

**Ссылка для цитирования этой статьи:**

Гаджиева З.Х., Сулейманова А.М. Классификация видов кибермошенничества в банковской сфере // Human Progress. 2025. Том 11, Вып. 8. С. 6. URL: [http://progress-human.com/images/2025/Tom11\\_8/Gadzhieva.pdf](http://progress-human.com/images/2025/Tom11_8/Gadzhieva.pdf) DOI 10.46320/2073-4506-2025-8a-13.

## **КЛАССИФИКАЦИЯ ВИДОВ КИБЕРМОШЕННИЧЕСТВА В БАНКОВСКОЙ СФЕРЕ**

**Гаджиева Зубайдат Хабибовна**

преподаватель кафедры экономических  
и общеобразовательных дисциплин,  
Дагестанский государственный университет,  
г. Избербаш, Российская Федерация

**Сулейманова Аминат Мусаевна**

кандидат экономических наук,  
доцент кафедры экономических и  
общеобразовательных дисциплин  
Дагестанский государственный университет,  
г. Избербаш, Российская Федерация

**Аннотация.** Одной из сфер, в которых киберпреступность достигает огромных масштабов, является банковская деятельность, так как в ней широко задействовано использование современных возможностей информационных технологий.

В статье рассматриваются теоретические вопросы формирования кибермошенничества в банковской сфере: сущность, классификация и основные виды киберпреступлений. Анализируются инциденты нарушения информационной безопасности при осуществлении банковских операций.

Кибермошенничество в банковской сфере – сложное и многоаспектное понятие, которое представляет собой использование различных технологий и методов для совершения незаконных действий с целью получения доступа к финансовым средствам, данным или другим активам клиентов и банков. Основной целью статьи является классификация видов кибермошенничества и выявление его ключевых признаков, а также для разработки эффективных мер защиты и противодействия данным угрозам.

**Ключевые слова:** банк, кибермошенничество, кибербезопасность, кибератака, цифровизация, онлайн-банкинг, банковская система, информационные системы.

Современное общество всё больше уходит в цифровое пространство. В связи с ускоренной цифровизацией экономических, финансовых и социальных процессов

наблюдается существенный рост количества преступлений, совершаемых с использованием электронных технологий. Одним из наиболее динамично развивающихся типов преступлений становится кибермошенничество – разновидность мошеннических действий, совершаемых в киберпространстве, часто с использованием Интернета, мобильных коммуникаций, поддельных сайтов и других инструментов цифровой среды.

Кибермошенничество представляет собой форму мошенничества, при которой обман и злоупотребление доверием совершаются посредством электронных коммуникационных технологий с целью хищения денежных средств, персональных данных, виртуальной валюты и других видов цифровых активов. С формально-правовой точки зрения, в Уголовном кодексе Российской Федерации понятию «кибермошенничество» прямого определения не дается, однако применяются нормы ст. 159 УК РФ (мошенничество), в том числе её модификации – например, ст. 159.6 (мошенничество в сфере компьютерной информации) [1].

Также применяется ст. 272–273 УК РФ (неправомерный доступ к компьютерной информации и создание вредоносных программ). Таким образом, «кибермошенничество» – это собирательный термин, охватывающий широкий спектр преступных действий, в которых применяются компьютерные и сетевые технологии в качестве инструмента реализации мошеннического замысла.

Сущность кибермошенничества можно понять через выявление его ключевых признаков:

Высокая степень анонимности. Мошенники, действующие в цифровой среде, могут скрыть своё местоположение, использовать VPN, подмену IP-адреса и различные формы виртуальных личностей, что затрудняет их идентификацию [3].

Использование компьютерных и телекоммуникационных технологий. Как правило, подобные преступления совершаются через электронные каналы: сайты, мобильные приложения, электронную почту, соцсети, мессенджеры, системы дистанционного банковского обслуживания (ДБО).

Массовость воздействия. В отличие от традиционного мошенничества, в киберпространстве злоумышленники могут одновременно охватить тысячи и даже миллионы потенциальных жертв – например, через массовую фишинговую рассылку или скомпрометированное приложение.

