Ростелеком
Солар

Кто он – типовой нарушитель в российской организации?

2018–2020

Содержание

1 Ключевые цифры

В рамках исследования проанализированы обезличенные данные отчетов о пилотировании DLP-системы Solar Dozor компании «Ростелеком-Солар» почти в **150** российских организациях **с 2018 по 2020** год.

Средний возраст нарушителя – **до 40 лет.**

Средний стаж работы нарушителя – около 5 лет.

Нарушителями в основном являются **мужчины** (**55%** зафиксированных инцидентов).

Наиболее частые сферы деятельности нарушителей в организации – бухгалтерия и закупки, техническая поддержка пользователей и содержание инженерной инфраструктуры: около 30% и 25% соответственно от общего числа нарушителей, для которых определено структурное подразделение.

Исследуемая выборка сотрудников составляет чуть менее **300 человек**.

Чаще всего нарушители занимают должности уровня специалиста (65% выявленных случаев).

Наиболее часто встречаются нарушения следующих типов: нецелевое использование рабочего времени, включая подработку; нарушения в порядке работы с документами и информацией ограниченного доступа, включая документы с грифом «ДСП».

Наиболее часто от инцидентов, связанных с нарушениями служебной дисциплины и информационной безопасности, страдают организации следующих сфер: производство, финансы, транспорт и логистика, оборонно-промышленный комплекс (ОПК).

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 трех лет: с 2018 по 2020 г.

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 100 сотрудников, 100–500 сотрудников, 500–1000 сотрудников и свыше 1000 сотрудников.

В исследование вошли такие рыночные сегменты, как добыча и переработка полезных ископаемых, производство оборудования и техники, образование, финансы, ретейл, транспорт и логистика, медицина (фармацевтика), ИТ/Телеком, государственное управление и ряд других – всего около 20 отраслей и направлений деятельности.

3 Введение

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

Аналитики «Ростелеком-Солар» изучили обезличенные данные отчетов о пилотировании DLP-системы Solar Dozor в **более чем 150 российских организациях** самых разных сфер деятельности, от производства систем автоматизации управления сложными производственными объектами до аренды автомобилей, от розничных продаж до информационного обеспечения деятельности органов государственной власти. Пилотные проекты проводились в период **с 2018 по 2020 год**. Исследуемая выборка лиц, фигурирующих в обнаруженных инцидентах безопасности, составила почти **300 человек**.

Изначально работа DLP-системы Solar Dozor направлена на выявление признаков утечек 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 организациях.

4 Результаты исследования

4.1. Типовой нарушитель: пол

Служебную дисциплину и правила информационной безопасности чаще нарушают… **мужчины.**

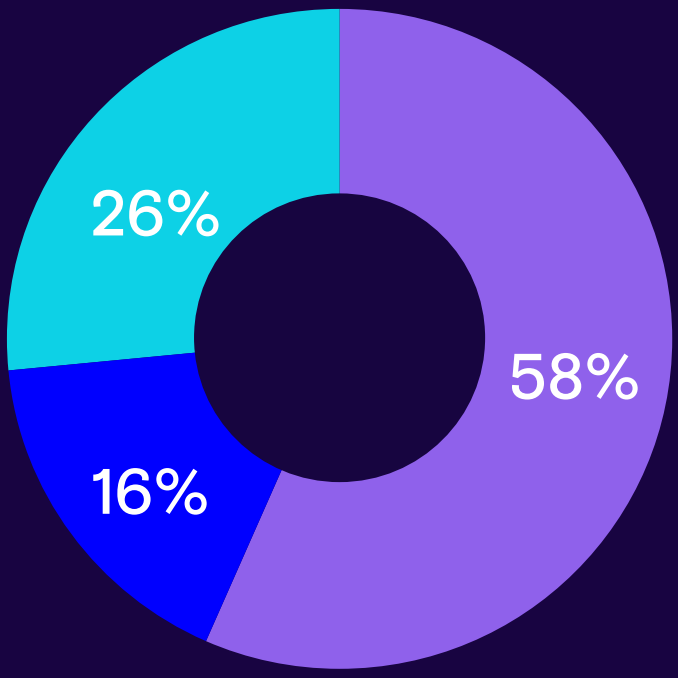
Несмотря на расхожее мнение о том, что женщины более импульсивны, что может, в частности, влечь за собой нарушение дисциплины. Женщин среди нарушителей в рамках исследования – 45%.

4.2. Типовой нарушитель: возраст

Основная часть нарушителей приходится на **молодых сотрудников в возрасте до 40 лет.** Их почти 60% в общем количестве нарушающих.

При этом для нарушителей-мужчин молодого возраста характерно наличие подработок в основное рабочее время, а для женщин – поиск работы (рассылка резюме и их публикация на сервисах по поиску работы).

