технологии кибербезопасности также помогают укрепить доверие к цифровым сервисам и продуктам, что способствует развитию цифровой экономики и обеспечивает стабильное функционирование цифровых инфраструктур. Кроме того, они способствуют сокращению ущерба от кибератак и повышению уровня безопасности в цифровом

пространстве, что является важным условием для устойчивого развития современного общества.,

Киберпреступность представляет значительную угрозу для предприятий и частных лиц в цифровую эпоху. Понимание типов киберпреступлений, их последствий и мер защиты имеет решающее значение для снижения рисков. Сотрудничество между государственными органами, компаниями, международными организациями и пользователями необходимо для эффективной борьбы с киберпреступностью. По мере развития технологий кибербезопасности адаптация и внедрение инновационных решений имеют решающее значение для защиты от постоянно меняющихся киберугроз, обеспечивая безопасное и надежное киберпространство.

Библиографические ссылки

1. *Головенчик Г. Г.* Цифровая экономика как новый этап глобализации // Цифровая трансформация. 2018. № 1(2). С. 26–36.

2. О Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. URL: https://pravo.by/document/?guid=3871&p0=C22100066.

3. Статистические данные по киберпреступлениям за 2017 год [Электронный ресурс] // Министерство внутренних дел Республики Беларусь. URL: http://mvd.gov.by/ru/main.aspx?guid=3311.

4. *Удалов Д. В.* Угрозы и вызовы цифровой экономики // Экономическая безопасность и качество. 2018. № 1(30). С. 12–18.