Автоматизация преступного процесса. Некоторые формы кибермошенничества (бот-сети, ключевые логгеры, трояны) позволяют автоматизировать взломы, рассылки и сбор информации, что делает киберпреступность оперативной и масштабной.

Многосценарность и гибкость. Кибермошенники постоянно адаптируют свои подходы и схемы: от обмана в соцсетях до сложных атак на банковские приложения с использованием программ-вымогателей, подделок сертификатов и методов социальной инженерии [2].

Кибермошенничество в банковской сфере представляет собой использование различных технологий и методов для совершения незаконных действий с целью получения доступа к финансовым средствам, данным или другим активам клиентов и банков [4].

По данным ЦБ, в 2024 году объём хищений у клиентов банков составил 27,5 млрд рублей. Это рекордный показатель за всё время ведения статистики. Основной объём средств (26,9 млрд рублей) был украден со счетов физических лиц, у юридических лиц – 667 млн рублей.

Основными каналами хищения средств были: дистанционное банковское обслуживание (ДБО, 9,6 млрд рублей), карты (8,5 млрд рублей), система быстрых платежей (СБП, 8,25 млрд рублей) [7].

Классификация видов кибермошенничества необходима для разработки эффективных мер защиты и противодействия данным угрозам.

По объекту воздействия атаки на банковскую инфраструктуру направлены на компьютерные системы, серверы и сетевое оборудование финансовых учреждений. В 2024 г. через Автоматизированную систему обработки инцидентов ФинЦЕРТ (АСОИ ФинЦЕРТ) от участников информационного обмена было получено более 750 сообщений о фактах компьютерных атак (КА) и компьютерных инцидентов. Основными КА, сведения о которых получил ФинЦЕРТ от финансовых организаций, стали DDoS-атаки, атаки с использованием вредоносного программного обеспечения (ВПО), компрометация учетных данных. [8] К ним относятся:

- DDoS-атаки на серверы банков («отказ в обслуживании»);
- Взлом корпоративной сети;
- Атаки на АБС (автоматизированные банковские системы);
- Внедрение вредоносного ПО в банковские системы;
- Атаки на системы межбанковских переводов (SWIFT, СПФС).
- Атаки на клиентов банков как тип мошенничества, по статистике ФинЦЕРТ, является наиболее распространенным – около 69% всех инцидентов в банковской сфере [8].

Злоумышленники обращаются напрямую к клиентам банка, минуя системы защиты финансовых организаций:

- Фишинг и его разновидности (смишинг, вишинг);

- Социальная инженерия;
- Кража персональных данных;
- Мошенничество с мобильными приложениями;
- Скимминг (использование специальных устройств для кражи данных карт).

Атаки на сотрудников банков. Банковские служащие также становятся объектами целенаправленных атак из-за их привилегированного доступа к информации и системам. По оценкам экспертов, около 40% утечек в банковском секторе происходит с участием персонала [5]:

- Целевой фишинг (spear phishing);
- Вредоносные вложения в электронных письмах;
- Внедрение инсайдеров;
- Социальная инженерия в отношении персонала.

По методам совершения можно провести такую классификацию:

• Технологические методы. Данные методы основаны на использовании технических средств и программного обеспечения:

- Вредоносное ПО (банковские трояны, программы-вымогатели);
- Эксплуатация уязвимостей в банковских системах;
- Подмена DNS и фарминг;
- Применение специализированных утилит для взлома;
- Man-in-the-Middle атаки.

Социально-инженерные методы. Мошенничество, основанное на манипуляции человеческим поведением. Согласно исследованиям Лаборатории Касперского, 63% инцидентов в банковской сфере используют именно эти методы [6]:

- Выманивание данных от сотрудников служб поддержки;
- Звонки от имени "службы безопасности банка";
- Манипуляции на основе страха потери денег;
- Создание срочности действий ("ваш счет будет заблокирован через час");
- Фишинговые письма, имитирующие официальную корреспонденцию.

