INFOWATCH®

аналитический отчет

ПРИЧИНЫ УТЕЧЕК ИНФОРМАЦИИ, ПРЕДСТАВЛЕНИЯ О РИСКАХ И НАПРАВЛЕНИЯХ УГРОЗ

Читайте материалы
экспертно-аналитического
центра InfoWatch

Оглавление

Только факты

Сокращения

Аннотация

Результаты исследования

- Причины утечек информации
- Оценка риска утечки данных
- Чему угрожают утечки информации

Заключение и выводы

Мониторинг утечек на сайте InfoWatch

Методика

Только факты

Среди главных причин утечек информации **44%** опрошенных назвали неумышленные действия персонала, **42%** — компьютерные атаки, **37%** — умышленные действия сотрудников.

✓ **Человеческий фактор в числе основных причин** утечек информации чаще всего называют представители организаций, в которых не было утечек.

✕ **На ошибки в настройках системы** в качестве основной причины утечек чаще всего указывают представители крупных компаний и государственных организаций.

Респонденты, **склонные считать основной причиной утечек умышленные действия**, чаще всего полагают, что к утечкам приводят совместные действия внутренних и внешних нарушителей — **32%** ответов.

Подавляющее большинство **(58%) уверенных в том, что к утечкам приводят неумышленные действия**, полагают, что утечки связаны с ошибками сотрудников.

40% опрошенных из числа оценивших риски утечек как несущественные считают, **что данные в их компаниях надежно защищены.**

67% из числа респондентов, считающих риски утечек несущественными, полагают, что **в их компаниях нет данных, которые могут заинтересовать** злоумышленников.

Примерно половина респондентов, оценивших риски утечек как умеренные, полагают, что системы безопасности в их компаниях требуют усиления, а некоторые данные могут представлять интерес для злоумышленников.

78% респондентов, оценивших риски утечек как значительные, считают, что **в их компаниях есть данные, представляющие интерес** для злоумышленников.

Более 50% участников опроса уверены, что утечки информации **угрожают деятельности** компании и ее репутации. При этом **48%** респондентов считают, что утечки информации в компании **несут угрозу ее клиентам.**

Сокращения

GDPR	General Data Protection Regulation (Регламент Евросоюза о ПДн от 27.04.2016 г., вступил в силу 25.05.2018 г.)
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ЭАЦ	Экспертно-аналитический центр ГК ИнфоВотч

Аннотация

Экспертно-аналитический центр ГК InfoWatch (ЭАЦ) представляет второй отчет из серии отчетов по результатам исследования на тему «Оценка ущерба от утечек информации в российских компаниях». Исследование по заказу InfoWatch проводилось в мае-августе 2024 г. независимой частной группой компаний ЦИРКОН, одним из старейших участников рынка социологических и маркетинговых исследований в России. В этом отчете приводятся результаты исследования, касающиеся мнений респондентов о причинах утечек конфиденциальной информации, осознании рисков, связанных с утечками данных, а также представлении руководителей и сотрудников о том, чему больше угрожают утечки данных.

Согласно методике исследования, люди, согласившиеся принять участие в опросах, могли выступать как от имени своей организации, так и занять «экспертную позицию», то есть отвечать в качестве независимых наблюдателей, обладающих (по их собственным словам) знаниями о проблемах информационной безопасности в разных организациях. Таким образом по ряду вопросов респонденты были разнесены по двум категориям, условно названным «представители организаций» и «эксперты».

В рамках исследования не рассматривались вопросы, связанные с утечками государственной тайны, изучался ущерб только от утечек конфиденциальной информации. Для этого в ходе подготовки перечней опрашиваемых организаций были исключены организации, относящиеся к органам государственной власти и управления, правоохранительным органам, вооруженным силам, оборонно-промышленному комплексу.

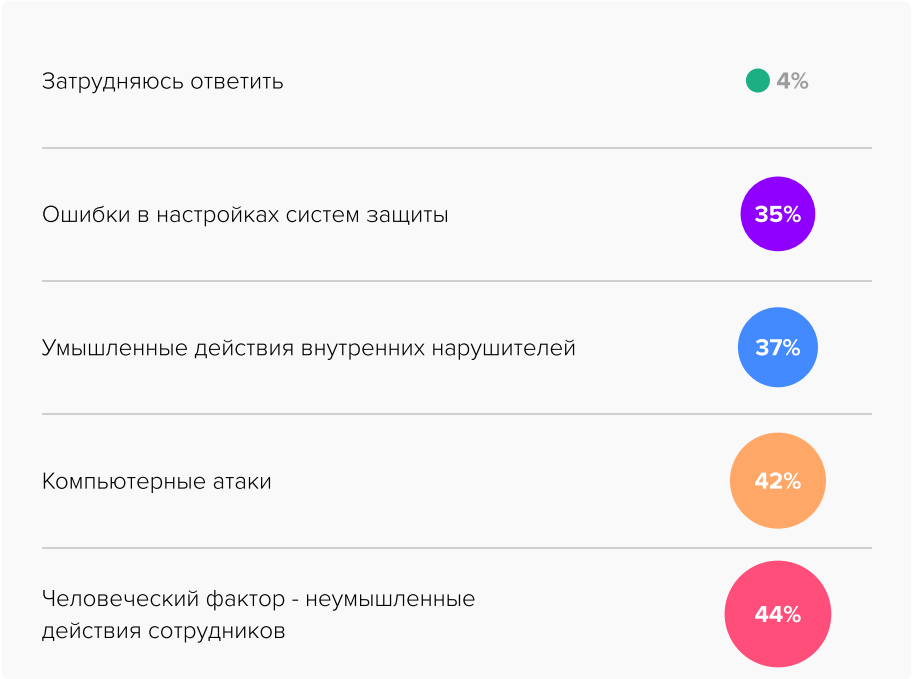
Исследование проблем ущерба основано на Методике сбора и обработки информации об ущербе, понесенном организациями в РФ вследствие утечек данных, о структуре ущерба, о величине и структуре затрат на восстановление после инцидента (разработана InfoWatch, зарегистрирована 31.07.2023 г. в Акционерном обществе «Национальный Реестр интеллектуальной собственности»).

