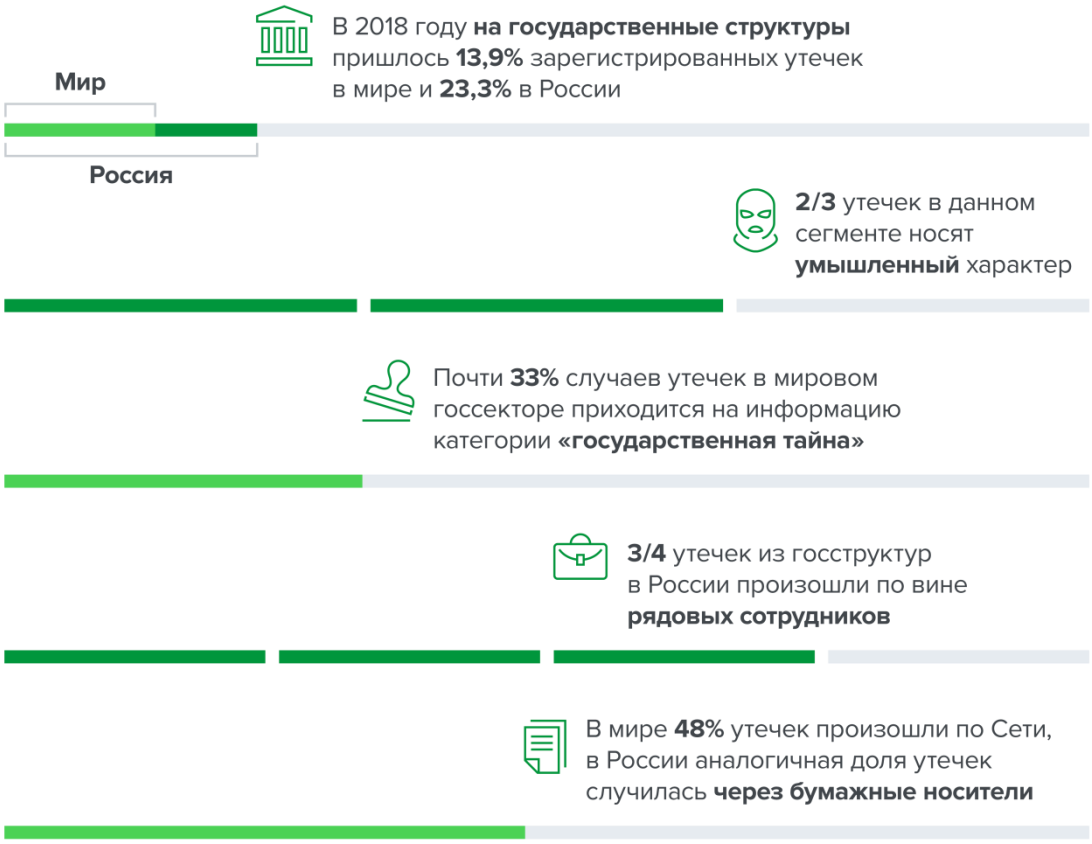
Исследование утечек информации ограниченного доступа в госсекторе. Мир – Россия. 2018 год

Оглавление

Только цифры



Аннотация

Аналитический центр компании InfoWatch представляет результаты исследования утечек информации в центральных органах власти стран, государственном секторе экономики и силовых структурах. Для краткости вся эта совокупность государственных организаций в отчете названа «госсектор». Данные об утечках приведены как в глобальном распределении, так и по России. Такое сравнение, на наш взгляд, позволяет показать основные сходства и различия в формировании картины утечек в глобальном и локальном разрезах.

Причем необходимо сделать важную оговорку. Дело в том, что публичную картину утечек более чем наполовину формируют сообщения из США, а также Соединенного Королевства и ряда других западноевропейских стран.

Во-первых, на Западе уже есть сложившееся законодательство в области защиты информации ограниченного доступа (прежде всего персональных данных), и компания, допустившая утечку, обязана сообщить об инциденте регулирующим органам.

