Кто он – типовой нарушитель в российской организации?

Второе ежегодное исследование «РТК-Солар»

rt-solar.ru
rt.ru

Ростелеком Солар

Содержание

Типичный портрет нарушителя

Ключевые цифры

35–40 лет

женщины

6,5 лет

работает в компании

Специалист
отдела кадров
в государственной
организации

Отправляет информацию
ограниченного доступа
на личную почту

Методология исследования

Исследование подготовлено на основе анализа обезличенных данных отчетов о пилотировании DLP-системы Solar Dozor в 2021 году

100

и более российских организаций приняли участие в исследовании

300

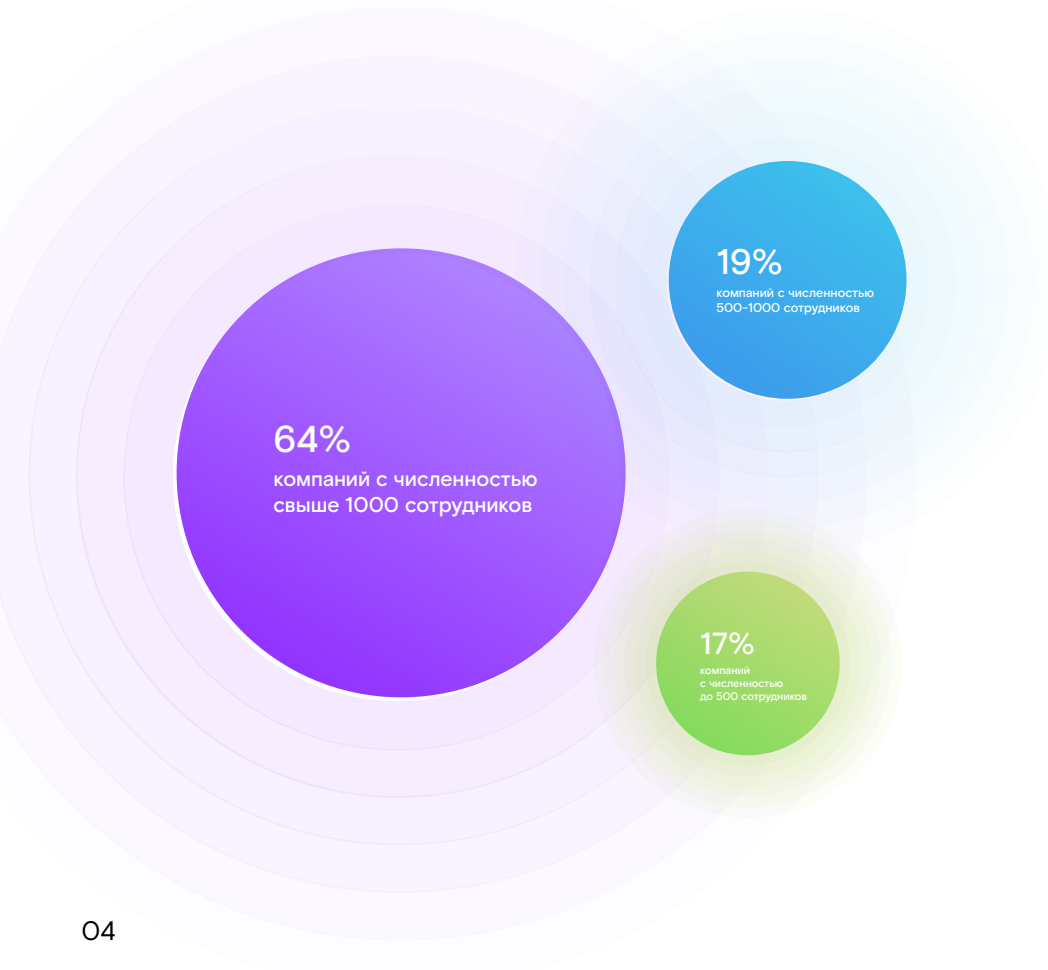
человек анализируемая выборка потенциальных нарушителей

11

11 отраслей приняли участие в исследовании, в том числе:

