Ростелеком
Солар

Кто он – типовой нарушитель в российской организации?

январь – декабрь 2021

МОСКВА, 2022

Содержание

1. Ключевые цифры и факты

- Возраст типичного нарушителя – **35–40 лет.**
- Средний стаж работы нарушителя – **6,5 года.** Это немногим больше данных предыдущего аналогичного исследования за 2018–2020 годы, где средний стаж работы составил 5 лет.
- Нарушителями в 2021 году несколько чаще становились **женщины** (**54%** зафиксированных инцидентов). По итогам предыдущего исследования за 2018–2020 годы среди нарушителей незначительно преобладали мужчины (55%).
- Стремительно набирающий популярность (**12%** в 2021 году против 3% в предыдущем исследовании за 2018–2020 годы) канал и источник наиболее нестандартных и разнообразных нарушений – **мессенджеры**.
- Самые частые сферы деятельности нарушителей в организации – **кадры (около 20% случаев), юристы, инженерные и ИТ-службы, а также делопроизводители (помощники руководства)** – каждая встречается примерно в **13% случаев**.
- Чаще всего нарушители занимают должности уровня **специалиста** (**48%** выявленных случаев). При этом значительно (с 4% в 2018–2020 годах до **14%** в 2021 году) выросла доля нарушителей из числа высшего управленческого звена.
- Наиболее часто встречаются нарушения следующих типов:
    - нарушения в порядке работы с документами и информацией ограниченного доступа, включая документы с грифом «ДСП» – **58%** нарушений;
    - нецелевое использование рабочего времени и ресурсов работодателя – **13%** нарушений.
- Наиболее погруженные в тему контроля утечек информации компании представлены в сфере **производства (27%) и государственного управления.** Примерно **каждая 4-я** из пилотировавших систему контроля утечек информации и служебной дисциплины организаций относится к органам государственной власти.
- В рамках исследования проанализированы обезличенные данные отчетов о пилотировании DLP-системы Solar Dozor компании «РТК-Солар» в **103**

российских организациях **в 2021** году. Исследованная выборка сотрудников составила **около 300 человек.**

2. Методология

- Данное исследование подготовлено на основе анализа обезличенных данных **отчетов о пилотировании DLP-системы Solar Dozor, в том числе модуля поведенческого анализа Dozor UBA,** в российских организациях на протяжении 2021 года.

  DLP-система Solar Dozor ведет сплошной анализ трафика с рабочих станций сотрудников на предмет наличия в их ежедневной работе за компьютером признаков нарушений в области информационной безопасности и нарушений служебной дисциплины. Анализируются такие источники данных, как: корпоративная электронная почта, веб-трафик (посещаемые интернет-сайты, сохранение информации на внешние облачные хранилища), хранение информации на рабочих компьютерах, ее копирование на съемные носители и сохранение на внутренних файловых хранилищах организации, печать документов.

  Пилотирование DLP-системы обычно проводится по желанию организации-заказчика перед принятием решения о покупке и позволяет бесплатно протестировать ее возможности на выбранном количестве реальных пользователей организации и оценить ее эффективность для решения реальных бизнес-задач потенциального заказчика.

  В соответствии с методикой анализа инцидентов информационной безопасности, использующейся в DLP-системе Solar Dozor, ***инцидент*** *– это случай нарушения политики информационной безопасности организации, подтвержденный службой информационной безопасности. Таким образом, нарушения, описанные в настоящем отчете, несут в себе существенные риски для нормальной работы «пилотных» организаций, – что* ***подтверждено самими организациями***.
- Организации, пилотировавшие Solar Dozor, относятся к сегментам Small&Middle Business, Small&Middle Enterprise и Large Enterprise. Для большей наглядности вошедшие в исследуемую выборку организации разбиты по численности сотрудников на следующие категории: до 500 сотрудников, 500–1000 сотрудников и свыше 1000 сотрудников.
- В исследование вошли такие рыночные сегменты, как оборонная промышленность, транспорт, финансы, органы государственной власти и государственное управление, химическая промышленность и организации здравоохранения, энергетика и ряд других – всего около **11 отраслей и направлений деятельности**.

3. Введение

Компания «РТК-Солар», национальный провайдер технологий и сервисов кибербезопасности, представляет второе регулярное исследование «**Кто он – типовой нарушитель в российской организации?**»

Аналитики «РТК-Солар» изучили обезличенные данные отчетов о пилотировании DLP-системы Solar Dozor в **более 100 российских организациях** самых разных сфер деятельности – от приборостроения до военно-промышленного комплекса, от финансового сектора до медицины. Пилотные проекты проводились в период **с января по декабрь 2021 года**. Исследуемая выборка лиц, фигурирующих в обнаруженных инцидентах безопасности, составила **чуть менее 300 человек**.

Изначально работа DLP-системы Solar Dozor направлена на выявление признаков утечки служебной информации / информации ограниченного доступа за пределы информационного периметра организации. Однако при анализе обнаруживаемых с помощью DLP-системы инцидентов становится очевидно, что значительная часть нарушений, попадающих в поле зрения служб безопасности, связана с широким спектром нарушений служебной дисциплины. Это и несоблюдение парольной политики организации, и нецелевое использование рабочего времени сотрудниками, и признаки конфликтных коммуникаций в переписке по корпоративной электронной почте, и многое другое.

Таким образом, результаты данного исследования можно рассматривать как пособие по нарушениям служебной дисциплины различного характера, имеющим место в самых разных российских организациях.

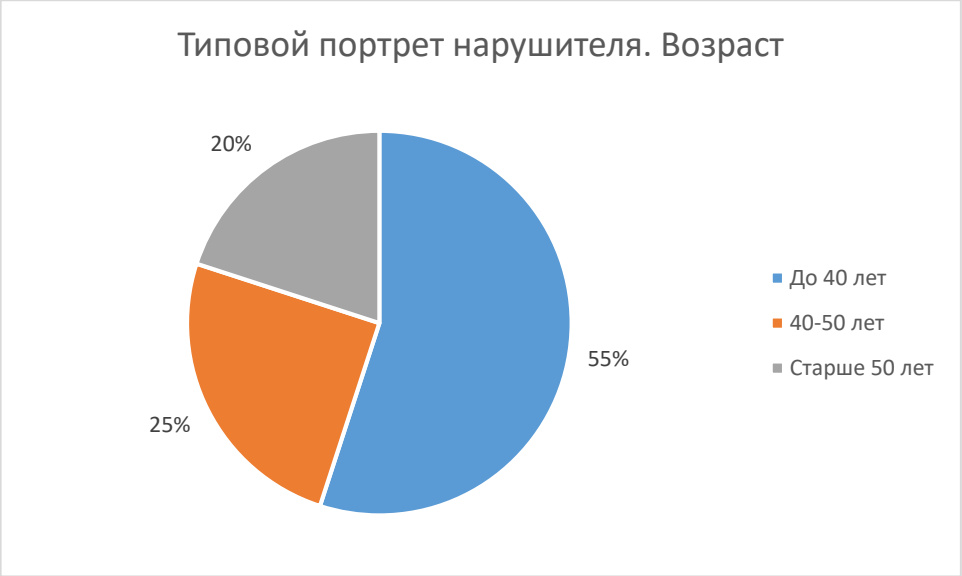
4. Результаты исследования

4.1 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%**.

4.2 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.



При этом ***для нарушителей-женщин*** **молодого (до 40 лет) возраста** наиболее распространенным нарушением (в половине наблюдаемых случаев) является небрежное хранение и неосторожное распространение учетных данных для работы с информационными системами.

Также среди частых нарушений – неконтролируемое с точки зрения работодателя распространение служебной 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.

Среди сотрудников старшей возрастной группы (**старше 40 лет**) наиболее типично небрежное обращение с чувствительной служебной информацией, конфиденциальной и

имеющей отметку «Для служебного пользования». Документы **в 4 случаях из 5** неконтролируемо распространяются за периметр организации (пересылаются на электронную почту), а **в каждом 5-м случае** – распечатываются.

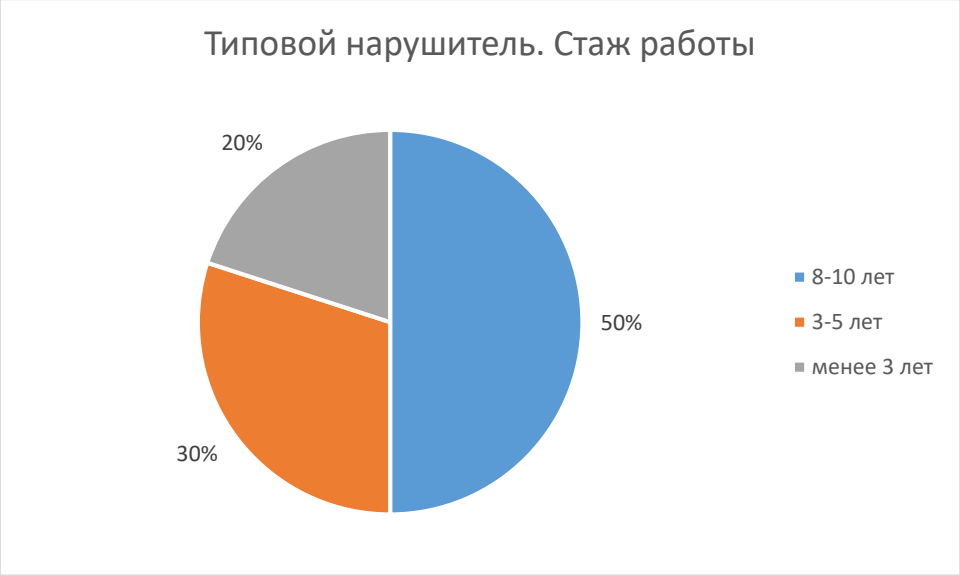
При этом нарушители в младшей возрастной группе (до 40 лет) в основном занимают должности специалистов и руководителей младшего уровня в организациях сферы государственного управления, а нарушители старшего возраста – руководителей среднего уровня (начальник отдела) в организациях оборонного комплекса. И это при том, что большинство организаций обеих этих категорий имеет четкие внутренние регламенты, в которых прописаны правила обращения сотрудников со служебной информацией!

4.3 Типовой нарушитель. Стаж работы

Среди сотрудников, для которых определен стаж работы в текущей организации, работников на испытательном сроке на этот раз не оказалось (в предыдущем исследовании за 2018–2020 годы их было чуть менее 40 процентов!). **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.

Прекращение нарушений со стороны сотрудников на испытательном сроке можно объяснить тем, что в течение первого года пандемии и тотальной удаленки большинству организаций удалось наладить рабочие процессы и контроль сотрудников, работающих в удаленном и гибридном формате, включая новичков, еще плохо знакомых с внутренними правилами и зачастую нарушающих по незнанию или в связи с отсутствием отлаженных процессов удаленного доступа к корпоративным ресурсам.

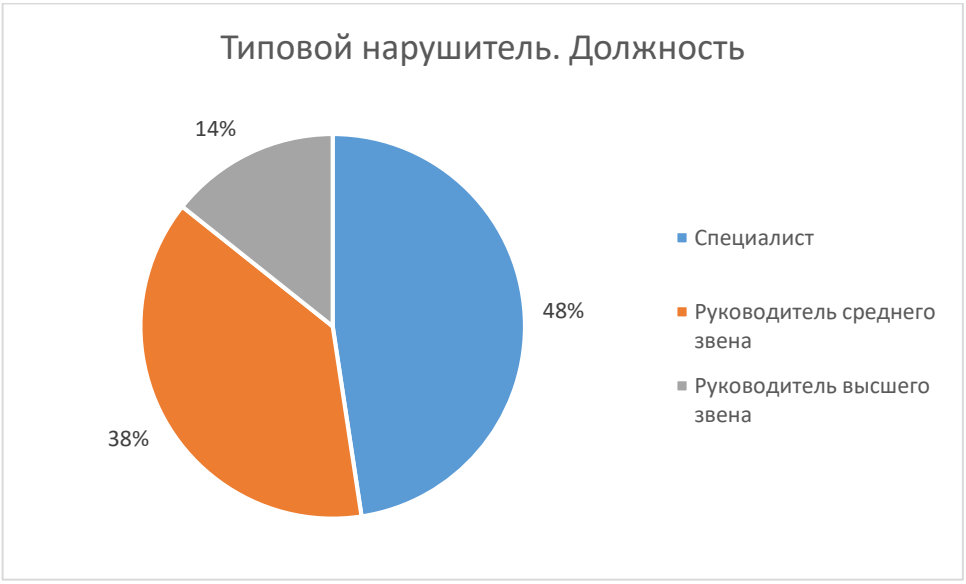
Почти в половине случаев стаж работы нарушителя приближается к 10 годам! Здесь, наряду с неконтролируемым распространением служебной информации за периметр организации-работодателя, встречается использование рабочего времени в развлекательных целях. А, например, случаи поиска работы наиболее опытными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



4.4 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%). При этом значительно (с 1% в 2018–2020 годах до **14%** в 2021 году) выросла доля нарушителей из числа **высшего управленческого звена.** Эти изменения можно объяснить, в частности, тем, что в государственных органах и организациях, занимающих существенную часть исследования, в этой группе фиксируется 44% нарушений.



4.5 Типовой нарушитель. Вид нарушения

Выявляемые с помощью DLP-системы нарушения, как и в предыдущем исследовании, разнообразны: это и копирование наработанных на текущем трудовом месте материалов в процессе трудоустройства в новую компанию, и изучение контента с элементами порнографии в социальных сетях и поисковых ресурсах, и подработка в сторонней организации в основное рабочее время.

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.

Данные отчетов 2021 года показывают, что одним из наиболее распространенных нарушений (почти **25%** зафиксированных инцидентов) по-прежнему являются нарушения в работе с документами, имеющими ограниченный уровень доступа, прежде всего с ДСП-документами и с информацией, носящей конфиденциальный служебных характер (сведения о штатной структуре и оплате труда в организации-работодателе, о контрагентах и клиентах, о заключенных контрактах).

Новый тип такой чувствительной информации в этом году (в предыдущем отчете за 2018–2020 годы он не фигурировал) – 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.

4.6 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).

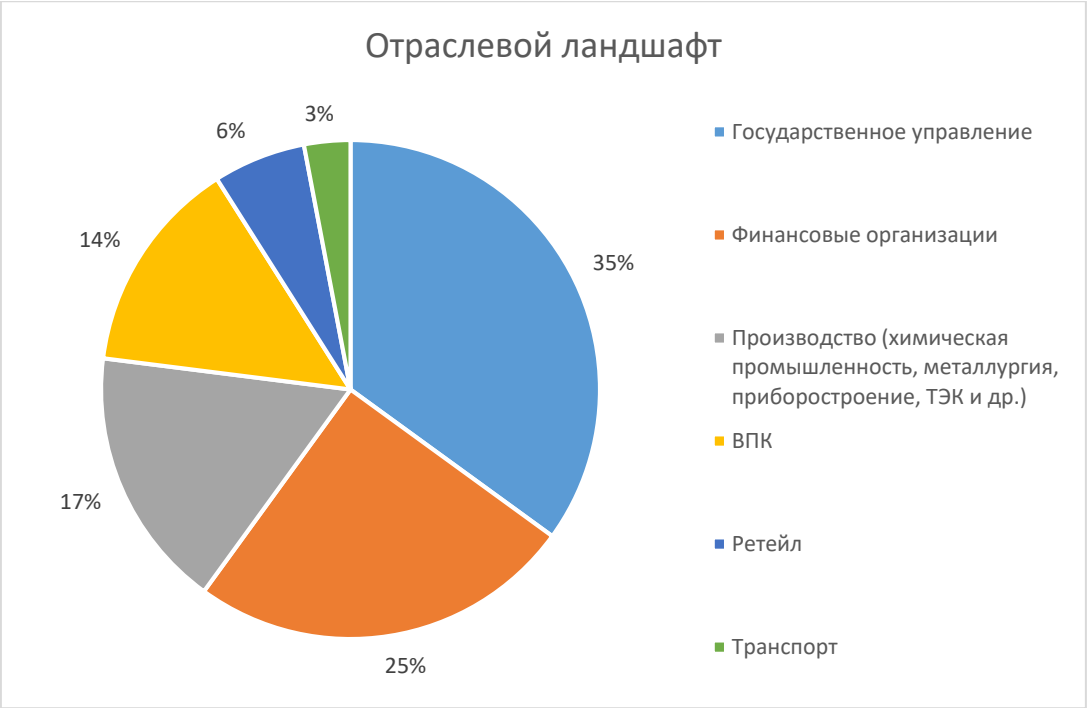
Следует отметить, что преобладание сферы государственного управления в отраслевом распределении нарушений связано скорее с ростом востребованности систем защиты от утечек в госсекторе нежели с тем, что в госорганизациях происходит больше нарушений. Так, в предыдущем исследовании (за 2018-2020 годы) доля госсектора в общем числе организаций, эксплуатировавших DLP-систему, составила 9,6%, а в данном исследовании 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.

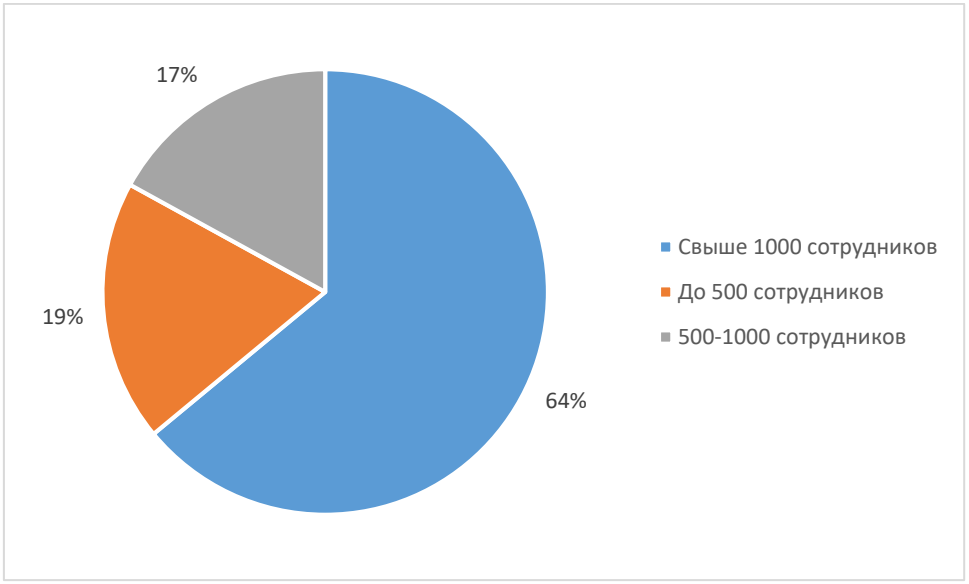
Для **производственного сектора** (в него включены предприятия химической промышленности, металлургическое производство, приборостроение и ТЭК) наиболее характерны (**более чем в 50% случаев**): небрежное обращение с чувствительной информацией (в том числе со сведениями с пометкой «Конфиденциально») – 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 отдельные признаки экономических правонарушений встречаются и в этой категории исследуемых организаций: это 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.

4.7 Размер опрошенных компаний



5. Выводы

Авторы исследования – эксперты компании «РТК-Солар» заключают: типовой нарушитель служебной дисциплины в российской организации в 2021 году – это, скорее, **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.**

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**.

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.

Контактная информация

Телефоны:

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

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

E-mail: info@rt-solar.ru

support@rt-solar.ru

Адреса:

125009, Москва, Никитский пер., 7, стр. 1

127015, Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд