Оригинальная статья
УДК: 336:004.056
ББК: 32.973-018.2

# Утечка информации: классификация каналов и влияние на типичные банковские риски

**Павел Владимирович Ревенков[1], Ефим Сергеевич Анисимов[2]**

[1, 2] Финансовый университет при Правительстве Российской Федерации
[1] PVRevenkov@fa.ru, [2] EAnisimov_Sci@mail.ru

***Автор, ответственный за переписку:*** Павел Владимирович Ревенков, PVRevenkov@fa.ru

***Аннотация.*** В статье детально рассмотрены каналы передачи информации и проанализированы возможные последствия утечек конфиденциальной информации на примере коммерческих банков. Особое внимание уделено стеганографическим каналам утечек информации. Дано описание взаимосвязи рисков недостаточного обеспечения информационной безопасности (ставших источником утечек конфиденциальной информации) и типичных банковских рисков.

***Ключевые слова:*** канал передачи данных, утечка информации, цифровая стеганография, банковские риски

**Для цитирования:** П. В. Ревенков, Е. С. Анисимов Утечка информации: классификация каналов и влияние на типичные банковские риски // В центре экономики. 2025. № 1. Т. 6. URL: https://vcec.ru/index.php/vcec/article/view/122/140

Original Paper
JEL Classification:
E59, G21, F65, L86

# Information Leak: Classification of Channels and Impact on Typical Banking Risks

**Pavel V. Revenkov[1], Efim S. Anisimov[2]**

[1, 2] Financial University under the Government of the Russian Federation
[1] PVRevenkov@fa.ru, [2] EAnisimov_Sci@mail.ru

***Corresponding author:*** Pavel V. Revenkov, PVRevenkov@fa.ru

***Abstract.*** The article examines in detail the channels of information transfer and analyzes the possible consequences of confidential information leaks using commercial banks as an example. Particular attention is paid to steganographic channels of information leaks. A description is given of the relationship between the risks of insufficient information security (which became the source of confidential information leaks) and typical banking risks.

***Keywords:*** data transmission channel, information leakage, digital steganography, banking risks

***For citation:*** P. V. Revenkov, E. S. Anisimov Information Leak: Classification of Channels and Impact on Typical Banking Risks. *In the Center of Economy*. 2025;1(6). URL: https://vcec.ru/index.php/vcec/article/view/122/140



**Введение / Introduction**

Постоянный рост объема обрабатываемой информации значительно повышает риски, связанные с недостатками в обеспечении информационной безопасности (ИБ).

В частности, высокая скорость взаимодействия по открытым каналам связи и хранение больших объёмов данных разного рода в электронных базах данных способствуют возникновению рисков реализации угроз конфиденциальности информации (если классифицировать угрозы по виду нарушаемого свойства безопасности информации). Класс угроз конфиденциальности информации включает различные примеры, среди которых в настоящее время наиболее актуальной является угроза утечек информации.

**Материалы и методы / Materials and Methods**

Обращаясь к статистическим данным ведущих организаций в сфере ИБ, утечки защищаемой информации стали основным последствием реализации атак на организации различных отраслей в 2023 году. По данным

компании Positive Technologies больше всего от утечек конфиденциальной информации пострадали организации сферы услуг, медицинские организации, торговые предприятия и IT-компании. Чуть ниже в отчете отмечены финансовые учреждения и организации науки и образования [9].

В материале компании BI.ZONE, выпущенном в октябре 2023 года, отмечается, что утечки информации негативно влияют на репутацию организаций [11]. Так в частности в 2022 году зафиксирован более чем трёхкратный рост по сравнению с 2021 годом как количества утекших баз данных, так и их общего объёма . Если в 2021 году утекли 305 баз данных размером 28,6 ГБ, то в 2022 - 925 баз данных размером 161 ГБ.

Наряду с этим отмечается продолжение этой тенденции в 2024 году, охватывающей всё больший круг организаций и частных лиц [8].

В состав похищаемой информации входили: персональные данные всех категорий (в том числе биометрических и специальных), коммерческая, банковская и профессиональная тайны, аутентификационная информация клиентов и сотрудников компании.

Анализ нормативных документов и научных работ показал, что по данной тематике используются следующие термины: «утечка информации», «передача данных» и «скрытый канал передачи данных».

