НАУЧНАЯ СТАТЬЯ
УДК 343.9

Средства совершения киберпреступлений

Вячеслав Александрович НАЗАРКИН ✉, Сергей Александрович ПОТАПОВ
ФГБОУ ВО «Тамбовский государственный университет им. Г.Р. Державина»
392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33
✉ nvaceslav385@gmail.com

Аннотация. Актуальность темы киберпреступности в современном мире сложно переоценить – мы наблюдаем фундаментальную трансформацию как самих средств совершения цифровых преступлений, так и их роли в структуре противоправной деятельности. Если традиционно под средствами киберпреступлений понималось преимущественно специализированное программное обеспечение, то сегодня мы имеем дело со сложными со сложными технологическими отдельными экосистемами, где границы между легальными и незаконными технологиями становятся все более размытыми. Современные киберпреступники активно используют достижения четвертой промышленной революции, создавая симбиоз передовых технологий и криминальной инфраструктуры. Особенностью текущего этапа является демократизация киберпреступности – благодаря развитию криминального аутсорсинга и сервисной модели. Даже технически неподготовленные злоумышленники могут осуществлять сложные атаки, что радикально увеличивает масштаб и частоту инцидентов.
Ключевые слова: киберпреступления, криминалистика, криптовалюта, ботнет, кибертерроризм, фишинг

Для цитирования: *Назаркин В.А, Потапов С.А.* Средства совершения киберпреступлений // Державинский форум. 2025. Т. 9. № 4. С. 437-444.

ORIGINAL ARTICLE
UDC 343.9

Means of committing cybercrimes

Vyacheslav A. NAZARKIN ✉, Sergey A. POTAPOV
Derzhavin Tambov State University
33 Internatsionalnaya St., Tambov, 392000, Russian Federation
✉ nvaceslav385@gmail.com

Abstract. The relevance of the topic of cybercrime in the modern world cannot be overestimated - we are witnessing a fundamental transformation of both the means of committing digital crimes and their role in the structure of illegal activities. If traditionally cybercrime tools were understood primarily as specialized software, today we are dealing with complex technological ecosystems, where the boundaries between legal and illegal technologies are becoming increasingly blurred. Modern cybercriminals actively use the achievements of the fourth industrial revolution, creating a symbiosis of advanced

technologies and criminal infrastructure. A special feature of the current stage is the democratization of cybercrime, thanks to the development of criminal outsourcing and a service model. Even technically untrained attackers can carry out complex attacks, which radically increases the scale and frequency of incidents.
Keywords: cybercrime, forensics, cryptocurrency, botnet, cyberterrorism, phishing

For citation: Nazarkin, V.A., & Potapov, S.A. (2025). Means of committing cybercrimes. *Derzhavinskii forum = Derzhavin Forum*, vol. 9, no. 4, pp. 437-444.

ВВЕДЕНИЕ

Современный этап развития общества характеризуется стремительной цифровизацией всех сфер жизнедеятельности, что поспособствовало появлению нового вида противоправных деяний – киберпреступлений. Основной особенностью совершения таких преступлений являются их средства, представляющие собой сложный симбиоз технических устройств, программного обеспечения и специальных знаний. Эти средства являются не только орудиями совершения преступлений, но и часто бывают самой средой, в которой такие преступления совершаются. К их числу относятся как широко распространенное легальное программное обеспечение, используемое злоумышленниками в преступных целях, так и специализированный криминальный инструмент: вредоносные программы, например, вирусы, трояны, программы-шифровальщики; средства обеспечения анонимности; ботнеты; фишинговые платформы и т. д. Эволюция данных средств происходит непрерывно, они становятся более доступными, технологичными и тяжелыми для обнаружения правоохранительными органами, что обуславливает высокую распространенность в криминальном мире, создавая высокую общественную опасность.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Ключевым современным трендом стало формирование полноценной преступной экономики с четким разделением труда, где средства совершения преступлений превратились в товар или услугу. Сервисы позволяют арендовать готовые платформы для атак, включая техническую поддержку и маркетинг. Например, другие платформы как предоставляют партнерские программы с обсуждением условий и разделом доходов, что напоминает легальный франчайзинг. Параллельно развивается рынок криминальных API, которые позволяют интегрировать различные функциональности в существующие системы. Отдельного внимания заслуживает развитие инфраструктуры для обналичивания средств – сервисы криптомикшинга. Они представляют собой одноразовые кошельки с автоматической конвертацией, и особенно децентрализованные протоколы, которые становятся идеальной средой для отмывания преступных доходов, благодаря своей анонимности и отсутствию регуляции. Электронные криптовалютные кошельки могут быть привязаны к блокчейну, чтобы гарантировать, что их баланс соответствует действительности, а новые транзакции проверяются с помощью данных в цепочке блоков для гарантии того, что каждая из них – настоящая и была произведена криптовалютой, которая реально принадлежит плательщику (или его кошельку). С одной стороны, такой подход обеспечивает безопасность производимых транзакций (взаимных расчетов). С другой стороны, идентифицировать отправителей и получателей указанных активов становится затрудни-

