

Криминологическое противодействие киберпреступлениям

Проблемы предупреждения преступлений, совершаемых посредством информационных технологий работниками банков

Аннотация. Статья посвящена анализу проблем предупреждения преступлений, совершаемых посредством информационных технологий работниками банков. Актуальность исследования определяется тем, что в последние годы фиксируется рост рассматриваемых преступлений, а также рост ущерба в результате их совершения, который причиняется не только банку, но и его клиентам. Банки несут также и репутационные риски. Сделан вывод о том, что первостепенное значение имеют применение превентивных мер непосредственно в банках, а также поиск новых форм предупреждения рассматриваемых преступлений. В качестве таких мер выделены: оптимизация деятельности подразделений службы безопасности банков; создание новых компьютерных программ, позволяющих всесторонне контролировать деятельность работников банков, совершенствование форм взаимодействия банков с правоохранительными органами. Результаты работы могут быть использованы в дальнейших научных исследованиях рассматриваемой проблемы, а также для разработки практических рекомендаций, применяемых в деятельности по предупреждению преступлений, совершаемых посредством информационных технологий работниками банков.

Ключевые слова: преступление, информационные технологии, преступное поведение, предупреждение преступлений, работники банков, правоохранительные органы



**Елена Николаевна
КЛЕЩИНА,**
профессор кафедры
криминологии
и уголовно-
исполнительного права
имени В. Е. Эминова
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
профессор
enkleschina@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

DOI: 10.17803/2311-5998.2025.129.5.181-188

Elena N. KLESCHINA,

*Professor of the Chair of Criminology and Executive Law Chair named after
E. V. Eminov of the Kutafin Moscow State Law University (MSAL),*

Dr. Sci. (Law), Associate Professor

enkleschina@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Problems of Preventing Crimes Committed by Bank Employees Using Information Technology

Abstract. *The article is devoted to the analysis of the problems of preventing crimes committed through information technology by bank employees. The relevance of the study is determined by the fact that in recent years there has been an increase in the crimes under consideration, as well as the damage caused not only to the bank, but also to its customers. Banks also carry reputational risks. It is concluded that the application of preventive measures directly in banks, as well as the search for new forms of prevention of the crimes under consideration, is of paramount importance. Such measures include: optimization of the activities of the bank's security service units; creation of new computer programs that allow comprehensive monitoring of the activities of bank employees, and improvement of banks' interaction with law enforcement agencies. The results of the work can be used in further scientific research of the problem under consideration, as well as for the development of practical recommendations used in the prevention of crimes committed through information technology by bank employees.*

Keywords: *crime, information technology, criminal behavior, crime prevention, bank employees, law enforcement agencies*

Число преступлений, совершаемых посредством информационных технологий, в последние годы возрастает, растет и ущерб в результате их совершения.

Так, по данным ГИАЦ МВД России, в 2024 г. всего зарегистрировано 1 911,3 тыс. преступлений. Из них количество преступлений с использованием информационно-коммуникационных технологий составляет 765,4 тыс., что на 13,1 % больше, чем за аналогичный период 2023 г. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8 % в январе — декабре 2023 г. до 40,0 %. Четыре преступления из пяти (84,8 %) совершаются с использованием сети Интернет (649,1 тыс.; +23,2 %), почти половина (45,2 %) — с использованием средств мобильной связи (346,0 тыс.; +14,3 %)¹.

На тенденцию роста преступлений, совершенных с использованием информационно-телекоммуникационных технологий, обращает внимание Президент Российской Федерации В. В. Путин, подчеркивая необходимость совершенствования

¹ Состояние преступности в России за 2024 год / ГИАЦ МВД России // URL: https://docs.yandex.ru/docs/view?tm=1751012961&tld=ru&lang=ru&name=Sbornik_UOS_2024.pdf&text.

методов борьбы с преступностью в этой сфере, взаимодействия МВД России с профильными ведомствами².