Результаты исследования

Причины утечек информации

В ходе социологического исследования отдельное внимание было уделено опросу о причинах утечек информации в российских организациях. Явного лидера среди вариантов не оказалось. Наибольшая доля респондентов — 44% — заявили, что основной причиной являются неумышленные действия сотрудников (Рисунок 1). При этом 42% опрошенных выделили компьютерные атаки, а 37% — умышленные действия персонала компаний. Ошибки в настройках систем защиты назвали 35% ответивших.

Рисунок 1. «Уточните, пожалуйста, какие причины утечек информации были основными?» Отметьте вариант ответа, указывающий на главную причину. Возможен выбор нескольких вариантов ответа.



> *Примечание: неумышленные действия сотрудников, а также ошибки в настройке систем защиты (особенность построения вопросов в исследовании), могут быть причиной успешной реализации компьютерных атак.*
>
> *В случае, если системный администратор или сотрудник ИБ-подразделения умышленно неверно настроил систему защиты, не установил патч на уязвимость, передал данные об этом или аутентификационную информацию внешним нарушителям, то такие ситуации мы рассматриваем как гибридные атаки. Но в силу того, что подобная информация становится известной редко и обычно по результатам расследований, т.е. через год-два, такие случаи, как правило, попадают в статистику умышленных внешних атак.*

Авторы исследования отметили, что оценка основных причин утечек информации варьируется в зависимости от размера организации, которую представляет участник опроса. **Человеческий фактор как ключевую причину утечек чаще других отмечали представители малых организаций** (50% из них), руководители организаций (53%) и линейные сотрудники (60%), которым топ-менеджеры поручили отвечать на вопросы анкеты, а также сотрудники тех организаций, в которых за последние три года не было утечек информации (60%) и тех, где не проводится оценка ущерба от утечек информации (50%).

Компьютерные атаки в качестве основной причины утечек данных чаще называли респонденты из средних и крупных компаний (с числом сотрудников от 500 до 999 (43%) и от 50 до 249 человек (50%), а также представители головных отделений организаций (49%), сотрудники обособленных филиалов (48%) и тех компаний, в которых за последние три года случилось по одной утечке информации (46%).

Внутренних нарушителей главным источником утечек чаще видят сотрудники средних компаний (43%), сотрудники обособленных подразделений (41%), руководители и заместители руководителей подразделений информационной, экономической и финансовой безопасности (48%).

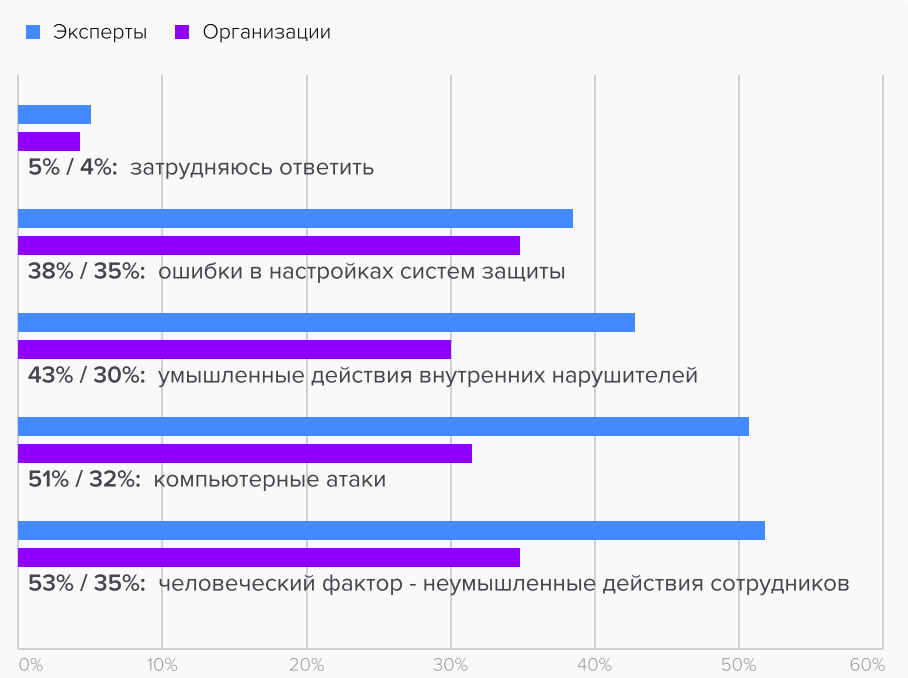
На ошибки в настройках системы защиты чаще указывают сотрудники крупных компаний и государственных организаций (55%), а также представители тех организаций, где за последние три года утечек информации не было (43%) или было от двух утечек (48%) и сотрудники, в чьих организациях применяется методика оценки от утечек (41%). **Можно отметить, что системами защиты информации чаще недовольны сотрудники крупных государственных организаций, обеспокоенные проблемой безопасности данных и компетентные в этом вопросе.**

Далее мнения о причинах утечек разделены по двум категориям респондентов — представителям организаций и участникам-экспертам*

> *К умышленным вариантам действий в опроснике исследования отнесены «умышленные действия внутренних нарушителей» (независимо от функциональной роли — рядовых сотрудников, технических специалистов, руководителей), а также «компьютерные атаки», то есть умышленные действия внешних нарушителей (хакеров). Соответственно, как варианты неумышленных нарушений рассматриваются «ошибки в настройках систем защиты» и «человеческий фактор - неумышленные действия сотрудников». Первый вариант здесь в основном относится к действиям технических специалистов, а второй - к действиям других категорий сотрудников.*

На Рисунке 2 показано распределение ответов представителей организаций и экспертов. Так, **эксперты существенно чаще выделяют проблемы утечек информации в результате неумышленных и умышленных действий персонала, а также в ходе компьютерных атак.** В то же время **для представителей организаций на первый план наряду с человеческим фактором вышли утечки из-за ошибок в настройках систем защиты.**

Рисунок 2. «Уточните, пожалуйста, какие причины утечек информации были основными?». «По вашему опыту, что чаще всего является причиной утечек информации в российских компаниях?». Отметьте вариант ответа, указывающий на главную причину. Возможен выбор нескольких вариантов ответа. Распределение ответов опрошенных от имени организаций и с позиций экспертов.