тельным для правоохранительных органов [1, с. 49]. Дополняя этот тезис, следует отметить, что растет число специалистов, которые заранее взламывают корпоративные сети и затем продают этот доступ другим преступным группам для последующих атак, чаще всего через вирус-вымогатель. Это создает новый уровень специализации: одна группа фокусируется на первоначальном взломе, вторая – на распространении вредоносного ПО, третья – на отмывании полученных денег.

Современные средства киберпреступлений демонстрируют беспрецедентную активность благодаря интеграции с искусственным интеллектом. В настоящее время мы наблюдаем переход от статического вредоносного ПО к самообучающимся системам, способным анализировать среду и адаптировать свое поведение. Некоторые вредоносные ПО на базе искусственного интеллекта могут определять наличие систем анализа угроз и приостанавливать вредоносную активность, имитируя легитимные процессы. Особую опасность представляют генеративные сети, используемые для создания фейковых видео – дипфейков (Deepfake) – как для мошенничества с идентичностью, так и для компрометации систем биометрической аутентификации. Пресс-служба MTS AI рассказала о том, каждый второй россиянин с дипфейк-атакой до конца 2025 г.[1]

В настоящее время проблема дипфейков является актуальной в условиях проведения Специальной Военной Операции [2, с. 32]. Распространение фейковой и дискредитирующей информации о деятельности российских Вооруженных Сил и государственных органов помимо подрыва их авторитета, нарушения прав граждан на объективную информацию направлено на формирование и радикализацию в стране протестных настроений, может привести к дестабилизации социально-политической обстановки и в условиях продолжающейся специальной военной операции представляет серьезную угрозу для национальной безопасности Российской Федерации [3, с. 27]. В связи с этим, были разработаны поправки в действующий Уголовный Кодекс РФ, а конкретнее, была введена «Статья 280.3. Публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, исполнения государственными органами Российской Федерации своих полномочий, оказания добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации или войска национальной гвардии Российской Федерации»[2].

На основе нововведенной статьи Уголовного Кодекса можно проанализировать количество обвинительных приговоров в период с 2022 по 2024 гг. (рис. 1).

Так называемый «Интернет вещей» создал принципиально новую сторону для атак, причем уязвимыми оказываются не только традиционные вычислительные устройства в лице ПК, но и критическая инфраструктура, медицинское оборудование, транспортные системы – Алексей Козлов, ведущий аналитик отдела мониторинга информационной безопасности (ИБ) компании «Спикател» ссылаясь на совместное с фирмой Service-

[1] Каждый второй россиянин столкнется с дипфейк-атакой до конца года // Известия. 05.05.2025. URL: https://iz.ru/1881222/2025-05-05/kazhdyi-vtoroi-rossiianin-stolknetsia-s-dipfeik-atakoi-do-kontca-goda (дата обращения: 26.09.2025).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 17.11.2025) (дата обращения: 26.09.2025).