- оборонная промышленность,
- транспорт,
- финансы,
- органы государственной власти и государственное управление,
- химическая промышленность,
- здравоохранение,
- энергетика

Представители среднего и крупного бизнеса (SMB, SME и Large Enterprise):



Результаты исследования

Женщины нарушают несколько чаще правила информационной безопасности, чем мужчины

Типовой нарушитель. Пол

В 2021 году служебную дисциплину и правила информационной безопасности в российских организациях несколько чаще нарушали женщины (в 55% случаев). Такой результат в целом подтверждает гипотезу о большей (в среднем по сравнению с мужчинами) психологической импульсивности женщин, что может, в частности, влечь за собой нарушение дисциплины. Впрочем, мужчин среди нарушителей в рамках исследования немногим меньше – 45%.

лет и меньше - возраст сотрудников, на которых приходится большая часть нарушений

Типовой нарушитель. Возраст

Основная часть нарушений по-прежнему приходится на молодых сотрудников в возрасте до 40 лет. Их, как и в предыдущем исследовании, больше половины (55%) в общем количестве нарушающих.

Для нарушителей-женщин молодого (до 40 лет) возраста наиболее распространенным нарушением является небрежное хранение и неосторожное распространение учетных данных для работы с информационными системами.

Также среди частых нарушений – неконтролируемое распространение информации с отметкой «Для служебного пользования» (ДСП): пересылка на личную почту на бесплатных почтовых сервисах или печать. А также – нецелевое использование рабочего времени и ресурсов работодателя: поиск работы, просмотр развлекательного контента и печать материалов для личного использования.

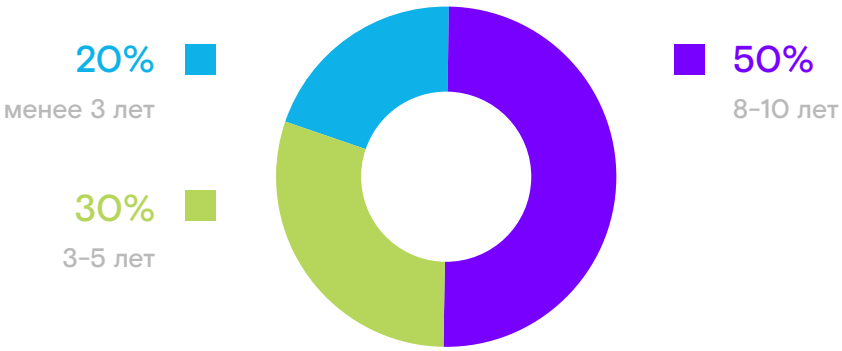
Для сотрудников старше 40 лет наиболее типично небрежное обращение с чувствительной служебной информацией, конфиденциальной и имеющей отметку «Для служебного пользования». В 4 случаях из 5 документы неконтролируемо передаются за периметр организации (по электронной почте), а в каждом 5-м случае – распечатываются.

Результаты исследования

Типовой нарушитель. Стаж работы

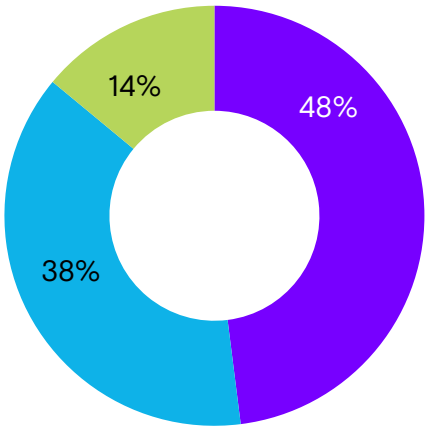
Минимальный стаж работы нарушителя составил чуть более 2 лет – им оказался руководитель подразделения верхнего уровня (уровень дирекции/управления). При этом его нарушение оказалось достаточно серьезным – отправка на личную почту на бесплатном почтовом (иностранном!) сервисе чувствительных внутренних данных о стратегических планах развития организации.

Почти в половине случаев стаж работы нарушителя приближается к 10 годам! Здесь, наряду с неконтролируемым распространением служебной информации за периметр организации-работодателя, встречается использование рабочего времени в развлекательных целях. А, например, случаи поиска работы наиболее опытными сотрудниками (с максимальным стажем) в пилотной выборке не встречаются.



Типовой нарушитель. Должность

Наиболее частые сферы деятельности нарушителей в организации – кадры (около 20% случаев), юридические службы, инженерные и ИТ-службы, а также делопроизводство (помощники руководителей), и каждая встречается примерно в 13% случаев от общего числа нарушителей, для которых указано структурное подразделение.

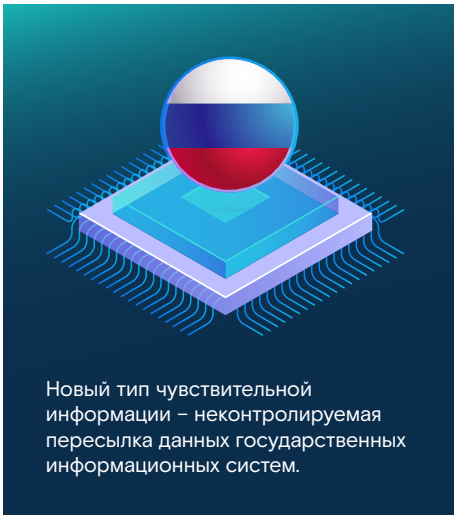


Чаще всего нарушители занимают должности уровня специалиста (48% выявленных случаев, в предыдущем исследовании доля специалистов составляла 65%). 38% - руководитель среднего звена. При этом значительно (с 1% в 2018–2020 годах до 14% в 2021 году) выросла доля нарушителей из числа высшего управленческого звена.

Отправка на личную почту на бесплатном почтовом сервисе внутренних данных - серьезное нарушение

процентов, нарушающих информационную безопасность, как правило, занимают должности уровня специалист

Результаты исследования



Новый тип чувствительной информации – неконтролируемая пересылка данных государственных информационных систем.

Типовой нарушитель. Вид нарушения

Наиболее часто – в 40% случаев – фиксируется неосмотрительное использование личной электронной почты для решения рабочих вопросов. На личные ящики (в том числе на иностранных почтовых ресурсах) оправляется самая разная информация, от вполне будничных рабочих документов до «чувствительных» документов с пометкой «ДСП» (Для служебного пользования) и информации, доступ к которой обусловлен исключительно служебным положением сотрудника: например, информация из государственных информационных систем. Еще в 18% случаев такие конфиденциальные документы копируются на флешки и распечатываются на принтере: дальнейшая их судьба неизвестна, и они вполне могут в таком виде покидать пределы организации.

Одним из наиболее распространенных нарушений (почти 25% зафиксированных инцидентов) являются нарушения в работе с документами, имеющими ограниченный уровень доступа (сведения о штатной структуре и оплате труда в организации-работодателе, о контрагентах и клиентах, о заключенных контрактах).

Новый тип чувствительной информации – данные государственных информационных систем. Нарушения, затрагивающие эту информацию, связаны с неконтролируемой ее пересылкой на личные почтовые ящики сотрудников, а также отправкой третьим лицам. Использование рабочего времени и служебных ресурсов в целях, не связанных с профессиональной деятельностью, по распространенности делит второе место (13%) с копированием служебных документов на флешки.

Среди нецелевой активности на работе, как и в прошлом году, распространены поиск и потребление развлекательного контента, поиск работы и подработка, печать на рабочем оборудовании материалов для личного использования.

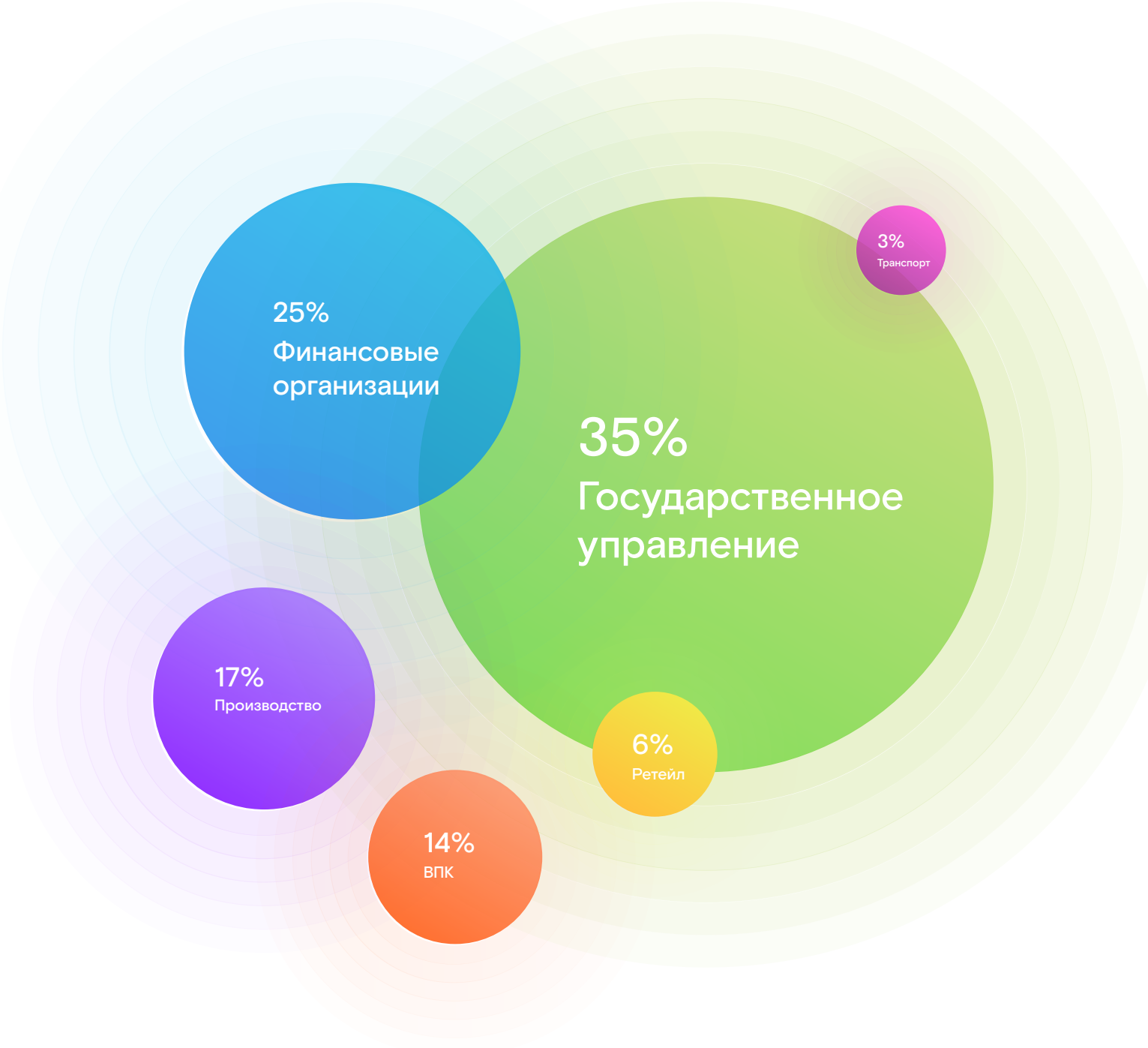
Результаты исследования

Типовой нарушитель.
Отраслевое распределение нарушений

Аналитики «РТК-Солар» провели развернутый анализ нарушений, зафиксированных в организациях 11 сфер экономики. По итогам пилотов DLP-системы Solar Dozor в 2021 году в организациях сферы государственного управления (федеральные и региональные органы власти) зафиксировано 35% от общего числа внутренних инцидентов информационной безопасности. Наиболее критичные нарушения с точки зрения возможного ущерба для организации-работодателя зафиксированы в организациях этого типа среди сотрудников среднего звена (примерный уровень – заместитель начальника отдела).

11

сфер экономики были затронуты нарушениями информационной безопасност.



Результаты исследования

В прошлом году в госсекторе выявилось больше нарушений, чем за 2018-2020 годы

Следует отметить, что преобладание сферы государственного управления в отраслевом распределении нарушений связано с ростом востребованности систем защиты от утечек в госсекторе, нежели с тем, что в госорганизациях происходит больше нарушений. Так, в предыдущем исследовании (за 2018-2020 годы) доля госсектора в общем числе организаций, эксплуатировавших DLP-систему, составила 9,6%, за 2021 год – уже 35%. Госсектор стал больше использовать системы защиты от утечек и, соответственно, выявлять больше нарушений, основная масса которых ранее просто не фиксировалась.

Второе место по количеству подтвержденных инцидентов занимает финансовый сектор (25%). Здесь почти четверть подтвержденных с помощью DLP -системы дисциплинарных нарушений связана с нецелевым использованием рабочего времени и ресурсов работодателя. В основном нарушители служебного распорядка в финансовых организациях занимают должности специалистов юридической службы или службы технической поддержки.

В условиях повсеместной борьбы за сокращение операционных издержек информация, собранная с помощью DLP-системы, может дать пищу для размышлений далеко не только службам информационной безопасности, но и ответственным за оптимизацию штатной структуры и затрат на персонал.

Среди наиболее серьезных нарушений – передача на электронную почту третьего лица на иностранном почтовом сервисе финансовых документов организации, а также признаки коммерческого сговора.

Для производственного сектора (предприятия химической промышленности, металлургическое производство, приборостроение и ТЭК) наиболее характерны (более чем в 50% случаев): небрежное обращение с чувствительной информацией – печать и пересылка третьим лицам, а также нецелевое использование рабочего времени.

Таким образом, расхожее мнение о том, что «на производстве люди делом заняты, а не в YouTube сидят», опровергается результатами исследования второй год подряд.

При этом в этой категории организаций встречаются и признаки конфликта интересов при заключении договора с подрядной организацией.

Четвертое место по числу нарушений – у организаций оборонно-промышленного комплекса. И снова фактически наблюдаемая ситуация опровергает устоявшееся мнение о высоком уровне служебной дисциплины у сотрудников этой категории работодателей.

Выводы проведенного исследования

Типовой нарушитель служебной дисциплины в российской организации в 2021 году – это женщина до 40 лет, со средним стажем работы 6,5 года, специалист одного из следующих подразделений: кадрового, юридического, инженерной или ИТ-службы, а также делопроизводства (помощники руководителя) в организациях сферы государственного управления / производственной сферы / финансовых услуг или организации оборонного комплекса.

Топ-1

менеджеры являются частыми нарушителями

При этом по сравнению с предыдущим исследованием наблюдается существенный прирост числа нарушителей среди высшего управленческого персонала (Топ-1), а наиболее серьезные нарушения (использование для получения коммерческой выгоды сведений из информационных систем организаций и признаки нарушения антикоррупционного законодательства) зафиксированы среди управленцев среднего звена.

E-mail

является главным инструментом нарушителя

Чаты

в мессенджерах также являются местом совершения нарушений

В большинстве случаев нарушители выводят чувствительную внутреннюю информацию за пределы информационного периметра работодателя: пересылают на собственные личные почтовые ящики либо передают неизвестному кругу получателей на их почтовые адреса.

Чаще всего нарушения осуществляются с использованием электронной почты – рабочей или личной, а также посредством бесконтрольного копирования чувствительной информации на съемные носители. Значительно выросла доля нарушений, связанных с выводом чувствительной информации за пределы организации с использованием мессенджеров.

Исследование подготовлено на основе анализа обезличенных данных отчетов о пилотировании DLP-системы Solar Dozor.

Solar Dozor – российская система предотвращения утечек конфиденциальной информации выявления признаков корпоративного мошенничества. Отличается производительностью, проработанным интерфейсом, полнофункциональным агентом под Linux и macOS, возможностью георасределенной работы и технологичностью (нейронные сети, UBA, поддержка VDI).

Узнать подробнее

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