

Леонид Леонидович Решетников

*кандидат технических наук, доцент, доцент кафедры экономической безопасности,
системного анализа и контроля Тюменского государственного университета,
г. Тюмень, I.I.reshetnikov@utmn.ru*

Полина Алексеевна Агеева

*студентка специальности «Экономическая безопасность»
Тюменского государственного университета,
г. Тюмень, ageeva2004@bk.ru*

Анастасия Андреевна Кочурова

*студентка специальности «Экономическая безопасность»
Тюменского государственного университета,
г. Тюмень kochurovanastia04@mail.ru*

СИСТЕМА ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ КАК ФАКТОР ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКИХ БАНКОВ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. В условиях цифровой трансформации происходит стремительное развитие банков и банковской системы в целом. В статье рассматривается такая важная тема, как защита конфиденциальной информации банковского сектора в эпоху цифровых технологий. В работе анализируется, как банк защищает коммерческую тайну в среде интернета, гаджетов и нейросетей. В данной статье на основе открытых данных были проанализированы технические средства защиты, правила работы с банковской информацией, а также нормативно правовые акты, которые помогают сохранить данные в безопасности. Целью анализа является выявление основных тенденций в области обеспечения конфиденциальности информации банковских организаций. В результате были сформированы практические рекомендации по улучшению системы защиты коммерческой тайны банков.

Ключевые слова: банковская тайна, защита информации, коммерческая тайна, цифровая трансформация.

Leonid Leonidovich Reshetnikov

*Candidate of Sciences (Technical), Associate Professor of the Department of Economic Security,
System Analysis and Control, University of Tyumen, Tyumen, I.I.reshetnikov@utmn.ru*

Polina Alekseevna Ageeva

*Student of the specialty "Economic Security" at Tyumen State University,
Tyumen, ageeva2004@bk.ru*

Anastasia Andreevna Kochurova

*Student of the specialty "Economic Security" at Tyumen State University,
Tyumen, kochurovanastia04@mail.ru*

SYSTEM OF PROTECTION OF COMMERCIAL SECRETS AS A FACTOR OF ECONOMIC SECURITY OF COMMERCIAL BANKS IN THE CONDITIONS OF DIGITAL TRANSFORMATION

Abstract. In the context of digital transformation, banks and the banking system as a whole are rapidly developing. The article discusses such an important topic as the protection of confidential information of the banking sector in the digital era. The work analyzes how a bank protects commercial secrets in the environment of the Internet, gadgets and neural networks. In this article, based on open data, technical means of protection, rules for working with banking information, as well as regulatory legal acts that help keep data safe were analyzed. The purpose of the analysis is to identify the main trends in the field of ensuring the confidentiality of information of banking organizations. As a result, practical recommendations were formed to improve the system of protecting commercial secrets of banks.

Keywords: banking secrecy, information protection, commercial secret, digital transformation.

В эпоху цифровизации, где цифровые технологии занимают господствующее положение, ключевым аспектом является защита данных и коммерческой тайны. В каждой отрасли бизнеса есть информация, которая не подлежит огласке, а особенно в банковском секторе. Коммерческая тайна в банковском секторе связана со значительными финансовыми рисками не только самой фирмы, но и ее многочисленных клиентов, поэтому имеет приоритетное значение для обеспечения экономической безопасности коммерческих банков.

В современном мире коммерческие банки являются незаменимым элементом экономики, обеспечивающие ее жизнедеятельность. Особенно сильно их роль проявляется в условиях динамичной цифровой трансформации, когда банковский сектор набирает высокие темпы развития. Однако на банки возлагается огромная ответственность. Именно эти структуры являются носителями большого количества секретной информации, недопустимой для обнародования. Таким образом, актуальность работы состоит в обеспечении надежной защиты коммерческой тайны, которая занимает одно из самых важнейших мест в работе банковских организаций в условиях цифровой трансформации. Актуальность не только правового, но и практического аспекта коммерческой тайны раскрыта в работе А.М. Аршакина, который выделяет коммерческую тайну как основополагающий элемент в системе защиты секретной информации, необходимой для поддержания эффективной, устойчивой работы финансовой организации. С практической точки зрения автор четко выделяет основные составляющие деятельности предприятия и конкретные примеры сведений, которые должны быть отнесены к коммерческой тайне банков [1, с. 27-28].