Комбинированные методы. Наиболее сложные и опасные схемы, сочетающие технологические и социально-инженерные подходы:

- SIM-свопинг (перевыпуск SIM-карты жертвы для перехвата SMS-подтверждений);
- Атаки через компрометацию электронной почты (BEC);
- Многоэтапные схемы с предварительным сбором данных;

- Целевые кампании по компрометации конкретных клиентов.

Классификация по каналам распространения угроз включает:

Интернет-каналы. Наиболее распространенный путь реализации мошеннических схем.

Через интернет-каналы осуществляется около 54% всех атак на банковский сектор [9]:

- Фишинговые сайты;
- Вредоносные ссылки в электронных письмах;
- Взломанные интернет-ресурсы;
- Мошеннические онлайн-объявления;
- Компрометация систем дистанционного банковского обслуживания.

Мобильные каналы. С ростом мобильного банкинга увеличивается и количество атак через мобильные устройства – около 35% всех инцидентов в 2024 году [10]:

- SMS с вредоносными ссылками;
- Поддельные банковские приложения;
- Перехват SMS-сообщений с кодами аутентификации;
- Мошеннические QR-коды;
- Эксплуатация уязвимостей мобильных операционных систем.

Физические каналы. Хотя доля физических каналов снижается, они по-прежнему используются в комбинированных атаках:

- Скимминг банкоматов и POS-терминалов;
- Установка шиммеров (тонких накладок на чип-ридеры карт);
- Физический доступ к инфраструктуре;
- Перехват карт, направляемых по почте.

Классификация по уровню сложности реализации:

Массовые (низкой сложности). Атаки, не требующие высокой квалификации и направленные на широкий круг потенциальных жертв:

- Массовый фишинг;
- Простые схемы социальной инженерии;
- Распространение вредоносного ПО через спам.

Целевые (средней сложности). Атаки, требующие более тщательной подготовки и ориентированные на определенную группу жертв:

- Целевые вишинг-кампании;
- Компрометация мобильных банковских приложений;
- Продвинутые методы социальной инженерии с предварительным сбором данных.

APT-атаки (высокой сложности). Сложные, многоэтапные операции с использованием передовых технологий. Обычно проводятся организованными группами. По данным FireEye, в 2024 году было зафиксировано увеличение на 23% количества APT-атак на финансовый сектор [11]:

- Длительное скрытное присутствие в сети;
- Использование уязвимостей нулевого дня;
- Эксплуатация сложных техник обхода защиты;
- Целенаправленные атаки на конкретные банковские системы.

Классификация видов кибермошенничества в банковской сфере демонстрирует многообразие и постоянную эволюцию угроз. Понимание типологии является ключевым элементом для построения эффективной системы защиты. При этом важно отметить, что с развитием технологий появляются новые методы и каналы реализации кибератак, что требует постоянного обновления классификации и модернизации систем безопасности.

### Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/](https://www.consultant.ru/document/cons_doc_LAW_10699/)
2. Алёхин А.А. Теоретические аспекты кибермошенничества: понятие, правовая природа и виды // Государственная служба и кадры. 2024. № 2. URL: <https://cyberleninka.ru/article/n/teoreticheskie-aspekty-kibermoshennichestva-ponyatie-pravovaya-priroda-i-vidy> (дата обращения: 11.08.2025).
3. Герасимова О.С. Особенности преступлений в сфере компьютерной информации // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2007. № 12-2.
4. Долотова Н.П. Киберпреступность в банковской сфере в РФ // Гуманитарные, социально-экономические и общественные науки. 2024. № 12.
5. Исследование InfoWatch "Утечки данных в финансовой сфере". М., 2024. URL: <https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-finansovykh-organizatsiyakh-mira-i-rossii-za-god>.
6. Лаборатория Касперского. "Финансовые угрозы в 2024 году". URL: <https://www.kaspersky.ru/about/press-releases/eksperty-nazvali-aktualnye-finansovye-kiberugrozy>.
7. Мошенники эксплуатируют банковскую инфраструктуру. URL: <https://www.kommersant.ru/doc/7515659>.