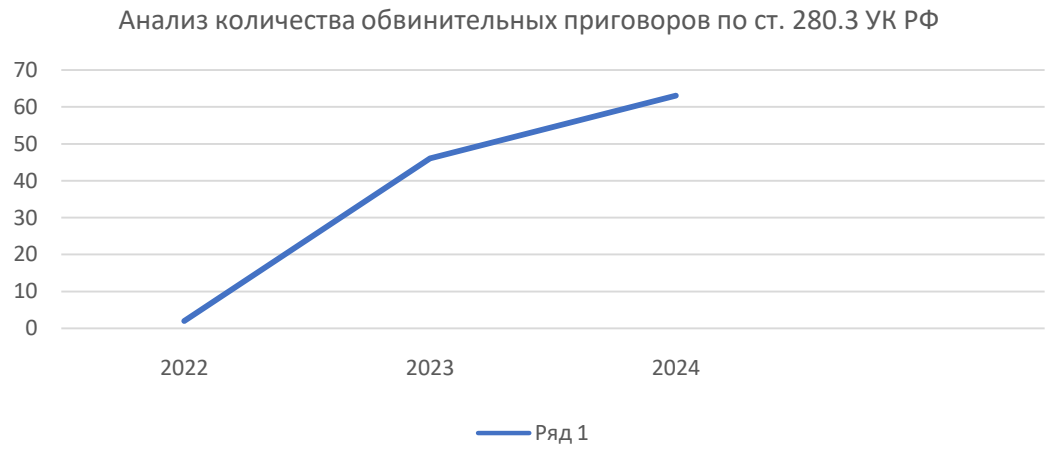

Рис. 1 Статистика, предложенная сайтом «Судебная статистика РФ»[3]
Fig. 1 Statistics provided by the "Russian Federation Judicial Statistics website"

pipe исследование сообщил «Количество разведывательных кибератак на российские компании за первые шесть месяцев 2025 г. выросло в три раза по сравнению с аналогичным периодом прошлого года: с 1,8 тыс. до 5,5 тыс. Большая их часть пришлась на компании из транспортной сферы. Такие атаки представляют собой сканирование IT-инфраструкту-ры на наличие уязвимостей для подготовки более масштабных взломов».[4] Ботнеты типа Mirai эволюционировали в сторону таргетированных атак на промышленные системы управления, где вредоносное ПО может манипулировать физическими процессами. Умные города с их централизованными системами управления становятся привлекательной мишенью для кибершантажа – достаточно вспомнить атаки на системы водоснабжения или энергосети. Киберпреступники все чаще проводят свои кибератаки на компании топливно-энерге-тического комплекса с целью шпионажа, отмечают специалисты по кибербезопасности BI.ZONE. «В целом число ИТ-атак на компании топливно-энергетического комплекса выросло за полгода на 40 %. Цель таких кампаний – завладеть финансовой информацией пользователей, а также шпионаж»[5]. Отдельную категорию составляют преступления в отношении киберфизических систем, где повреждение цифрового компонента приводит к физическим последствиям – от вывода из строя кардиостимуляторов до вмешательства в работу автономного транспорта. Важным аспектом является проблема долгого жизненного цикла устройств, связанных с Интернетом вещей. Отсутствие механизмов регулярного обновления приводит к созданию «цифровых свалок» из миллионов устройств, которые ни одно десятилетие

[3] Уголовное судопроизводство. Данные о назначенном наказании по статьям УК // Судебная статистика РФ. URL: https://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения: 27.09.2025).

[4] В России резко выросло число разведывательных хакерских атак на транспортный сектор // Газета.ru. 29.07.2025. URL: https://www.gazeta.ru/tech/news/2025/07/29/26374334.shtml (дата обращения: 27.09.2025).

[5] За полгода число кибератак российский топливно-энергетический комплекс выросло на 40 %. Большинство инцидентов связано со шпионажем // cnews. 03.07.2025. URL: https://www.cnews.ru/news/top/2025-07-03_za_polgoda_chislo_hakerskih (дата обращения: 27.09.2025).

могут быть частью ботнетов. Кроме того, растет угроза цепочкам поставок, когда уязвимость в одном компоненте, производимым сторонней компанией, ставит под угрозу безопасность тысяч итоговых продуктов.

Технологии дополненной и виртуальной реальности создают новые векторы для мошенничества – уже фиксируются случаи создания виртуальных фишинговых сред, имитирующих банковские приложения или корпоративные порталы. В этих системах формируется теневая экономика с использованием НФТ и виртуальных активов для отмывания средств. Блокчейн-технологии, кроме легального использования, породили смарт-контракты для автоматизации приступной деятельности – например, контракты, которые автоматически выплачивают вознаграждение за компрометацию определенных систем или осуществляют шантаж с временным замком. Стоит добавить растущую проблему криптографических преступлений, таких как «криптоджекинг» – тайное использование вычислительных мощностей жертв для майнинга криптовалют, которые незаметно устанавливаются на устройство и тяжелы для обнаружения [4, с. 52]. Также появляются новые формы мошенничества, например, «атаки на мгновенные займы», позволяющие злоумышленникам манипулировать курсами активов жертвы и похищать крупные суммы денег за одну транзакцию.

Особенностью современного эта развития является процесс сближения киберпреступности с другими формами организованной преступности. Криптовалютные сервисы обналичивания, кибертерроризм, кибернаемничество – все это создает полноценную экосистему. При этом, средства анонимизации, используемые преступниками при совершении киберпреступлений, становятся более совершенными: одноразовые идентификаторы, децентрализованные системы хранения данных, протоколы с нулевым разглашением – затрудняют расследование в области киберпреступлений. Зашифрованность прежде заключается в том, что VPN-сервис изменяет IP-адрес вашего технического средства на свой собственный. Таким образом все данные передаются к внешним ресурсам, которые вы, соответственно, запрашиваете с VPN-сервиса [5, с. 13]. Депутат Государственной думы Антон Немкин напомнил о том, что VPN-сервисы могут собирать и продавать данные о пользователях.[6]

Мобильные устройства превратились в ключевой инструмент преступности – от банковских троянов до приложений управления ботнетами. В основе схемы лежит банковский троян, способный списывать средства со счетов жертв через банкоматы без их ведома. Современные криминальные экосистемы активно вербуют сотрудников внутри компаний и государственных органов, в попытках использовать их привилегированный доступ для обхода систем защиты. Это сочетание технических и социальных методов делает атаки практически неуязвимыми для чисто технологических мер защиты.

В ответ на развитие технологий защиты, киберпреступники переходят к файллесс-атакам, которые использует легитимные инструменты операционной системы, например, PowerShell в Windows, что затрудняет их обнаружение, так как система защиты не видит опасности, воспринимая встроенную программу за свою. Сегодняшние атаки носят многоэтапный характер. Проникнув в сеть, злоумышленники могут оставаться там

[6] В Госдуме указали на опасность использования VPN-сервисов // Известия. 28.06.2025. URL: https://iz.ru/1912086/2025-06-28/v-gosdume-ukazali-na-opasnost-ispolzovania-vpn-servisov (дата обращения: 28.09.2025).

месяцами, постепенно перемещаясь по всей системе, повышая привилегии и изучая строение устройства изнутри, чтобы нанести значительный ущерб в самый неожиданный момент. Это требует от «защитников» перехода от обнаружения единичных инцидентов к непрерывному мониторингу поведения и выявлению аномальных активностей в сети или устройстве. Защита от такого вида киберпреступности проявляется с помощью выпускаемых обновлений, которые не стоит игнорировать.

Аналитики из компании ReliaQuest го также предупреждает о частом применении нового способа совершения киберпреступлений – Квишинг[7]. Он представляет собой разновидность фишинга, основанная на использовании QR-кодов. Сканируя QR-код, жертва может попасть на фальшивый сайт, который может предложить установить новое приложение для отслеживания следующей посылки, которое крадет данные карт, пароли, получить доступ к личным или корпоративным аккаунтам.

ВЫВОДЫ

Таким образом, современные средства совершения киберпреступлений представляют собой не просто набор технических инструментов, а сложные адаптивные системы, интегрирующие достижения последних технологических открытий. Их развитие характеризуется интеграцией с искусственным интеллектом и сближением с легальными технологиями и ПО. Борьба с этим требует не только быстрого реагирования в лице технических контрмер, но и развития правового регулирования, международного сотрудничества, а также сбора и анализа статистических данных для предотвращения киберугроз. Анализ природы и функциональности этих средств однозначно демонстрирует, что они являются не просто пассивными орудями, а активными компонентами, которые формируют основу современной киберпреступности. Борьба с этим явлением не может быть без глубоко и непрерывного изучения криминального мира. Следовательно, противодействие киберпреступности требует опережающего развития цифровой криминалистики, совершенствования законодательной базы и формирования комплексного подхода, который сочетал бы в себе технические, правовые и организационные меры, а также международное сотрудничество.

К правовым вызовам можно отнести следующие пункты:

1. Пробелы в юрисдикции. Транснациональный характер киберпреступности делает сложным определение того, право какой страны должно применяться, если преступление вышло за границы одного государства.

2. Разработка нового законодательства. Законодательные процессы не всегда успевают за скоростью развития технологических изменений. Также необходима разработка международных стандартов, связанных с криптосферой.

3. Расширение полномочий правоохранительных органов. Действия органов должны быть законодательно проработаны так, чтобы не возникал конфликт в связи с нарушением неприкосновенности частной жизни граждан.

[7] Мобильный, гад же ты: эксперты предупредили о резком росте квишинга // Известия. 25.11.2023. URL: https://iz.ru/1609447/dmitrii-alekseev/mobilnyi-gad-zhe-ty-eksperty-predupredili-o-rezkom-roste-kvishinga (дата обращения: 29.09.2025).