Во-вторых, поиск информации об утечках во многих странах осложнен вследствие ряда особенностей – экономических, политических, культурных, языковых и т.д. Например, из ряда стран Африки и Азии отсутствуют новости о случаях компрометации данных из-за низкого уровня развития экономики и коммуникаций, из Китая, вероятно, доходит лишь малая часть сообщений об утечках в силу особенностей информационной инфраструктуры этого государства (в т.ч. изолированность от глобальной Сети) и особенностей её регулирования.

В-третьих, регулярный поиск информации об утечках ведется только на английском и русском языках, лишь фрагментарно мы подключаем к мониторингу специалистов, владеющих арабским и несколькими другими языками.

Госсектор любой страны сегодня обладает большими объёмами и широким спектром информации ограниченного распространения. Это, прежде всего, данные, относящиеся к категории «государственная тайна» (военные и разведывательные секреты, сведения об экономической политике государства, информация о внешнеполитической деятельности и т.д.), а также персональные данные граждан. Причем надо учитывать, что государства – крупнейшие агрегаторы личной информации о резидентах. Правительственные организации (министерства, ведомства, агентства и др.) могут поддерживать реестры данных колоссального масштаба, где сведения о каждом гражданине распределены по разным параметрам. Например, в Индии национальная система идентификации AADHAAR представляет из себя базу данных более 1 млрд граждан, включая их биометрическую информацию. Вполне естественно, что подобные системы – это настоящий кладезь в цифровую эпоху. Набор персональных данных гражданина можно использовать для получения различных услуг и конвертировать в «живые деньги», поэтому информация

из госреестров становится все более лакомым куском как для хакеров, так и для внутренних злоумышленников.

Имея уникальное сочетание набора сведений категории «гостайна» с самым широким спектром информации о гражданах, государственные организации должны поддерживать особые, многоступенчатые механизмы защиты информации, основанные на анализе больших данных и прогностических моделях. На наш взгляд, прежде всего это касается защиты от умышленных нарушений внутреннего характера.

Методология

Исследование проводится на основе собственной базы данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу попадают публичные сообщения[1] о случаях утечки информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов, которые произошли вследствие умышленных или неосторожных действий[2] сотрудников и иных лиц[3].

В ходе наполнения базы каждая утечка классифицируется по ряду критериев, таких как сфера деятельности (отрасль), размер причинённого ущерба[4], тип утечки (по умыслу), канал утечки[5], типы утекших данных, вектор воздействия[6].

Инциденты также классифицируются по характеру действий нарушителя. Наряду с неквалифицированными «простыми» утечками авторы исследования выделяют «квалифицированные» — случаи, когда деструктивное поведение сотрудников выражается в использовании легитимного доступа к данным в мошеннических целях (манипуляции с платежными данными, инсайдерской информацией); случаи превышения прав доступа, когда сотрудник знакомится, копирует, передает данные, к которым не должен иметь доступа по роду службы или работы.

По оценке авторов, исследование охватывает не более 1% случаев предполагаемого совокупного количества утечек из-за высокого уровня латентности инцидентов, связанных с компрометацией информации. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (совокупности категорий) содержали достаточное или избыточное количество элементов — фактических случаев утечки. Такой подход к формированию поля исследования позволяет считать полученную выборку теоретической, а выводы исследования и выявленные с учетом данной выборки закономерности — репрезентативными для генеральной совокупности.

При формировании диаграмм по отдельным разрезам из выборки исключены утечки, классифицированные по основному критерию разреза как неопределенные. Например, разрез по вектору воздействия, куда входят утечки под воздействием

---

[1] Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах, иных открытых источниках.

[2] Утечки данных разделяются на умышленные (злонамеренные) и неумышленные (случайные) в зависимости от наличия вины в действиях лица, которые привели к утечке данных. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы. См. Глоссарий.

[3] Авторы классифицируют утечки по виновнику (источнику) инцидента. Наряду с внутренними нарушителями, в данную классификацию попадает внешний нарушитель. См. Глоссарий.

[4] Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ.

[5] Под каналом утечки мы понимаем такой сценарий (совокупность действий пользователя корпоративной информационной системы, направленных на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. Каналы утечек определяются только для таких утечек, которые спровоцированы действиями внутреннего нарушителя.

[6] Вектор воздействия – признак действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников, направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников, атакующих системы защиты изнутри (нелегитимный доступ к ресурсам, неправомерные действия с инсайдерской информацией и проч.).

внешних атак и внутреннего нарушителя, не содержит утечек, для которых вектор не удалось определить. То же справедливо для распределений по виновнику, умыслу и другим критериям.

Инциденты безопасности, не повлекшие утечки данных, а также инциденты – утечки из неизвестным источника (от неизвестного оператора и/или владельца информации) в данную выборку не включены.

Авторы настоящего исследования не ставили перед собой задач определить точное количество произошедших утечек, оценить причинённый ими реальный или возможный ущерб организациям. Исследование направлено на выявление текущего состояния процессов, характеризующих глобальную и российскую картину происшествий, связанных с утечками в госсекторе.

Результаты исследования

Во всем мире на долю государственных и силовых структур в 2018 г. пришлось 13,9% утечек конфиденциальной информации, зарегистрированных аналитическим центром InfoWatch. В России на эту сферу пришлось почти четверть утечек (Рисунок 1).

Рисунок 1. Распределение утечек: госсектор – другие отрасли, Мир – Россия, 2018 г.

По нашему мнению, такое соотношение не определяется каким-то одним фактором. Пожалуй, ключевая причина относительно высокой доли госсектора в российских утечках – его доминирующее положение в экономике. Разброс в оценках довольно большой, приведем лишь одну: по данным Федеральной антимонопольной службы, доля государства в российской экономике в 2018 г. превышала 50%. В странах Запада (США, Соединенное Королевство и Европейский Союз) – а именно они в основном формируют глобальную картину утечек – развит частный сектор, прежде всего сфера услуг, и вклад государственных компаний в экономику, по некоторым оценкам, составляет не более 30%.

Как на Западе, так и в России государство довольно трепетно относится к утечкам информации, относящейся к сфере национальной безопасности.

> *SecurityLab: В США в самолете были обнаружены забытые копии документов Министерства внутренней безопасности (МВБ) США о мерах по обеспечению безопасности на финале национального чемпионата по американскому футболу «Супербоул». Документы с отметками "важно для национальной безопасности" и "для служебного пользования" содержали информацию о реакции властей Миннеаполиса, где в 2018 году проходил «Супербоул», на учения, в ходе которых была произведена симуляция атаки с использованием спор сибирской язвы.*

КоммерсантЪ: Следственная группа ФСБ провела обыски в кабинетах сотрудников Центрального научно-исследовательского института машиностроения (ЦНИИмаш), а также в офисе директора исследовательско-аналитического центра Объединенной ракетно-космической корпорации (ОРКК). Оперативные мероприятия проводятся в рамках уголовного дела, возбужденного по ст. 275 УК РФ (государственная измена). ФСБ установила, что западным спецслужбам стали известны результаты секретных разработок российской промышленности в области гиперзвука.

Соотношение утечек умышленного и непредумышленного (случайного) характера в глобальном распределении и российском разрезе оказалось практически одинаковым. Две трети утечек произошли в результате умышленных действий различных нарушителей (Рисунок 2).

