Ростелеком
Солар

Исследование

«Случайные утечки информации в госорганах»

Ноябрь-декабрь 2021

Оглавление

1. Ключевые цифры

- **51%** опрошенных считает, что случайных и умышленных утечек в госорганах поровну, **36,2%** – что умышленных утечек больше, а **12,8%** – что больше случайных.
- Более **90%(!)** представителей госаппарата осознает, что случайные утечки создают серьезные риски. Из них **53,2%** полагает, что эти риски даже выше, чем вследствие умышленных сливов конфиденциальных данных.
- Почти в **60%** случаев из госорганов непреднамеренно утекают служебные документы и внутренняя конфиденциальная переписка, вследствие их пересылки госслужащими на личную электронную почту
- **51%** случайных утечек конфиденциальной информации из госорганов происходит через Интернет (соцсети, внешние облачные хранилища, интернет-почта и т.п.).
- Более **50%** ненамеренных утечек в госорганах допускают руководители среднего звена в возрасте от 30 до 50 лет.
- Более **55%** респондентов уверены: причиной случайных утечек в госорганах является нехватка у госслужащих знаний в области информационной безопасности.

2. Методология

Данное исследование проведено методом электронного опроса части аудитории порталов TAdviser, Global CIO и ComNews сегмента государственных органов власти и организаций, а также соответствующей аудитории социальной сети Facebook.

В опросе приняли участие порядка 100 представителей организаций, размер опрошенных компаний представлен категориями «до 500 сотрудников», «500–1000 сотрудников» и «свыше 1000 сотрудников». География участников исследования охватила все 8 федеральных округов РФ.

Опрос проводился в ноябре 2021 года. В ходе опроса респондентам предлагалось выбрать один из предложенных вариантов ответа или указать свой вариант ответа в свободной форме.

3. Введение

Исследование продолжает серию аналитических отчетов «Ростелеком-Солар» по проблематике утечек информации в различных сферах деятельности и отраслях экономики. Ранее в 2021 году Центр продуктов Dozor опубликовал результаты отчета о специфике утечек информации в банковской сфере. Некоторые результаты отчета по тематике финансовой сферы как части коммерческого сегмента дали основание для сравнения аналогичных показателей утечек информации в данном отчете, охватывающем государственный сегмент.

В последние годы цифровизация в государственных органах идет семимильными шагами. А вместе с ней растет и количество угроз информационной безопасности – хакерских атак, утечек информации и т.п. По оценкам экспертов глобального рынка ИБ, в сегменте госорганов соотношение умышленных и случайных утечек информации является практически равным. Это исследование было подготовлено с целью подтвердить справедливость данной экспертами оценки, а также выяснить причины и основные факторы, способствующие тому, что случайные утечки в органах государственной власти не уступают по частоте инцидентам со злым умыслом.

В данном исследовании рассмотрен уровень рисков для государственных органов в результате утечек конфиденциальной информации, основные источники и каналы утечек, даны некоторые характеристики госслужащих, которые допускают случайную утечку чувствительных данных, а также основные причины неумышленных утечек в организациях этой сферы. Результаты исследования будут полезны службам безопасности и руководителям органов государственной власти, а также всему аппарату госслужащих.

4. Результаты исследования

Чтобы подтвердить или опровергнуть мнения экспертов о том, что в госорганах ситуация с намеренными утечками «чувствительной» информации обстоит лучше, чем в бизнесе, аналитики «Ростелеком-Солар» спросили у представителей государственных органов власти, какие утечки, по их наблюдениям, чаще происходят в их организациях – умышленные или случайные.

Более половины опрошенных – **51%** - полагают, что в ежедневных рабочих активностях сотрудников государственных органов и организаций присутствуют в равной мере риски и случайных, и умышленных утечек чувствительной информации. Это подтверждает основной вывод аналогичных исследований, проведенных экспертами «Ростелеком-Солар» ранее: необходимо внимательно наблюдать за рабочими активностями всех сотрудников, так как потенциально в «группу риска» в связи с утечками может попасть любой.