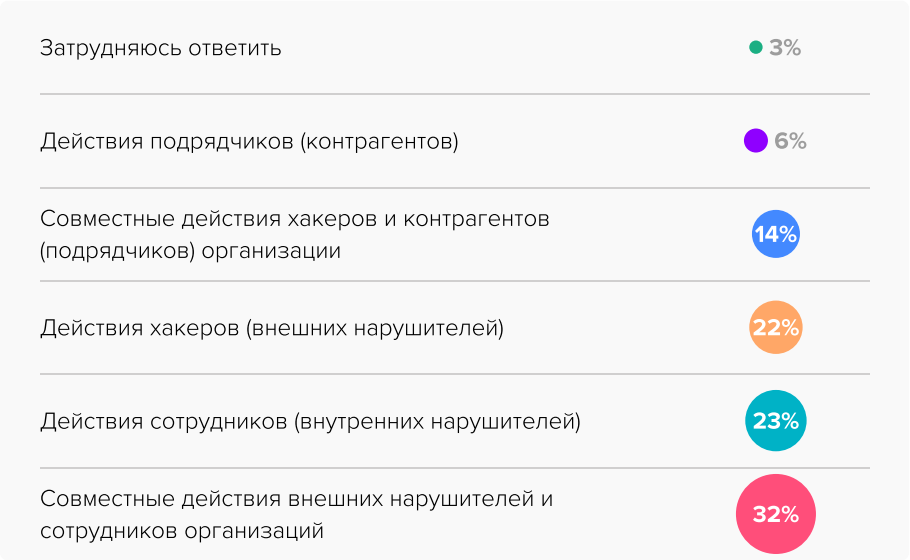
** Респонденты могли выступать как от имени своей организации, так и занять «экспертную позицию», то есть давать ответы в качестве независимых наблюдателей, обладающих (по их собственным словам) знаниями о проблемах информационной безопасности не только у нынешнего работодателя, но и в других организациях.*

При анализе ответов на этот вопрос специалисты исследовательской группы вновь подчеркнули отмеченную ранее закономерность: эксперты старались обобщать свою позицию, поэтому чаще выбирали несколько вариантов ответов или даже все варианты, в то время как большинство представителей организаций ограничились выбором одного-двух вариантов.

Умышленные действия как причины утечек информации

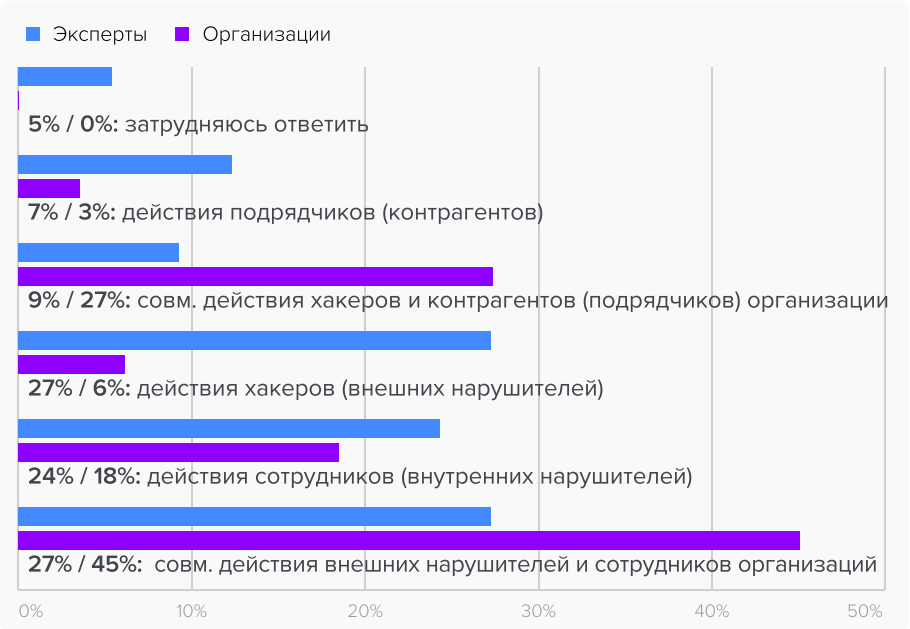
Респонденты, которые склонны считать, что к утечкам чаще приводят умышленные действия, чаще говорили о совместных действиях сотрудников и внешних нарушителей (32%) — см. Рисунок 3. Реже всего в качестве источника умышленных утечек участники опроса называли контрагентов (6%). Отметим, что при ответе на этот вопрос можно было выбрать только один вариант.

Рисунок 3. «Чьи умышленные действия стали причиной утечки?» Доли ответов тех респондентов, которые считают, что основными



Отметим, что совместные действия хакеров с контрагентами или сотрудниками дают 46% ответов всей группы респондентов о причинах утечек в случае умышленных действий. Однако, мнения на этот счет расходятся: почти половина (45%) опрошенных из организаций основной причиной утечек называют совместные действия внутренних и внешних нарушителей, в то время как среди тех, кто принял экспертную позицию, такого мнения придерживаются только 27%, **хотя для обеих категорий эта причина является главной.** Респонденты в целом реже называли основными виновниками утечек умышленного характера сотрудников (24%), но среди представителей организаций такое мнение ещё менее популярно - его озвучили только 18% ответивших в этой категории (см. Рисунок 4).