Коммерческая тайна — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [2].

В условиях динамичного развития экономики и возрастающей конкуренции в банковском секторе коммерческая тайна становится основным активом, который обеспечивает финансовую устойчивость организации. В современном мире информация — это специфический вид товара, который также обладает высокой ценностью. Именно благодаря информации банки могут разрабатывать инновационные продукты, уникальные услуги для получения прибыли, которые, безусловно, являются составляющей коммерческой тайны. Однако высокая ценность коммерческой информации подвержена воздействию множества угроз, как внутренним, так и внешним (рис. 1).

Представленная на рис. 1 классификация угроз, направленная на распространение коммерческой тайны, позволяет систематизировано оценить внешние и внутренние факторы. Внутренние угрозы часто возникают как из-за умышленных противоправных действий сотрудников, так и путем халатности и недостаточной осведомленности в вопросах конфиденциальной информации. К тому же, ключевым фактором является неэффективность организационных процессов, включая отсутствие регламентированных процедур по работе с конфиденциальной информацией. Это создает благоприятную почву для реализации как умышленных, так и неумышленных угроз. Внешние же угрозы напрямую связаны с целенаправленными действиями третьих лиц, ориентированными на получение несанкционированного доступа к внутренней информации.

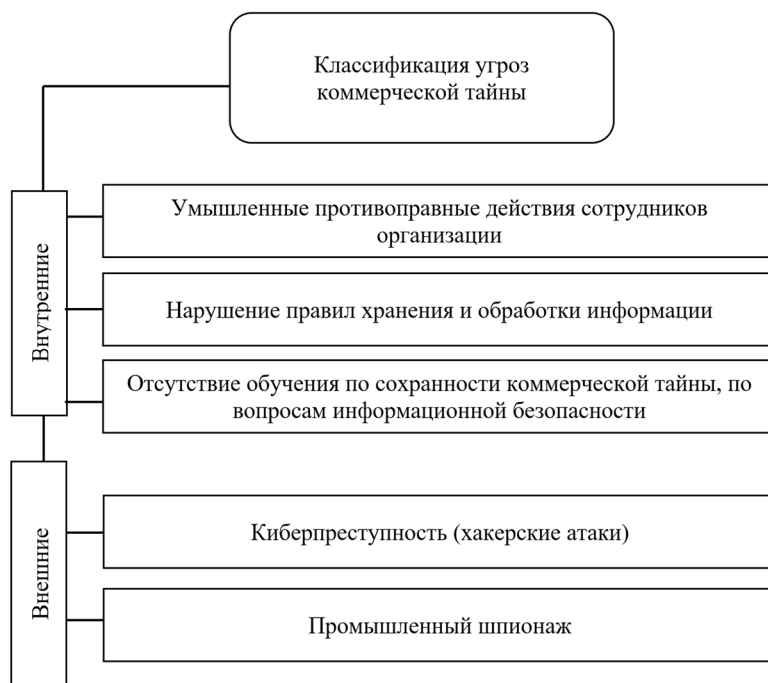


Рис. 1. Классификация угроз коммерческой тайны

Источник: составлено авторами.

Разглашение конфиденциальной информации может привести к большим проблемам как в деятельности предприятия, так и в экономике в целом. Так, например, автор В.А. Пушкарева в своей работе приводит статистические данные с 1997 по 2009 года, которые демонстрируют динамику роста преступлений, связанных с разглашением коммерческой тайны. В связи с этим, важна не только правовая охрана данных, но и надежная защита информационных систем и ресурсов. Автор пишет, что «отключение систем от несанкционированного доступа к локальным корпоративным сетям приведет к банкротству 25-30% средних компаний в течение суток, 40 — 45% средних и 20% крупных фирм разорятся в течение нескольких дней, 30% кредитных организаций лопнут за 2-5 часов, 45% банков перестанут существовать через 2-3 дня». Это еще раз подтверждает приоритетность задачи по защите режима коммерческой тайны [3, с. 85].

