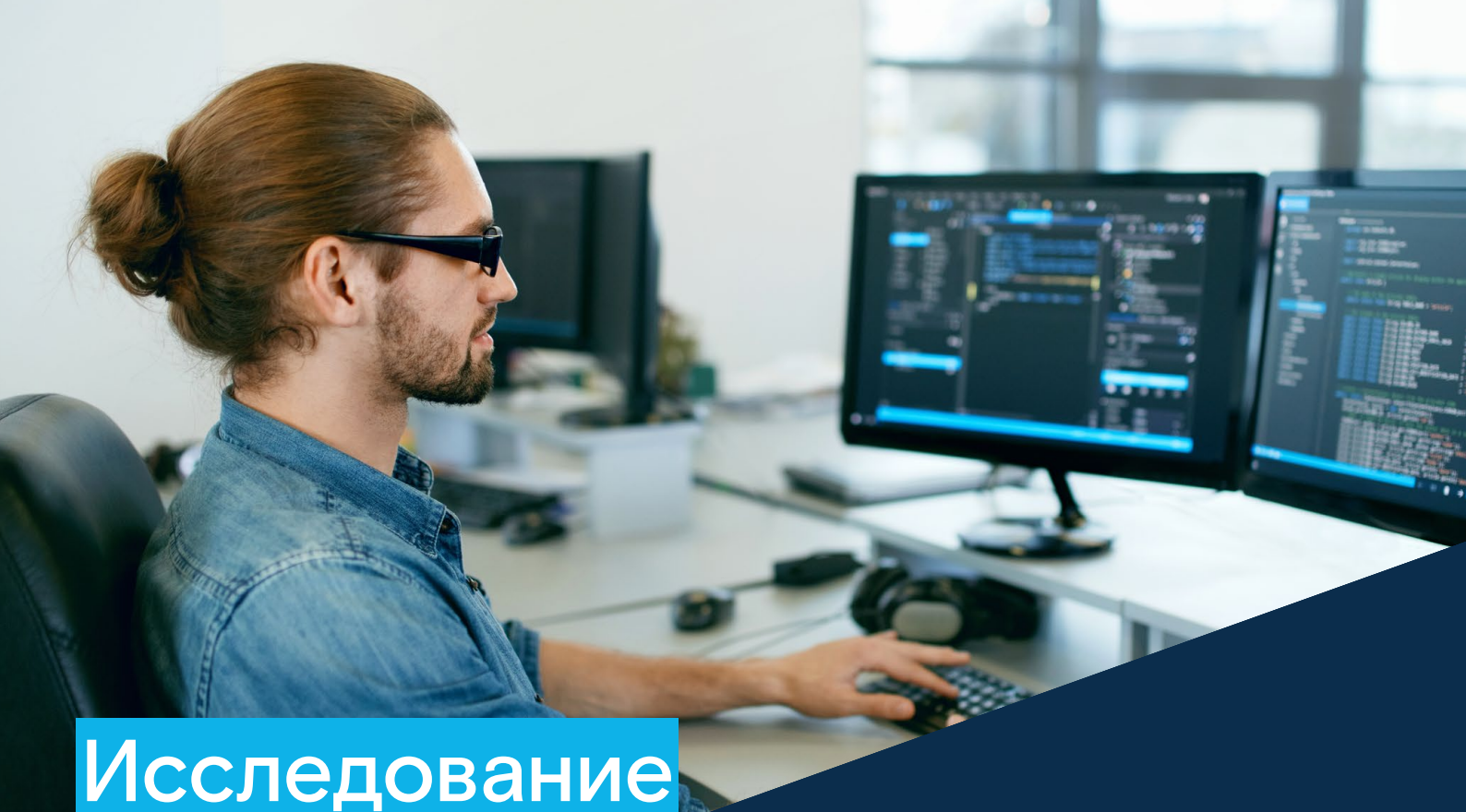


Исследование «Мошенничество и слив данных в российских организациях»

Апрель – май 2022

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

Ростелеком Солар

Содержание

Ключевые цифры

87%

респондентов заявили, что в их организациях за последний год наблюдались случаи мошенничества со стороны сотрудников

30–35 лет

наиболее распространенный возраст нарушителей (более 70% нарушений)

Наиболее частотные виды нарушений

- мошеннические действия сотрудников продающих подразделений (почти 20% случаев)
- различные хищения или предоставление необоснованных преимуществ при закупках (по 14% случаев)

В 20%

случаях размер ущерба составил от 10 до 100 млн рублей – в организациях с численностью сотрудников 500–1000 человек

Более 100 млн рублей

составила сумма ущерба от мошенничества со стороны сотрудников производственной организации (более 1000 сотрудников), базирующейся в одном из отдаленных регионов России

Методология

Данное исследование проведено методом электронного опроса аудиторий изданий E-xecutive.ru и Генеральный Директор (целевые рассылки по базам подписчиков категории «руководители и владельцы бизнеса»).

В опросе приняли участие представители свыше 120 российских организаций из различных сфер деятельности (от e-commerce до атомной промышленности). Размер опрошенных компаний представлен категориями «малый бизнес» (до 100 сотрудников), «средний бизнес» (от 500 до 1000 сотрудников), и «крупный бизнес» (свыше 1000 сотрудников).

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

Опрос проводился в апреле — мае 2022 года.

Введение

Исследование продолжает серию отчетов «РТК-Солар» об изменениях в рабочем поведении рядовых сотрудников, руководителей организаций и связанных с этим внутренних нарушениях ввиду массового перехода к гибридному формату работы. Гибридный офис — это формат работы компании, при котором основная часть сотрудников постоянно работают в офисе, часть работает удаленно, и есть такие, кто совмещает работу в офисе и дома.

В 2021 году в Трудовом кодексе Российской Федерации были детально регламентированы основные процедуры удаленной занятости, в связи с чем соответствующая практика получила устойчивое распространение в организациях самых разных сфер деятельности.

Поддерживать «офисный» уровень контроля, физически находясь с сотрудниками в разных местах, на постоянной основе не под силу практически никому. Соответственно — и вполне ожидаемо — растет и количество самых разных нарушений: и простых дисциплинарных, и таких, которые способны нанести бизнесу значительный урон. Цифровые следы таких нарушений остаются в корпоративной инфраструктуре. В своем исследовании «РТК-Солар» выяснил, насколько в гибридном формате занятости распространены различные нарушения, а также их ключевые негативные последствия для организаций.

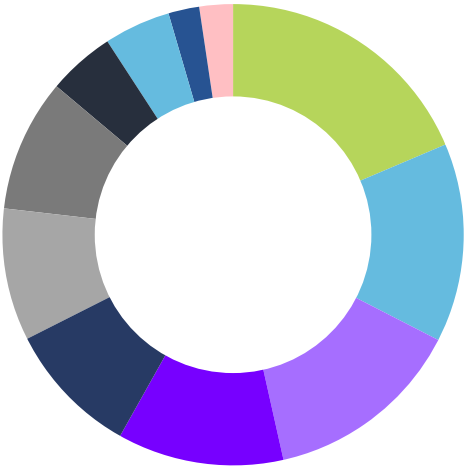
Результаты исследования будут полезны специалистам различных служб безопасности российских организаций — информационной, внутренней, экономической безопасности, сотрудникам финансово-экономического блока, а также руководителям российских компаний.

Результаты исследования

1. Портрет нарушения

87% респондентов заявляют, что в организации, которую они представляют, за последний год наблюдались случаи мошенничества со стороны сотрудников. Наиболее часто встречающиеся в российских компаниях виды нарушений — мошеннические действия сотрудников продающих подразделений (почти 20% случаев), различные хищения или предоставление необоснованных преимуществ при закупках (по 14% случаев). Наименее распространенные — экзотические нарушения: кража клиентской базы и данных о клиентах с целью продажи этой информации (примерно в 5% случаях) и хищение разработок компании в целях получения личной выгоды (менее 3% нарушений).

Какое мошенничество допускали сотрудники?



18,6%

Мошенничество с продажами

14%

Хищение денег, товарно-материальных ценностей и других активов

14%

Предоставление необоснованных преимуществ

11,6%

Вывмогательство/ взяточничество

9,3%

Слив конфиденциальной информации с целью продажи

9,3%

Мошенничество с закупками

9,3%

Искажение финансовой отчетности

4,7%

Мошеннические выплаты

4,6%

Попытка увода клиентской базы

2,3%

Хищение разработок компании в целях личной экономической выгоды

2,3%

Другое

Чаще всего мессенджеры становятся основными каналами в реализации мошеннических схем. С их помощью совершается треть нарушений (33%). В половине случаев это различные виды мошенничества, связанные с продажами (предоставление безосновательных преимуществ, взяточничество). Интересно, что именно в мессенджерах реализовывались мошеннические схемы с наибольшим зафиксированным ущербом.

Наиболее частые каналы реализации мошеннических схем

33,3%
Мессенджеры

25%
Флешки и другие съемные носители

8,3%
Облачные хранилища

8,3%
Личная почта

8,3%
Корпоративная электронная почта

4,2%
Подкуп IT-специалисата

4,2%
Сговор

4,2%
Мобильная связь

4,2%
Весь набор каналов, включая публикации в научных журналах

2. Портрет нарушителя

Однозначный лидер среди неблагонадежных подразделений — отдел продаж (33% инцидентов), далее с большим отрывом следуют производственные подразделения (16.7%), закупки (13%), бухгалтерия и финансы, хранение и логистика (по 10% случаев нарушений).

В каких подразделениях произошли инциденты?

33%
Отдел продаж

16,7%
Производство

13,3%
Отдел закупок/ тендерный отдел

10%
Бухгалтерия и финансы

10%
Логистика и хранение

6,8%
Органы управления

3,4%
Отдел маркетинга

3,4%
Юридическая служба

3,4%
Аутсорс IT

В целом, результаты этого исследования хорошо коррелируют с данными другого исследования «РТК-Солар», «Типовой портрет нарушителя», где наиболее часто встречающийся возраст нарушителя — 35-40 лет.

Преобладание среди нарушителей сотрудников отделов продаж по сравнению с теми же закупками можно объяснить двумя факторами: общей численностью (как правило, менеджеров по продажам в организациях больше, чем сотрудников закупочных подразделений) и отсутствием четкой законодательной регуляции процедур в сфере продаж, в отличие от закупок.

Подавляющее число нарушений (более 70%) происходит по вине сотрудников среднего возраста (30-50 лет). Любопытно, что лиц старшей возрастной группы (от 50 лет) вообще нет среди фигурантов нарушений.

3. Размер ущерба

Суммы причиненного организациям ущерба существенны: почти в 20% случаев его размер составляет от 10 до 100 млн рублей. При этом такой ущерб в основном фиксируют оранизации с численностью сотрудников от 500 до 1000 человек. Нужно отметить, что приобретение DLP-системы для контроля сотрудников для подобной организации ориентировочно стоит 10 млн рублей в год, что соответствует нижнему уровню возможного ущерба.

Наиболее крупный по размеру причиненного ущерба случай мошенничества со стороны сотрудников зафиксирован в производственной организации (более 1000 сотрудников), базирующейся в одном из отдаленных регионов России. Его размер составил более 100 млн руб. Учитывая, что зафиксированные нарушения имели место в разных подразделениях организации и, скорее всего, происходили на протяжении достаточно длительного периода времени, можно сделать вывод, что в организации с большой вероятностью не использованы никакие инструменты для своевременного выявления подобных ситуаций, в том числе DLP-системы.

4. Последствия для организации-жертвы

Интересно, что ни один из случаев самых крупных по масштабу нарушений не стал для организаций-жертв поводом для использования ИБ-средств контроля потенциально опасных действий сотрудников. О приобретении DLP-систем по итогам выявленных нарушений сообщили 10% организаций, при этом ущерб во всех был незначительным. Объяснить такую легкомысленность можно либо недостаточной осведомленностью высшего руководства организаций о потенциальном решении проблемы в виде DLP-системы, либо отсутствием квалифицированных кадров для её эксплуатации – хотя данный пробел давно заполняют решения по аналитическому аутсорсу и возможности вендоров провести качественное обучение inhouse-аналитиков DLP, как это, например, делает «РТК-Солар».

Какие меры были приняты для исправления ситуации?

30,4%

Увольнение виновных

30,4%

Ужесточение процедур контроля

21,8%

Никакие

8,7%

Дисциплинарные меры в отношении виновных

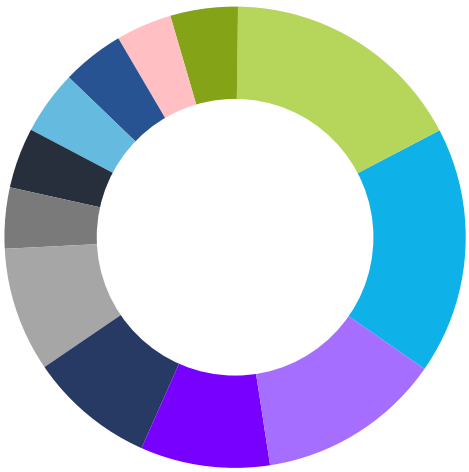
8,7%

Установлена система контроля действий сотрудников/DLP-система

5. География и отраслевой ландшафт жертв нарушений

Инциденты с участием сотрудников происходят в организациях из различных отраслей и регионов. Это подтверждают отраслевой ландшафт и география участников опроса: более 10 разнообразных сфер деятельности, 5 федеральных округов.

Отраслевое распределение респондентов



17,4%

Производство

17,4%

Ритейл

13%

Строительство

8,8%

Финансы

8,8%

IT

8,8%

Торговля

4,3%

E-commerce

4,3%

Атомная отрасль

4,3%

Наука

4,3%

Недвижимость

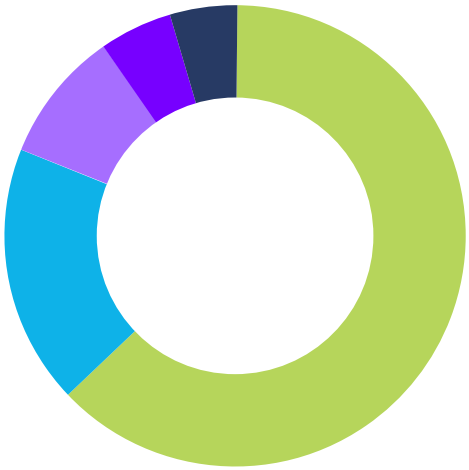
4,3%

Образование

4,3%

Другое

Региональное распределение респондентов



63,6%

Центральный ФО (включая Москву)

18,2%

Северо-Западный ФО (включая Санкт-Петербург)

9,2%

Приволжский ФО

4,5%

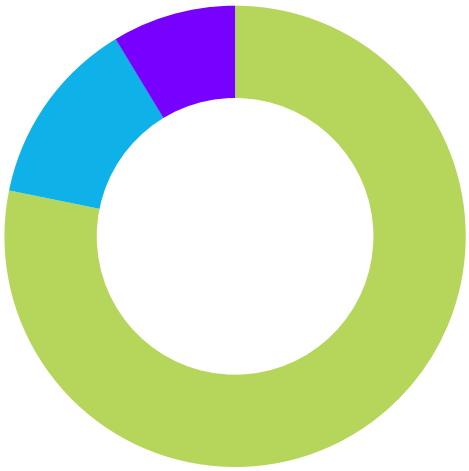
Дальневосточный ФО

4,5%

Северо-Кавказский ФО

Важно отметить, что почти четверть опрошенных — средние и крупные организации.

Размер опрошенных компаний



78,3%

До 500 сотрудников

13%

500-1000 сотрудников

8,7%

Свыше 1000 сотрудников

При этом, традиционная проблема многих крупных организаций – уровень дисциплины в филиальной сети, который, как правило, существенно ниже центрального аппарата. Запрос на контроль филиальной сети как приоритетная задача встречается почти у каждого крупного заказчика DLP-системы.

Выводы

Подводя итоги исследования, аналитики «РТК-Солар» обращают внимание DLP-сообщества на очень тревожный факт: ни одна из компаний, для которой мошенничество сотрудников и слив информации вылились в крупный ущерб, в результате не озадачилась внедрением инструментов защиты от утечек. Это может означать, что DLP- ситсемы интересны в основном службам ИБ, а также то, что системы такого класса ассоциируется с борьбой утечек данных. А низкие размеры штрафов за такого вида нарушения (за исключением финансового сектора) — слабый мотив для топ-менеджмента задумываться о выделении ресурсов для внедрения DLP в организации.

При этом, DLP-системы — особенно отечественные — в своих возможностях давно перешагнули изначальный, достаточно узкий функционал контроля утечек конфиденциальной информации за пределы организаций. Сейчас они выступают полноценными партнерами и для служб, ответственных за экономическую безопасность, и даже для кадровых служб, которым предлагается набор самых разных метрик — от продолжительности и содержания деятельности на ПК в течение рабочего дня сотрудников до мягкого мониторинга психологического климата в коллективе.

Solar Dozor - система для предотвращения утечек конфиденциальной информации (Data Leak Prevention, DLP) корпоративного класса. Ее возможности обеспечивают контроль коммуникаций сотрудников, блокировку или изменение нежелательных сообщений, выявление и мониторинг групп риска, а также ретроспективный анализ архива коммуникаций для проведения расследований.

Узнать подробнее

Solar Dozor анализирует поведение пользователей (User Behavior Analytics), что позволяет выявлять аномалии поведения, круг общения и приватные контакты сотрудников, а также профилировать их на основе 20 устойчивых паттернов поведения и предотвращать инциденты безопасности до того, как произошла утечка.

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