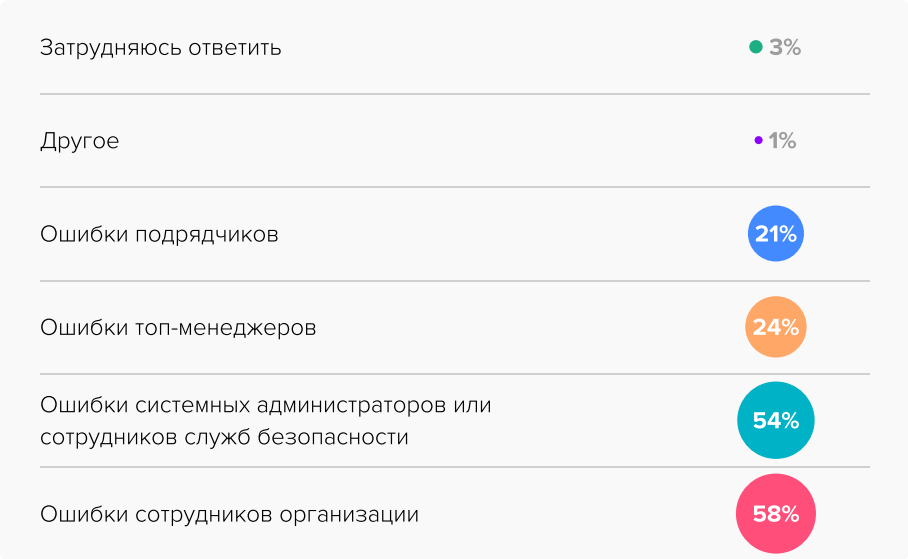
Рисунок 4. «Чьи умышленные действия стали причиной утечки?» - «Чьи умышленные действия чаще всего становятся причиной утечки в российских компаниях, похожих на вашу?» Доли ответов от тех, кто отметил, что основными причинами утечки являются умышленные действия. Сопоставление ответов опрошенных от имени организаций и с позиций экспертов.



Неумышленные действия как причины утечек информации

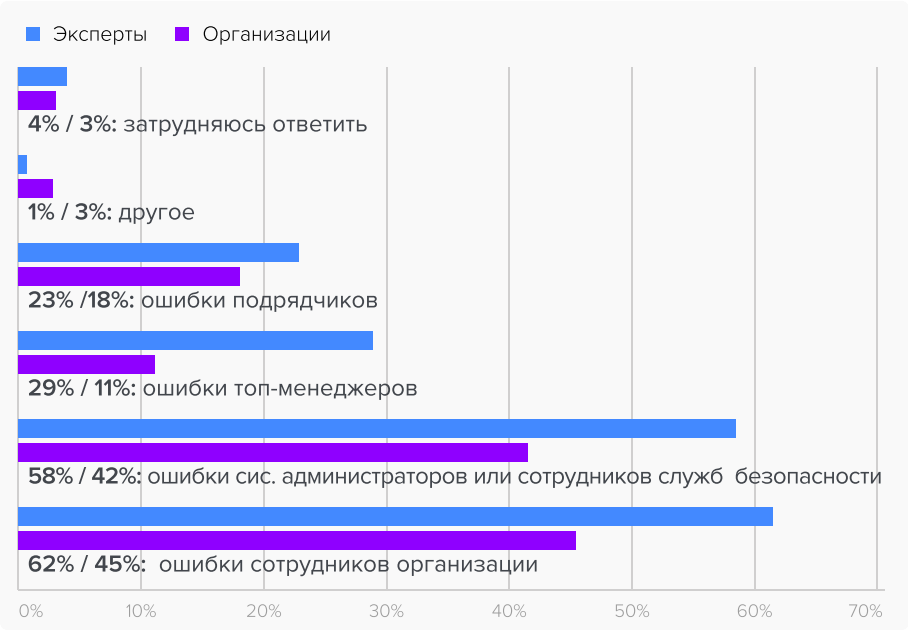
Среди участников опроса наиболее распространено мнение о том, что к утечкам информации чаще всего приводят неумышленные действия персонала. Подавляющее большинство (58%) респондентов с такой позицией уверены, что данные утекают из-за ошибок сотрудников (Рисунок 5).

Рисунок 5. «Чьи ошибки (неумышленные действия) стали причиной утечки? Отметьте все варианты ответов». Ответы тех, кто отметил, что основными причинами утечек информации являются неумышленные действия



Из диаграммы на Рисунке 6 можно заметить, что наибольшая доля опрошенных считают, что чаще всего к утечкам информации приводят неумышленные действия сотрудников. Чуть меньше респондентов полагают, что к утечкам приводят ошибки со стороны технических специалистов и сотрудников СБ, то есть ответственность респонденты возлагают на тех, кто настраивает системы безопасности и занимается их эксплуатацией (это также неумышленные действия, но такой вариант выделен в связи с методикой исследования).

Рисунок 6. «Чьи неумышленные действия стали причиной утечки? Отметьте все подходящие варианты ответов» или «Чьи ошибки чаще всего становятся причиной утечек в российских компаниях? Отметьте все подходящие варианты ответов». Ответы тех, кто отметил, что основными причинами утечек являются неумышленные действия. Сопоставление ответов опрошенных от имени организаций и с позиций экспертов.



Таким образом, по результатам анкетирования, можно представить два основных сценария, в результате которых случались утечки информации в компаниях:

- «невнимательность в работе сотрудника»;
- «ошибки в действиях технического специалиста».

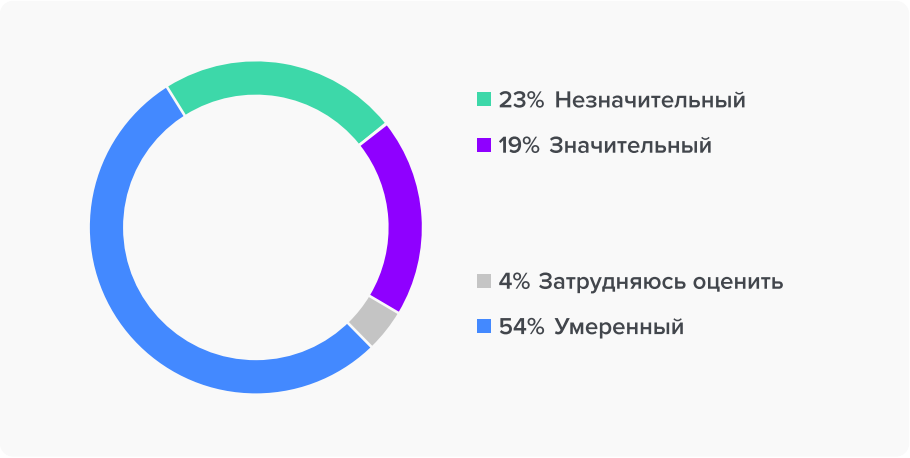
В первом сценарии, который наиболее распространен, утечка данных происходит в результате неумышленных действий персонала, например, когда сотрудники переходят по вредоносным ссылкам, отправляют письма по некорректным адресам электронной почты или иным способом непреднамеренно компрометируют информацию. Второй сценарий является менее распространенным. Он тоже предполагает неумышленные действия, но уже со стороны тех, кто настраивает системы безопасности данных. Из-за некорректных настроек системного администратора (оператора) система может оказаться неспособной противостоять угрозам. Возможные причины – от невнимательности до отсутствия нужной квалификации, а также высокой загрузки сисадминов.