Распространенными являются преступления, совершаемые посредством информационных технологий работниками банков, в том числе такие, как мошенничество в сфере компьютерной информации, неправомерный доступ к компьютерной информации, незаконное использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения.

Председатель правления ПАО «Сбербанк» Г. Греф еще в 2019 г. подчеркивал, что «самая большая проблема в киберрисках — это не внешние риски, а внутренние», однако бывают также ситуации, «когда мошенники снаружи и внутри договариваются»³.

С. Кузнецов, являющийся заместителем председателя правления ПАО «Сбербанк», указал на то, что «банку удастся защитить своих клиентов от атак мошенников в 97 % случаев. Но, сосредоточившись на внешней угрозе, Сбербанк не заметил ее изнутри»⁴.

С учетом отмеченного, важнейшее значение имеет оптимизация мер предупреждения преступлений, совершаемых посредством информационных технологий работниками банков, поскольку ущерб от таких преступлений причиняется не только банку, но и его клиентам. Банки несут также и репутационные риски.

Приведем примеры судебной практики, в которых очевиден процесс совершения преступлений работниками банка.

Так, приговором Батайского городского суда Ростовской области от 20.06.2024 № 1-111/2024 установлено, что у С., которая являлась старшим менеджером группы продаж частным клиентам отделения регионального управления ПАО «Мин-Банк», возник умысел на хищение денежных средств клиентов банка с использованием своего служебного положения. С. после устройства на работу в банк был выдан логин. Используя логин, путем введения известного лишь ей пароля, она имела право доступа к электронной системе. Реализуя свой преступный умысел, С. совершала вмешательство в функционирование средств хранения и обработки компьютерной информации, похищая денежные средства клиентов банка. По результатам рассмотрения уголовного дела действия С. были квалифицированы судом по ч. 4 ст. 159⁶ и по ч. 3 ст. 272 УК РФ.

Приговором Дзержинского районного суда г. Волгограда от 13.03.2023 № 1-33/2023 установлено, что подсудимый К. в 2019 г. был принят на работу в ООО «ХКФ Банк» на должность менеджера. В январе 2021 г. у К., который в этом банке уже являлся ведущим менеджером, возник преступный умысел,

² Президент Российской Федерации В. В. Путин выступил на Ежегодном расширенном заседании коллегии МВД России. 05.03.2025 // URL: <http://kremlin.ru/events/president/news/76408> (дата обращения: 06.03.2025).

³ Греф сообщил о случаях мошенничества с участием сотрудников Сбербанка // URL: <https://amp.rbc.ru/rbcnews/finances/19/05/2019/5ce14eed9a79473f540ecc5e>

⁴ Кузнецов С. О мошенничестве методом социальной инженерии, защите данных и проблемах кибербезопасности // Ведомости. 17.02.2020.



направленный на хищение чужого имущества, принадлежащего банку и его клиентам, путем ввода и модификации компьютерной информации. Зная о порядке удаленного оформления кредитных договоров в банке, имея доступ к базе данных клиентов, К. получил сведения о клиенте Ф., включая абонентский номер оператора сотовой связи ПАО «ВымпелКом», используемый для получения кодов посредством смс-сообщений, необходимых для удаленного подписания простой электронной подписью документов с банком и получения денежных средств в виде потребительского кредита. После этого он узнал от менеджера по прямым продажам ООО «Атон-Р», осуществляющего продажу сим-карт оператора сотовой связи ПАО «ВымпелКом», что данный абонентский номер находится в продаже. После этого К., зная, что абонентский номер Ф. не используется, приобрел в г. Волгограде у И., не осведомленного о его преступных намерениях, сим-карту оператора сотовой связи ПАО «ВымпелКом» с данным абонентским номером.

Затем К., действуя как ведущий менеджер банка, путем удаленного доступа, с использованием сети Интернет, посредством служебной программы банка сформировал от имени Ф. заявление о предоставлении потребительского кредита по карте и открытии текущего счета, без обращения Ф. в банк, т.е. произвел без согласия клиента банка ввод и модификацию компьютерной информации. Имея доступ к счету кредитной карты «Карта Кредитная Польза», он совершил хищение денежных средств с банковского счета в размере 94 919 руб. Аналогичными преступными действиями он оформил еще ряд потребительских кредитов на общую сумму 995 040 руб.

Преступные действия К. были раскрыты работниками отдела защиты бизнеса данного банка. Из показаний представителя этого отдела следует, что в банке действует система, в которой фиксируются все договоры, которые заключают сотрудники. Если по ним возможны какие-либо риски, то проводится проверка. Поступило большое количество дефолтных договоров, всего их было 41, по которым не осуществлялось погашение, заключенных именно К. в период с января по май. В ходе проверки было обнаружено, что договоры заключались онлайн, с телефонных номеров, принадлежащих клиентам банка, но телефонных разговоров с клиентами не было. При дальнейшей проверке было установлено, что часть денежных средств от этих кредитных договоров была переведена на счета К.

Из приведенных примеров судебной практики очевиден и процесс виктимизации банка и клиентов банка. Поэтому важнейшее значение имеет совершенствование мер предупреждения преступности в этой сфере.

В криминологии предупреждение преступности рассматривается как многоуровневая система государственных и общественных мер, направленных на выявление, устранение, ослабление или нейтрализацию причин и условий преступности, ее отдельных видов и конкретных деяний⁵, реализуемых разными субъектами⁶.

⁵ См., например: Криминология : учебник / под ред. Н. Ф. Кузнецовой, В. В. Лунеева. 2-е изд., перераб. и доп. М., 2004. С. 185 ; *Мацкевич И. М.* Причины экономической преступности : учебное пособие. М., 2019. С. 249.

⁶ Криминология : учебник / под ред. А. И. Долговой. 4-е изд., перераб. и доп. М., 2010. С. 484.

Сложный характер развития причинных связей требует разностороннего комплексного подхода к организации работы по предупреждению преступности⁷.

Как отмечал В. Н. Кудрявцев, в зависимости от типа причинно-следственных связей и характера условий преступности такая работа должна строиться по различным направлениям, в том числе путем устранения организационных и других дефектов, способствующих достижению противоправного результата⁸. Поэтому в деятельности по предупреждению рассматриваемых преступлений необходим комплексный и системный подход. В статье остановимся на отдельных аспектах.

Первостепенное значение, по нашему мнению, имеет применение действенных превентивных мер непосредственно в банках. Эти меры должны включать как контроль за деятельностью работников, осуществляющих оформление договоров с клиентами банков, другие финансовые операции, так и изучение личности работников банка, проведение мониторинга их личностного поведения в рамках трудовой деятельности.

Важным является проведение проверок претендента на замещение соответствующей должности при устройстве его на работу в банк, а также проведение периодических проверок работников банка в процессе их деятельности.

Во втором приведенном нами примере судебной практики очевидно, что подсудимый К., реализуя свой преступный умысел на хищение чужого имущества, оформил 41 договор о потребительском кредите на клиентов банка путем ввода и модификации компьютерной информации. По этим договорам, как установили работники отдела защиты бизнеса данного банка, не осуществлялось погашение кредитов, заключенных К. в период с января по май, что является достаточно длительным периодом. В этой связи очевидна необходимость сокращения сроков проверки заключаемых с клиентами договоров, проведения других финансовых операций, выполнения клиентами обязательств по договорам и т.д., что позволит в том числе выявить нарушения в деятельности работников банка.

Для предупреждения совершения работниками банков рассматриваемых преступлений следует также предусмотреть такую меру, как формирование характеристики (профиля) «благонадежного работника банка» и использование положений, составляющих этот профиль, в практической деятельности при проведении проверок в отношении них. Так, к характеристике (профилю) благонадежного работника банка следует отнести: критерии нормативного поведения работников; признаки, которые обеспечивают устойчивость личности и защищают от девиантного, в том числе делинквентного, поведения.

Кроме того, следует сформировать систему факторов, с учетом которых работники банков могут совершать преступления, а также определить особенности поведения работника банка на разных этапах совершения преступления.

Рассмотрим характеристики (профиля) благонадежного работника банка. К критериям нормативного поведения работника следует отнести: выполнение работы в соответствии с регламентом (согласно установленным требованиям в банке); осуществление деятельности согласно распорядку трудового дня; реализация

⁷ Криминология : учебник / отв. ред. И. М. Мацкевич. М., 2023. С. 132.

⁸ Кудрявцев В. Н. Причинность в криминологии. О структуре индивидуального преступного поведения. М., 2019. С. 106.



на высоком уровне своих профессиональных компетенций; качественное выполнение порученной работы.

К признакам, которые обеспечивают устойчивость личности и защищают от девиантного, в том числе делинквентного, поведения, следует отнести: высокий уровень правового сознания (имеет значение и в том случае, если деятельность не связана с применением норм права в банковской сфере); корпоративную солидарность; стремление не подвести руководство и коллектив; способность нести личную ответственность за свои поступки, отстаивать свои позиции; адекватная оценка работником складывающейся ситуации, имеющей противозаконный характер, оценка ее последствий, а также адекватность реагирования на предложения, имеющие противоправный характер; психологическая устойчивость; отсутствие (невыраженность) рискованных акцентуаций характера.

Приведенная модель профиля благонадежного работника банка может быть использована в практической деятельности подразделений службы безопасности банка.

Выделим систему факторов, с учетом которых работники банков могут совершать преступления, а также определим особенности поведения работника банка на разных этапах совершения преступления. Так, к факторам, носящим условно нейтральный характер, которые в зависимости от характера ситуации могут повлиять на принятие решения о совершении преступления, следует отнести: круг общения как в коллективе (организации), так и вне его; проявление интереса к профессиональным навыкам (роду, направлению деятельности) конкретного работника со стороны другого (других работников).

Рассмотрим особенности поведения работников банка на разных этапах реализации преступления.

Следует учитывать, что механизм преступного поведения включает: формирование мотивации совершения преступления; планирование преступных действий; исполнение преступления и наступление общественно опасных последствий.

На формирование мотивации к совершению преступления могут оказывать влияние среда общения; медиапространство, где, например, продемонстрированы реализация преступления и безнаказанность за его совершение; перспективы получения значительного (солидного) для работника банка дохода от преступной деятельности; исключительные ситуации, связанные с финансовыми трудностями (например, долги, болезнь близкого человека и т.д.).

При планировании преступления банковский работник может стремиться получить доступ к личным данным клиентов банка, в том числе и vip-клиентам (если это не входит в его должностные обязанности); совершать какие-либо операции во время перерыва, после окончания трудового дня, что является нестандартным временем; совершать какие-либо операции, которые не входят в круг его должностных обязанностей. В составе группы лиц по предварительному сговору (организованной группы) работник на этапе планирования и подготовки к совершению преступления может неоднократно контактировать с работниками, выполняющими деятельность на различных других направлениях банковской деятельности, пытаться в качестве подготовки выполнять определенные действия или проверять возможность их выполнения.

В механизме преступного поведения этап исполнения преступления и наступления общественно опасных последствий предполагает совершение непосредственно преступных действий как лично работником банка, так и совместно с другими работниками в составе группы лиц по предварительному сговору или организованной группы.

Изучение и выявление указанных факторов, с учетом которых работники банков могут совершать преступления, и особенностей поведения на разных этапах совершения преступления представляется важным, поскольку работники службы безопасности банков в своей деятельности могут их выявлять.

В качестве превентивной меры следует обозначить информирование работников банков о произошедших нарушениях в банке, правовых аспектах в связи с выявленными нарушениями, в том числе об ответственности.

В качестве еще одной профилактической меры следует назвать организацию работы службы экономической безопасности банка по изучению причин и условий, способствующих совершению преступлений работниками банка посредством информационных технологий. Получить соответствующую информацию возможно путем изучения судебной практики, находящейся в открытом доступе, например приговоров судов общей юрисдикции. Обобщение судебной практики позволит выделить ряд факторов, обуславливающих рассматриваемые преступления, и своевременно принять превентивные меры.

Одной из проблем предупреждения преступлений, совершаемых работниками банка посредством информационных технологий, на современном этапе является нехватка квалифицированных кадров IT-специалистов. В этой связи нередко принимаются на работу специалисты, требования к которым снижены, что прямо влияет на качество их деятельности и ее результаты в области обеспечения безопасности.

Важное значение в предупреждении рассматриваемых преступлений имеет эффективное взаимодействие между банками и органами внутренних дел. Учитывая «закрытость» деятельности банков, взаимодействие в основном осуществляется в связи с выявленным преступлением в банке и сообщением о преступлении.

Следует отметить, что чрезвычайно важен поиск новых эффективных форм взаимодействия и предупреждения совершения преступлений в банках посредством информационных технологий. Например, после внесения изменений и дополнений в ст. 26 Федерального закона «О банках и банковской деятельности» Федеральным законом от 20.10.2022 сотрудники МВД России имеют полномочия оперативно получать данные о финансовых операциях из автоматизированной системы Банка России ФинЦЕРТ с соблюдением требований закона о банковской тайне. В то же время информацию, полученную от правоохранительных органов, банки могут учитывать для предотвращения мошеннических операций.

В качестве новой меры можно указать «создание компьютерной программы, позволяющей пользователю, загрузив комплекс переменных, получить результат планируемой или проведенной банковской операции. Использование такого инструмента позволит перепроверять действия банковских служащих небольших по штату банковских офисов, в которых зачастую один работник совмещает



несколько должностей и может практически без согласования совмещать многие операции»⁹.

Таким образом, на современном этапе важнейшее значение имеет оптимизация мер предупреждения преступлений, совершаемых посредством информационных технологий работниками банков, поскольку ущерб от таких преступлений причиняется не только банку, но и его клиентам. Банки несут также репутационные риски.

Первостепенное значение имеют применение превентивных мер непосредственно в банках, а также поиск новых форм предупреждения рассматриваемых преступлений. В качестве таких мер выделены: формирование характеристики (профиля) благонадежного работника банка; формирование системы факторов, с учетом которых работники банков могут совершать преступления, использование этих моделей в практической деятельности подразделений службы безопасности банков; оптимизация деятельности службы экономической безопасности банков; создание новых компьютерных программ, позволяющих всесторонне контролировать деятельность работников банков; совершенствование форм взаимодействия банков с правоохранительными органами.

БИБЛИОГРАФИЯ

1. Долганов С. И., Желудков А. С. Некоторые аспекты использования информационных технологий в предупреждении корпоративного мошенничества в сфере банковской деятельности // Академическая мысль. — 2020. — № 2 (11).
2. Криминология : учебник / под ред. А. И. Долговой. — 4-е изд., перераб. и доп. — М., 2010.
3. Криминология : учебник / под ред. Н. Ф. Кузнецовой, В. В. Лунеева. — 2-е изд., перераб. и доп. — М., 2004.
4. Криминология : учебник / отв. ред. И. М. Мацкевич. — М., 2023.
5. Кудрявцев В. Н. Причинность в криминологии. О структуре индивидуального преступного поведения. — М., 2019.
6. Мацкевич И. М. Причины экономической преступности : учебное пособие. — М., 2019.

⁹ Долганов С. И., Желудков А. С. Некоторые аспекты использования информационных технологий в предупреждении корпоративного мошенничества в сфере банковской деятельности // Академическая мысль. 2020. № 2 (11). С. 57.