8. Обзор основных типов компьютерных атак в финансовой сфере в 2024 году. URL: [https://cbr.ru/Collection/Collection/File/55129/Attack\\_2024.pdf](https://cbr.ru/Collection/Collection/File/55129/Attack_2024.pdf).

9. Positive Technologies. "Актуальные киберугрозы 2024 Q4. Банковский сектор". URL: [https://safe.cnews.ru/news/line/2024\\_positive\\_technologies\\_o\\_glavnyh\\_kiberugrozah](https://safe.cnews.ru/news/line/2024_positive_technologies_o_glavnyh_kiberugrozah).

10. ESET. "Ландшафт угроз в сфере мобильного банкинга". URL: <https://www.itsec.ru/news/eset>.

11. FireEye. "M-Trends: The Trends Behind Today's Advanced Attacks", 2022.

## CLASSIFICATION OF TYPES OF CYBERBULLYING IN THE BANKING SECTOR

**Gadzhieva Zubaidat Khabibovna**

Lecturer of the Department of Economic and General Education Disciplines,  
Dagestan State University,  
Izberbash, Russian Federation

**Suleymanova Aminat Musaevna**

PhD in Economics,  
Associate Professor of the Department of Economic and General Education Disciplines,  
Dagestan State University,  
Izberbash, Russian Federation

**Abstract.** One of the areas where cybercrime is on a huge scale is banking, as it involves the use of modern information technology capabilities.

The article discusses the theoretical issues of cyber fraud in the banking sector: the essence, classification, and main types of cybercrimes. It also analyzes incidents of information security violations during banking operations.

Cyber fraud in the banking sector is a complex and multifaceted concept that involves the use of various technologies and methods to commit illegal acts in order to gain access to financial resources, data, or other assets of customers and banks. The main goal of this article is to classify the types of cyber fraud and identify its key characteristics, as well as to develop effective measures for protecting against these threats.

**Keywords:** bank, cyber fraud, cybersecurity, cyber attack, digitalization, online banking, banking system, information.

### References

1. Federal Code of the Russian Federation № 63-FZ dated 13.06.1996. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_10699/](https://www.consultant.ru/document/cons_doc_LAW_10699/)
2. Alan A.A. Theoretical studies of cyberspace: understanding, the main reason and types // Civil service and personnel. 2024. № 2. URL: <https://cyberleninka.ru/article/n/teoreticheskie-aspekty-kibermoshennichestva-ponyatie-pravovaya-priroda-i-vidy> (date of access: 08/11/2025).
3. Gerasimova O.S. Features of crimes in the field of computer information // Bulletin of Tambov University. Series: Humanities. 2007. № 12-2.
4. Dolotova N.P. Cybercrime in the banking sector in the Russian Federation // Humanities, socio-economic and social sciences. 2024. № 12.
5. InfoWatch research "Genre data leaks", Moscow, 2024. URL: <https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-finansovykh-organizatsiyakh-mira-i-rossii-za-god>.

6. Kaspersky Lab. "Financial levels in 2024". URL: <https://www.kaspersky.ru/about/press-releases/eksperty-nazvali-aktualnye-finansovye-kiberugrozy>.
7. Monikexploits banking tools: URL: <https://www.kommersant.ru/doc/7515659>.
8. Overview of the main types of computer games in the genre environment in 2024. URL: [https://cbr.ru/Collection/Collection/File/55129/Attack\\_2024.pdf](https://cbr.ru/Collection/Collection/File/55129/Attack_2024.pdf).
9. Positive technologies. "Relevant cyber threats 2024, fourth quarter. The banking sector". URL: [https://safe.cnews.ru/news/line/2024\\_positive\\_technologies\\_o\\_glavnyh\\_kiberugrozah](https://safe.cnews.ru/news/line/2024_positive_technologies_o_glavnyh_kiberugrozah).
10. ESET. "Landhat ugolek in the sulfur of a mobile bank". URL: <https://www.itsec.ru/news/eset>
11. FireEye. "M-trends: the trends behind modern advanced attacks", 2022.