> *По результатам опроса, проведенного в конце 2023 года и начале 2024 года экспертно-аналитическим центром ГК InfoWatch при участии «Код ИБ», 67% респондентов назвали риск утечек по вине сотрудников наиболее актуальным среди ожидаемых рисков 2024 года.*
>
> *Согласно исследованию латентности утечек информации (о сокрытии фактов утечек), проведенному в 2023 году ЭАЦ InfoWatch, респонденты сообщали, что как минимум 75% утечек данных в их компаниях произошли по вине действующих и бывших сотрудников.*

Оценка риска утечки данных

Большинство респондентов довольно оптимистично оценивают вероятность наступления в их компаниях инцидентов, связанных с кражами или потерями конфиденциальных данных (Рисунок 7). Около 54% опрошенных считают риски таких инцидентов умеренными, а 23% — незначительными. Только примерно каждый пятый участник исследования оценивает риски компрометации данных своей компании как значительные.

Рисунок 7. «Как вы оцениваете риск того, что ваша организация столкнется с кражей или потерей данных?» Доли ответов от всех опрошенных.



Исследование показало, что за сохранность данных больше всего опасаются представители крупных организаций (штатная численность от 1000 сотрудников). Из этой категории опрошенных 40% считают риск утечки информации из своих организаций значительным.

В небольших компаниях, напротив, чаще оценивают риск утечки данных как незначительный. Респонденты из организаций такого масштаба риск утечек считают незначительным в 29% ответов. Представители коммерческих компаний оценивают риск значительным чаще, чем респонденты из государственных организаций.

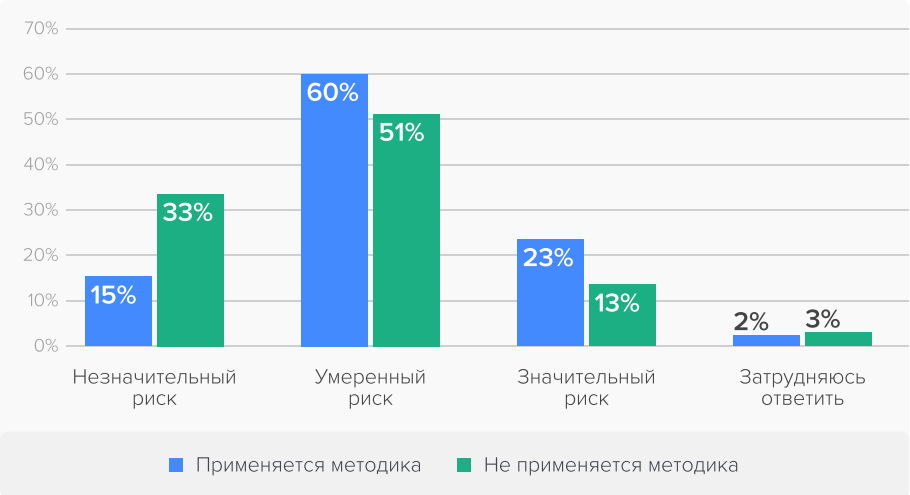
> *В то же время исследования ЭАЦ показывают, что фокус утечек данных сместился в сторону малых и средних компаний. На долю организаций с количеством сотрудников до 500 пришлось 68% утечек информации, случившихся в I полугодии 2024 года.*

Что касается должностной принадлежности респондентов, **наибольший уровень тревоги в отношении безопасности информации демонстрируют специалисты подразделений информационной, экономической и финансовой безопасности** - 33% опрошенных в этой категории считают риск утечек в их организациях значительным. В то же время можно назвать крайне осторожной позицию тех, кто отвечал на вопросы анкеты по поручению руководства. В этой категории 34% опрошенных отметили, что риск утечки данных незначительный, что может говорить либо о низкой осведомленности таких сотрудников о проблемах ИБ, либо отражает опасения откровенно говорить о проблемах, пусть даже с санкции руководства.

Среди опрошенных, которые представляют компании, пережившие две утечки информации за последние три года, вероятность новой утечки как незначительную оценивают 27%. Вероятно, это связано с тем, что во многих подобных организациях после инцидентов ИБ были приняты меры по минимизации рисков возникновения утечек информации в будущем. Организации, пережившие более двух утечек информации, в 68% ответов оценивают риск как умеренный.

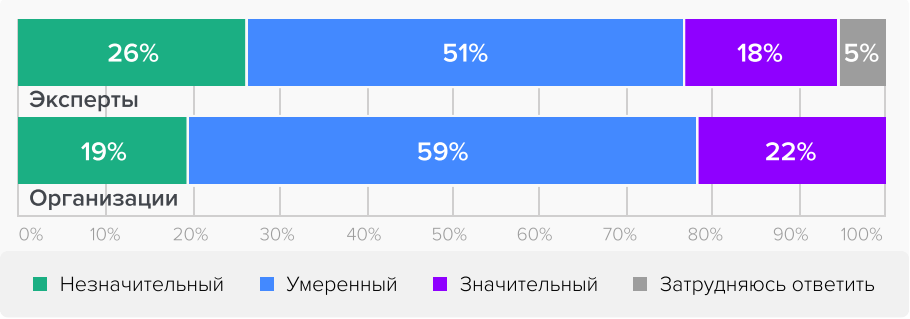
Ответы на вопросы о рисках утечек информации были проанализированы и в разрезах наличия и отсутствия методики оценки ущерба от утечек. Выяснилось, что **риски утечек данных как несущественные намного чаще оценивают опрошенные, которые представляют организации, где нет методики оценки ущерба от утечек.** А те, кто заявил о наличии подобной методики в своих организациях, напротив, чаще оценивают риски утечек информации как значительные (Рисунок 8). Такое отношение может быть связано с тем, что в организациях, обладающих методикой оценки ущерба от инцидентов, связанных с утечками данных, более объективно оценивают риски и не склонны «почивать на лаврах» даже при отсутствии инцидентов.