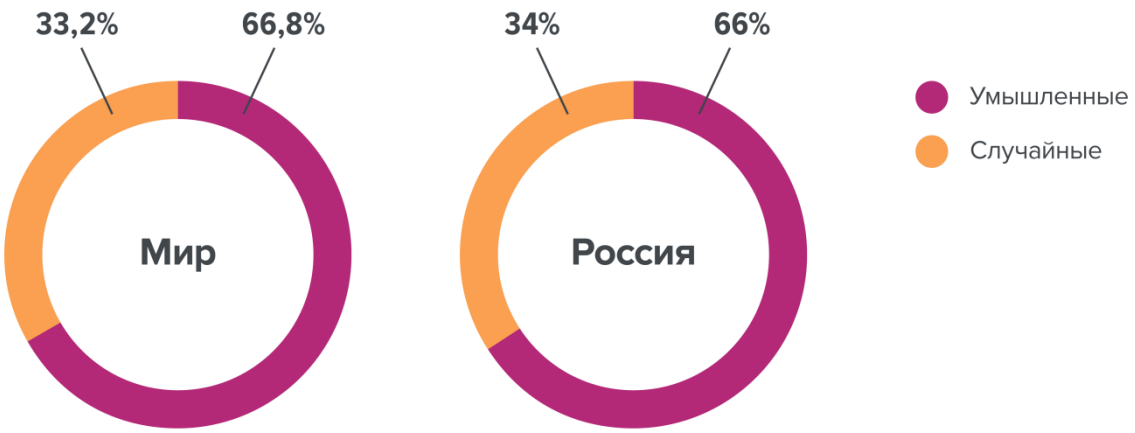


Рисунок 2. Распределение утечек в госсекторе по умыслу: Мир - Россия, 2018 г.

The Telegraph: Британский подросток Кейн Гэмбл взломал компьютеры бывшего главы ЦРУ Джона Бреннана и других высокопоставленных чиновников США. Юноша получил доступ к контактам и переписке Бреннана. Кроме того, в распоряжении хакера оказались базы данных американской разведки.

АиФ-Казань: Сотрудник отдела собственной безопасности МВД по Республике Татарстан за деньги предоставлял третьим лицам персональные данные граждан. Когда эти факты были выявлены, мужчину уволили из органов[7].

[7] Приговор: 2 года условно: https://www.business-gazeta.ru/article/437779

Принципиально иную картину дало распределение утечек по умыслу среди внутренних нарушителей. Если в глобальном масштабе соотношение оказалось 50/50, то в России со стороны сотрудников и руководителей государственных организаций превалируют умышленные нарушения (Рисунок 3).

Рисунок 3. Распределение утечек в госсекторе по умыслу среди внутренних нарушителей: Мир - Россия, 2018 г.

На наш взгляд, повышенная доля умышленных утечек внутреннего характера в России связана не только и не столько с недостаточным развитием систем и средств защиты информации (прежде всего, персональных данных), сколько с отношением к такой информации со стороны тех, кому она доверена в организациях. Привить массовому сотруднику уважительное и бережное отношение к персональным данным только предстоит. А пока публичное информационное пространство буквально пестрит сообщениями о сливе персональных данных, среди виновников зачастую оказываются работники государственных структур. Например, недобросовестные сотрудники полиции продают сведения об умерших гражданах похоронным агентствам, специалисты соцзащиты занимаются мошенничеством с использованием персональных данных.

> *News.ru: Ассоциация профессиональных пользователей соцсетей и мессенджеров выявила массу случаев утечки персональных данных граждан, регистрирующихся в качестве индивидуальных предпринимателей в Федеральной налоговой службе. Сразу после подачи заявлений в налоговую «новых» бизнесменов начинают*

осаждать банки с предложениями услуг. Ассоциация направила в Роскомнадзор письмо с просьбой проверить собранные им примеры таких случаев[8].

Среди типов утекшей информации в России доля персональных данных оказалась существенно выше, чем в глобальном распределении. В то же время в мире почти в 1,5 раз выше доля утечек государственных и военных секретов. (Рисунок 4).

Рисунок 4. Распределение по типам утекших данных в госсекторе: Мир – Россия, 2018 г.

Такое соотношение можно объяснить тем, что в России защите государственных секретов исторически уделяется особо пристальное внимание, в то же время тема безопасности персональных данных у нас приобрела актуальность совсем недавно. До сих пор во многих отечественных организациях можно сталкиваться с халатным отношением к личной информацией. Отсюда многочисленные «небрежные утечки», когда, например, архивы документов с персональными данными выбрасываются на ближайшую свалку вместо того, чтобы утилизировать эти бумаги по всем правилам.

В цифровую эпоху каждая запись персональных данных имеет вполне конкретную ценность, что быстро поняли недобросовестные сотрудники, в т.ч. госслужащие.