Для того, чтобы сохранить конфиденциальную информацию и тем самым не подвергнуть организацию большим рискам, необходимо обеспечивать высокий уровень информационной безопасности в банковских сферах. Об этом в своей работе пишут Садыков Р.Ф. и Байлов К.А. Особое внимание они уделяют практическим рекомендациям, соблюдение которых позволит снизить риски утечки информации. В частности, они подчеркивают важность наличия дополнительных ресурсов в защиту информационных систем и клиентских данных, например, фаерволы, антивирусы. Также авторы акцентируют внимание на обучение сотрудников банков по вопросам информационной безопасности, потому что, как уже упоминалось ранее, именно персонал организации является одним из внутренних угроз по утечки коммерческой тайны [4, с. 1274].

Вопрос о разглашении тайной информации сотрудниками поднимает в своей статье автор Харальд Иргенс-Йенсен. Он уделяет особый акцент на практику многих работодателей по заключению дополнительных соглашений о неразглашении или включение обязательств о конфиденциальности информации в свои трудовые договоры. Это позволит с психологической точки зрения повысить у людей уровень ответственности перед компанией, а также поможет снизить риски утечки информации [5, с. 495].

Для обеспечения надежной защиты коммерческой тайны банков существует множество методов и способов. На основе проведенного анализа литературы и обобщения уже имеющихся знаний нами разработана схема, демонстрирующая, по нашему мнению, наиболее эффективные и популярные подходы по защите конфиденциальной информации (рис. 2).



Рис. 2. Методы по обеспечению защиты коммерческой тайны банков

Источник: составлено авторами.

Нормативно-правовое регулирование коммерческой тайны предприятий, в том числе и банковского сектора, является важным составляющим информационной безопасности. Защита коммерческой тайны способствует созданию благоприятной среды для развития предприятия, поддержанию конкурентоспособности на рынке и устойчивому финансовому положению компании.

Основопологающим документом по коммерческой тайне в России с точки зрения законодательства является Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 09.03.2021) «О коммерческой тайне». Он гласит, что «обладатель информации, составляющей коммерческую тайну, — лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны» [6]. Из этого следует, что информация, признанная коммерческой тайной, остается недоступной для завладения ею лицами, не имеющих законных оснований на это. За нарушение данного закона в зависимости

от размера причиненного ущерба, ответственность за незаконное разглашение или использование банковской тайны наступает согласно либо Уголовному кодексу Российской Федерации, либо кодексу административных правонарушений Российской Федерации. Согласно УК РФ, данное правонарушение влечет за собой различные виды санкций, например, в виде штрафа в размере до одного миллиона рублей или лишение свободы до двух лет [7]. Согласно КоАП РФ — это правонарушение влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц — от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц — от ста тысяч до двухсот тысяч рублей [8].

Разграничение между уголовной и административной ответственностью по распространению коммерческой тайны зависит от ряда объективных и субъективных факторов. Основными факторами являются тяжесть последствий и умысел. Если разглашение конфиденциальной информации доставило крупный ущерб организации и это деяние было совершено умышленно из корыстных целей человека, обладающим данной информацией, то его действия будут квалифицироваться согласно УК РФ. Если же распространение коммерческой тайны не повлекло видимых последствий либо их не было вовсе, но факт разглашения имеет место, то наступает административная ответственность.

Таким образом, система нормативно-правового регулирования коммерческой тайны в России имеет свои особенности и принципы, которые необходимо учитывать для поддержания режима конфиденциальности в банковском секторе.