Рисунок 8. «Как вы оцениваете риск того, что ваша организация столкнется с кражей или потерей данных?» Доли ответов опрошенных в зависимости от применения методики оценки ущерба от утечек информации.



Респонденты, которые отвечали на вопросы анкеты с позиций экспертов, чаще склонны считать риски утечек данных незначительными (Рисунок 9).

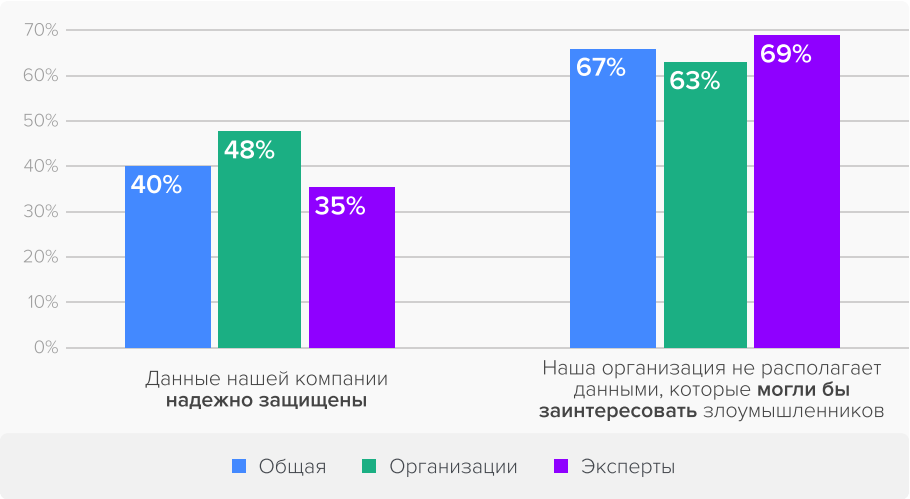
Рисунок 9. «Как вы оцениваете риск того, что ваша организация столкнется с кражей или потерей данных?» Сопоставление ответов представителей организаций и ответов респондентов с экспертной позицией.



При этом большинство опрошенных считают, что риски утечки данных умеренные. Среди представителей организаций значительным риск утечек информации чаще считают сотрудники обособленных подразделений (31%), а также руководители и заместители руководителей (30%). Среди экспертов риск утечек значительным чаще считают сотрудники обособленных подразделений (31%) и руководители с их заместителями (39%).

Самый распространенный аргумент, который респонденты приводили в пользу того, что утечка данных в их организациях маловероятна, - это отсутствие данных, которые могли бы заинтересовать злоумышленников. Так считают 67% тех, кто уверены в маловероятном наступлении подобных инцидентов (Рисунок 10). При этом еще более популярно такое мнение среди представителей малых организаций — 75% ответивших. О том, что утечка данных маловероятна благодаря наличию надежной системы защиты, чаще заявляют респонденты из крупных организаций — 63% ответивших. Здесь есть некоторое противоречие с высокой оценкой рисков со стороны представителей крупных компаний. Вероятно, многие из них считают внедренные решения достаточно эффективными в краткосрочной перспективе, но, обладая довольно глубокими знаниями в области ИБ, понимают, что через некоторое время уровень угроз может существенно вырасти. При этом пока многие специалисты могут сомневаться в том, успеют ли вендоры и интеграторы в сфере информационной безопасности своевременно отреагировать на новые угрозы.

Рисунок 10. «Вы оценили риск утечек в вашей организации как несущественный. Поясните, пожалуйста, почему вы дали такую оценку. Можете выбрать подходящий ответ или написать свой». Доли респондентов, считающих, что риск утечек незначительный, а также сопоставление ответов представителей организаций и ответов респондентов с экспертной позицией.



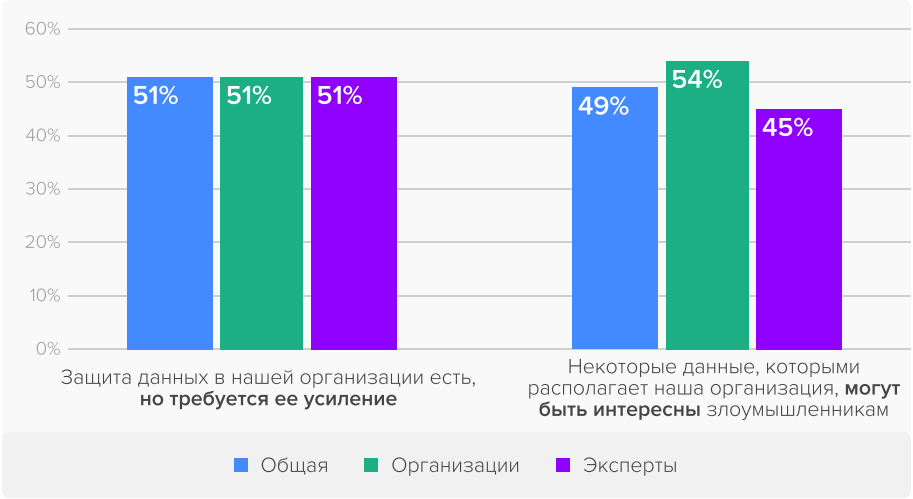
Интересно, что чаще других интерес злоумышленников к своим данным оценивается как низкий сотрудниками промышленных предприятий, а также экспертами, которые работают в сфере HoReCa.

> *Но в отраслевом распределении утечек информации пока доля утечек в промышленных компаниях сравнительно невелика. По данным экспертноаналитического центра InfoWatch, в 2023 году она составила 3,9%. В то же время совокупная доля организаций торговли, туризма, гостеприимства и общественного питания (HoReCa входит в эту отраслевую группу) в распределении утечек составила 24,5%. Поэтому можно сказать, что представители компаний из сферы HoReCa сильно недооценивают риски утечек информации.*

Для тех респондентов, которые оценивают риск утечки данных в своих организациях как умеренный, одинаково актуальны оба аргумента: 51% считают, что существующая система ИБ требует усиления, а 49% уверены, что некоторые данные, которым располагает их организация, могут быть интересны злоумышленникам (Рисунок 11). Отметим, что представители организаций и респонденты с экспертной позицией при ответе на этот вопрос проявили единодушие. Большинство участников отметили оба варианта ответа.