**Результаты и обсуждение/ Results and discussion**

Передача данных в Федеральном законе № 152-ФЗ «О персональных данных» определяется триадой процедур, в совокупности и составляющих передачу данных: распространение, предоставление и доступ [1]. Подобный подход к формулировке определения с точки зрения процессного содержания термина оправдан в рамках указанного нормативного акта, поскольку он направлен на регулирование безопасности процессов, связанных с оборотом персональных данных. По мнению авторов, больший интерес представляют не формы передачи данных, а место передачи данных в системах обеспечения информационной безопасности. По этой причине в определении передачи данных целесообразнее зафиксировать роль этого процесса, а также его влияние на свойства безопасности информации. Исходя из этого под передачей данных, мы будем понимать процесс, в ходе которого происходит перемещение данных от отправителя к получателю. Взаимодействие между отправителем и получателем в рамках отмеченного процесса происходит посредством канала передачи данных, который может быть совершенно различной природы.

Канал передачи данных является скрытым, если он изначально не предусматривался в составе информационной системы или используется для передачи нетипичных данных. Один из примеров организации скрытого канала передачи данных — применение стеганографических методов скрытия информации. В самом названии стеганографии раскрывается её смысл — скрытое письмо [6]. Развитие компьютерных систем не обошло стороной и данное направление по сокрытию информации, породив направление компьютерной и цифровой стеганографии. В основе компьютерной стеганографии лежат идеи использования особенностей форматов данных в сетях. Цифровая стеганография включает механизмы использования в целях сокрытия данных избыточности цифровых медиа-форматов, изначально аналоговых (например, звук и изображения) [4].

Утечка защищаемой информации в одном из национальных стандартов толкуется как неконтролируемое распространение защищаемой информации по итогу её разглашения и несанкционированного доступа к ней [2]. Единственным уточнением к такому определению, по мнению авторов, может стать обозначение стороны, с точки зрения которой распространение является неконтролируемым. Распространение информации после утечки является неконтролируемым стороной защиты (исходная трактовка допускает возможность прочтения, что организаторы утечки также не обладают контролем над движением информации — это неверно, поэтому отмечен этот факт). Заметим, что подобная характеристика раскрыта в работе [5], где автором формулируются определения «канала передачи данных» и «канала утечки информации» на основании отличий в контроле со стороны владельца над процессами, связанными с этими каналами.

Независимо от угрозы, реализация которой приводит к утечке защищаемой информации, нарушители получают изначально утекшую информацию в результате её передачи. Данное действие можно классифицировать на основании канала, который используется для организации утечки. Подобные классификации представляют определённую практическую значимость, поскольку их знание позволит предпринять меры защиты от угроз, исходящих от внутренних нарушителей, заинтересованных в утечке информации из организации, а также от внешних нарушителей, имеющих несанкционированный доступ к информационной системе организации.

Обзор научных работ показывает, что вопросам классификации каналов утечки информации уделяется не так много внимания по сравнению с описанием самих последствий утечек. Выделить можно труды следующих экспертов в области обеспечения ИБ: Г.А. Атаманова, А.А. Хорева. В своих работах они предложили подробные классификации каналов утечки информации.

Одна из классификаций представляет следующую структуру каналов утечки информации:

— оперативные:

а) с использованием технических средств разведки;

б) без применения технических средств разведки.

— технические:

а) потенциальные;

б) реальные.

В открытых научных публикациях больше изложены технические каналы утечки информации, которые существуют благодаря особенностям функционирования технических средств обработки, хранения и передачи информации. Например, в работе [7] предлагается

классифицировать технические каналы утечки информации по их природе: электромагнитные, параметрические и электрические.

С течением времени происходят изменения как в техниках атакующих, так и в средствах защиты информации, поэтому важно отслеживать тенденции, отмечая при этом направления, которым на практике может уделяться меньшее внимание. Одним из подобных потенциально недооценённых звеньев можно считать стеганографические каналы утечки информации.

С учётом отмеченного перечислим основные методы предотвращения утечек защищаемой информации:

— организационные;

а) разработка и утверждение внутренних документов, устанавливающих режим обращения с конфиденциальной информацией;

б) ознакомление под подпись сотрудников с политиками информационной безопасности;

в) установление мер ответственности для сотрудников за нарушения правил;

г) организация режима физического доступа на территорию, в здания и в помещения.

— технические:

а) контроль и управление доступом к объектам;

б) использование двухсторонней аутентификации при передаче данных;

в) контроль целостности информационных активов;

г) контроль и управление коммуникацией сотрудников внутри организации и с внешними лицами (посредством электронной почты, телефонной сети и сети Интернет), включая проведение контентного анализа содержания;

д) контроль использования съёмных носителей информации;

е) контроль и управление процессами печати бумажных документов;

ж) регистрация действий пользователей, ведение архива действий пользователей в информационных системах;

з) применение стеганографических методов для создания уникальных единиц документов (например, цифровые водяные знаки);

и) проведение стеганографического анализа медиафайлов, передаваемых из организации посредством сети Интернет и электронной почты, а также циркулирующих в рамках внутренней коммуникации между сотрудниками с различными наборами прав доступа.