При этом, **36,2%** респондентов все же считают, что умышленных утечек в госорганах происходит несколько больше, а еще **12,8%**, наоборот, склоняются к преобладанию в госорганизациях утечек случайного характера.

Для сравнения: в коммерческих организациях финансовой сферы 50% опрошенных полагают, что случайных и умышленных утечек в банках поровну, наличие скорее умышленных утечек признают 20% респондентов, а скорее случайных – 30%.

При этом сотрудники государственных органов, в отличие от бизнеса, гораздо быстрее сменили временный «домашний» формат работы на привычный офисный. Получается, что на госслужбе риски утечек не зависят от известной закономерности «чем ниже уровень контроля при удаленной работе, тем выше уровень рисков», а существуют всегда.

4.1 Риски при случайных утечках

Одной из основных целей исследования стала оценка возможных рисков для государственного органа в случае неумышленной утечки информации. Ответы на вопрос «насколько высок риск при случайной утечке» со всей очевидностью демонстрируют – подавляющее большинство (**более 90%!**) представителей госаппарата осознает, что случайные утечки информации создают серьезные риски.

Причем **больше половины** из этой выборки полагает, что риски от случайных утечек превышают опасности, грозящие организации вследствие умышленных сливов конфиденциальных данных. Это может быть связано с тем, что при полном отсутствии контроля за внешне «благополучными» сотрудниками всегда существует риск пропустить действительно серьезное – хотя и совершенно непреднамеренное – нарушение.

Например, многие ли задумываются, что каждый раз, отправляя себе на почту или в облако наиболее «чувствительную» информацию (таблицы в любом формате, содержащие персональные данные, данные о финансовом состоянии физических или юридических лиц, проекты служебных документов, например, находящиеся в процессе разработки нормативные правовые акты, ведомственную переписку, материалы, имеющие отношение к закупкам для государственных нужд и т.д.), служащие подвергают ее опасности стать достоянием хакеров?..

Все ли служащие понимают, что с каждым новым участником пересылки «интересного» документа/факта риск потери контроля над его распространением становится абсолютно неуправляемым? Особенно с учетом масштабов распространения культуры «шеров, лайков и репостов» среди поколения наиболее молодых сотрудников.

Получается, что чувствительная информация, которой делится вполне «благополучный» сотрудник со своим ближайшим окружением, на любом этапе передачи потенциально становится миной замедленного действия. Контролировать ее распространение за пределами информационного периметра

организации невозможно в принципе – получается, что проще максимально предотвращать выход информации из этого самого периметра.

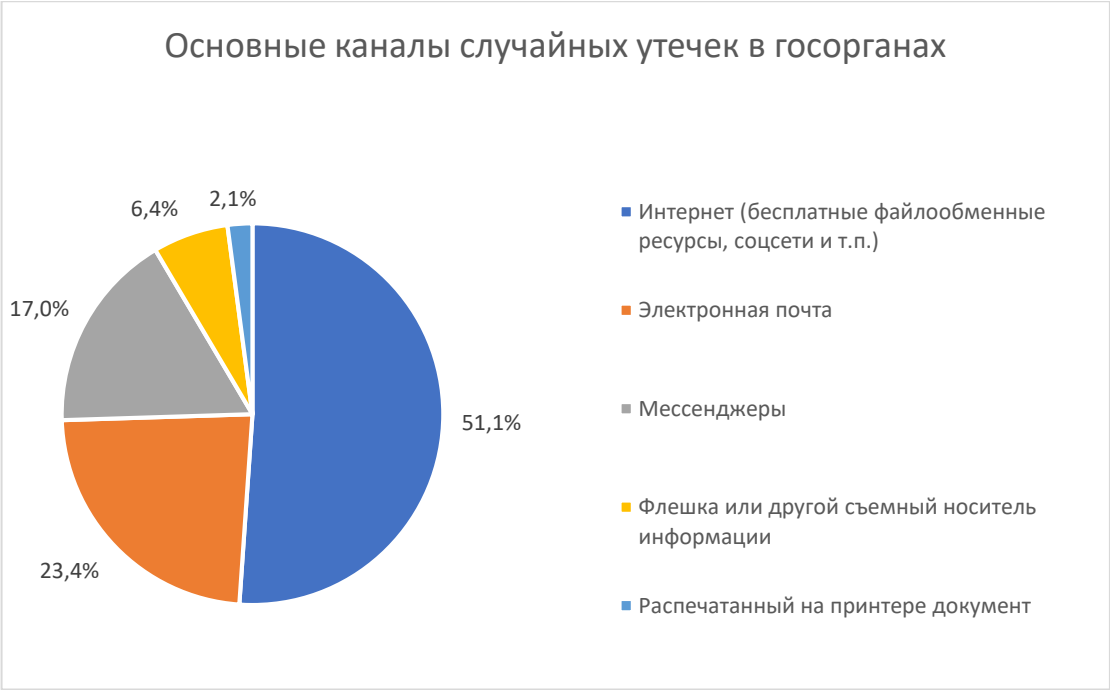
4.2 Источники случайных утечек в госорганах

