**БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ:
ПРАВООХРАНИТЕЛЬНЫЙ АСПЕКТ**
**The fight against cybercrime is one of the most
important modern tasks of the state and civil society**

А. А. Нерлова, студент
Уральский юридический институт МВД России
(Екатеринбург, ул. Корепина, 66)

Аннотация

В статье рассматривается киберпреступность и борьба с ней как с одним из ведущих вызовов современности. Оценивается важность данной задачи и инновационных подходов к ней.

Ключевые слова: киберпреступность, it-преступления, защита информации, информационное общество.

Summary

The article examines cybercrime and the fight against it as one of the leading challenges of our time. The importance of this task and innovative approaches to it are assessed.

Keywords: cybercrime, it-crimes, information protection, information society.

Цифровизация предоставляет конкурентные преимущества, но сопряжена с рисками киберугроз. Для их минимизации необходима реализация комплексной стратегии, включающей технологическую защиту, юридическую базу и обучение персон. Высокотехнологичность приносит значительные плюсы (увеличение эффективности, автоматизацию, удобство), также ведет к увеличению киберпреступности. Это требует всесторонних усилий по противодействию на технологическом, правовом и международном уровнях.

В целях противодействия коррупции исследователи отмечают, что система электронной подачи обращений «одно окно» оказывается крайне эффективной. Анализ данных уже давно успешно используется в органах исполнительной власти. Наиболее наглядным примером является использование онлайн-камер в общественных местах для поиска преступников, а также возможность подачи обращений в компетентные органы через интернет. Одним из основных достижений цифровизации государственного управления является значительное сокращение бумажной волокиты и бюрократии при оформлении документов. Справки и паспорта можно запрашивать с помощью приложений, которые также позволяют хранить и обновлять все необходимые данные.

В условиях стремительного развития цифровых технологий обеспечение безопасности в киберпространстве становится все более важной задачей, требующей комплексного подхода как со стороны бизнеса, так и со стороны государственных структур. Киберпреступность, на данный, способствует появлению серьезных угроз во время пользования интернет ресурсами и оказывает негативное влияние на работоспособность информационных технологий [1].

Развитие технологий и цифровая зависимость общества являются ключевыми факторами, способствующими росту киберпреступности.

Высококвалифицированные киберпреступники представляют значительную угрозу, поскольку активно эксплуатируют уязвимости в системах безопасности на глобальном уровне.

Для результативной борьбы с киберпреступностью и сведения к минимуму ее влияния на социум необходимо взаимодействие и скоординированные действия государств, предпринимательского сектора и гражданского общества.

Одним из ключевых инструментов в борьбе с киберпреступностью является развитие и укрепление законодательства. Правительства по всему миру принимают более жесткие законы и нормативные акты, направленные на определение, классификацию и преследование киберпреступлений.

В условиях быстрого развития технологий необходимо укреплять взаимодействие между государствами, полицией и бизнесом. Обмен информацией между ними позволит эффективнее понимать и предотвращать новые формы киберпреступности.

Только тесное сотрудничество между правительствами, правоохранительными органами и частными компаниями позволит эффективно противостоять растущей киберпреступности. Совместное использование информации и знаний – ключ к своевременному обнаружению и предотвращению новых видов киберпреступлений, порожденных технологическим прогрессом.

Эффективное противодействие киберпреступности обеспечивается путем внедрения современных технологий защиты информации и использования сертифицированных систем безопасности. Регулярное обновление программно-аппаратного комплекса является необходимым условием для снижения уязвимостей и предотвращения несанкционированного доступа. Повышение уровня осведомленности пользователей в вопросах кибербезопасности, в том числе обучение распознаванию и предотвращению мошеннических действий, также является критически важным.

Защита от киберпреступности требует комплексного подхода, включающего в себя: использование современных антивирусных программ и межсетевых экранов, применение сертифицированных систем защиты информации, своевременную установку обновлений безопасности для программного и аппаратного обеспечения, а также регулярное обучение сотрудников распознаванию фишинговых писем, вредоносных ссылок и других видов кибермошенничества.

В настоящее время борьба с киберпреступностью требует активного участия сообщества специалистов в области кибербезопасности. Эксперты, известные как «белые хакеры», играют ключевую роль в раннем выявлении и реагировании на киберугрозы. Они осуществляют командные исследования через проникновение в информационные системы с целью тестирования их уязвимостей и разработки эффективных мер, направленных на предотвращение потенциальных атак.