— криптографические.

Из представленного перечня направлений защитных мер отдельно скажем о пунктах З) и И) группы технических мер предотвращения утечек. При их отсутствии представленный комплекс мер во многом бы повторял базовый состав мер защиты информации, содержащийся в национальном стандарте ГОСТ Р 57580.1-2017, которым руководствуются финансовые организации при обеспечении защиты информации в своей деятельности [3]. Этот стандарт в отношении передаваемых данных содержит только меры контентного анализа без уточнения его детальности и «глубины». Однако злоумышленники, желающие нарушить конфиденциальность защищаемой информации, передавая её за разрешённые пределы, представляют о наличии в контурах безопасности организации подобных средств, тем самым заставляя себя искать методы их обхода. Контентный анализ может оказаться менее эффективной мерой в случаях сокрытия информации стеганографическими методами, что требует принятия дополнительных мер защиты (например, как отмечено в пункте И).

При этом значимым остаётся факт сложности обнаружения и предотвращения стеганографических каналов. Это отмечается, среди прочего, и в описаниях техник MITRE ATT&CK T1001.002, T1027.003, T1406.001, которые охватывают своим применением не только угрозы утечки, но и процессы доставки вредоносного программного обеспечения, а также взаимодействия нарушителей с командным сервером (C2 Server) [12]. Подобная характеристика может служить весомым мотивом для применения стеганографических механизмов нарушителями, поскольку сравнительно низкая степень обнаружения увеличивает вероятность более длительного закрепления в информационных системах целевых организаций, что можно считать одной из отличительных особенностей высококвалифицированных киберпреступников. По этой причине подтверждается актуальность добавления отмеченных мер защиты на общую карту контуров безопасности учреждения.

Относительно цифровых водяных знаков допустимо упомянуть случаи утечки информации без применения сетевой инфраструктуры организации. Ярким примером является фотографирование документов, дальнейшая передача результатов которого осуществляется в личной переписке сотрудника или путём передачи носителя фотографии. За счёт «уникализации» стеганографическими процедурами выводимых на экран или на печать документов сужается круг лиц, потенциально причастных к утечке информации. Подобный механизм, хоть и в меньшей степени предотвращает утечку информации — на такие сценарии оперативное реагирование более вероятно при наличии средств видеоконтроля (средства телевизионные - в помещениях, контроль с видеокамеры - на конкретных автоматизированных рабочих местах), упрощает и ускоряет процесс расследования инцидента и привлечения нарушителей к ответственности.

В контексте обращения к содержанию национального стандарта, профильного для финансового сектора, рассмотрим описание характера влияния риска утечек защищаемой информации, в том числе по скрытым каналам, на типичные для сектора риски. Как известно, управление риском — это один из основополагающих факторов успеха любой деятельности, сопряжённой с ним. Среди типичных банковских рисков выделим стратегический риск, правовой, репутационный, операционный и риск ликвидности. Риск утечки защищаемой информации является полноценным фактором перечисленных групп рисков.

Он расширяет профиль правового риска, поскольку

нормативными актами предъявляются к некоторой информации особые требования по обеспечению её конфиденциальности (персональные данные клиентов и сотрудников организации, банковская тайна, служебная и коммерческая тайны, а также прочая информация ограниченного доступа). Для коммерческих банков особо следует отметить, что в случае реализации риска утечки в зависимости от состава информации, конфиденциальность которой была нарушена, возможно нарушение действующего законодательства, а также договоров и соглашений с контрагентами, что, в свою очередь, может повлечь наложение на юридическое лицо штрафов и прочих санкционных опций вплоть до отзыва лицензии на осуществление банковских операций.

Описанное негативное влияние результатов реализации риска утечки лавинообразно захватывает и другие типичные банковские риски. Распространение информации о произошедшей утечке в СМИ и других открытых источниках приводит к снижению доверия к организации со стороны клиентов (как действующих, так и потенциальных. Доверие падает также со стороны инвесторов, что может повлечь снижение капитализации компании.

Репутационный ущерб, в свою очередь, может не ограничится потерей новых клиентов и рыночной переоценкой, расширившись на отток действующих клиентов, что приводит к увеличению вероятности снятия остатков денежных средств на счетах, тем самым повышая величину операционных рисков и рисков ликвидности.

В совокупности отмеченные направления влияния угрозы утечки защищаемой информации на некоторые типичные банковские риски приводят к росту величины стратегического риска [10].