По мнению исследователей, это может говорить о существовании в компаниях довольно сильного запроса на внедрение более надежных инструментов защиты информации, независимо от размера, формы собственности организаций и используемых в них технологий.

Рисунок 11. «Вы оценили риск утечек в вашей организации как умеренный. Поясните, пожалуйста, почему вы дали такую оценку. Можете выбрать подходящий ответ или написать свой». Доли респондентов, считающих, что риск утечек умеренный, а также сопоставление ответов представителей организаций и ответов респондентов с экспертной позицией.

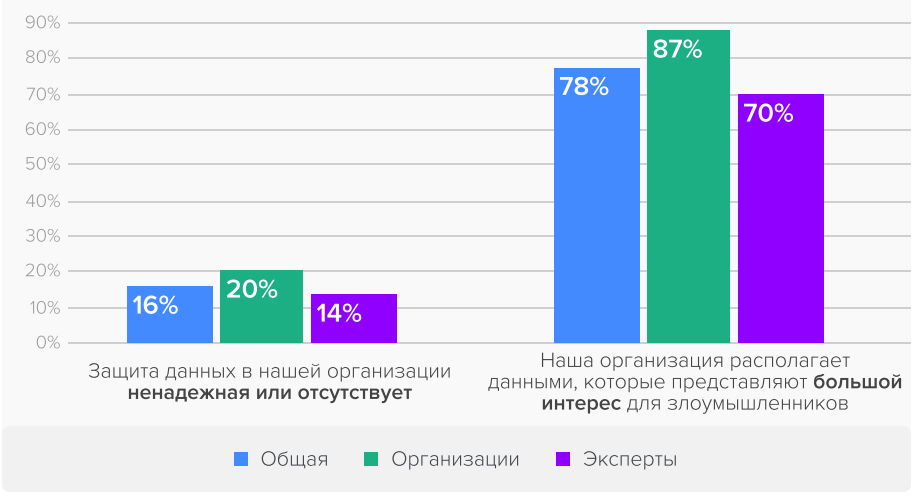


Потребность в совершенствовании систем защиты информации чаще всего выражают сотрудники из организаций среднего размера (от 250 до 499 сотрудников — 64% ответивших), а также сотрудники обособленных подразделений компаний (56%), специалисты финансовых и юридических подразделений (58%), сотрудники организаций, в которых не было утечек в последние три года (60%) и представители организаций, в которых ущерб от утечек оценивают лишь в общих чертах (68%).

О том, что организации, в которых они работают, располагают потенциально интересными для злоумышленников данными, чаще беспокоятся сотрудники средних организаций (52%), сотрудники головных отделений (60%), государственных организаций (60%), специалисты подразделений информационной, экономической и финансовой безопасности (58%), а также сотрудники организаций, в которых ущерб от утечек информации не оценивают (80%).

Оценивая риск утечек данных как значительный (существенный), в качестве основной причины 78% респондентов отмечают наличие данных, которые представляют интерес для злоумышленников (Рисунок 12). О недостаточно надежной системе защиты данных сообщили 20% представителей организаций, которые оценивают риск утечек как значительный. В этой группе больше представителей частных организаций, в которых не применяется оценка ущерба от утечек. Процентные данные о распределениях, касающиеся этой группы респондентов, не приводятся ввиду ее малочисленности.

Рисунок 12. «Вы оценили риск утечек в вашей организации как значительный. Поясните, пожалуйста, почему вы дали такую оценку. Можете выбрать подходящий ответ или написать свой». Доли респондентов, считающих, что риск утечек значительный, а также сопоставление ответов представителей организаций и ответов респондентов с экспертной позицией.



О наличии данных, представляющих большой интерес для злоумышленников, чаще сообщают респонденты, представляющие: головные отделения организаций (84%), организации, в которых случались утечки (89%), организации, в которых применяется методика оценки ущерба от утечек информации (93%).