Для обеспечения конфиденциальности и целостности коммерческой информации банков в условиях цифровой трансформации применяются, как было сказано ранее, различные методы защиты. В ходе работы мы выявили еще несколько методов, которые, на наш взгляд, обеспечат более надежную защиту банковской тайны. Один из таких методов — шифрование данных. Шифрование данных является значительно важным методом защиты банковской тайны, обеспечивая конфиденциальность информации как при хранении, так и при передаче ее по различным каналам связи. С помощью алгоритмов шифрования данные будут преобразовываться в нечитаемый формат, что делает их бесполезными для неавторизованных лиц. Этот метод позволяет предотвратить утечки информации при кибератаках, несанкционированном доступе к базам данных и перехвате трафика. Использование надежных алгоритмов шифрования, своевременная смена ключей шифрования и строгий контроль за их доступом являются необходимыми условиями эффективной защиты банковской тайны в современном цифровом мире. Однако данный метод защиты имеет свои недостатки и главный из них, это возможная потеря производительности. То есть процесс шифрования данных может существенно замедлить работу банков, особенно при обработке большого объема транзакций в режиме реального времени.

Для обеспечения целостности конфиденциальной информации банки могли бы применять методы цифровой подписи. Цифровая подпись является надежным инструментом для обеспечения защиты банковской тайны, гарантируя подлинность и полноту электронных документов и транзакций. Она позволяет однозначно идентифицировать отправителя и подтвердить, что информация

не была изменена после подписания. Применение цифровой подписи в банковской сфере способствует минимизации рисков подделки документов, несанкционированных операций и мошеннических действий, укрепляя доверие клиентов и обеспечивая соответствие регуляторным требованиям в области защиты конфиденциальной информации. Минусом такого метода защиты конфиденциальной информации будет являться неудобство обращения. То есть не у всех клиентов банка есть возможность иметь цифровую подпись. Например, для людей пенсионного возраста, это будет достаточно проблематично.

В банковских структурах серверные помещения являются основными обладателями информации. В них хранятся конфиденциальные данные сотрудников, клиентов, программное обеспечение, необходимого для осуществления банковских операций. Незаконное проникновение в эти помещения могут послужить утечке конфиденциальной информации, краже данных и оборудования, что нанесет значительный ущерб работе банка. Для предотвращения таких рисков и угроз могут быть использованы биометрические терминалы доступа в серверные помещения. Они основаны на использовании индивидуальных биологических особенностей человека для идентификации и контроля доступа к закрытым ресурсам. Например, это могут быть терминалы с распознаванием отпечатков пальцев или геометрии лица для узкого круга лиц. Однако такие технологии довольно чувствительны к загрязнению, повреждению кожи, что может поспособствовать ограничению доступа к информации во время выполнения различных важных задач. Также существуют риски, связанные с централизацией. Например, если центральный сервер, управляющий биометрическими терминалами, придет в негодность, то это приведет к блокировке доступа в серверные помещения. В связи с этим, нужно принимать во внимание все достоинства и потенциальные ограничения, связанные с внедрением биометрических систем для эффективной реализации мер по защите конфиденциальной информации

Также в условиях роста объемов информации и данных традиционные методы по их защите требуют дополнительных возможностей. Внедрение технологий искусственного интеллекта (AI) становится одним из основных факторов экономической безопасности коммерческой тайны банков. Искусственный интеллект способен автоматизировать рутинные задачи, связанные с защитой информации, такие как мониторинг и аудит. Также он может быстро анализировать большие объемы данных, выявлять потенциальные угрозы и риски, что значительно оптимизирует работу. Автоматизация процессов искусственного интеллекта снижает риск ошибок, связанных с человеческим фактором, тем самым повышается эффективность защиты информации. Однако существует и ряд недостатков, связанных с внедрением такой системы. Использование искусственного интеллекта может потребовать передачи конфиденциальных данных третьим лицам, например, разработчикам системы, что в свою очередь создает риски утечки информации. В таком случае необходимо заключать дополнительные соглашения о неразглашении, определяющих ответственность сторон за сохранность информации. Также AI — это компьютерная система, которая подвержена кибератакам и взломам. Необходимо уметь адаптироваться к новым видам вирусов, чтобы минимизировать риски заражения и обеспечивать стабильность работы системы. При правильном подходе AI может

стать мощнейшим инструментом экономической безопасности по защите коммерческой тайны банков.