Список источников

1. *Любавский А.Ю.* Повышение эффективности поиска криптокошельков на машинных носителях информации // Проблемы противодействия киберпреступности: материалы II Междунар. науч.-практ. конф. Москва: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. С. 49-54. https://elibrary.ru/qkwvuy
2. *Киселев М.Б.* Противодействие распространению фейков о деятельности российских Вооруженных Сил, добровольческих формирований, государственных органов и их дискредитации в условиях специальной военной операции // Проблемы противодействия киберпреступности: материалы II Междунар. науч.-практ. конф. Москва: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. С. 31-37.
3. *Бугера Н.Н., Лихолетов А.А., Лихолетов Е.А.* Публичное распространение заведомо ложной информации о деятельности Вооруженных Сил Российской Федерации: некоторые вопросы толкования уголовного закона // Вестник Волгоградской академии МВД России. 2022. № 2 (61). С. 25-30. https://doi.org/10.25724/VAMVD.AAAA, https://elibrary.ru/ljpqnn
4. *Марданов Г.Д., Мамедов С.И.* Киберпреступления и методы профилактики // Ученые записки Казанского юридического института МВД России. 2023. № 2 (16). С. 47-55. https://elibrary.ru/uwpeli
5. *Антропов А.Н.* Способы анонимизации трафика в сети интернет, механизмы противодействия анонимизации и их перспективы // Проблемы противодействия киберпреступности: материалы II Междунар. науч.-практ. конф. Москва: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. С. 11-17. https://elibrary.ru/flihjx

References

1. Lyubavskii A.Yu. (2024). Improving the efficiency of searching for cryptos on machine media. *Materialy II Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Problemy protivodeistviya kiberprestupnosti» = Proceedings of the 2th International Scientific and Practical Conference "Problems of Countering Cybercrime"*. Moscow, Sukharev Moscow Academy of the Investigative Committee of the Russian Federation Publ., pp. 49-54. (In Russ.) https://elibrary.ru/qkwvuy
2. Kiselev M.B. (2024). Countering the spread of fakes about the activities of the Russian armed forces, volunteer formations, and government agencies and their discrediting in the context of a special military operation. *Materialy II Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Problemy protivodeistviya kiberprestupnosti» = Proceedings of the 2th International Scientific and Practical Conference "Problems of Countering Cybercrime"*. Moscow, Sukharev Moscow Academy of the Investigative Committee of the Russian Federation Publ., pp. 31-37. (In Russ.) https://elibrary.ru/nzkzdw
3. Bugera N.N., Likholetov A.A., Likholetov E.A. (2022). The public spreading of misleading information about the activity of the armed forces of the Russian Federation: some issues of interpretation of the criminal law. *Vestnik Volgogradskoi akademii MVD Rossii = Journal of the Volgograd Academy of the Ministry of the Interior of Russia*, no. 2 (61), pp. 25-30. (In Russ.) https://doi.org/10.25724/VAMVD.AAAA, https://elibrary.ru/ljpqnn
4. Mardanov G.D., Mamedov S.I. (2023). Cybercrimes and their prevention. *Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii = Scientific Notes of Kazan Law Institute of MIA of Russia*, no. 2 (16), pp. 47-55. (In Russ.) https://elibrary.ru/uwpeli
5. Antropov A.N. (2024). Methods of anonymization of traffic on the internet, mechanisms for countering anonymization and their prospects. *Materialy II Mezhdunarodnoi nauchno-prakticheskoi konferentsii «Problemy protivodeistviya kiberprestupnosti» = Proceedings of the 2th International Scientific and Practical Conference "Problems of Countering Cybercrime"*. Moscow, Sukharev

Moscow Academy of the Investigative Committee of the Russian Federation Publ., pp. 11-17. (In Russ.) https://elibrary.ru/flihjx

Информация об авторах

Назаркин Вячеслав Александрович, студент института права и национальной безопасности, Тамбовский государственный университет им Г. Р. Державина, г Тамбов, Российская Федерация, nvaceslav385@gmail.com

Потапов Сергей Александрович, кандидат юридических наук, доцент, доцент кафедры уголовно-правовых дисциплин, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, potapov.1995@yandex.ru

Information about authors

Vyacheslav A. Nazarkin, Student of Law and National Security Institute, Derzhavin Tambov State University, Tambov, Russian Federation, nvaceslav385@gmail.com

Sergey A. Potapov, Cand. Sci. (Law), Associate Professor, Associate Professor of the Criminal Law Disciplines Department, Derzhavin Tambov State University, Tambov, Russian Federation, potapov.1995@yandex.ru

Статья поступила в редакцию / The article was submitted 15.10.2025
Одобрена после рецензирования / Approved after reviewing 26.11.2025
Принята к публикации / Accepted for publication 28.11.2025