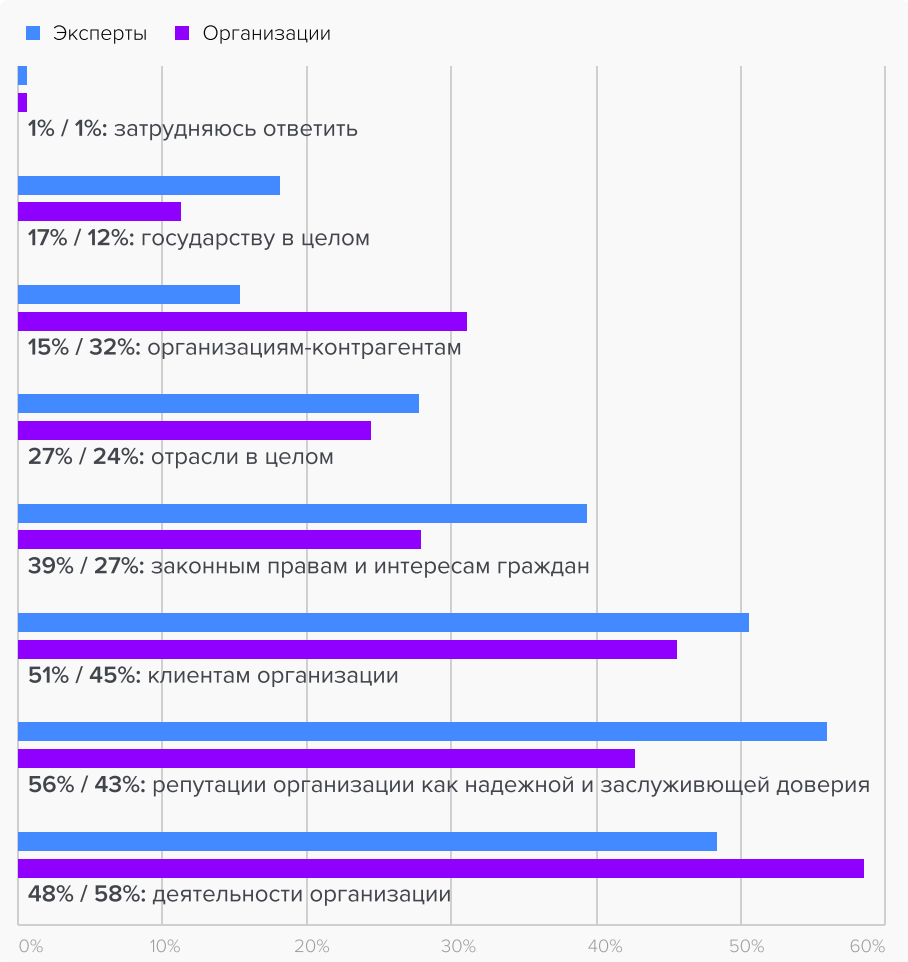
Чему угрожают утечки информации

Ущерб от утечек информации в представлении респондентов в основном является локальным и состоит в угрозе деятельности организации, ее репутации и персональным данным клиентов (Рисунок 13). Полученное распределение указывает на то, что респонденты воспринимают утечку информации как быстрый инцидент, требующий решения «здесь и сейчас» (ad hoc), программного или технического. То есть **респонденты не рассматривают утечку как системную проблему, касающуюся отрасли и государства в целом и требующую планомерного выстраивания системы мер для ее решения.**

Рисунок 13. «Чему, как правило, угрожают утечки информации? Выберите три наиболее существенные угрозы». Распределение ответов от всех опрошенных.

Можно отметить, что в оценке направленности основных угроз представители организаций и эксперты сходятся. Ярко выраженное исключение заключается в том, что **среди опрошенных респондентов из организаций вдвое выше доля тех, кто считает, что утечки данных в первую очередь угрожают контрагентам** (Рисунок 14). В то же время среди экспертов существенно больше тех, кто полагают, что утечки несут основную угрозу репутации компании и законным правам граждан.

Рисунок 14. «Чему, как правило, угрожают утечки информации? Выберите три наиболее существенные угрозы». Распределение ответов от всех опрошенных.



Таким образом, респонденты довольно серьезно относятся к последствиям утечек информации в организациях, в которых они работают, и в основном считают, что такие инциденты в первую очередь негативно сказываются на организации и ее интересах, а не на обществе в целом.

Заключение и выводы

Представления о причинах утечек информации существенно различаются в зависимости от размера компании, типа подразделения, должности респондента, а также от того, случались ли в компании утечки. Так, компьютерные атаки ключевой причиной утечек называли 56% респондентов из крупных компаний и 50% из небольших компаний, а также 49% сотрудников головных подразделений и 48% представителей филиалов, 46% сотрудников тех компаний, в которых за последние три года не было зарегистрировано утечек информации.

Внутренних нарушителей в качестве основных источников утечек данных называли 43% респондентов, работающих в средних компаниях, 41% сотрудников обособленных подразделений, а также 48% руководителей и заместителей руководителей подразделений информационной, экономической и финансовой безопасности.

Два основных сценария, которые, по мнению респондентов, привели к утечкам информации по вине внутреннего нарушителя, — это «ошибка сотрудника» и «ошибка технического специалиста».

Сценарий «ошибка сотрудника» наиболее распространен и предполагает, что утечка информации произошла в результате неумышленных действий сотрудника организации, который перешел по вредоносной ссылке, отправил данные по неверному адресу электронной почты или иным способом непреднамеренно скомпрометировал данные. Принимая во внимание этот сценарий, организации готовы инвестировать в обучение сотрудников. Как правило, эта мера быстро дает положительный эффект.

> *В отчете об утечках информации ограниченного доступа в России за 2022-2023 годы приведены результаты опроса по поводу мер, которые предприняли организации по обеспечению информационной безопасности в 2023 году. В ходе опроса* ***59% участников сообщили, что их организации провели обучающие мероприятия по ИБ и информационной гигиене.***

Сценарий «ошибка технического специалиста» менее распространен, но тоже представляет серьезную опасность. Он предполагает ошибки при настройке системы ИБ, в результате которых она оказалась не в состоянии противостоять угрозам (компьютерным атакам, возможности несанкционированного копирования данных и т.п.). Масштабы подобных нарушений зачастую весьма велики, поэтому подобный сценарий является нишей для продвижения отдельного класса программных решений.

Недооценка рисков утечек данных характерна для небольших организаций, которые не обеспечивают надежную защиту данных и не сталкивались с утечками прежде, что выражается в отсутствии методики оценки ущерба от утечек информации и в целом в более беспечном отношении к проблеме, чем у крупных компаний. Вероятно, отчасти из-за этого в последнее время доля утечек, приходящихся на малые организации, существенно выросла.

Наиболее остро риски утечек осознают представители государственных организаций, крупных компаний, те, кто неоднократно сталкивался с утечками информации, а также специалисты из сферы информационной безопасности.

Более 50% участников опроса уверены, что утечки информации угрожают деятельности компании и ее репутации. При этом 48% респондентов считают, что утечки информации в компании несут угрозу ее клиентам.

Для большинства респондентов (а это те, кто оценивают риски утечек информации как умеренные) одинаково остро стоят вопросы надежной и эффективной системы обеспечения безопасности данных и специфики деятельности организации, поскольку они располагают конфиденциальной информацией довольно чувствительного характера, которая может быть интересна злоумышленникам.

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.
Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

РАССЫЛКА INFOWATCH /infowatchout /infowatch

Методика

Исследование проводилось по заказу компании InfoWatch на базе методики сбора и обработки информации об ущербе, понесенном организациями в РФ вследствие утечек данных (информации), о структуре ущерба, о величине и структуре затрат на восстановление после инцидента (зарегистрирована 31.07.2023 г. в Акционерном обществе «Национальный Реестр интеллектуальной собственности»).

Объект интеллектуальной собственности может быть предоставлен Депоненту на основании заявления или по запросу органов государственной власти.

В рамках исследования был проведен опрос экспертов-представителей российских организаций. Опрос проводился в формате онлайн. Опросный инструментарий позволял участникам отвечать как от имени организации, в которой он или она работают, отражая в ответах опыт данной организации, так и занять экспертную позицию и отвечать на вопросы в целом, опираясь на собственный профессиональный опыт в целом.

При обработке данных ответы от имени организаций и экспертные ответы были и проанализированы отдельно, и объединены для совместного анализа. При обработке данных был проведен частотный анализ и анализ совместных частотных распределений полученных данных, результаты аналитической работы по интерпретации данных приведены в настоящем отчете.