Важнейшим методом, который обеспечивает надежную защиту банковской тайны, является установление антивирусных систем. Они играют критически важную роль при борьбе с киберугрозами, направленными на кражу персональных, финансовых данных, нарушение работы компьютерных систем.

История киберпреступности хранит критический случай, связанный с распространением вируса «Carbanak» в 2014 году. Эта система была нацелена исключительно на банковский сектор. Международная хакерская группировка в течение двух лет совершала атаки и в совокупности ей удалось похитить сотни миллионов долларов со счетов около 100 банков по всему миру. Ведущий антивирусный эксперт Сергей Голованов отметил, что «эти ограбления банков отличаются от остальных тем, что киберпреступники применяли такие методы, которые позволяли им не зависеть от используемого в банке ПО, даже если оно было уникальным. Хакерам даже не пришлось взламывать банковские сервисы. Они просто проникали в корпоративную сеть и учились, как можно замаскировать мошеннические действия под легитимные. Это действительно профессиональное ограбление». Злоумышленники, проникая к внутренней сети банка, могли отследить все манипуляции сотрудников. Они также имитировали их действия при переводе денег на фальшивые счета [9].

«Carbanak» был очень сложным вирусом, который использовал продвинутые техники обхода защиты, поэтому даже высокотехнологичные антивирусы не смогли с ним справиться.

Таким образом, безопасность коммерческой тайны должна основываться на многоуровневом процессе. Антивирусная защита — это лишь один из важнейших инструментов, который используют банки, но он не должен оставаться единственным по борьбе с внутренними и внешними угрозами.

По результатам проведенного анализа нами была разработана таблица, в которой представлены методы защиты коммерческой тайны, которые на наш взгляд наиболее эффективнее, а также их преимущества и недостатки (табл. 1).

Таблица 1

Методы защиты конфиденциальной информации коммерческих банков

<i>Название метода</i>	<i>Суть метода</i>	<i>Преимущества</i>	<i>Недостатки</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
Шифрование данных	С помощью алгоритмов шифрования данные будут преобразовываться в нечитаемый формат, что делает их бесполезными для неавторизованных лиц	Минимизация утечки информации при кибератаках, несанкционированном доступе к базам данных и перехвате трафика	Замедление работы банка, в особенности при обработке больших объемов транзакций в режиме реального времени

1	2	3	4
Цифровая подпись	Позволяет однозначно идентифицировать отправителя и подтвердить, что информация не была изменена после подписания	Минимизации рисков подделки документов, несанкционированных операций и мошеннических действий, укрепляя доверие клиентов и обеспечивая соответствие регуляторным требованиям в области защиты конфиденциальной информации	Не у всех клиентов банка есть возможность иметь цифровую подпись. Например, для людей пенсионного возраста, это будет достаточно проблематично
Биометрические терминалы	Использование индивидуальных биологических особенностей человека для идентификации и контроля доступа к закрытым ресурсам	В серверные помещения допускаются только лица, имеющие соответствующие права доступа. Несанкционированное проникновение исключено. Доступ к закрытым ресурсам регулируется системой контроля доступа	Такие технологии довольно чувствительны к загрязнениям, повреждениям кожи, что может способствовать ограничению доступа к информации во время выполнения различных важных задач; Если центральный сервер, управляющий биометрическими терминалами, придет в негодность, то это приведет к блокировке доступа в серверные помещения
Искусственный интеллект (AI)	Автоматически отслеживает и анализирует данные для обнаружения признаков утечки коммерческой тайны	Автоматизация рутинных задач, связанные с защитой информации; быстрый анализ больших объемов данных, выявление потенциальных угроз и рисков; снижение рисков ошибок, связанных с человеческим фактором	Передача конфиденциальных данных разработчикам системы; AI как и любая компьютерная система подвержена кибератакам и взломам

1	2	3	4
Антивирусные системы	Обеспечение специализированной защиты от кибератак, которые направлены на дестабилизацию работы банков (получение конфиденциальных сведений, финансовых активов и т.д.)	Представленный метод является единственным средством противодействия киберугрозам, действующим внутри компьютерной системы	Ограниченная способность оперативно адаптироваться к новым, мощным вирусным угрозам, что обуславливает их недостаточную эффективность против новых атак

Источник: составлено авторами.

Таким образом, эффективная система защиты коммерческой тайны сочетает в себе различные методы, и она является ключевым фактором обеспечения экономической безопасности коммерческих банков в современных условиях. В целях защиты коммерческой тайны, а особенно когда она является очень уязвимой в условиях цифровой трансформации, банкам следует постоянно совершенствовать систему защиты. Это может быть внедрение современных технических средств шифрования или переход на цифровую подпись. Инструментов защиты достаточно много и все они разнообразны, однако важнейшим методом остается антивирусная безопасность. На сегодняшний день современные пользователи компьютеров сталкиваются с высоким риском заражения вирусов при скачивании программ и приложений, что может привести к раскрытию конфиденциальной информации. Исходя из этого, надежная антивирусная защита в сочетании с другими инструментами — ключ к экономической безопасности банковского сектора в эпоху цифровой трансформации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Виды и сущность коммерческой тайны, ее место в системе информации экономической безопасности коммерческого банка / А. М. Аршакян // Форум молодежной науки. — 2021. — № 4. — С. 22-34.
2. Об информации, составляющей коммерческую тайну, в рамках рассмотрения дела о нарушении антимонопольного законодательства, проведении проверок соблюдения антимонопольного законодательства, осуществлении государственного контроля за экономической концентрацией: Разъяснение Президиума ФАС России от 21.02.2018 № 13 // КонсультантПлюс: надежная правовая поддержка: сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_293112/ (дата обращения: 09.04.2025).
3. Пушкарева В. А. Банковская и коммерческая тайна: правовой анализ / В. А. Пушкарева // Всероссийский криминологический журнал. — 2010. — № 4. — С. 83-88.
4. Байлов К. А. Актуальность и проблемы обеспечения информационной безопасности банковских систем / К. А. Байлов, Р. Ф. Садыков // Экономика и социум. — 2024. — № 1 (116). — С. 1271-1275.
5. Departing Employees, Confidentiality Clauses and European Trade Secret Protection / I.-J. Harald // IIC — International Review of Intellectual Property and Competition Law. — 2023. — № 54. — С. 495-526.

6. О коммерческой тайне: федеральный закон от 29.07.2004 № 98-ФЗ : принят Государственной Думой 9 июля 2004 года : одобрен Советом Федерации 15 июля 2004 года // КонсультантПлюс: надежная правовая поддержка : сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 26.05.2025).
7. Уголовный кодекс Российской Федерации: от 13 июня 1996, № 63-ФЗ : ред. от 28.02.25: принят Государственной думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года // КонсультантПлюс: надежная правовая поддержка : сайт. — URL: / https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 09.04.2025).
8. Кодекс российской федерации об административных правонарушениях: от 30 декабря 2001, № 195-ФЗ : ред. от 03.02.2025: принят Государственной думой 20 декабря 2001 года : одобрен Советом Федерации 26 декабря 2001 года // КонсультантПлюс: надежная правовая поддержка : сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 09.04.2025).
9. «Лаборатория Касперского» описала признаки поразившего 100 банков вируса // РБК: сайт. — URL: https://www.rbc.ru/technology_and_media/16/02/2015/54e1d92f9a7947630510f166 (дата обращения: 09.04.2025).