**Выводы / Inferences**

Таким образом, обзор существующих взглядов на тему каналов утечки защищаемой информации предоставил подтверждения актуальности учёта скрытых каналов передачи данных в контексте принятия комплекса мер защиты от утечек информации. Использование злоумышленниками стеганографических процедур позволяет скрывать некоторую информацию внутри легитимных файлов-документов, что формирует возможности по созданию канала утечки защищаемой информации. Механизмами стеганографического анализа следует дополнять существующие средства защиты информации, а также расширять перечень методов анализа в средствах с уже встроенными подобными механизмами с целью покрытия большего числа угроз информационной безопасности, в частности отмеченной угрозы утечки информации. Кроме того, применение цифровых водяных знаков, которое на текущий момент, например, получает широкое распространение в решениях класса типа VDR (Virtual Data Room — Виртуальная комната данных) и IRM (Information Rights Management — Управление правами на доступ к информации), вносит позитивный вклад в решение вопроса борьбы с утечками информации, проводимых посредством фотографирования конфиденциальной информации в организации на личные устройства сотрудников или приглашённых специалистов.

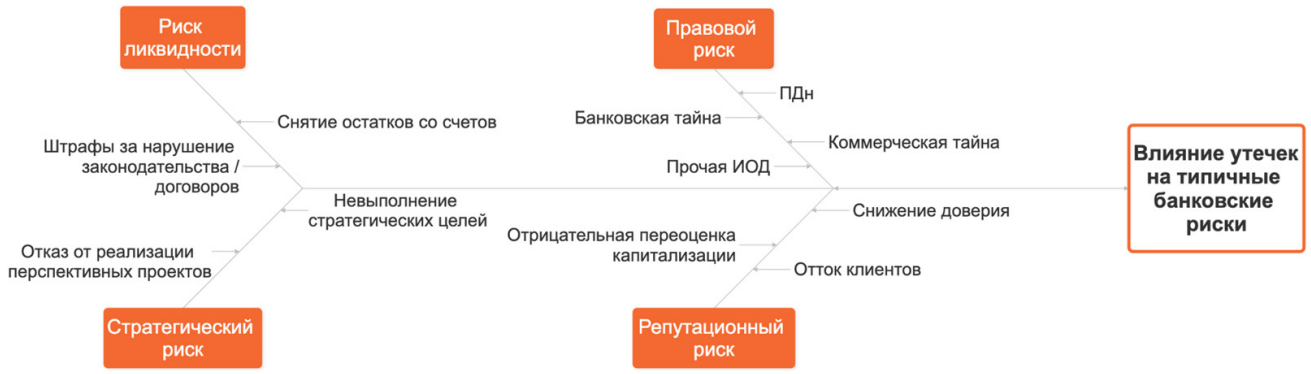


**Рис. 1 / Fig 1. Аспекты влияния утечек защищаемой информации на типичные банковские риски. Источник: составлено авторами по материалам исследования / Aspects of the impact of leaks of protected information on typical banking risks. Source: compiled by the authors based on research materials**

**Список источников**

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

3. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

4. Абазина Е.С., Ерунов А.А. Цифровая стеганография: состояние и перспективы. Системы управления, связи и безопасности. – 2016. – № 2. – С. 181-201. – eISSN: 2410-9916. – EDN UDWGNJ.

5. Атаманов Г.А. Технические каналы утечки информации: определение, сущность, классификация. Инсайд. – 2010. – № 1. – С. 28-33. – ISSN 2413-3582.

6. Теренин А.А., Мельников Ю.Н., Погуляев В.В. Использование цифровых водяных знаков для борьбы с инсайдерами. Специальная техника. – 2008. – № 1. – С. 27-30. – ISSN: 1996-0506. – EDN IJTAET.

7. Хорев А.А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи. Специальная техника. – 1998. – № 2. – С. 41-46. – ISSN: 1996-0506.

8. Актуальные киберугрозы: III квартал 2024 года. Positive Technologies. [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id1 (дата обращения: 11.11.2024).

9. Кибербезопасность в 2023-2024 гг.: тренды и прогнозы. Часть пятая. Самые громкие инциденты и наиболее атакуемые отрасли. Positive Technologies. [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/ (дата обращения: 30.10.2024).

10. Кибербезопасность в условиях электронного банкинга. / Практическое пособие под ред. П.В. Ревенкова. М.: Прометей. 2020. – 522 с. – ISBN 978-5-907244-61-0.

11. Связи с общественностью. Как компании сохранить репутацию после киберинцидента. BI.ZONE. [Электронный ресурс]. Режим доступа: https://bi.zone/expertise/business-continuity-management/svyazi-s-obshchestvennostyu-kak-kompanii-sokhranit-reputatsiyu-posle-kiberintsidenta/ (дата обращения: 30.10.2024).

12. Techniques. MITRE ATT&CK. [Электронный ресурс]. Режим доступа: https://attack.mitre.org/techniques/ (дата обращения: 11.11.2024).

**Reference**

1. Federal Law of July 27, 2006 No. 152-FZ «On Personal Data».

2. GOST R 50922-2006. Information Security. Basic Terms and Definitions.

3. GOST R 57580.1-2017. Security of Financial (Banking) Transactions. Information Security of Financial Institutions. Basic Composition of Organizational and Technical Measures.

4. Abazina E.S., Erunov A.A. Digital Steganography: Status and Prospects. *Control, Communication and Security Systems*. 2016;2:181-201. eISSN: 2410-9916. EDN UDWGNJ.

5. Atamanov G.A. Technical Information Leakage Channels: Definition, Essence, Classification. *Insider*. 2010;1:28-33. ISSN 2413-3582.

6. Terenin A.A., Melnikov Yu.N., Pogulyaev V.V. Using digital watermarks to combat insiders. *Special equipment*. 2008;1:27-30. ISSN: 1996-0506. EDN IJTAET

7. Khorev A.A. Classification and characteristics of technical channels for leaking information processed by TSPI and transmitted via communication channels. *Special equipment*. 1998;2:41-46.

8. Current cyber threats: Q3 2024. Positive Technologies. [Electronic resource]. Access mode: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id1 (accessed: 11.11.2024).

9. Cybersecurity in 2023-2024: trends and forecasts. Part five. The most high-profile incidents and the most attacked industries. Positive Technologies. [Electronic resource]. Access mode: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pyataya/ (accessed: 10/30/2024).

10. Cybersecurity in the context of electronic banking. Practical guide edited by P.V. Revenkov. Moscow: Prometheus. 2020. 522 p. ISBN 978-5-907244-61-0.

11. Public Relations. How a company can maintain its reputation after a cyber incident. BI.ZONE. [Electronic resource]. Access mode: https://bi.zone/expertise/business-continuity-management/svyazi-s-obshchestvennostyu-kak-kompanii-sokhranit-reputatsiyu-posle-kiberintsidenta/ (date of access: 10/30/2024).

12. Techniques. MITRE ATT&CK. [Electronic resource]. Access mode: https://attack.mitre.org/techniques/ (date of access: 11/11/2024).

***Информация об авторах***

**П. В. Ревенков** – доктор экономических наук,
профессор кафедры информационной безопасности,
Финансовый университет при Правительстве Российской Федерации
Адрес: 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия
E-mail: PVRevenkov@fa.ru
ORCID ID: 0000-0002-0354-0665
**Е. С. Анисимов** – магистрант,
Финансовый университет при Правительстве Российской Федерации
Адрес: 4-й Вешняковский проезд, д. 4, корп. 2, г. Москва, 109456, Россия
E-mail: EAnisimov_Sci@mail.ru
ORCID ID: 0000-0002-2632-4439

***Information about the authors***

**P. V. Revenkov** – Doctor of Economics,
Professor of the Information Security Department,
Financial University under the Government of the Russian Federation,
Address: 4th Veshnyakovsky Proezd, 4, Bldg. 2, Moscow, 109456, Russia.
E-mail: PVRevenkov@fa.ru
ORCID ID: 0000-0002-0354-0665
**E. S. Anisimov** – Master's student, Financial University under the Government of the Russian Federation,
Address: 4th Veshnyakovsky Proezd, 4, Bldg. 2, Moscow, 109456, Russia.
E-mail: EAnisimov_Sci@mail.ru
ORCID ID: 0000-0002-2632-4439

***Вклад авторов***

**Ревенков П. В.** – научное руководство; концепция исследования; развитие методологии; написание и доработка текста; итоговые выводы.

**Анисимов Е. С.** – участие в написании исходного текста, оформление статьи.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

***Contribution of the authors***

**Revenkov P. V.** – scientific guidance; research concept; development of methodology; writing and revision of the text; final conclusions.

**Anisimov E. S.** – participation in the writing of the source text; design of the article.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

Статья поступила в редакцию: 10.12.2024;
одобрена после рецензирования: 21.12.2024;
принята к публикации: 09.01.2025.

The article was submitted: 10.12.2024;
approved after reviewing: 21.12.2024;
accepted for publication: 09.01.2025.