Какие организации чаще других становятся жертвами внутренних нарушений?

2022

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

Ростелеком Солар

Содержание

Ключевые цифры и факты

Самая частая жертва нарушителей

организация производственной сферы с численностью сотрудников более 1000 человек, где каждое 30-е нарушение носит статус «Критичное».

Топ-3 самых нарушающих отраслей

производственная сфера (29% всех нарушений), государственные организации (24% нарушений), финансы (15% нарушений).

Лидер по числу критичных нарушений

организация финансовой сферы: 87% всех зарегистрированных событий (7817) в ней были критичными.

Наиболее распространенные внутренние нарушения

неконтролируемый вывод конфиденциальной информации за периметр организации (36%), нецелевое использование рабочего времени (25%), признаки коммерческого сговора, нарушения ограничений и запретов, конфликт интересов (16%).

Наиболее частые каналы нарушений

пересылка конфиденциальной информации на личные внешние почтовые ящики (чуть более 37%), копирование на флешки и слив данных в мессенджерах (по 17% каждый).

Методология

DLP-система Solar Dozor ведет полный 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 DLP-системе Solar Dozor, в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044-2007, используется так называемая инцидентная модель управления рисками информационной безопасности. При проведении пилотирования инцидентом является случай нарушения политики информационной безопасности организации, подтвержденный ответственным сотрудником ИБ-службы. Таким образом, все упомянутые в данном исследовании инциденты и статистика на их основе признаны самими заказчиками как нарушения.

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, 100–200 сотрудников, 200–500 сотрудников, 500–1000 сотрудников, свыше 1000 сотрудников.

В выборку вошли такие рыночные сегменты, как переработка и реализация природных ресурсов, приборостроение, химическая промышленность, финансы, ретейл, ИТ и интеграция, государственное управление и ряд других направлений — всего свыше 10 отраслей.

Данное исследование подготовлено на основе анализа обезличенных данных отчетов о пилотировании DLP-системы Solar Dozor в 307 российских организациях в 2021 году.

Результаты данного исследования можно рассматривать как «пособие» по нарушениям трудовой дисциплины и их трендам, имеющим место в самых разных организациях.

Введение

Аналитики компании «Ростелеком-Солар» изучили обезличенные данные отчетов о пилотировании DLP-системы Solar Dozor более чем в 300 российских организациях самых разных сфер деятельности, от ИТ-сопровождения деятельности органов государственной власти до транспортно-логистических услуг, от переработки полезных ископаемых до ретейла. Пилотные проекты проводились в 2021 году. Исследуемая выборка лиц, фигурирующих в обнаруженных инцидентах безопасности, составила около 800 человек.

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

Результаты исследования

1. Портрет организации, подверженной нарушениям

Полученный по результатам исследования портрет организации, наиболее подверженной различным видам нарушений сотрудниками трудовой дисциплины, включая нарушение правил безопасного обращения со служебной информацией, выглядит следующим образом: это организация производственной сферы с численностью сотрудников более 1000 человек.

Выявленными в них нарушениями чаще всего становятся:

- пересылка служебной информации на личную почту на внешнем почтовом сервисе (что автоматически делает неконтролируемым ее дальнейшее распространение и использование);
- передача служебной информации третьим лицам;
- использование рабочего времени в личных интересах, в том числе для подработки или поиска работы.

В среднем каждое 30-е нарушение, которое фиксирует в такой организации DLP-система, носит статус «Критичное».

2. Отраслевой ландшафт и размеры организаций, наиболее подверженных нарушениям

2.1. Самые «нарушающие» отрасли

Отраслью, в которой за минувший год было зафиксировано наибольшее количество (29%) внутренних нарушений информационной безопасности, включая утечки информации, нецелевое использование рабочего времени и др., стала производственная сфера. На втором месте – государственные организации (24% нарушений), замыкает тройку антилидеров финансовая отрасль (15% нарушений).

Следует отметить, что производство лидировало по объему внутренних нарушений и в предыдущем исследовании за 2020 год. А вот государственная сфера за минувший год обогнала финансовые организации по количеству выявленных внутренних нарушений, переместившись с 3-го места в 2020-м году на 2-е в 2021-м. Однако аналитики «Ростелеком-Солар» связывают это скорее не с резким ростом нарушений в госорганизациях, а с интенсивным внедрением систем защиты от внутренних угроз в государственной сфере, где раньше процент их использования был невысок. Так, в 2021 году объем пилотирования и внедрения систем защиты от утечек информации (DLP) в организациях сферы государственного управления составил почти четверть (24%) от общего числа организаций, пилотировавших DLP-систему Solar Dozor, против 10% – в 2020 году.

«Ростелеком-Солар», обладая опытом внедрения самой большой в Европе инсталляции DLP-системы (250 тысяч рабочих мест сотрудников Сбербанка), выглядит безусловно привлекательным для финансовых организаций как поставщик DLP-решения.

Также существенно (с 7% до 12%) вырос интерес к системам контроля нарушений информационной безопасности и служебной дисциплины среди разработчиков ПО и ИТ-интеграторов. Аналитики «Ростелеком-Солар» полагают, что растущее число громких утечек персональных данных пользователей различных интернет-сервисов подталкивает их разработчиков, традиционно настроенных достаточно консервативно, тестировать новые инструменты защиты. В целом на рынке DLP-систем наблюдается оживление спроса, компании-пользователи становятся квалифицированнее и легче идут на апробацию новых для себя вариантов защиты от внутренних угроз, где решающей становится не цена продукта, а его реальная эффективность, доля обнаруженных нарушений.

Устойчивый интерес к DLP-системам год от года проявляют организации финансовой сферы. Аналитики связывают это с наличием формальных требований со стороны регуляторов к финансовым организациям по использованию средств защиты от утечек данных клиентов.

2.2. Размер самых «нарушающих» компаний

Большинство организаций, где зафиксированы внутренние нарушения, являются крупными компаниями со штатом свыше 1000 сотрудников. Однако не стоит думать, что в небольших компаниях нет нарушений – просто там в большинстве случаев нет систем мониторинга внутренних угроз, которые крупные организации, как правило, взяли себе на вооружение.

3. Наиболее частые каналы нарушений

Результаты исследования говорят о том, что наиболее частыми каналами для совершения внутренних нарушений в 2021 году стали: пересылка конфиденциальной информации (в том числе служебных документов с грифом «Для служебного пользования») на личные внешние почтовые ящики (чуть более 37%), копирование этой информации на флешки и слив данных в мессенджерах (по 17% каждый). В последние годы именно эти каналы являются наиболее востребованными у злоумышленников, поскольку они наиболее просты и удобны в использовании.

Наиболее частые каналы нарушений

37,3%
Пересылка конфиденциальной информации на личную почту, почту третьих лиц

17,0%
Копирование конфиденциальной информации на съемные носители

17,0%
Мессенджеры

13,8%
Использование личной почты для решения рабочих вопросов

6,4%
Печать конфиденциальной информации на принтере

6,4%
Несанкционированное хранение конфиденциальной информации на рабочей станции

2,1%
Хранение и использование потенциально вредоносного ПО

При этом практика мало коррелирует с представлениями специалистов по информационной безопасности о том, какие каналы передачи информации необходимо контролировать прежде всего. В приоритете безопасников – контроль веб-трафика, печати документов и использования съемных носителей информации (перехват данных в каждом из этих каналов коммуникации тестируется в половине всех пилотных проектов Solar Dozor).

В этом смысле образ «типового нарушения», сложившийся у службы информационной безопасности, выглядит несколько архаичным – по крайней мере, для технологически продвинутых регионов. Очевидно, что в 21 веке для вывода информации за периметр организации существуют гораздо более доступные средства, чем, например, флешка или – тем более – печать на бумаге. В этом смысле гораздо более оправданным выглядит контроль мессенджеров, которые как рисксодержащий канал коммуникации в пилотных проектах DLP-системы Solar Dozor незначительно, но тем не менее уступают по популярности тем же съемным носителям и печати (41% пилотов).

Контроль веб- и десктопных версий Telegram, WhatsApp и прочих мессенджеров – даже используемых с рабочего компьютера в основное рабочее время – все еще является юридически недостаточно проработанным шагом для большинства работодателей.

Объем и плотность трафика (интенсивность переписки по разным каналам и других действий пользователей на рабочих станциях) по-прежнему значительно различаются от организации к организации.

4. События и нарушения

Согласно статистике собранного во время пилотирования DLP-системы трафика среднее число проанализированных сообщений в каждой организации составило 900 тысяч единиц. Это почти на 30% больше показателя из предыдущего исследования (589 тысяч единиц).

Рост числа перехватываемых сообщений аналитики «Ростелеком-Солар» связывают с дальнейшей адаптацией работодателей и сотрудников к гибридному и удаленному режиму работы в 2021 году, что во многих случаях сопровождается увеличением объема онлайн-коммуникаций.

При таком объеме анализируемого трафика среднее количество выявляемых нарушений разного типа и уровня критичности (от потенциальной угрозы низкого уровня критичности до реального инцидента, подтвержденного службой безопасности) в каждой из пилотных площадок составило около 10 тысяч. То есть каждое 9-е анализируемое с помощью DLP-системы сообщение содержит в себе потенциальную угрозу для организации.

Объем анализируемых коммуникаций зависит от целого ряда факторов: продолжительности пилотного проекта, количества пользователей под наблюдением, количества самих каналов перехвата (в одном случае под мониторинг попадает только переписка по электронной почте, а в другом — добавляется переписка через внешние почтовые ресурсы, переписка во всевозможных мессенджерах, а также копирование и печать файлов и их размещение в файловых хранилищах) и т. д.

Наибольшее количество перехваченных сообщений — более 3,5 млн — получено за время пилотного проекта длительностью 3 месяца в крупной организации металлургического комплекса (лидер предыдущего исследования — финансовая сфера). При этом выборка сотрудников для мониторинга во время пилота составила 800 человек, у которых контролировались все основные каналы коммуникаций: корпоративная почта, веб-трафик, мессенджеры, файловые системы, съемные носители, печать.

Отметим, что средний объем анализируемого трафика на 1 сотрудника в месяц в этой организации выше среднего, он составил порядка 1500 сообщений. При этом среднее количество анализируемых сообщений в организациях, по которым соответствующая статистика была доступна, составляет 1100 в месяц на одного сотрудника.

Явным экстремумом выглядят данные одного из клиентов — финансовой организации, где за 2,5 месяца было проанализировано порядка 1,7 млн сообщений 30 сотрудников, включенных в пилотную выборку. Таким образом, среднее количество сообщений на 1 сотрудника здесь составило 23 тысячи сообщений в месяц. Нужно заметить, что финансовые организации традиционно являются лидерами по интенсивности коммуникаций сотрудников, поскольку их ежедневные рабочие процессы связаны с многотысячными клиентскими базами.

Антилидером по доле событий критичного и высокого уровня угрозы в общем объеме событий информационной безопасности, зарегистрированных системой Solar Dozor, стала другая финансовая организация. 87% всех зарегистрированных событий (7817) в ней были маркированы как имеющие «критичный» и «высокий» уровень угрозы.

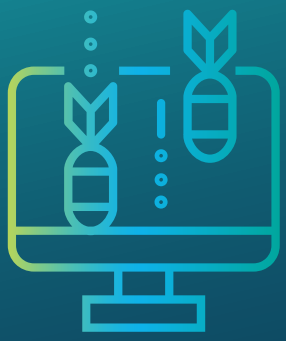
Аналитики «Ростелеком-Солар» считают данный факт отчасти следствием того, что в финансовых компаниях введены очень строгие правила информационной безопасности и работы с конфиденциальной информацией. Также следует учесть, что в организациях финансовой сферы у сотрудников выше соблазн к разного рода нарушениям и мошенничеству ввиду близости к деньгам.

На втором месте по количеству критичных инцидентов расположилась организация производственной сферы (приборостроение) — в ней зафиксировано 53% критичных инцидентов от всего объема событий безопасности. Тройку замыкает направление консалтинга (информационно-аналитическое сопровождение ИТ-решений) — здесь из всего объема событий безопасности 52% могут нанести ощутимый ущерб компании.

Среди обнаруживаемых нарушений чаще всего (36% зафиксированных случаев) по-прежнему встречается неконтролируемый вывод за информационный периметр работодателя служебной информации. Сотрудники пересылают рабочие документы себе на личную почту, а также делятся ею с третьими лицами. В перспективе такой свободный информационный обмен делает совершенно неконтролируемым использование выведенной за периметр информации. Похоже, личные почтовые ящики бывших сотрудников самых разных организаций хранят много интригующих подробностей об их бывших работодателях.

Почти в 16% случаев выявлены признаки других нарушений служебного поведения (ограничений и запретов) сотрудниками в основном органов государственной власти, включая признаки конфликта интересов.

Популярностью у нарушителей пользуются различные виды нецелевого использования рабочего времени и технических ресурсов, оплаченных работодателем: посещение развлекательных интернет-ресурсов, поиск работы или даже выполнение работы в интересах другого работодателя (подработка). Каждое четвертое нарушение — из этой категории.



Эксперты по информационной безопасности советуют пользователям DLP-систем анализировать объем ложноположительных срабатываний (ЛПС). Аналитиками «Ростелеком-Солар» экспертно установлен средний уровень ЛПС для адекватно настроенной политики в 20%.

Самые распространенные внутренние нарушения

36,4%
Неконтролируемый вывод служебной информации за периметр организации

13,6%
Копирование служебной информации на съемные носители

25%
Нецелевое использование рабочего времени

6,8%
Отправка служебной информации, в том числе с грифом ДСП, на печать

15,9%
Признаки коммерческого сговора, нарушения ограничений и запретов, конфликт интересов

2,3%
Нарушение парольной политики

5. Отраслевое распределение компаний — участников исследования

Отраслевой ландшафт организаций, проводивших пилотирование Solar Dozor в 2021 году, включает самые разные сферы деятельности — от розничных продаж до приборостроения и химической промышленности, от переработки и реализации полезных ископаемых до госорганизаций и органов государственной власти, а также организаций, обеспечивающих их ИТ-сопровождение, всего порядка 10 сфер.

Отраслевое распределение компаний

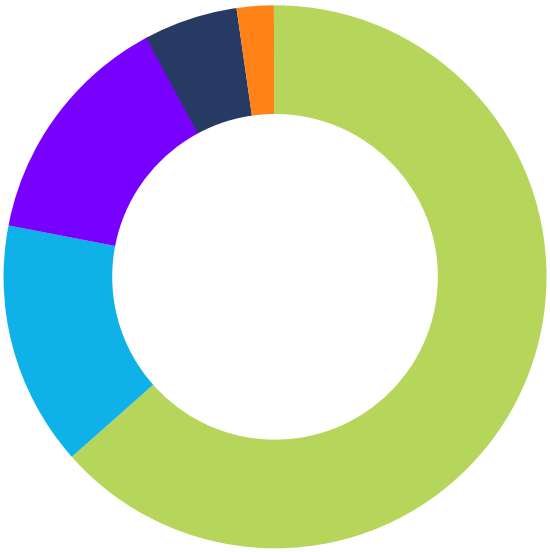
- 23,7% Госструктуры
- 14,3% Финансы
- 11,9% Разработка ПО, интеграция
- 9,5% Переработка и реализация природных ресурсов
- 9,5% ТЭК
- 7,1% Химическая промышленность
- 4,8% ВПК
- 4,8% Приборостроение
- 2,4% Транспорт и логистика
- 2,4% Услуги
- 2,4% Ретейл
- 2,4% Строительство
- 2,4% Аутсортинг
- 2,4% Рекрутмент

Эффективная эксплуатация DLP-системы требует от организации существенных ресурсов. При этом все чаще наблюдается тенденция превалирования функциональности (эффективности) DLP-решения над его ценой.

6. Размер компаний — участников исследования

В отношении размеров участников исследования по-прежнему преобладают средние и крупные заказчики. Доля организаций численностью свыше 500 человек выросла в 2021 году до 78% от исследуемой выборки (67% – в предыдущем исследовании). При этом подавляющее большинство в этой категории составляют Enterprise-организации численностью свыше 1000 человек (81%), или чуть более 63% от всех участников исследования.

Размер компаний — участников исследования



63,4%
Более 1000 сотрудников

4,9%
100-200 сотрудников

14,6%
200-500 сотрудников

2,5%
Менее 100 сотрудников

14,6%
500-1000 сотрудников

Выводы

Аналитики «Ростелеком-Солар» отмечают, что параллельно с развитием удаленных и гибридных форматов работы, а также с развитием цифровых инструментов, помогающих организовать работу сотрудников, растет риск как возможных ошибок, так и намеренных действий, направленных на причинение ущерба работодателю. В то же время растут и возможности систем контроля коммуникаций пользователей, которые давно переросли свой изначальный основной функционал – контроль утечек конфиденциальных данных. Разнообразие нарушений трудовой дисциплины со стороны сотрудников, выявляемых на пилотных проектах DLP-систем, – лучшее тому подтверждение.

Эксперты «Ростелеком-Солар» отмечают: большинство из описанных в исследовании проблемных тенденций «поведения» организации, процессы управления которой переходят в онлайн, на самых разных уровнях – от рядовых сотрудников до топ-менеджеров – вполне поддаются достаточно эффективному контролю. Как минимум, те активности сотрудников, которые они выполняют на своих рабочих компьютерах, могут в автоматическом режиме агрегироваться и исследоваться на предмет их адекватности рабочим функциям и задачам.

Также подлежит автоматизированному анализу и внутренняя среда организации в целом: интенсивность, продуктивность и тональность коммуникаций. Как именно это происходит и что дает компаниям? Ответом на эти вопросы вскоре должна стать новая категория решений по оценке продуктивности труда офисных сотрудников, которая сейчас активно разрабатывается российской ИТ-индустрией.

В ситуации растущего диапазона нарушений избежать излишней нагрузки на сотрудников служб безопасности помогает вдумчивая настройка системы в начале и в процессе эксплуатации. Производители готовы помогать и делиться опытом.

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