Противодействие преступлениям в цифровом пространстве требует разработки комплексной стратегии, которая будет включать в себя законодательные, технологические и образовательные меры. Только объединяя ресурсы и действуя совместно, можно обеспечить защиту как отдельных пользователей, так и всего общества от киберугроз, а также гарантировать безопасность в онлайн-среде.

В условиях современного информационного общества, где технологии играют ключевую роль, киберпреступность становится одной из наиболее актуальных проблем. Злоумышленники постоянно совершенствуют свои методы взлома и обмана, что создает необходимость в разработке и внедрении передовых решений для обеспечения защиты [2].

Применение искусственного интеллекта (ИИ) значительно улучшает борьбу с киберпреступностью, позволяя выявлять и устранять угрозы в цифровом пространстве. ИИ не подвержен коррупции и обладает навыками анализа больших данных и обнаружения аномалий, что помогает выявлять потенциальные кибератаки. Интеллектуальные системы на базе ИИ способны быстро реагировать на угрозы и обеспечивать информационную безопасность.

В качестве одного из перспективных направлений в борьбе с киберугрозами предлагается использование квантовых вычислительных машин. Эти устройства, основанные на принципах квантовой физики, обладают значительно более высокой вычислительной мощностью и быстродействием по сравнению с традиционными компьютерами. Данное преимущество открывает новые возможности для разработки защитных алгоритмов и систем, способных эффективно противодействовать сложным криптографическим методам, используемым злоумышленниками в киберпространстве.

Искусственный интеллект может помочь в автоматизации процессов обнаружения и реагирования на кибератаки, анализируя большие объемы данных в реальном времени и выявляя аномалии, которые могут указывать на потенциальные угрозы. Алгоритмы машинного обучения способны адаптироваться к новым видам атак, обучаясь на предыдущем опыте [3].

Блокчейн-технология обеспечивает децентрализованное хранение данных, что значительно повышает их защищенность от манипуляций и несанкционированного доступа. Внедрение смарт-контрактов может способствовать увеличению уровня доверия в процессах транзакций и взаимодействия между сторонами.

Квантовые компьютеры представляют собой перспективное направление в области криптографии, предлагая инновационные методы шифрования, которые способны существенно укрепить безопасность данных. Однако с развитием квантовых технологий возникают и новые вызовы, такие как необходимость адаптации существующих систем защиты к изменяющимся условиям.

Таким образом, интеграция блокчейн- и квантовых технологий в единую систему кибербезопасности может значительно повысить эффективность защиты цифровых активов и минимизировать риски, связанные с киберпреступностью. Важно, чтобы компании и организации регулярно пересматривали свои стратегии и подходы, учитывая динамично изменяющийся ландшафт угроз [4].

Делая выводы, можно сказать, что:

1. Цифровизация необратима и приносит значительные benefits, но требует управления рисками.
2. Киберпреступность эволюционирует вместе с технологиями, становясь глобальной угрозой.
3. Будущее кибербезопасности связано с прорывными решениями, такими как квантовые технологии и децентрализованные системы.
4. Эффективная защита возможна только при сочетании:
 - инновационных технологий (ИИ, блокчейн);
 - сильного законодательства;
 - кооперации между государствами, бизнесом и гражданами.

Исследование подчеркивает двустороннюю природу цифровизации – ее потенциал для прогресса и необходимость создания устойчивой системы защиты от киберугроз.

Библиографический список

1. Никуленко А. В. О некоторых вопросах кибербезопасности в современном мире: взгляд дилетанта / А. В. Никуленко // Криминология: вчера, сегодня, завтра. 2019. № 4(55). С. 37-41.
2. Сахабутдинова А. С., Корчагин А. Г. Цифровая преступность: причины, виды, тенденции преступности, личность преступника, меры противодействия // Аграрное и земельное право.

2023. № 8 (224). URL: <https://cyberleninka.ru/article/n/tsifrovaya-prestupnost-prichiny-vidy-tendentsii-prestupnosti-lichnost-prestupnika-mery-protivodeystviya> (дата обращения: 18.05.2025).

3. *Евдокимов К. Н.* Самодетерминация технотронной преступности в Российской Федерации // *Российский судья*. 2020. № 7. С. 48- 53. DOI 10.18572/1812-3791-2020-7-48-53. EDN VLDNTX.

4. *Воронин Ю. А.* Преступления в сфере обращения цифровой информации и их детерминанты // *Виктимология*. 2020. № 1 (23). С. 74-83.