Также достаточно большая доля нарушений приходится на сотрудников в возрасте **40–50 лет**: почти **25%**. Для мужчин этого возраста более характерно нецелевое использование рабочего времени (в основном для посещения развлекательных ресурсов), а для женщин все так же актуален поиск работы. Кроме того, нарушители-женщины замечены в пересылке на внешние почтовые адреса, в том числе личные, данных о штатной структуре и оплате труда в организациях-работодателях. Такая специфика, скорее всего, определяется тем, что в составе подразделений, где хранится эта информация (бухгалтерия и отделы кадров), в России традиционно преобладают женщины.



Распределение увольнений по отраслям

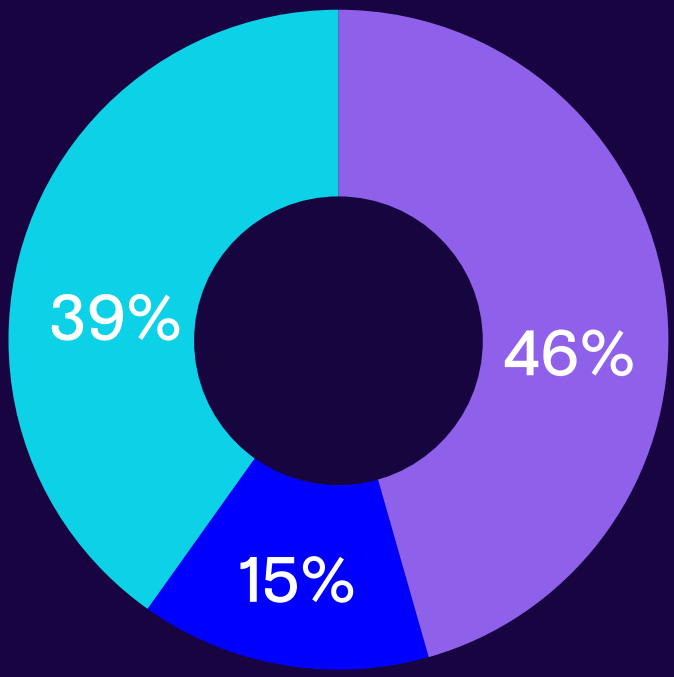
- До 40 лет
- 40-50 лет
- 50+ лет

В целом данные о возрастном составе нарушителей служебной дисциплины, выявленные с помощью Solar Dozor, подтверждают общие гипотезы современных социологов об особенностях поведения, например, поколения «до 40»: эти люди, как правило, более мобильны в выборе места работы, а также свободны в использовании средств интернет-коммуникаций. Они чаще и охотнее общаются по электронной почте, в мессенджерах и социальных сетях, в том числе обсуждая рабочие вопросы, и психологически более предрасположены к пересылке и публикации служебной информации и документов за пределы организации-работодателя.

Интересно, что эти тенденции находят подтверждение и для сотрудников организаций оборонно-промышленного комплекса – при том что большинство таких компаний имеет хорошо оформленную политику обращения сотрудников со служебной информацией. Как минимум в 5 организациях научно-производственного профиля ОПК зафиксированы случаи отправки сотрудниками на внешние почтовые адреса (в том числе адреса иностранных публичных почтовых ресурсов типа gmail.com) информации и документов ограниченного уровня доступа, в частности с грифом секретности.

4.3. Типовой нарушитель: стаж работы

Из сотрудников, для которых удалось установить стаж работы в текущей организации, чуть менее 40% нарушителей находились на испытательном сроке! Все они относятся к младшей возрастной категории, их возраст не превышает 30 лет. Основным нарушением для всех является нецелевое использование рабочего времени (просмотр развлекательного контента, поиск в сети интернет и печать материалов для личного использования). Сотрудники, чей стаж работы превышает 5 лет, чаще всего заняты поиском работы, в том числе в организациях – конкурентах своего текущего работодателя.

