Актуальные тренды утечек информации в финансовом секторе 2022

rt-solar.ru
solar@rt-solar.ru

Ростелеком
Солар

Оглавление

Ключевые цифры и факты

1 млн. руб. максимальный ущерб от утечек данных, зафиксированный в финансовом секторе в 2022 году

50% финансовых организаций сэкономили от **10** до **100 млн руб.** в результате внедрения DLP-системы

75% финансовых организаций используют «надежные средства защиты от утечек»

67% утечек в финансовых организациях являются умышленными

90% утечек из финансовых организаций составляют утечки коммерческой тайны, данных о финансовых операциях и персональных данных клиентов и сотрудников

>60% утечек в финансовом секторе происходит с использованием интернет-технологий (облачные хранилища, интернет-почта, веб-версии мессенджеров соцсетей)

Методология

Данное исследование проведено методом электронного опроса аудитории издания «Банковское обозрение» и части аудитории ресурса TAdviser, относящихся к финансовому сектору (проведены целевые рассылки по базам подписчиков).

В опросе приняли участие представители свыше 350 российских организаций. Размер опрошенных компаний представлен категориями «малый бизнес» (до 100 сотрудников), «средний бизнес» (от 500 до 1000 сотрудников) и «крупный бизнес» (свыше 1000 сотрудников).

Опрос проводился в октябре 2022 года.

В ходе опроса респондентам предлагалось выбрать один из предложенных вариантов ответа или указать свой вариант ответа в свободной форме.

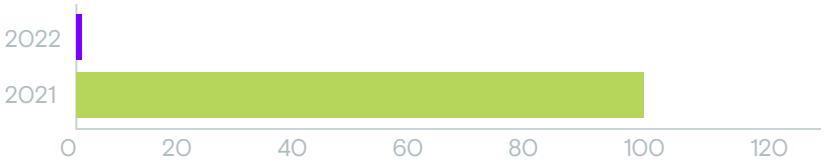
>350 российских организаций приняли участие в опросе

Результаты исследования

Размер утечек и уровень проникновения DLP-систем

В 2022 году крупных утечек в финансовом секторе стало заметно меньше, их размер сильно снизился (нет подтвержденных респондентами утечек «стоимостью» больше **1 млн руб.**). Напомним, в 2021 году две финансовые организации зафиксировали у себя ущерб от утечек данных клиентов, превысивший 100 млн руб.

Максимальный размер ущерба от утечек, млн руб.



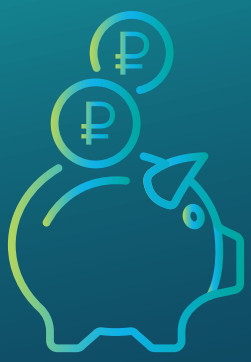
При этом значительно увеличился размер сэкономленных финансовыми организациями средств за счет предотвращения утечек благодаря использованию DLP-системы: **в половине случаев** он составляет **10–100 млн руб.** Тогда как годом ранее столь внушительную экономию отметило только 36% «финансистов».

> Мнения экспертов
>
> Похоже, что службы ИБ финансового сектора с повышенной эффективностью используют инструменты контроля утечек.

Эти данные также подтверждают, что не оправдались пессимистичные прогнозы участников опроса, который «Ростелеком-Солар» проводил в конце 2021 года: тогда **почти 90%** респондентов заявили, что в 2022 году ситуация с утечками в финансовых организациях ухудшится.

При этом финансовые организации также оптимистично смотрят в будущее: **половина** из них считает, что в краткосрочной перспективе (до конца 2022 года) ситуация с утечками еще улучшится: **утечек станет меньше,** так как совершенствуются используемые для борьбы с ними технические средства. В 2021 году оптимистов было всего около 10%. Эта уверенность обоснованна: популярность DLP-систем среди финансовых организаций продолжает расти. **75%** респондентов **используют «надежные средства защиты от утечек»,** в первую очередь DLP-системы. В 2021 году доля респондентов-банков, подтвердивших наличие систем контроля утечек информации, составляла 70%.

> Мнения экспертов
>
> Такие высокие показатели по отрасли (средний уровень распространенности DLP-систем в остальных отраслях – от 30 до 50 %) достаточно логичны и объясняются жесткими требованиями регулятора в сфере финансовых услуг – Центрального банка Российской Федерации – к участникам рынка.

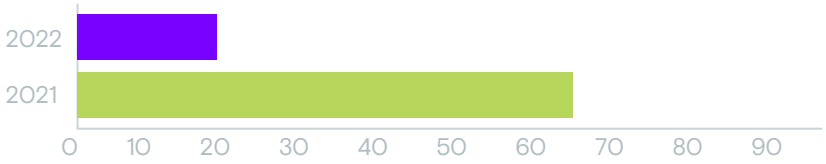


Значительно увеличился размер сэкономленных финансовыми организациями средств за счет предотвращения утечек благодаря использованию DLP-системы.

Финансовые организации оптимистично смотрят в будущее: половина из них считает, что утечек станет меньше, так как совершенствуются используемые для борьбы с ними технические средства.

В отличие от предыдущего исследования, где отмечалось незначительное, но все же преобладание случайных утечек, в этом году финансовые организации склонны считать утечки в банках делом скорее умышленным.

Объем умышленных утечек от общего числа утечек, 2021 vs 2022



Мнения экспертов

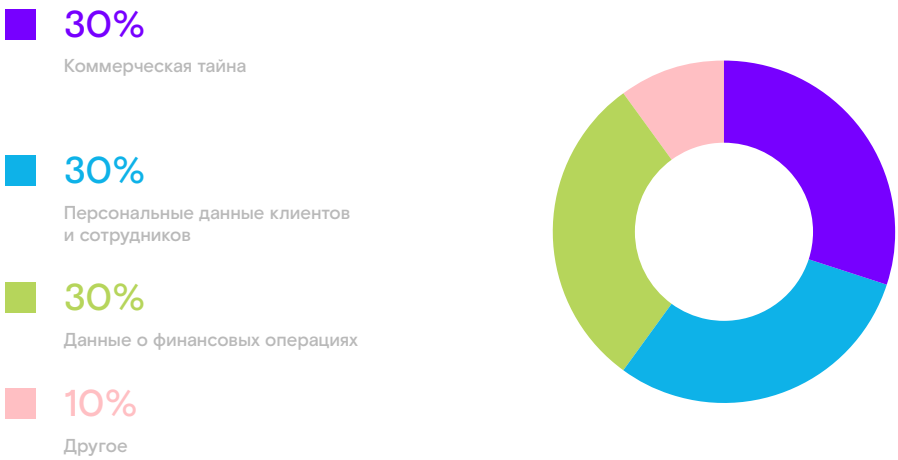
Сказывается специфика отрасли. Во-первых, здесь сотрудники работают с исключительно ценным активом – финансовой информацией людей: цена ошибки слишком высока, чтобы позволять ее себе в принципе. При этом, если в 2021 году 30% респондентов предполагали наличие скорее случайных, нежели умышленных, утечек, в актуальном исследовании доверчивых оптимистов не оказалось совсем, на преобладание умышленных утечек указывают 2/3 специалистов ИБ финансовых организаций. Во-вторых, свою роль играет и повсеместное внедрение в финансовом секторе DLP-систем, которые отлично справляются с защитой от случайных утечек.

Какие данные утекают

Утекающие данные по-прежнему отличаются большим разнообразием: здесь и сведения о финансовых операциях, и персональные данные клиентов, и материалы, классифицируемые как коммерческая тайна, инвестиционные планы, результаты маркетинговых исследований, внутренняя закупочная информация и др.

Среди подверженной риску информации увеличилась частота упоминания респондентами **коммерческой тайны:** с 10% ответов в 2021 году **до 30%** в текущем исследовании.

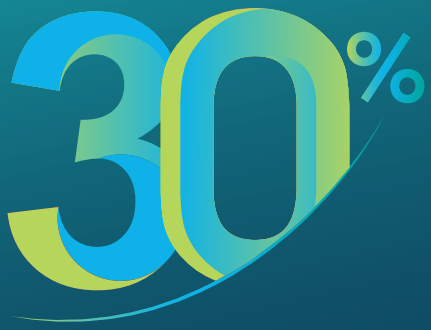
Виды утекающей информации



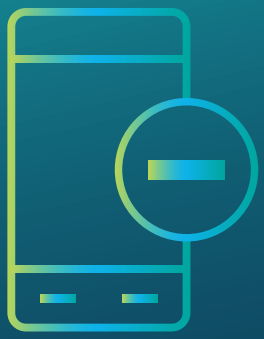
> **Мнения экспертов**
>
> На фоне ужесточившейся конкуренции на рынке финансовых услуг все более важной становится роль конкурентной разведки в маркетинговых войнах.

В этой связи у авторов исследования есть неприятные новости: в отличие от массивов клиентских/операционных данных (ФИО клиента, паспортные данные, номера карт/счетов и т. п.), единичными записями которых сложно заинтересовать нарушителей, информация из категории коммерческой тайны (презентации, выдержки из внутренних документов, неформальная переписка и др.) может быть вообще никак не структурирована. А значит, существенно усложняются алгоритмы выявления подобной информации с помощью DLP-системы в трафике всей организации, позволяющие вовремя заметить их несанкционированное и потенциально опасное распространение.

Единственный действенный совет в такой ситуации – уделять особое внимание вдумчивому описанию бизнес-процессов, в рамках которых возникает особо уязвимая для распространения вовне информация: целей и задач подразделений, участников, обладающих доступом к такой информации, возможных сценариев с указанием выгодоприобретателей от ее утечки, с последующей настройкой политики фильтрации трафика в DLP-системе.



Среди подверженной риску информации увеличилась частота упоминания респондентами коммерческой тайны: с 10% ответов в 2021 году до 30% в 2022 году.



В 2022 году ужесточилась позиция финансовых организаций – участников опроса на предмет использования на рабочем месте каналов коммуникации с внешним миром. Две трети респондентов считают обоснованным запрет на использование сотрудниками социальных сетей и мессенджеров.

Каналы утечек информации

Наиболее часто упоминаемым каналом утечек в финансовых организациях второй год подряд остается передача информации вовне с использованием веб-технологий: **облачных хранилищ, интернет-почты, веб-версий мессенджеров соцсетей (более 60% респондентов).**

> Мнения экспертов
>
> Корпоративная почта выпала из числа фаворитов: похоже, растет не только профессиональный уровень офицеров служб безопасности в борьбе с утечками, но и осведомленность злоумышленников о том, что их действия со служебной информацией контролируются – по крайней мере, на уровне официального почтового обмена.

Соответственно, для служб безопасности возрастает важность контроля широкого спектра каналов коммуникаций, хранения и передачи информации, помимо официального почтового трафика: веб-трафика, съемных носителей (в опросе встречаются примерно в **30% случаев**).

Больше в ответах не встречаются и десктопные версии мессенджеров среди потенциально рискованных каналов коммуникаций.

> Мнения экспертов
>
> Возможно, такая тенденция – следствие общей политики ужесточения использования внеслужебных онлайн-коммуникаторов на рабочих местах сотрудников. С другой стороны, это может быть связано и с активной заменой в 2022 году многими крупными российскими бизнесами иностранных средств онлайн-коммуникации на отечественные аналоги. В этом году на российском рынке появилось сразу несколько отечественных аналогов, контролировать которые используемые DLP-решения, возможно, пока не в состоянии. А ваша DLP-система контролирует Express, VKTeams и «Самовар»?

В 2022 году ужесточилась позиция финансовых организаций – участников опроса на предмет использования на рабочем месте каналов коммуникации с внешним миром. **Две трети респондентов считают обоснованным запрет на использование сотрудниками социальных сетей и мессенджеров.** В 2021 году сторонников ограничения таких коммуникаций было менее половины (44%).

> Мнения экспертов
>
> Возможно, это отражение общего тренда на ограничение внешних коммуникаций сотрудников в мессенджерах и социальных сетях, особенно ярко проявившегося в 2022 году в секторе государственного управления.

Выводы

При существующих трендах к усилению использования специальных систем для защиты от утечек информации эксперты «Ростелеком-Солар» ожидают, что размер фактического ущерба (в случаях, когда утечки все-таки будут происходить) стабилизировался и меняться не будет. С одной стороны, ухудшающаяся экономическая ситуация будет подталкивать злоумышленников искать новые способы заработка, с другой – будут развиваться возможности тех же DLP-систем вслед за изобретением новых технологий слива ценной информации.

Что касается соотношения случайных и умышленных утечек, при условии, что финансовые организации-работодатели будут последовательно ограничивать использование альтернативных рабочей почте каналов вывода информации и усиливать служебную дисциплину сотрудников (например, ограничивая возможность работать с домашнего оборудования), должна закономерно снижаться доля случайных утечек.

Отдельно следует сказать про эволюцию видов утекающей из финансовых организаций информации. В этом направлении аналитики «Ростелеком-Солар» не ожидают глобального изменения структуры утекающих данных. В финансовом секторе самым ценным активом всегда будут данные клиентов. Клиентов миллионы, случаев, в которых информация об этих клиентах может кому-то понадобиться, десятки. Частота утечек такого типа всегда будет выше – это статистически закономерно.

Ростелеком
Солар

rt-solar.ru
rt.ru

Email:

solar@rt-solar.ru
support@rt-solar.ru

Телефоны:

+7 (499) 755-07-70 - продажи и общие вопросы
+7 (499) 755-02-20 - техническая поддержка

Адреса

125009, Москва, Никитский пер., 7, стр. 1
127015, Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд