Исследование

«Мошенничество и слив данных в российских организациях»

Апрель - май 2022

МОСКВА, 2021

Оглавление

1. Ключевые цифры

- **87%** респондентов заявили, что в их организациях за последний год наблюдались случаи мошенничества со стороны сотрудников
- **30-50 лет** – наиболее распространенный возраст нарушителей: более **70%** нарушений происходит по вине сотрудников такого возраста
- 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%** случаев размер ущерба составил от **10 до 100 млн** рублей –в организациях с численностью сотрудников **500-1000** человек
- **Более 100 млн рублей** – наиболее крупный ущерб от мошенничества со стороны сотрудников – зафиксирован в крупной (более 1000 сотрудников) производственной организации, базирующейся в одном из отдаленных регионов России

2. Методология

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

В опросе приняли участие представители свыше 120 российских организаций более чем 10 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)

Опрос проводился в апреле – мае 2022 года.

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

3. Введение

Компания «РТК-Солар», национальный провайдер технологий и сервисов кибербезопасности, представляет исследование «Мошенничество и слив данных в российских организациях».

Исследование продолжает серию отчетов «РТК-Солар» об изменениях в рабочем поведении рядовых сотрудников и руководителей организаций и связанных с этим внутренних нарушениях в связи с массовым переходом к гибридному режиму работы. Напомним, гибридный режим работы подразумевает, что одна часть сотрудников работает на стационарных рабочих местах в офисе, а другая – дистанционно: из дома, а в летние месяцы, возможно, и находясь на даче.

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

Удаленка ожидаемо расхолаживает, 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.

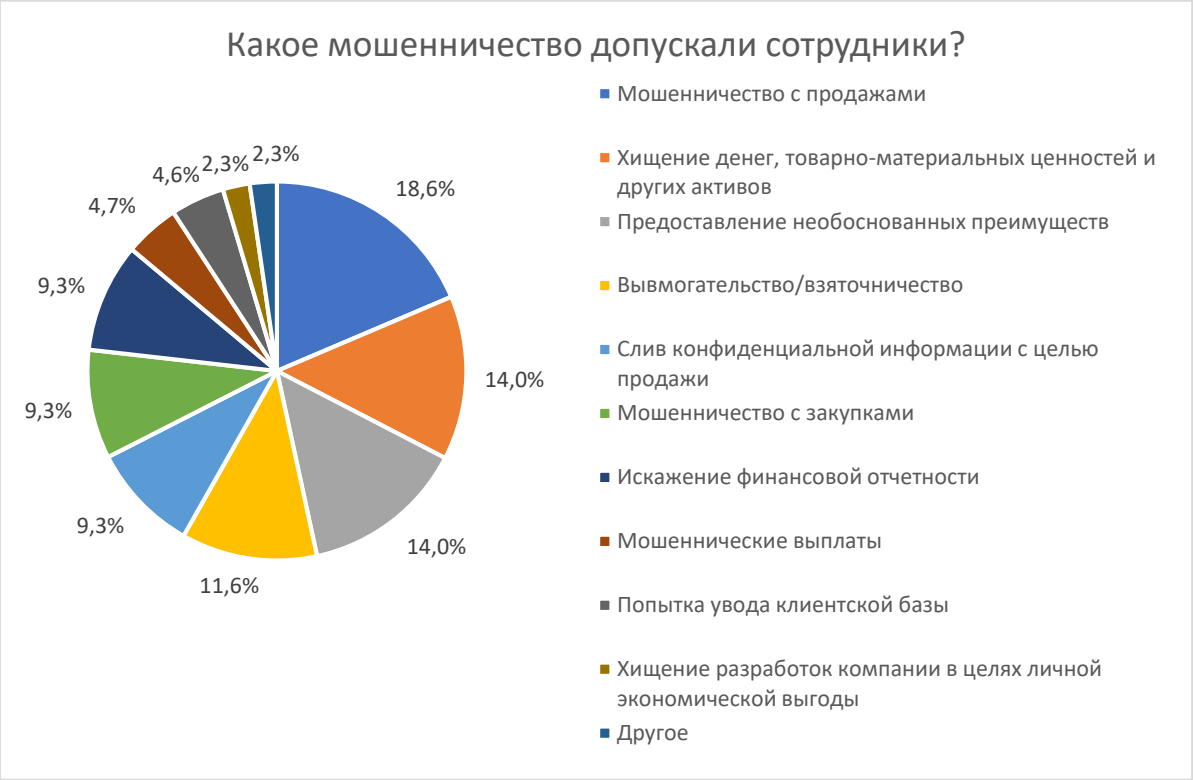
Результаты исследования будут полезны специалистам различных служб безопасности российских организаций – информационной, внутренней, экономической безопасности, сотрудникам финансово-экономического блока, а также руководителям российских компаний.

4. Результаты исследования

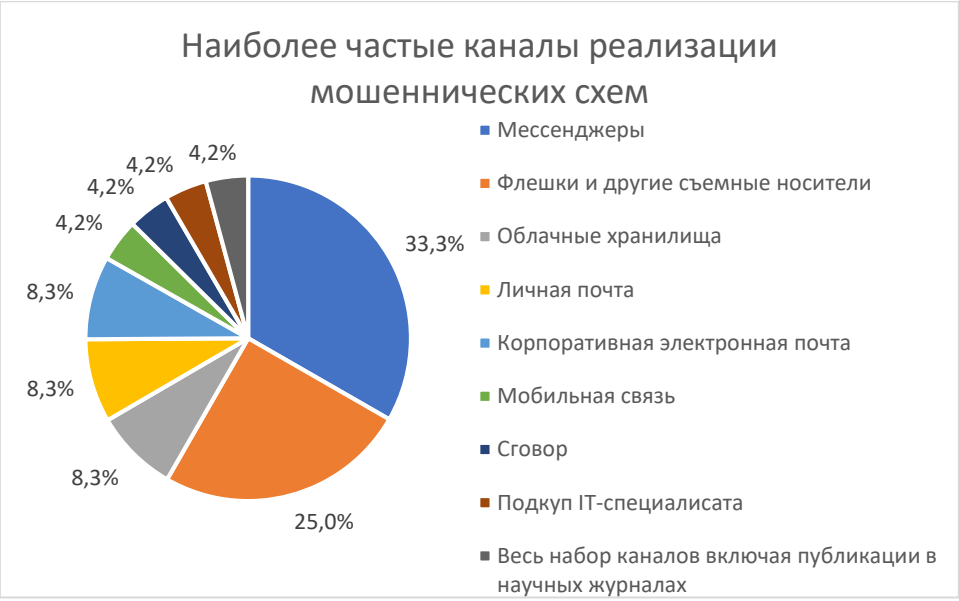
4.1 Портрет нарушения

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%** случаев) и хищение разработок компании в целях получения личной выгоды (менее **3%** нарушений)

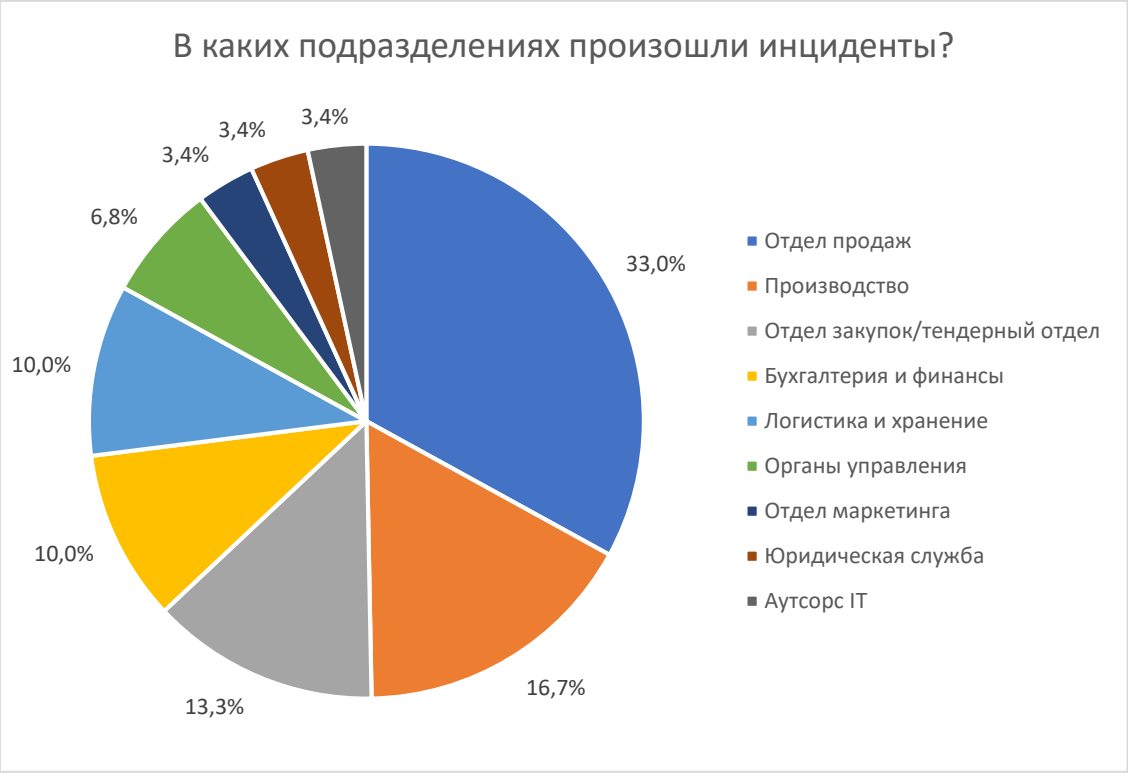


Канал-лидер в реализации мошеннических схем – мессенджеры. С их помощью совершена треть нарушений (**33%**). В половине случаев это различные виды мошенничества с продажами (предоставление безосновательных преимуществ, взяточничество). Интересно, что **именно в мессенджерах реализовывались мошеннические схемы с наибольшим зафиксированным ущербом**.



4.2 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 и хранение и логистика (по **10%** случаев нарушений).



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 (старше 50 лет) вообще нет среди фигурантов нарушений.

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.

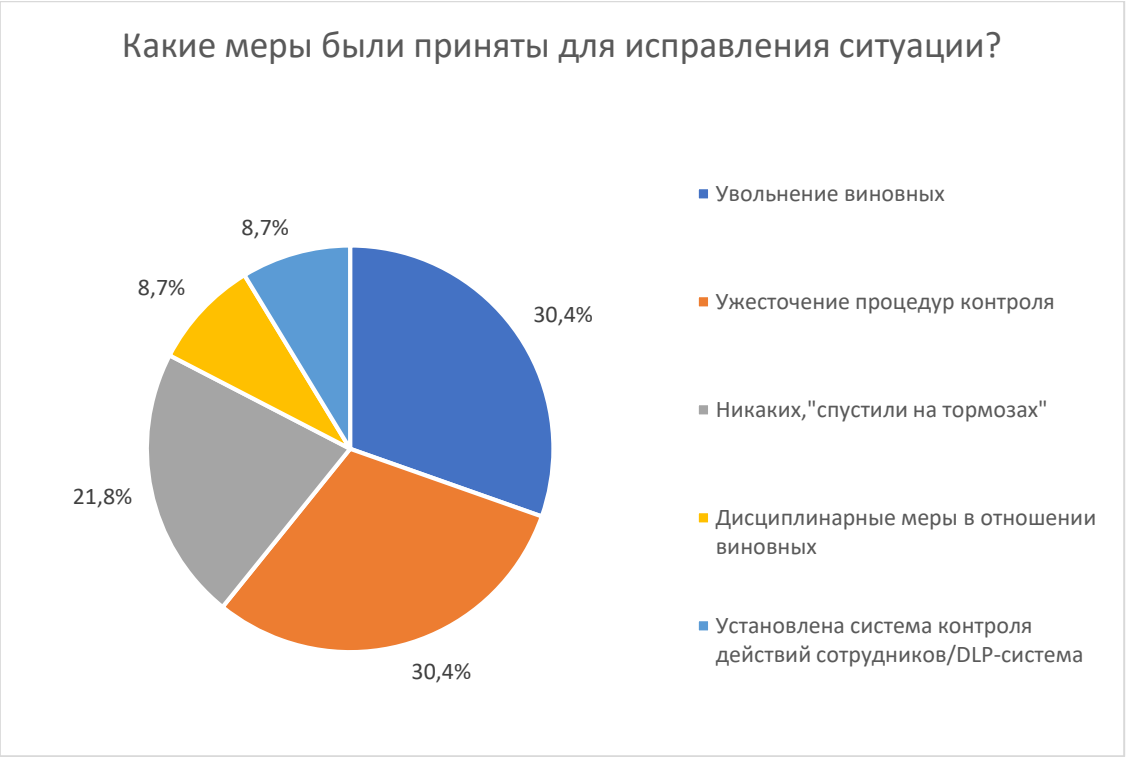
4.3 Размер ущерба

Суммы причиненного организациям ущерба существенны: почти в **20%** случаев его размер составил от **10 до 100 млн рублей**, при этом такой ущерб фиксируют организации среднего размера с численностью сотрудников 500-1000 человек. Нужно отметить, что приобретение DLP-системы для контроля сотрудников для ВСЕЙ такой 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 крупной (более 1000 сотрудников) производственной организации, 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.

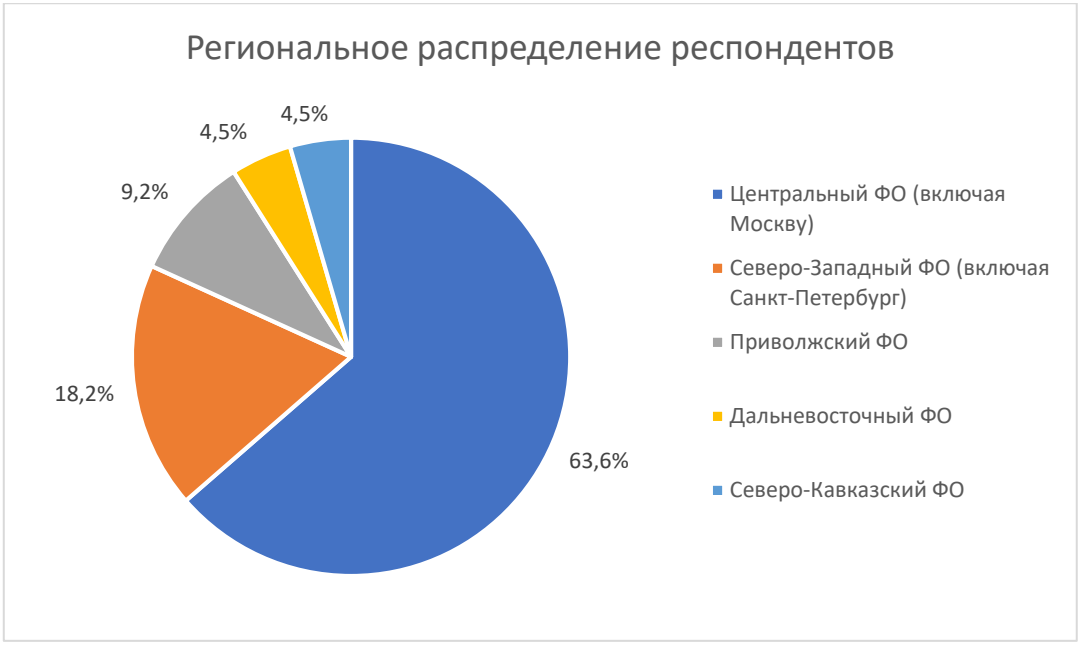
4.4 Последствия для организации-жертвы

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».

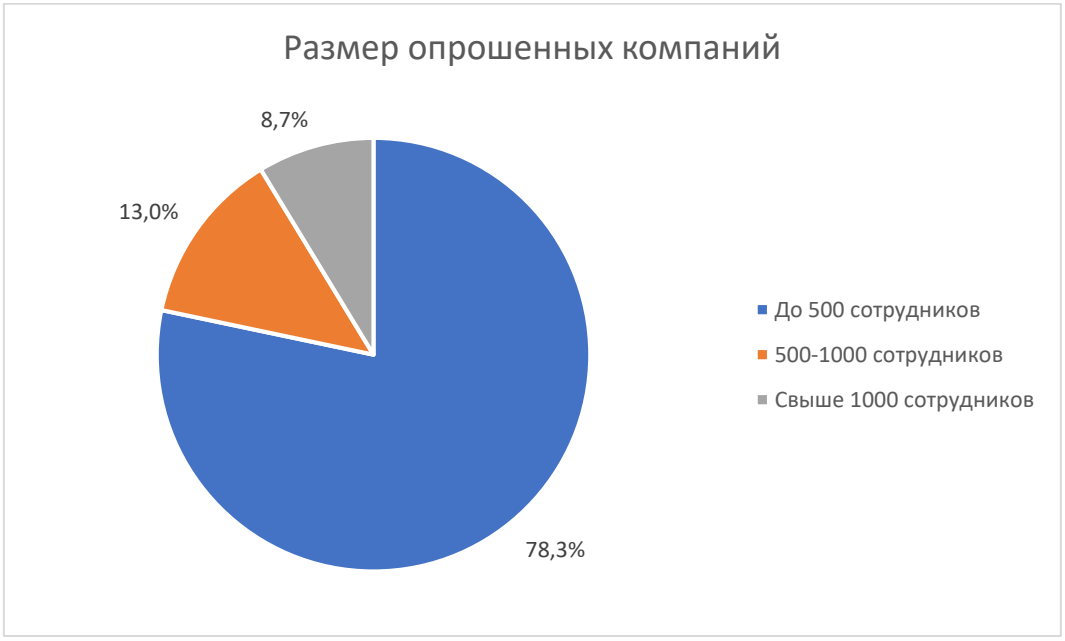


4.5 География и отраслевой ландшафт жертв нарушений

Риск инцидентов с участием сотрудников – удел организаций в самых разных отраслях и регионах. Это подтверждают отраслевой ландшафт и география участников опроса: более 10 разнообразных сфер деятельности, 5 федеральных округов.



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



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.

5. 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. Похоже, что DLP пока – в основном сфера сугубых интересов служб ИБ, либо ассоциируется система такого класса в основном с борьбой с утечками данных. А низкие размеры штрафов за такого вида нарушения (за исключением, пожалуй, финансового сектора) – слабый мотив для топ-менеджмента задумываться о выделении ресурсов для появления DLP в организации.

При этом, DLP-системы – особенно отечественные – в своих функциональных возможностях давно уже 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.

Контакты

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

+7 (499) 755-07-70
продажи и общие вопросы

+7 (499) 755-02-20
техническая поддержка

125009 г. Москва, Никитский переулок, 7с1