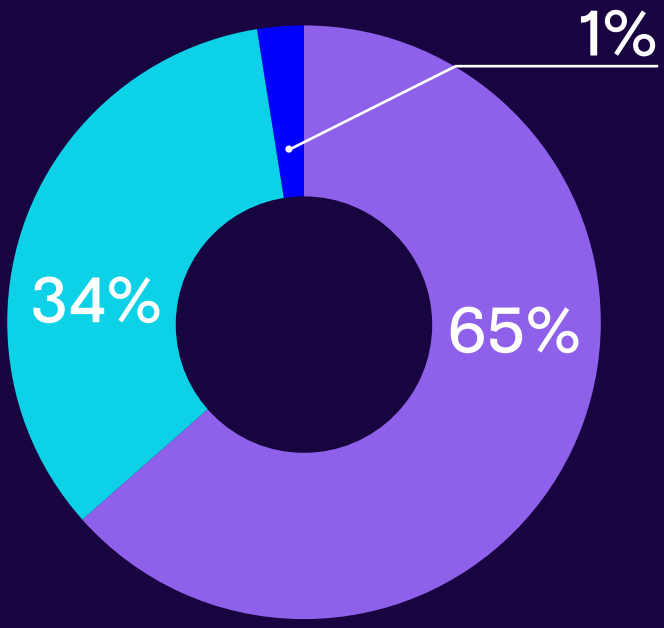


Распределение увольнений по отраслям

- Стаж свыше 5 лет
- На испытательном сроке
- Стаж до 5 лет

4.4. Типовой нарушитель: должность

Более чем в 30% случаев нарушают служебную дисциплину, в том числе политику информационной безопасности организации, руководители различного уровня. Это и функциональные руководители (бухгалтерия, охрана труда, делопроизводство), и руководители структурных подразделений, и руководство высшего звена (заместители руководителя организации). В выявленных инцидентах – 3 нарушителя из последней категории. При этом в абсолютном выражении среди нарушающих преобладают сотрудники, занимающие должности специалистов (65% исследуемых).



Распределение увольнений по отраслям

- Специалист
- Руководитель
- Руководитель высшего звена

4.5. Типовой нарушитель: вид нарушения

Вариативность нарушений разнообразна: это и копирование наработанных на текущем месте работы 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 (почти в 30% случаев) фиксируемое нарушение – нецелевое использование рабочего времени и служебных ресурсов в целях, не связанных с профессиональной деятельностью: поиск и потребление развлекательного контента, подработка, печать на рабочем оборудовании материалов для личного использования.

Достаточно тревожным является тот факт, что следующим по частоте (23% зафиксированных инцидентов) видом нарушений являются нарушения в работе с документами, имеющими ограниченный уровень доступа, прежде всего с ДСП-документами. А также с информацией, носящей конфиденциальный служебный характер: сведения о штатной структуре и оплате труда в организации-работодателе, о контрагентах и клиентах, о заключенных контрактах, оценочные суждения и подробности организации внутренних бизнес-процессов. Эта информация

неконтролируемо распространяется посредством пересылки на личные почтовые ящики сотрудников, а также отправки третьим лицам.

Пожалуй, наиболее показательными в этом смысле являются зафиксированные в крупной судостроительной организации случаи отправки конструкторской документации на внешние почтовые адреса на иностранных почтовых ресурсах типа gmail.com. А также неоднократно фиксировавшиеся случаи пересылки на внешние почтовые адреса публичных почтовых сервисов служебной информации сотрудниками организаций ВПК.

4.6. Отраслевой ландшафт опрошенных компаний

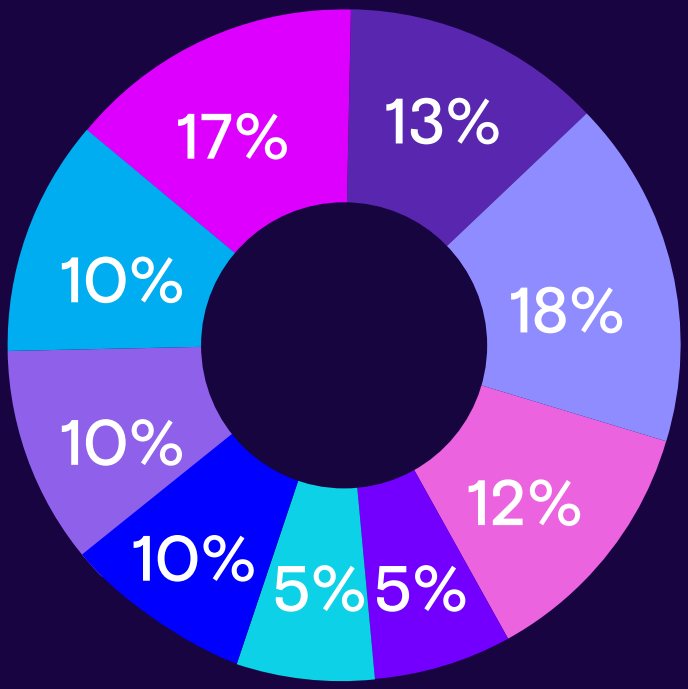
Проанализировав ситуацию в отраслях, в которых были зафиксированы нарушения сотрудниками руководящего звена, аналитики «Ростелеком-Солар» отметили следующие интересные факты: наибольшее число нарушающих служебную дисциплину руководителей представляют организации финансовой сферы, а также компании, оказывающие транспортно-логистические услуги: 20% и 15% соответственно.

Также интересно, что признаки нарушения политик информационной безопасности среди руководителей различного уровня зафиксированы почти в 10% случаев в организациях оборонного комплекса! Среди подозрительных действий здесь – копирование на съемные носители документации ограниченного доступа, нецелевое использование рабочего времени и поиск работы руководителем молодого возраста.

При этом наиболее критичные нарушения руководителей – с точки зрения возможного ущерба для организации-работодателя – зафиксированы в организациях направления «Транспорт и логистика». В нескольких случаях наблюдалось массовое (более 100 единиц) копирование на съемные носители ДСП-документов, в том числе закупочной документации, а также документов с грифом «Коммерческая тайна»; также выявлены признаки сговора при создании нового юридического лица между бывшими и действующими сотрудниками и распространения информации о распределении бонусных выплат в организации.

Среди других серьезных нарушений – перемещение за информационный периметр организации (пересылка на внешние адреса) расчетных ведомостей и налоговых деклараций сотрудников органа государственной власти.

В целом же лидером по числу нарушений информационной безопасности и служебной дисциплины являются сотрудники организаций производственного сектора (начиная от производства продуктов питания и заканчивая производством оборудования для предприятий химической промышленности и электроэнергетики, а также строительством объектов для ВПК): на их долю приходится почти 5-я часть всех зафиксированных нарушений. Очевидно, что здесь основная доля нарушений фиксируется среди так называемого офисного, или административного, персонала производственных предприятий.



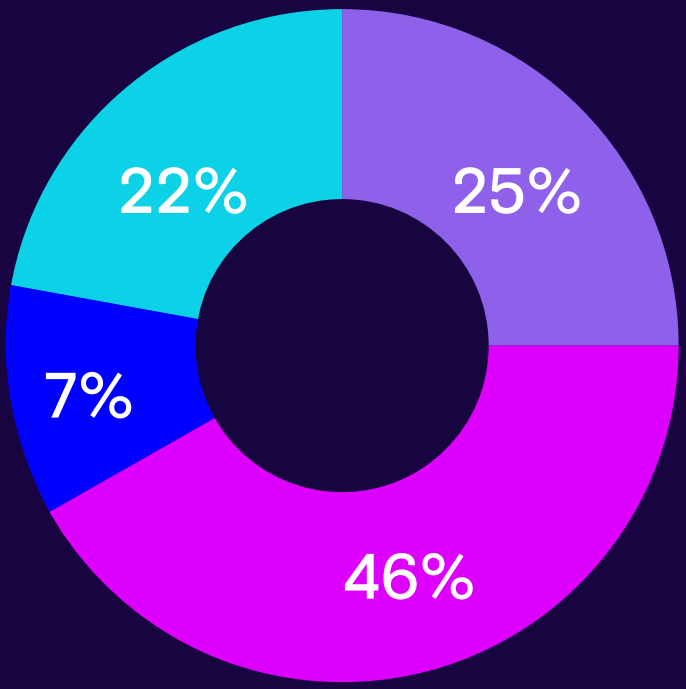
Отраслевой ландшафт

- Производство и строительство
- Финансы
- ВПК
- Транспорт и логистика
- Органы государственной власти
- Оптово-розничная торговля
- Другое
- Сфера услуг
- Разработка ПО/интеграция

Нужно отметить, что данная тенденция категорически опровергает расхожее мнение о том, что «на производстве люди делом заняты, а не в Youtube сидят». Практически не отличается количеством нарушителей от производства и сфера финансов. Третье 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.

Также среди интересных тенденций в отношении отраслевого состава компаний, в которых были выявлены нарушители, необходимо отметить: значительное количество нарушителей было выявлено среди сотрудников государственных органов и организаций, обеспечивающих функционирование их информационно-телекоммуникационной инфраструктуры. Всего на 5 организаций этого типа приходится 27 нарушителей, что составляет чуть менее 10% от всей исследуемой выборки.

4.7. Размер опрошенных компаний



Разделение по количеству сотрудников

- Свыше 1000
- От 500 до 1000
- От 100 до 500
- До 100

5 Выводы

Авторы исследования – эксперты компании «Ростелеком-Солар» заключают: типовой нарушитель служебной дисциплины в российской организации – это, скорее, мужчина до 40 лет, со средним стажем работы около 5 лет, специалист в сфере финансов (закупок) или технической поддержки организации производственной сферы / финансовых услуг или организации оборонного комплекса, в лучшем случае занятый в течение рабочего дня просмотром развлекательного контента, а в худшем – осуществляющий бесконтрольную отправку внутренних служебных документов и информации неизвестному кругу получателей за пределами организации-работодателя либо массово копирующий информацию с грифом «ДСП» на личный съемный носитель.

Ростелеком
Солар

rt.ru
rt-solar.ru

E-mail:
info@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, ул. Вятская, 35/4, БЦ «Вятка», 1-й подъезд