Вышеописанные риски подтверждаются ответами на следующие два вопроса исследования. Наиболее популярные источники потенциальных утечек (**около 60%** случаев) – служебные документы и внутренняя конфиденциальная переписка, пересылаемые госслужащими на личную электронную почту. Также, почти **в каждом пятом случае** источником потенциальных утечек названы обсуждения с третьими лицами позиции руководства по рабочим вопросам и содержания внутренних служебных документов.

Особого внимания заслуживают ответы в категории «Другое». В основном респонденты признают наличие слабых мест в системах защиты информационного периметра государственных органов. В частности, упоминается несовершенство защиты служебных информационных систем: по всей видимости, имеются в виду обеспечивающие системы электронного документооборота, кадровые и т.д. или специальные ведомственные ГИС. Также участники исследования отметили среди источников утечек человеческий фактор в лице недовольного сотрудника: правда, в этом случае скорее нужно говорить о целенаправленном злом умысле в действиях такого человека.

4.3 Каналы случайных утечек в госорганах

Больше половины неумышленных утечек конфиденциальной информации из органов государственной власти, по мнению респондентов, происходит через различные Интернет-каналы (соцсети, внешние облачные хранилища, интернет-почту и т.п.). Также часто чувствительная информация случайно покидает периметр организации по каналам служебной электронной почты (более **23%** случаев) или через мессенджеры (**17%** случаев). На съемные носители информации госслужащие копируют чувствительные данные значительно реже.



Следует отметить, что соотношение основных каналов, по которым случайно утекает конфиденциальная информация из госорганов, полность соответствует картине распределения каналов утечек в коммерческом сегменте, в частности в банковской сфере. Это подтверждается данными исследования «Особенности защиты конфиденциальной информации в финансовом секторе». По мнению авторов данного исследования, это свидетельствует о том, что цифровизация российских органов государственной власти достигла высокого уровня, сопоставимого с коммерческим сегментом. А значит, для государственных организаций столь же, а в некоторых случаях и более, актуальны все современные угрозы информационной безопасности – целевые атаки, утечки, взломы, инциденты несанкционированного доступа, эксплуатация уязвимостей и т.п.

4.4 Виновники случайных утечек в госорганах

Интересны результаты ответа участников исследования на вопрос, по чьей вине чаще всего в государственных органах происходят случайные утечки данных. То, что это редко (лишь в **10%** случаев) происходит по вине руководителей высшего звена, аналитиков «Ростелеком-Солар» не удивило – в этом случае уровень должности полностью определяет уровень ответственности. Работает многолетняя тренировка искусства взвешивания каждого слова, сказанного «вовне».

Однако объясним и тот факт, что невнимательное отношение к чувствительной информации в органах государственной власти в 1,5 раза чаще присуще руководителям среднего звена, нежели рядовым служащим. Руководящие позиции в том числе на госслужбе в последнее время все чаще занимают представители поколения «миллениалов» в возрасте 30-40 лет, для многих из которых нормальным является принятие быстрых решений/действий в условиях постоянно интенсивного информационного потока. Здесь действуют обычные статистические законы: чем выше скорость и больше количество отправленных писем или собщений – тем выше вероятность пропустить тот самый «потенциальный риск».

4.5 Возраст «случайных нарушителей»

Вопреки расхожим представлениям о том, что рассеянностью в основном страдают люди старшего возраста и именно они больше склонны к случайным ошибочным действиям, результаты опроса показали: **больше чем в половине** случаев ненамеренные утечки конфиденциальной информации из госорганов происходят по вине служащих среднего возраста. Чуть реже (в **42%** случаев) – по вине молодых людей, и лишь изредка (чуть более **6%** случаев) – из-за неверных действий старшего поколения. Это целиком подтверждает выводы предыдущего вопроса: те самые «руководители-миллениалы» попадают в две наиболее многочисленные выборки потенциальных случайных нарушителей. Суммарно это более 90% от их общего числа.

4.6 Почему происходят случайные утечки в государственных органах и организациях

Более **55%** участников исследования уверены, что сотрудникам государственных органов и организаций просто не хватает знаний в области информационной безопасности. **Еще треть** опрошенных полагает, что во всем виновата перегруженность многочисленными задачами, что порождает спешку и, как следствие, ошибки в обращении с чувствительной информацией. А **чуть более 10%** полагают, что причиной случайных утечек в госорганах является простая невнимательность, тот самый человеческий фактор, негативный эффект от которого можно побороть только с помощью применения автоматизированных систем защиты информации.

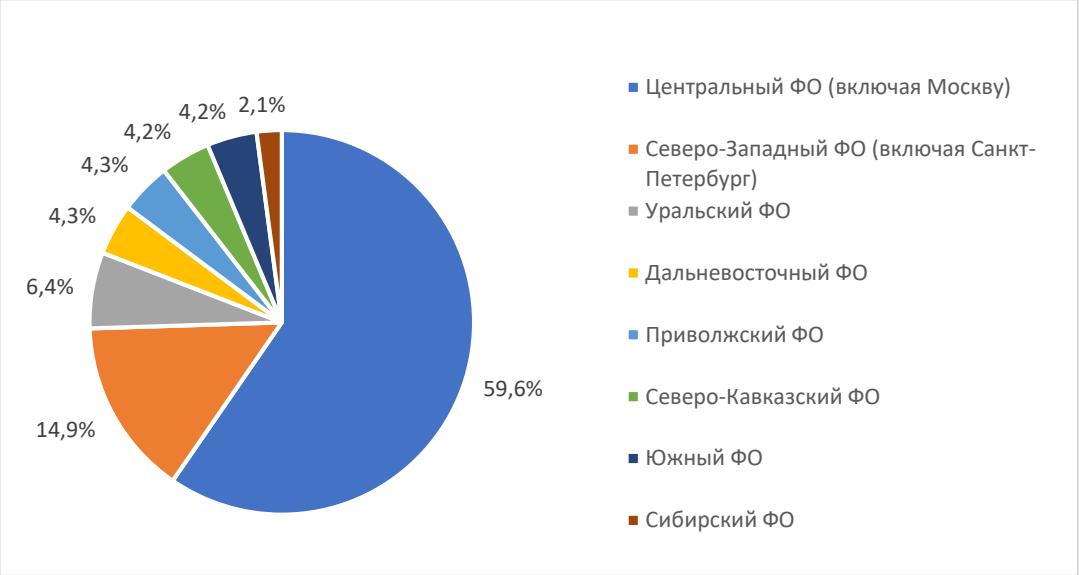
В этом вопросе интересен «территориальный» фактор: так, в наибольшей степени запрос на обучение сотрудников основам кибербезопасности проявлен в организациях, расположенных в Центральном федеральном округе (центральные аппараты федеральных органов государственной власти, иные организации). Здесь **почти 70%** респондентов признают недостаточность компетенций в области информационной безопасности среди сотрудников. Доля аналогичных ответов среди респондентов в регионах – **менее 30%.** Здесь значительно больше верят в негативный эффект перегрузки госслужащих рабочими задачами: как основной фактор утечек перегрузку называют **почти 60%** региональных участников исследования.

В целом, основным фактором снижения числа случайных утечек в органах государственной власти участники исследования посчитали обучение госслужащих основам безопасного обращения с конфиденциальной информацией. Однако максимального эффекта можно ожидать, лишь комбинируя качественное обучение людей и использование автоматизированных средств защиты от утечек любого типа: и случайных, и преднамеренных.

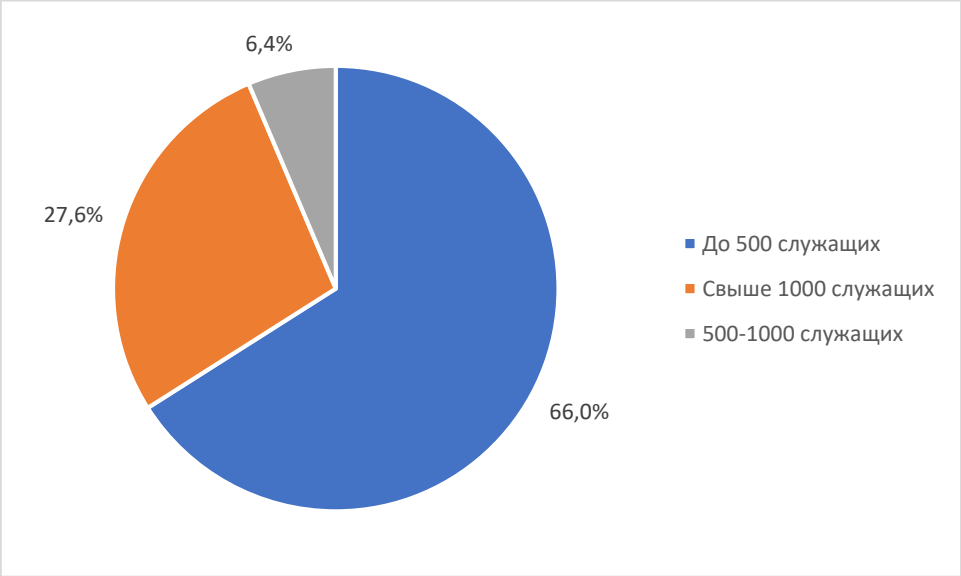
Что касается разнообразия потенциальных источников утечек и каналов, по которым может распространяться эта информация – здесь выдвигаются высокие требования к гибкости настроек автоматизированных средств защиты информации и их способности работать с максимальным количеством каналов передачи данных.

5. Характеристики респондентов

5.1 Региональный ландшафт опрошенных организаций



5.2 Распределение опрошенных организаций по размеру



6. Выводы

Результаты исследования показали, что госорганы в равной мере подвержены как случайным, так и умышленным утечкам информации – так утверждает более половины участников исследования. Еще треть респондентов выражает меньше доверия к госслужащим, полагая, что все-таки в государственных организациях преобладают умышленные утечки. В связи с этим можно сделать вывод о том, что необходимо контролировать рабочие активности всех сотрудников, так как потенциально в «группу риска» в связи с утечками может попасть любой.

Про этом подавляющее большинство представителей госаппарата считает, что случайные утечки информации создают серьезные риски.

Чаще всего из государственных организаций ненамеренно утекают служебные документы и внутренняя конфиденциальная переписка, пересылаемые госслужащими на личную электронную почту.

Наиболее часто информация из госорганов случайно утекает через различные Интернет-каналы – соцсети, внешние облачные хранилища, интернет-почту и т.п.

Виновниками неумышленных утечек чаще становятся госслужащие-руководители среднего звена в возрасте от 30 до 50 лет.

А основной причиной случайных утечек в государственных организациях участники исследования посчитали нехватку у госслужащих знаний в области информационной безопасности.

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