Аналитический отчет

Оценка ущерба вследствие утечек информации

Оглавление

Сокращения

АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ЭАЦ	Экспертно-аналитический центр ГК InfoWatch

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch представляет отчет по результатам исследования оценки ущерба вследствие утечек информации.

Для отчета использованы материалы анонимного опроса, проведенного путем целевых и массовых рассылок от имени группы компаний InfoWatch и Ассоциации по защите деловой информации (BISA).

Опрос проводился в июле 2023 г. Основную долю респондентов составили специалисты из промышленного сектора.

Только факты

- → Основными участниками опроса стали крупные частные или государственные организация из промышленного сектора.
- → Каждая пятая из опрошенных организаций, в которой внедрена система DLP, — это крупное частное предприятие из сферы производства.
- → Треть организаций столкнулись с утечками информации за последние 3 года.
- → Почти у половины организаций отсутствует методика по оценке ущерба от утечки информации. Кроме того, большинство организаций не застрахованы от ущерба.
- → Чаще всего подвергались компрометации персональные данные, а размер сумм ущерба от их потери превышал 1 млн. рублей.
- → Внутренний нарушитель представляет наибольшую угрозу компрометации данных.
- → В подавляющем большинстве случаев (70%) утечка данных является следствием умышленных действий.
- → 79% случаев утечек произошли по вине внутреннего нарушителя. В большинстве случаев нарушения со стороны персонала имели умышленный характер.

Проблематика вопросов оценки ущерба от утечек информации

Утечки информации ограниченного доступа несут для пострадавшей организации угрозу причинения различных видов ущерба — от материального до репутационного. В современной практике ИБ проблема в отношении оценки ущерба от утечек информации заключается в отсутствии проверенных и экономически обоснованных методик, которые позволили бы объективно и комплексно оценить ущерб и структуру понесенных затрат, а на основании полученных данных подготовить оценку рисков ущерба и финансово-экономическое обоснование для создания и эксплуатации системы защиты от утечек информации.

На зарубежном рынке исследованием ущерба от утечек данных регулярно занимается Ponemon Institute при финансовом содействии корпорации IBM. Согласно последним данным из отчета «Cost of a Data Breach Report 2023», средний ущерб после утечки (в целом по вине внешнего и внутреннего нарушителя) составил $4,5 млн, что на 15% выше, чем три года назад. Отдельно стоит отметить, что ущерб от утечки по вине внутреннего нарушителя выше — сумма потерь в таком случае составила $4,9 млн. В совместном отчете компаний Proofpoint и Ponemon Institute отмечается, что для пострадавшей организации средняя стоимость кражи учетных данных в результате действий внутреннего нарушителя составила $4,6 млн, а утечка из-за халатности работника (неумышленная) обошлась в среднем в $6,6 млн.
Таким образом, затраты на обнаружение и ликвидацию последствий утечки по вине внутреннего нарушителя обходятся организации дороже, чем комплекс реагирования на утечки в результате хакерских атак.

При этом ущерб от инцидентов информационной безопасности может затрагивать не только отдельные организации, но и целые города. Так, по недавним сообщениям СМИ, городской совет Далласа выделил из бюджета города $8,6 млн на оплату услуг ИБ-компаний, участвовавших в восстановлении информационной инфраструктуры города после кибератаки. Используя программу-вымогатель, злоумышленники украли персональные данные 26 тыс. человек.

В то же время структура затрат, статьи финансового учёта, размеры оплаты услуг и штрафов в США, Канаде, странах Евросоюза значительно отличаются от российских, поэтому приводимые в зарубежных отчетах данные практически не соотносятся с российскими реалиями. В связи с этим ГК InfoWatch разработала и зарегистрировала собственную методику сбора информации для оценки ущерба от утечки информации, которая частично использована в данном исследовании.

Результаты исследования

В ходе опроса респондентам были заданы вопросы о фактах утечек информации ограниченного распространения из их организаций, о наличии методик оценки ущерба и страховании рисков утечек данных, о размере ущерба, о видах «утекшей» информации, о каналах и причинах утечек, а также о наличии в организации системы защиты информации от утечек из ИС/АС.

Портреты организаций

Наиболее часто встречаемый тип организации из тех, которые представляли респонденты, — это крупное частное или государственное предприятие из промышленного сектора.

По размеру организации (см. Рисунок 1):

- более половины (53%) организаций, принявших участие в опросе, являются крупными, со штатом свыше 500 человек;
- 35% участников опроса представляли средние компании;
- 12% респондентов работали в малых компаниях.

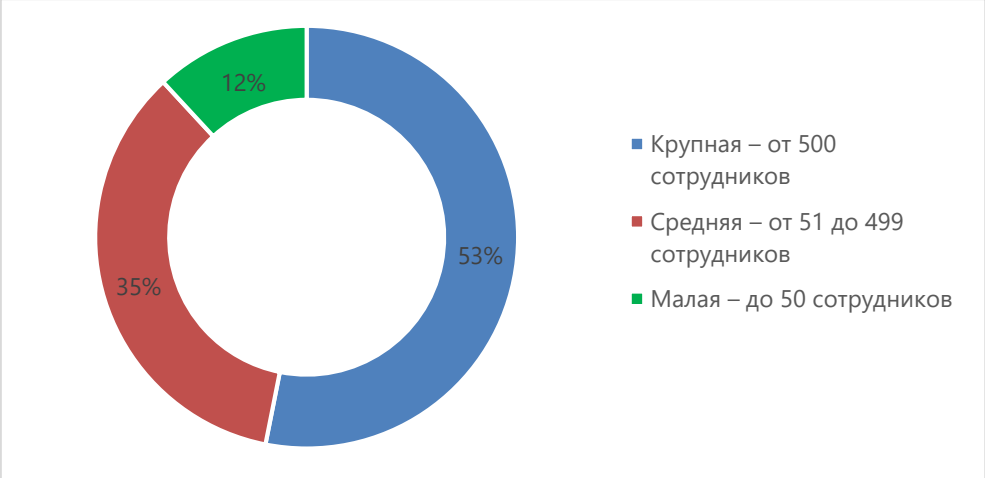

Рисунок 1. Доли респондентов по размеру представляемой организации

В отраслевом разрезе наибольшая доля респондентов представляла организации из двух секторов: промышленность, информационные технологии и информационная безопасность.

В опросе также приняли участие представители госсектора, ТЭК и других секторов экономики (см. Рисунок 2).

Рисунок 2. Отраслевая принадлежность организаций, участвующих в опросе.

Организации частной формы собственности представляют более половины (52%) участников опроса. На втором месте государственный сектор (31%) — см.Рисунок 3.

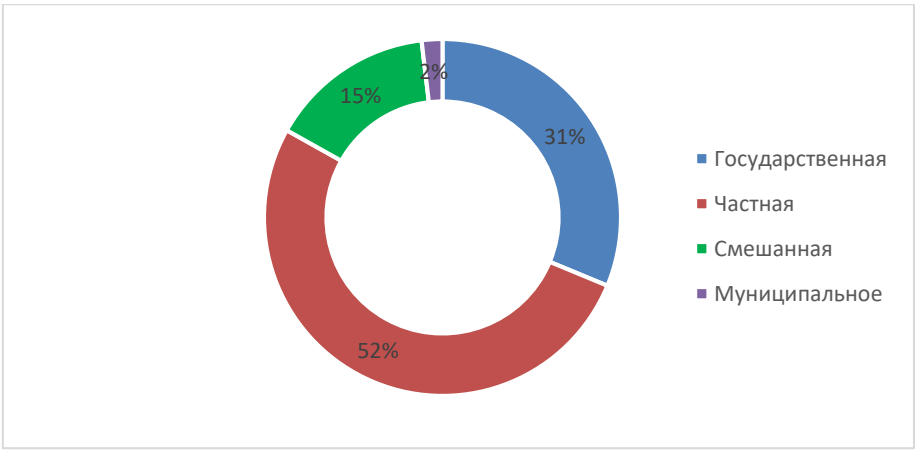

Рисунок 3. Форма собственности организаций, которые представляли участники опроса.

Исходя из функциональных обязанностей, наибольшую долю опрошенных составили специалисты ИБ — 46%, следующую по величине долю занял топ-менеджмент компаний — 14%.

Специалисты ИТ составили 9% респондентов, а специалисты по экономической безопасности — 8%. Подробнее на Рисунке 4:

Рисунок 4. Роли респондентов в организациях

В результате опроса выяснилось, что DLP-системы внедрены почти у половины организаций (48%):

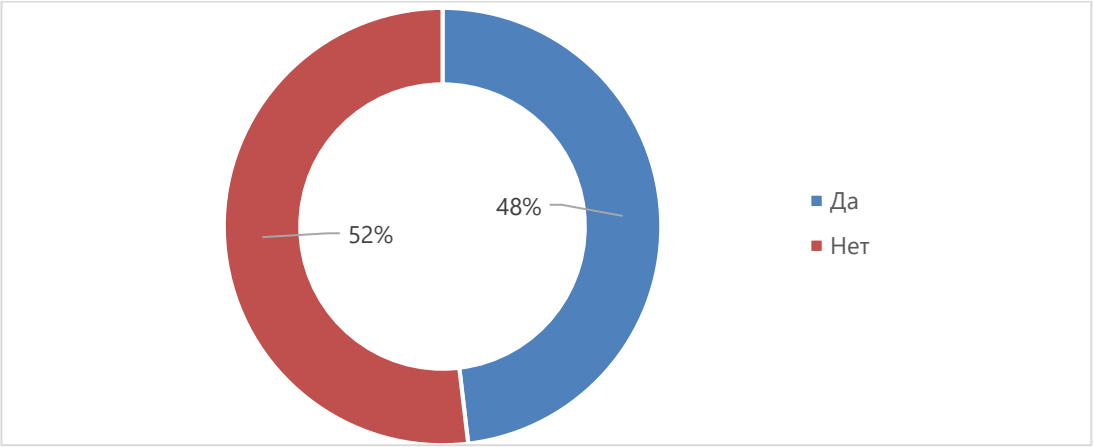

Рисунок 5. В вашей организации внедрена DLP-система?

Распределение организаций-респондентов по отраслевой принадлежности приведено на Рисунке 6, а по размеру и форме собственности — на Рисунке 7.

В ходе исследования выяснилось, что самый распространенный тип организации, в которой внедрена система DLP, — это крупное частное предприятие из сферы производства (почти каждая пятая компания).

Рисунок 6. Организации, в которых внедрены DLP-системы. По отраслям

Следом за производством и промышленностью идут организации из ИТ и ИБ — доля 18%. Третье место занимает образование — 12%. Банки и финансовые услуги представляют 10% участников опроса.

Согласно рисунку 7, **DLP-системы в подавляющем числе случаев внедрены в крупных организациях, их доля составила 77%**. Средние организации составили 19%, а малые только 4%. Исходя из формы собственности, системы предотвращения утечек внедрены в основном в частных организациях — 56%.

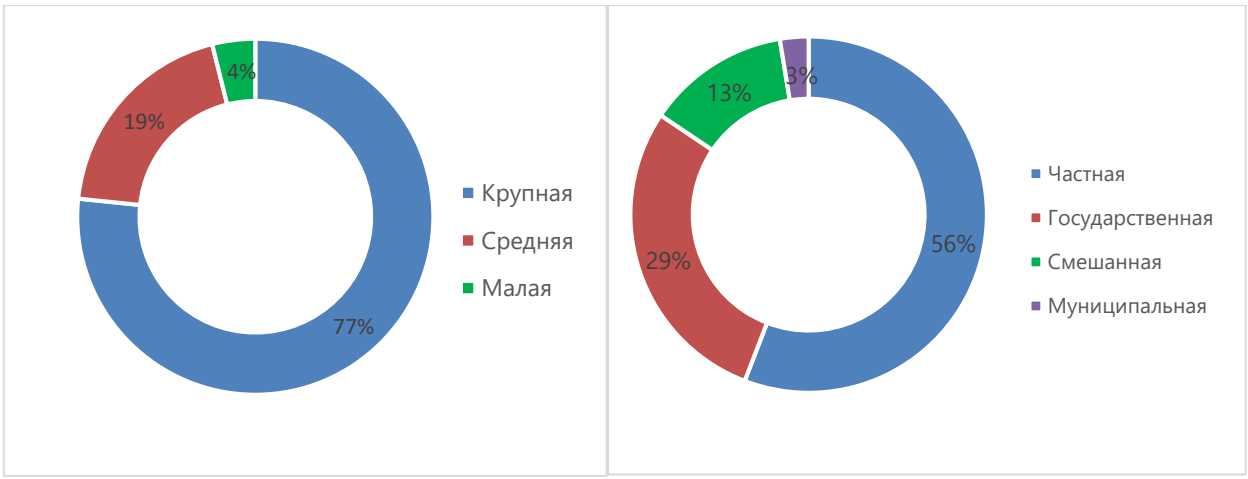

Рисунок 7. Организации, в которых внедрены DLP-системы. По размеру компании и форме собственности

Также участникам исследования было предложено ответить на вопрос о том, случались ли в их организациях утечки информации.

- **27% организаций столкнулись с фактами утечки информации за последние 3 года,**
- **48% ответили, что их организации с утечками не сталкивались**,
- 25% затруднились ответить на данный вопрос.

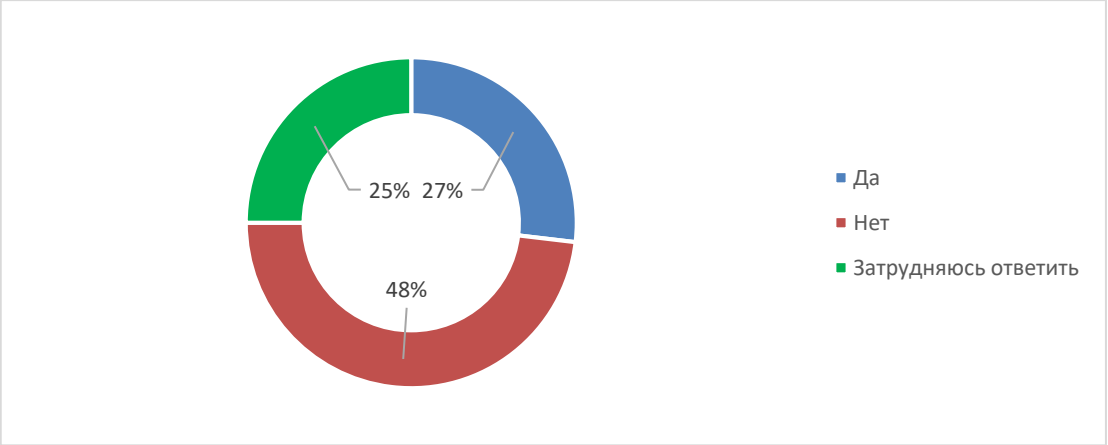

Рисунок 8. Был ли факт утечки информации в организациях за последние три года?

Согласно исследованию IBM «Cost of a Data Breach Report 2023», только 33% организаций собственными силами обнаруживают утечки данных.

По результатам опроса InfoWatch, выяснилось, что почти **у половины организаций (47%) отсутствует методика по оценке ущерба от утечки информации:**

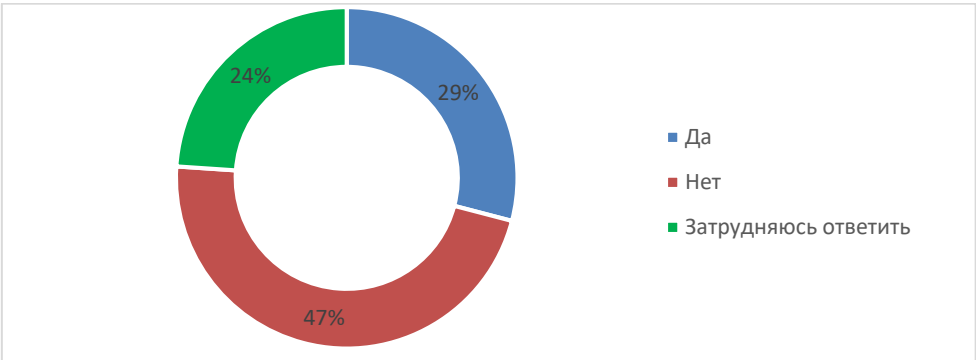

Рисунок 9. Разработана ли в организации методика оценки ущерба от утечки?

Отдельно стоит отметить, что **все респонденты, сообщившие, что в их организациях есть методика оценки ущерба, также ответили, что они либо не страдали от утечек информации, либо затруднились ответить, регистрировались ли у них утечки информации**.

При этом опрос показал, **что подавляющее большинство организаций (71% опрошенных) не застрахованы от ущерба в случае утечки информации.**

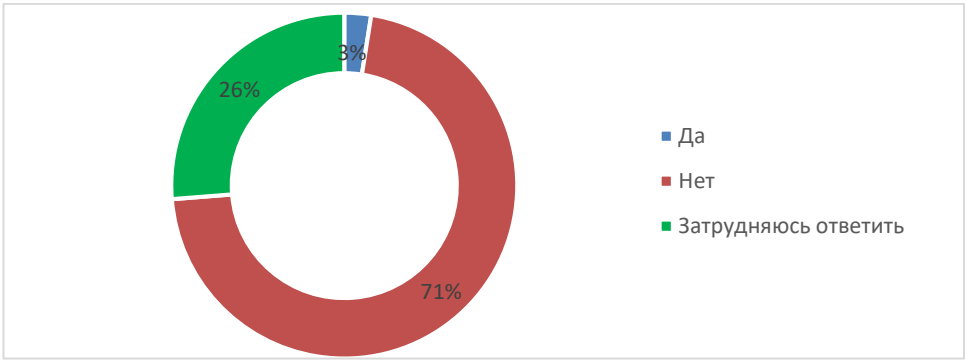

Рисунок 10. Застрахована ли ваша организация от ущерба?

Застрахованными оказались организации только из трех секторов — образование, банки и финансовые услуги, топливно-энергетический комплекс. У этих же организаций, приняты методики оценки ущерба от утечки информации.

Портреты организаций, в которых произошли утечки информации

Рассматривая отраслевую принадлежность организаций, в которых произошли утечки данных за последние три года, можно отметить, что она совпадает с общей выборкой респондентов. Чаще всего о случаях компрометации данных сообщали представители крупных частных предприятий из промышленного сектора (см. Рисунок 11).

Рисунок 11. Отрасли организаций, в которых произошли утечки информации.

На рисунке 12 представлено распределение организаций, в которых, согласно ответам участников опроса, произошли утечки информации, по размеру и форме собственности.

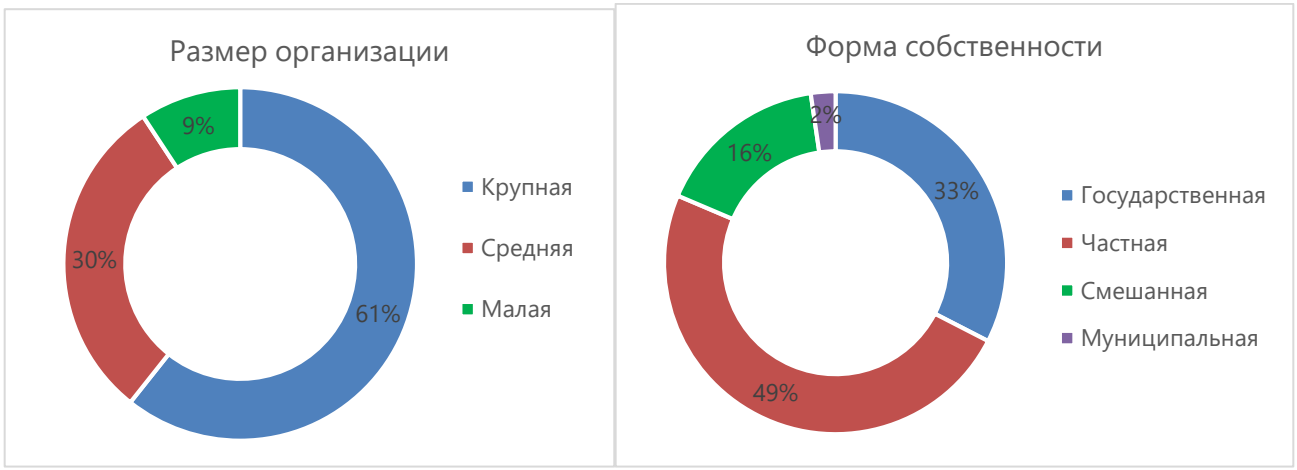

Рисунок 12. Размер и форма собственности организаций, в которых произошла утечка информации

На рисунке 13 приведено распределение случаев утечек по каналам.

Почти половина утечек (46%) произошли через подключение корпоративной или промышленной сети, ЦОД к сети Интернет, а также через корпоративную электронную почту. Далее по частоте инцидентов идут потеря и кража съемных носителей (14%).

В 9% случаев утечка информации произошла через бумажные носители, также информация «утекала» вследствие нелегитимного использования мобильных устройств (7%) и через облачные сервисы (5%).

9% отметили «Другое». Один из респондентов, выбравших такой вариант, уточнил, что сотрудником был подготовлен съемный HDD с базами для выноса. По словам другого участника опроса, бывшим сотрудником были использованы решения компании

Рисунок 13. Каналы утечки информации

На Рисунке 14 дано распределение утечек по характеру умысла (виды нарушений как умышленного, так и случайного характера). **Согласно полученным ответам, в 37% случаев утечка являлась следствием умышленных действий сотрудника организации.**

Следующей по частоте причиной утечки стала ошибка сотрудника организации — 16%, а совместные умышленные действия сотрудника и внешнего нарушителя составили 14% ответов. Также 14% утечек произошли вследствие компьютерных атак.

Рисунок 14. Следствием каких событий была утечка информации?

Если распределить нарушения на умышленные и неумышленные, то **в подавляющем большинстве случаев (70%) утечка данных является следствием умышленных действий (Рисунок 15):**

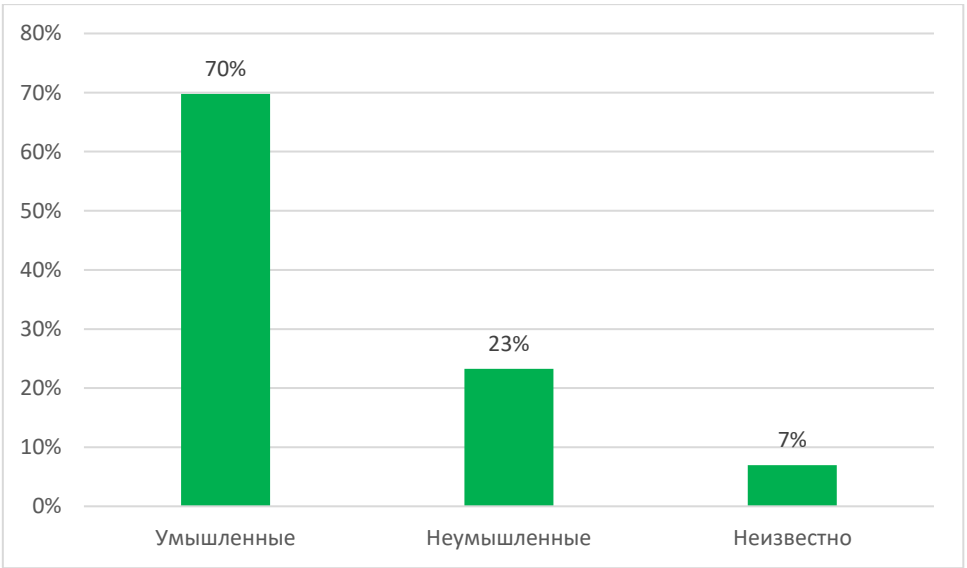

Рисунок 15. Утечки информации по характеру умысла

Данные опроса соотносятся с выводами последних аналитических отчетов ЭАЦ ГК InfoWatch по утечкам в России. Согласно этим исследованиям, последние годы отмечается рост доли утечек данных в результате умышленных нарушений.

Важно отметить, что в 63% случаев утечки произошли по вине внутреннего нарушителя (еще 16% составили утечки гибридного вида, когда данные утекали в результате сговора сотрудников с внешними нарушителями).

Таким образом, **персонал причастен к 79% всех зафиксированных утечек информации (Рисунок 16).**

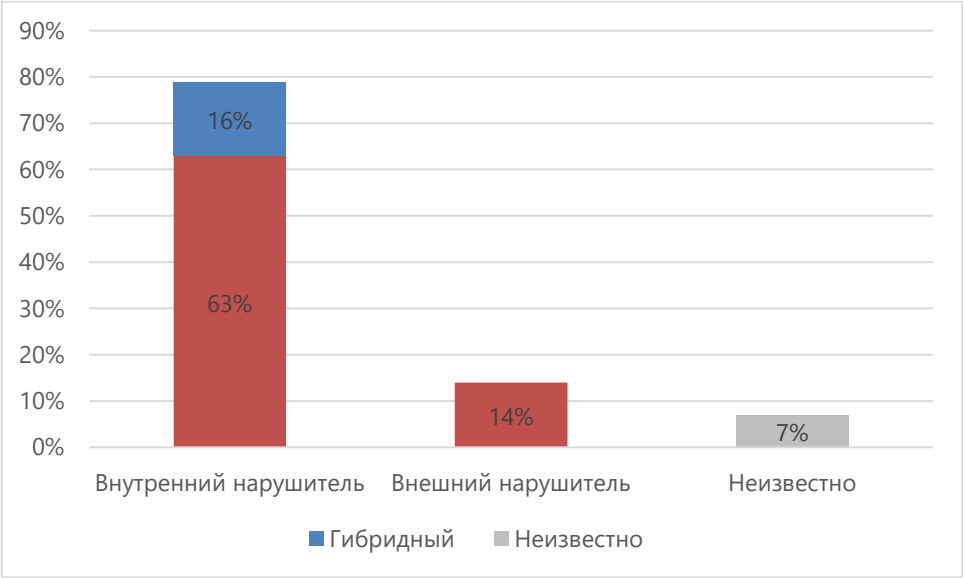

Рисунок 16. Вид нарушителя

Среди утечек по вине внутреннего нарушителя большинство случаев — результат умышленных действий (Рисунок 17).

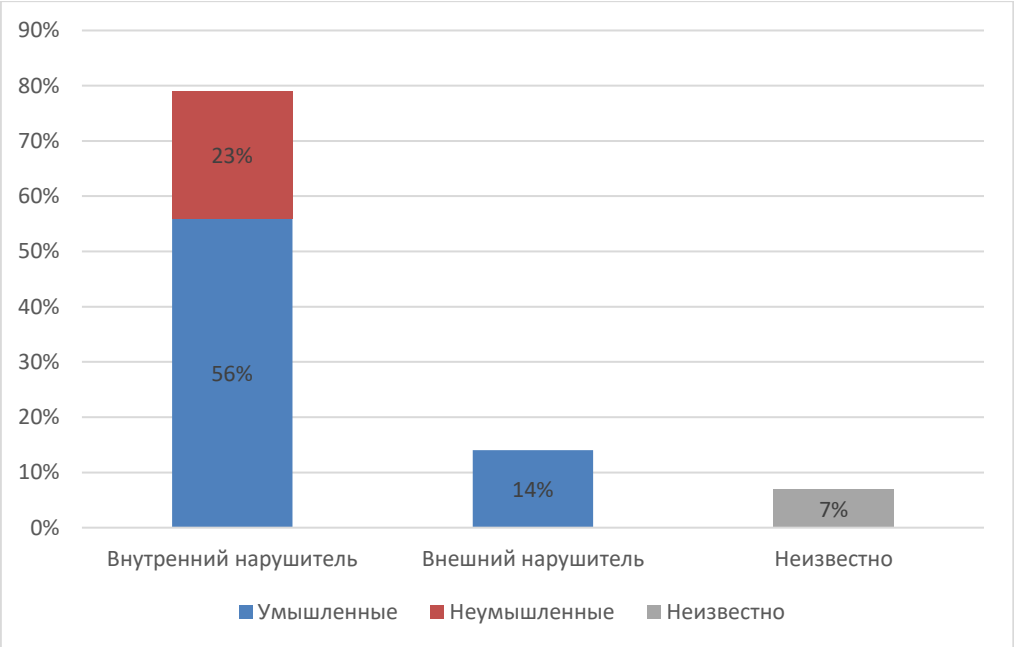

Рисунок 17. Соотношение вида нарушителя и умысла

Большинство организаций, в которых произошли утечки информации за последние три года, оказались не застрахованы (Рисунок 18).

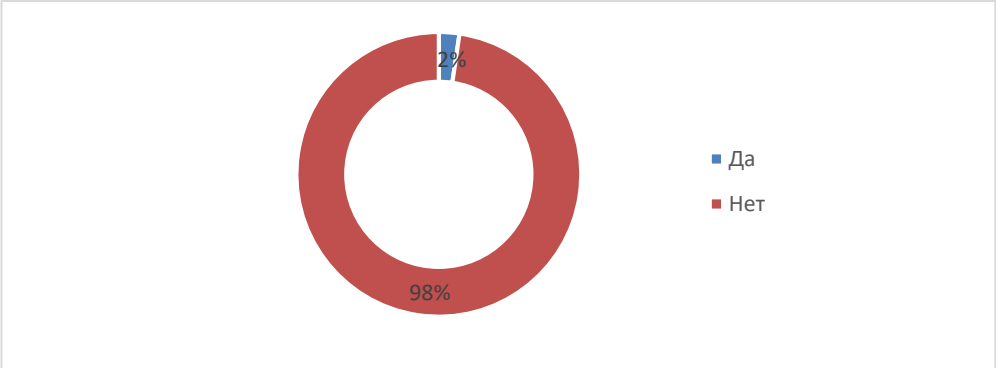

Рисунок 18. Были ли застрахованы организации, пострадавшие от утечки информации

Виды скомпрометированной информации

Персональные данные подвергались компрометации чаще всего (Рисунок 19).

Первую тройку «утекших» данных составили следующие категории:

- персональные данные (39%);
- коммерческая тайна (24%);
- служебная тайна (18%).

Полученные в опросе данные по приоритетам совпадают с другими исследованиями ЭАЦ ГК InfoWatch, основанными на статистике.

Рисунок 19. Какая информация утекла

Полученное по результатам опроса распределение видов скомпрометированной информации совпадает с данными исследований ГК InfoWatch об утечках за предыдущие годы с той разницей, что в отчетах третье место занимает «Государственная тайна». Такое расхождение ожидаемо, поскольку данные об утечках государственной тайны, в основном, поступают из открытых источников, в опросе такую информацию, как правило, не предоставляют.

Кто больше информирован об утечках

Рассмотрим, какие специалисты оказались более информированными об утечках информации (Рисунок 20).

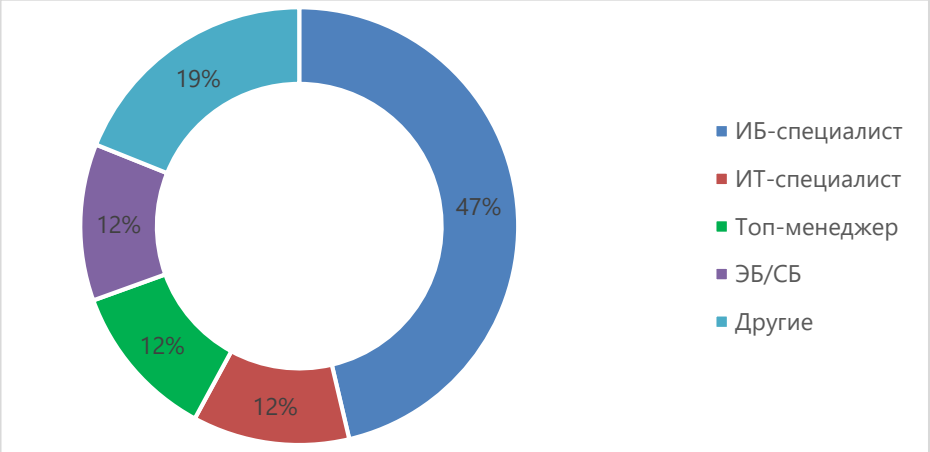

Рисунок 20. Ответы специалистов, которые сообщили, что в организации была утечка информации

Чаще всего об утечках информации осведомлены ИБ-специалисты. Довольно высокую долю (12%) заняли специалисты по экономической безопасности — несмотря на то, что в общей выборке по функциональным ролям среди респондентов экономическая безопасность занимает меньшую долю.

Отметим, что 58% опрошенных ЭБ-специалистов — это представители крупных компаний.

На Рисунке 21 представим распределение ответов представителей служб экономической безопасности по типам утекших данных.

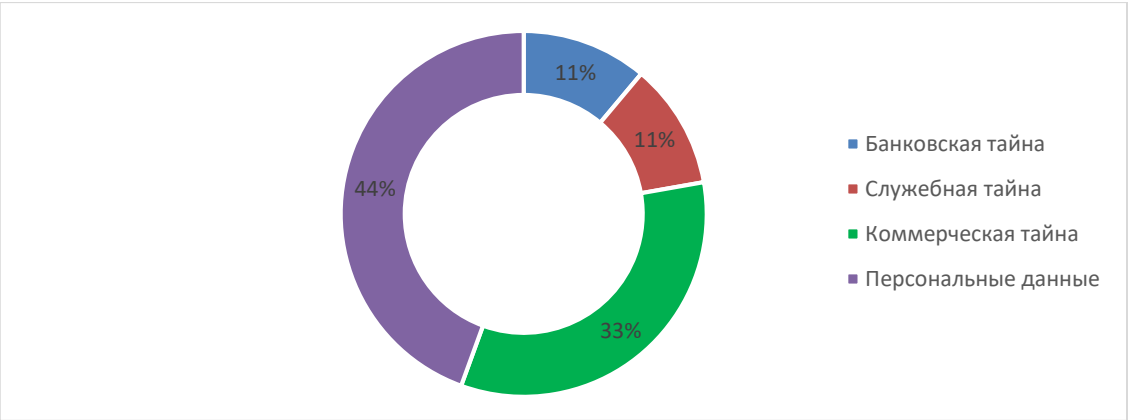

Рисунок 21. Какая утекла информация, ответы специалистов ЭБ

Данные, которые сообщили специалисты по экономической безопасности, совпадают с общей статистикой по виду скомпрометированной информации. Таким образом, можно предположить, что сотрудники служб ЭБ в организациях **обладают довольно полными данными о фактах утечек конкретных видов информации**.

Связь утечек информации с наличием DLP-систем

Отдельно были рассмотрены пункты опроса о наличии DLP-систем в организациях тех респондентов, которые затруднились ответить, была ли в их организации утечка информации. По сравнению с данными по общей выборке, в таких организациях в 2/3 случаев отсутствуют внедренные DLP-системы.

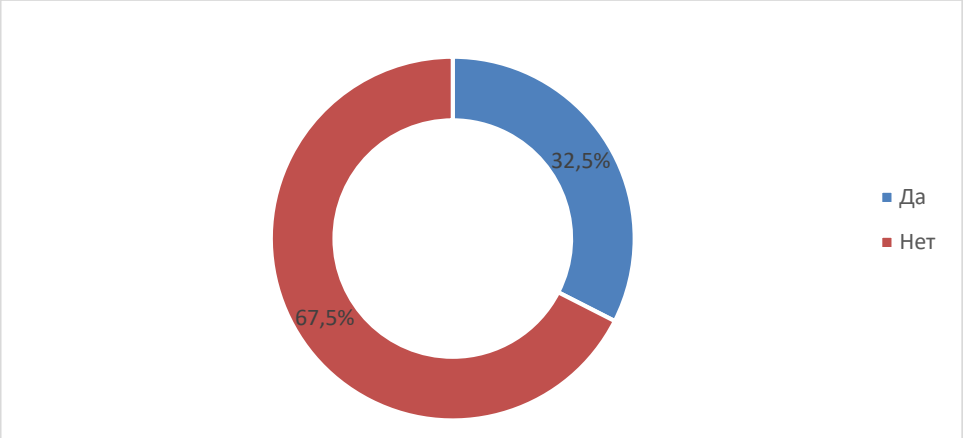

Рисунок 22. Наличие DLP-системы в организациях, которые затрудняются ответить о факте утечки информации

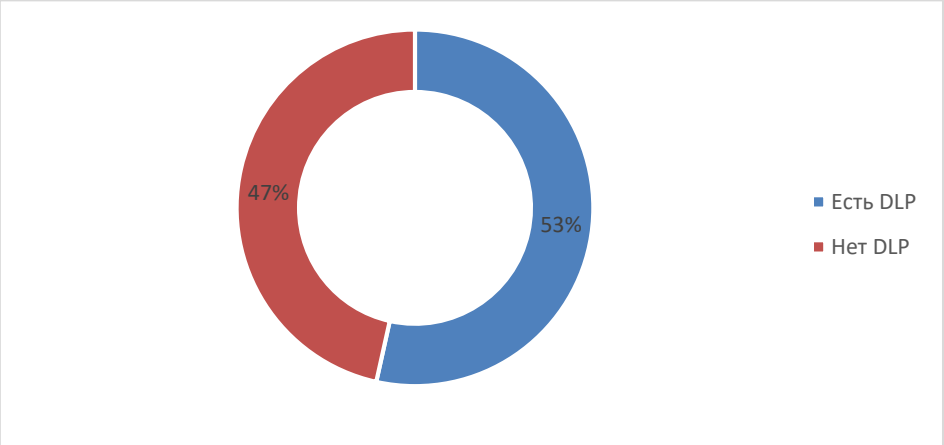

Рисунок 23. Наличие внедренных DLP-систем в организациях, в которых произошли утечки информации

Также проведено сравнение и связь между наличием DLP-систем с осведомленностью респондентов о происходивших утечках информации (Рисунок 24).

При наличии в организации внедренной DLP-системы специалисты гораздо чаще знают об утечках, т.е. варианты «Затрудняюсь ответить» встречается вдвое реже.

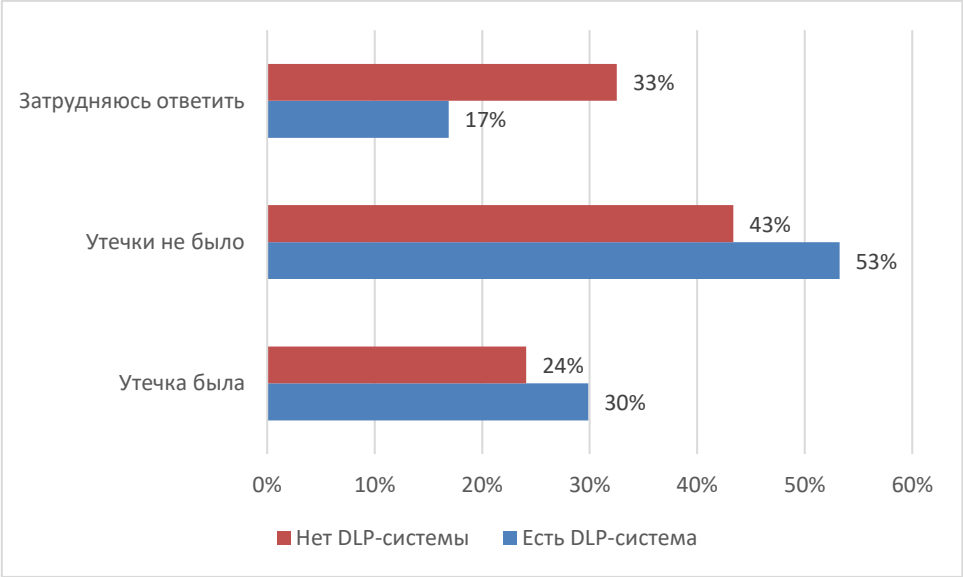

Рисунок 24. Наличие DLP-системы и осведомленность об утечках информации

Как показал опрос, наличие внедренной DLP-системы сокращает перечень причин, по которым произошла утечка данных. Так, например, в организациях с внедренным DLP-системами отсутствуют утечки по вине подрядчика.

Ущерб и его оценка

Как показал опрос, **ущерб в случае утечки информации оценивали более половины (51%) пострадавших организаций** (Рисунок 25).

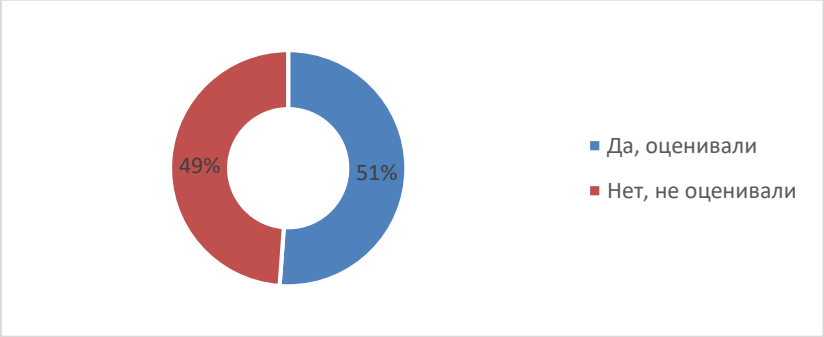

Рисунок 25. Оценивали ли в организациях ущерб от утечки информации

DLP-системы были внедрены у 55% организаций, которые оценивали ущерб (Рисунок 26).

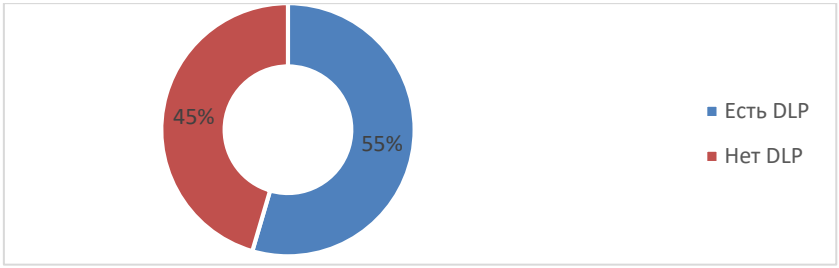

Рисунок 26. Наличие внедренных DLP-систем у организаций, которые оценивали ущерб от утечки данных

При просьбе указать сумму понесенного ущерба, большая часть (37%) сообщила, что не рассчитывали убытки, а 23% сообщили, что по результатам оценки организация не понесла ущерба.

Однако в тех организациях, в которых ущерб был подсчитан, в 14% случаев он составил более 1 млн рублей (Рисунок 27):

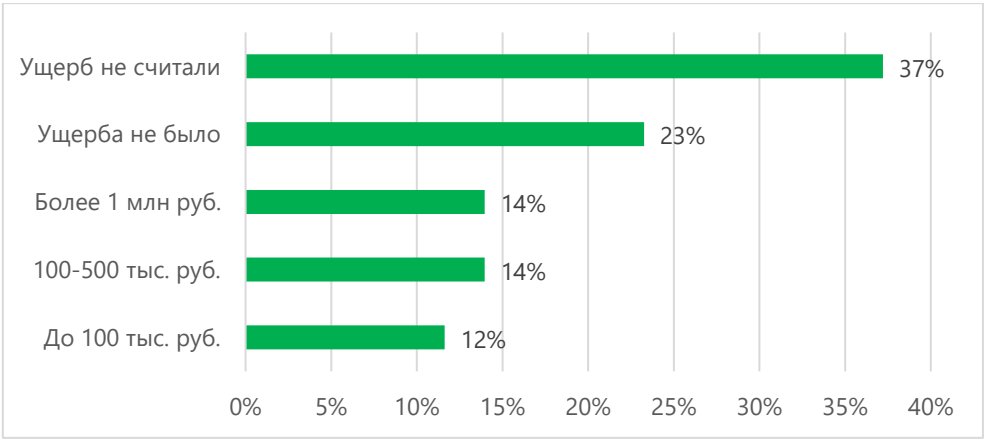

Рисунок 27. Общая сумма ущерба, понесенного вследствие утечки информации

Половина сообщений о крупном ущербе более 1 млн рублей была от специалистов по экономической безопасности предприятия. Это подтверждает мнение, что специалисты по экономической безопасности из представителей всех функциональных направлений наиболее осведомлены об ущербе от утечек информации, который несут их организации:

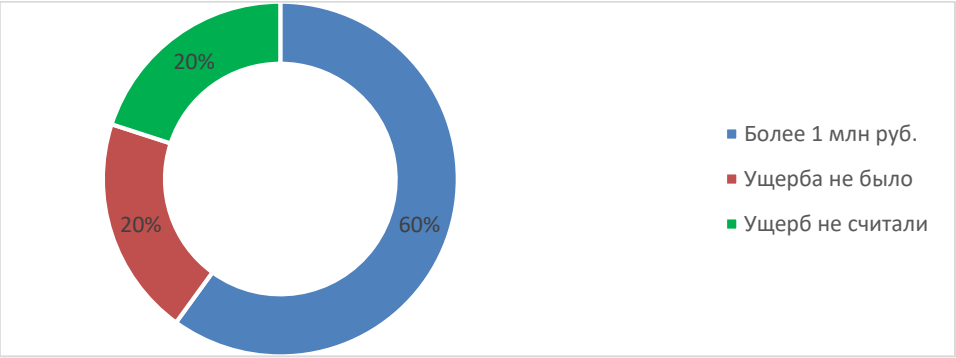

Рисунок 28. Размер ущерба, о котором сообщили специалисты ЭБ

Ущерб оценивают, в основном, крупные и средние предприятия, принадлежащие к секторам: промышленность и финансы.

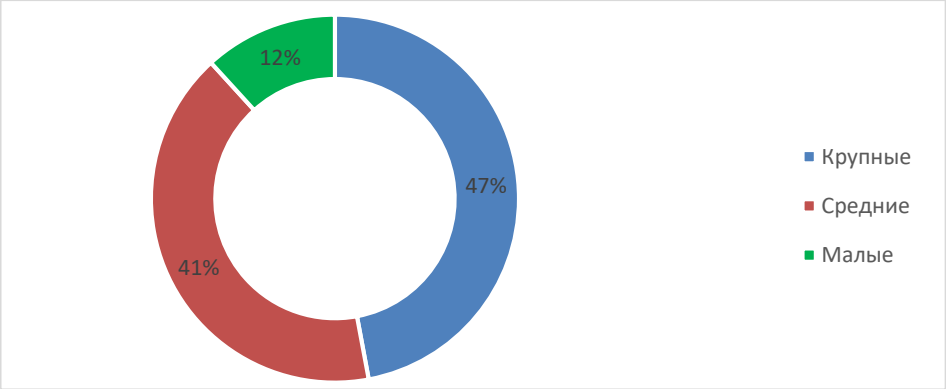

Рисунок 29. Какие организации оценивали ущерб после утечки информации, по размеру

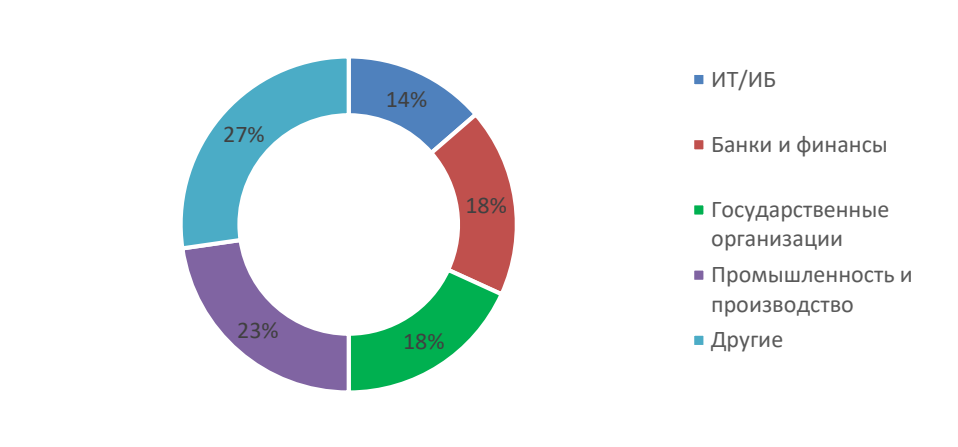

Рисунок 30. Какие организации оценивали ущерб после утечки информации, по отрасли

В половине случаев к ущербу приводят утечки информации, связанные с умышленными действиями сотрудника организации (50%). Еще 18% — это совместные действия внешнего нарушителя и внутреннего сотрудника.

В общем и целом, 73% утечек, которые приводят к ущербу, носят умышленный характер, и 68% из них связаны с умышленными действиями именно сотрудников организаций.

Рисунок 31. Следствием каких событий была утечка информации, которая привела к ущербу

В большинстве случаев к ущербу привела утечках данных через корпоративную электронную почту, что отличается от распределения ответов по всей выборке ответов (в том случае по количеству лидируют утечки через подключение к сети Интернет). Полный список каналов утечек данных, которые привели к ущербу, можно увидеть на рисунке ниже.

Рисунок 32. Утечка по каким каналам привела к ущербу

Крупный ущерб

Самыми дорогими утечками стали сведения, составляющие коммерческую тайну и ноу-хау (секреты производства) вследствие потери или кражи съемных носителей, а также утечки персональных данных.

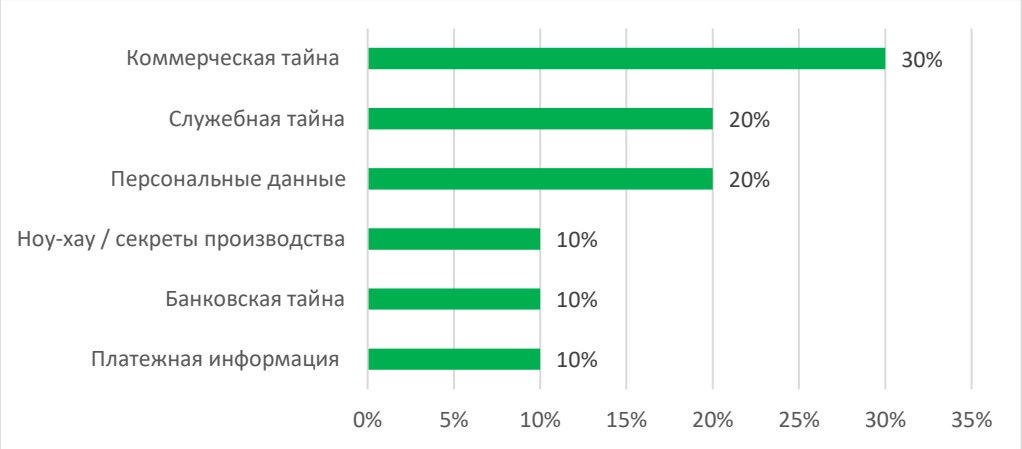

Рисунок 33. Утечка каких видов информации привела к ущербу более 1 млн руб.

При этом, например, к крупному ущербу привела ошибка топ-менеджера из-за потери съемного носителя — произошла утечка коммерческой тайны, которая обошлась организации более 1 млн рублей.

Также к ущербу более 1 млн руб. приводили:

- ошибка сотрудника, который скопировал секреты производства на съемный носитель,
- умышленные действия подрядчика организации, в результате которых произошла утечка персональных данных, а также банковской и служебной тайны.
- Умышленные действия сотрудника, в результате которых через корпоративную электронную почту произошла утечка коммерческой, служебной тайны и персональных данных.

К менее крупному ущербу (от 100 до 500 тыс. руб.) в половине случаев также привели утечки персональных данных, зачастую одновременно с утечками коммерческой тайны.

Стоит заметить, что все организации, оценившие ущерб, оценивали его без наличия методики для оценки ущерба. Также у всех этих организаций нет было страхования на случай утечки информации.

Опрошенные организации, у которых есть методика оценки ущерба, либо не страдали от утечек информации за прошедший трёхлетний период, либо затруднились ответить, были ли у них утечки информации.

Заключение и выводы

Проведенное исследование показало, что ущерб от утечки информации оценивали более половины пострадавших организаций. При этом у всех этих организаций отсутствовала методика оценки ущерба.

Наличие в организации методики оценки ущерба вследствие утечек информации и, одновременно, отсутствие за последние три года утечек позволяет предположить, что подобные организации имеют более высокий уровень зрелости информационной безопасности.

Ущерб оценивают, по большей части, крупные и средние организации, принадлежащие к секторам промышленности и финансов. При этом специалисты по экономической безопасности более осведомлены о крупном ущербе от утечек информации и обладают всей полнотой данных о фактах утечек.

Самыми дорогими утечками информации стали утечки сведений, составляющих коммерческую тайну и ноу-хау (секреты производства) вследствие потери или кражи съемных носителей, а также утечки персональных данных.

Наличие внедренной DLP-системы сокращает перечень причин утечек данных. Например, в таких организациях отсутствуют утечки по вине подрядчика.

По итогам опроса видно, что внутренний нарушитель представляет наибольшую угрозу получения ущерба от утечек данных. 73% утечек, которые приводят к ущербу, носят умышленный характер, и 68% из них связаны с умышленным действием сотрудников организаций.

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
- ВКонтакте
- Telegram

Методика исследования

Исследование проводилось на основании собственной оригинальной Методики.

Акционерное общество «Национальный Реестр интеллектуальной собственности» подтверждает, что 31.07.2023 г. файл «Методика 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» по заявлению: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ЛАБОРАТОРИЯ ИНФОВОТЧ" (ОГРН 1087746543367, ИНН 7734583888), зашифрован и помещен в виртуальную ячейку АПК НРИС.