[8] Роскомнадзор ответил, что за утечку несут ответственность сами предприниматели) https://riafan.ru/1133154-v-roskomnadzore-obyasnili-kto-neset-otvetstvennost-za-utechku-dannykh-ip

Отсюда нарастающий поток утечек, участившиеся случаи мошенничества с данными граждан.

> NewsNN.ru: *В Нижегородской области двое бывших сотрудников полиции пошли под суд за продажу персональных данных граждан. Оперуполномоченные, состоявшие в родственных отношениях, наладили незаконную передачу данных из ведомственных баз МВД. За несколько лет обвиняемые заработали на этом порядка 700 тыс. рублей.*

Посмотрим на распределение по типам утекших данных в результате умышленных нарушений. На диаграмме, отражающей российские утечки, доли изменились незначительно. В мире же заметен крен активности злоумышленников в сторону государственных секретов (Рисунок 5).

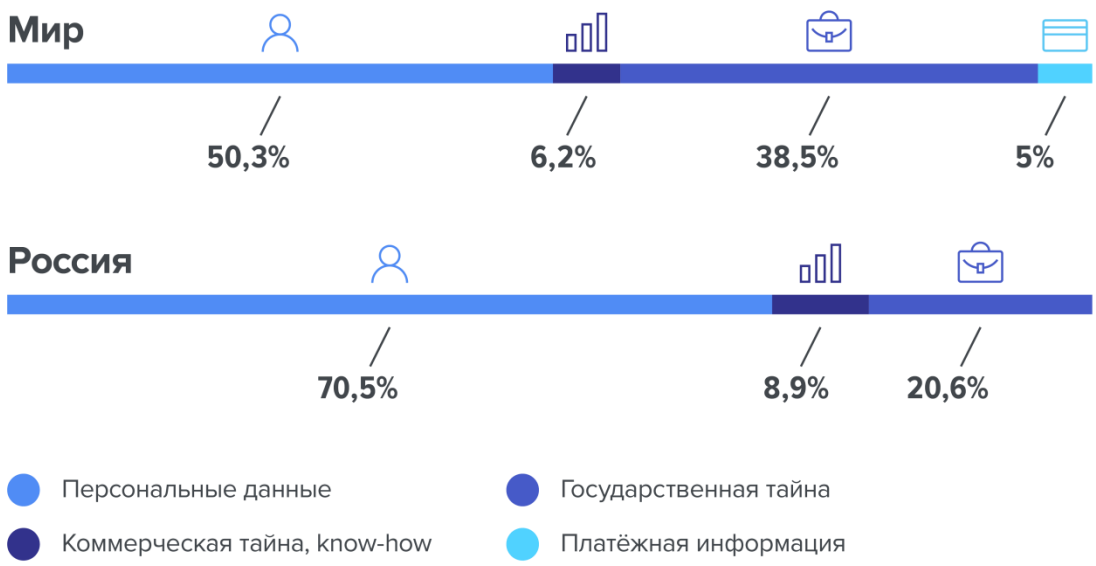


Рисунок 5. Распределение по типам утекших данных в госсекторе, только умышленные нарушения: Мир – Россия, 2018 г.

Российская Газета: Так называемое "бразильское крыло" хакерского объединения Anonymous под названием AnonOpsBR сообщило об успешном взломе одного из серверов министерства обороны Бразилии. В результате кибератаки злоумышленникам удалось получить доступ к персональным данным сотрудников военного ведомства. При этом, судя по оглашенной информации, в Сеть утекли конфиденциальные сведения, затрагивающие военное руководство страны.

АиФ-Уфа: В Уфе за разглашение гостайны к 5 годам и 6 месяцам лишения свободы приговорена бывшая майор полиции. Следователи ФСБ доказали, что женщина умышленно разгласила доверенные ей данные о проведении оперативных мероприятий

Главными виновниками утечек конфиденциальной информации из государственных структур являются непривилегированные сотрудники. Но если в мировом распределении по их вине произошла половина нарушений, то в России рядовые сотрудники, злонамеренно или непредумышленно, спровоцировали почти три четверти утечек (Рисунок 6).

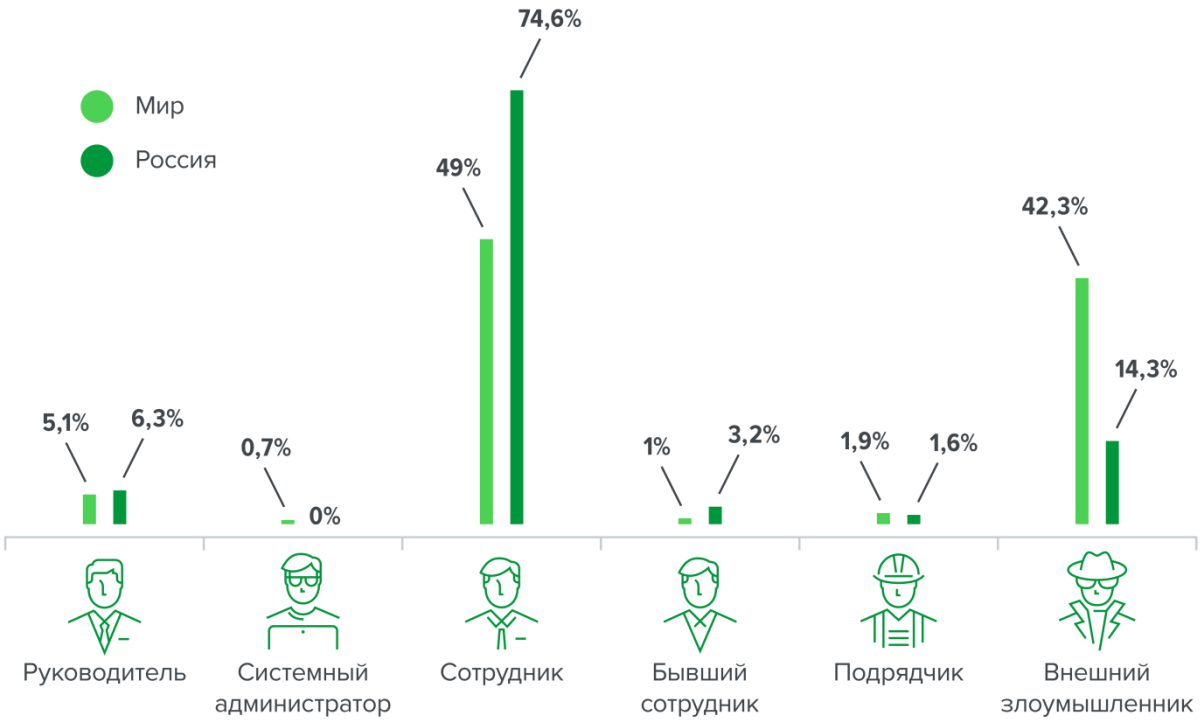


Рисунок 6. Распределение утечек в госсекторе по виновникам: Мир – Россия, 2018 г.

The Next Web: Сотрудник главного управления внутренней безопасности Франции (GDIS) арестован за продажу секретной информации. Агент

сотрудничал с организованными преступными группировками и некоторыми экономистами, сливая им конфиденциальные данные за вознаграждение в биткойнах. Служба внутренней безопасности GDIS выявила инсайдера, проанализировав компьютерную активность по индивидуальному коду сотрудника.

РИА Новости: В городе Асбест Свердловской области на помойке обнаружены архивы местного отделения полиции. В числе найденных документов оказались персональные данные сотрудников, оперативные данные, различные приказы, информация по уголовным делам. Некоторые материалы были помечены грифом "секретно". По одной из версий, имела место провокация, устроенная уволенным сотрудником.

В государственных организациях по всему миру почти половина утечек конфиденциальной информации происходит через сетевой канал, в России примерно такую же долю занимают утечки через бумажные носители (Рисунок).

Рисунок 7. Распределение утечек в госсекторе по каналам: Мир - Россия, 2018 г.

Softpedia News: Персональные данные более 540 тыс. человек украдены из электронной базы французского министерства Европы и иностранных дел. Взломав сайт министерства, хакерам удалось получить доступ к именам, номерам телефонов, адресам электронной почты всех людей, внесенных

в хранилище. Эта база используется для экстренной связи с гражданами, выезжающими за рубеж.

Ura.ru: В Москве, в заброшенном здании полиции и бывшей Федеральной миграционной службы, обнаружили кипы документов, в том числе и невыданных паспортов. Здание это никто не охраняет, злоумышленники могли бы легко в него проникнуть и подделать документы.

Посмотрим, какие каналы наиболее часто используются злоумышленниками для кражи и передачи информации ограниченного доступа из госорганов (Рисунок 8). Чем выше оказывается доля того или иного канала, тем он более привлекателен для нарушителей, а значит, требует особого внимания служб безопасности. Как видно из представленной группы диаграмм, в мире примерно 2/3 всех утечек через сеть в госсекторе происходят в результате умышленных действий, тогда как в России менее половины. При этом российский госсектор чаще страдает от преднамеренных утечек по электронной почте. Что касается случаев компрометации данных на бумаге, то здесь доли оказались примерно одинаковыми – порядка 40%. По каналу мгновенных сообщений (текстовые, голосовые и видео-сообщения) процент умышленных утечек оказался самым высоким как в глобальном, так и в российском распределении.

Рисунок 8. Доля умышленных утечек в госсекторе по отдельным каналам: Мир - Россия, 2018 г.

Заключение и выводы

Госсектор хранит не только «святая святых» – гостайну, но и огромные объемы персональных данных граждан. Еще одно направление ИБ, которое приобретает все большую актуальность для государств, – это защита критической информационной инфраструктуры (в т.ч. АСУ ТЭК, атомных станций, транспорта и промышленности, сети электросвязи и т.д.).

Сегодня государственным структурам целесообразно придерживаться комплексного подхода при защите конфиденциальной информации. Во-первых, им важны как централизованные программы безопасности (кстати, многие страны уже утвердили национальные стратегии информационной безопасности), которые будут охватывать как все аспекты защиты информации в той или иной стране, так и межведомственные мероприятия по защите информации. Кроме того, в глобальном информационном мире постепенно растет роль межгосударственных консультаций в области кибербезопасности. Во-вторых, целесообразно придерживаться стратегий безопасности, которые будут учитывать различные компоненты: выявление рисков, снижение уязвимостей, подавление угроз, смягчение последствий инцидентов. В третьих, госсектор, несмотря на свой «некоммерческий характер», вполне может оценивать эффективность мероприятий в сфере ИБ, формировать статистику по отдаче вложенных в кибербезопасность средств. На наш взгляд, эффективная защита государствами своих информационных ресурсов благотворно скажется на мировой экономике.

Очевидно, что на защиту конфиденциальной информации в госсекторе влияют такие факторы, как внутренние угрозы со стороны злонамеренных инсайдеров и случайных нарушителей, а также появление все новых внешних угроз и их подвижный ландшафт. Создание систем защиты данных в госсекторе также осложняют быстрое развитие искусственного интеллекта и других современных технологий, рост проникновения Интернета и совершенствование сетей связи.

Помимо создания эшелонированных систем защиты от утечек, вызванных внешним воздействием, государственным структурам необходимо выстраивать отвечающие вызовам времени системы защиты данных от внутренних нарушителей. Здесь особую роль играют системы контроля защищенности (в том числе, корректно настроенные DLP-решения), использование функционала по анализу больших данных и предиктивная аналитика.

Мониторинг утечек на сайте InfoWatch

На сайте Аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Telegram

Аналитический центр InfoWatch

www.infowatch.ru/analytics

Сокращения

98-ФЗ	Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»
АС	Автоматизированная система
ГОСТ	Государственный (национальный) стандарт
ИС	Информационная система
ГК РФ	Гражданский кодекс Российской Федерации от 30 ноября 1994 года N 51-ФЗ
КоАП РФ	Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. от 195-ФЗ
КС	Конституционный суд Российской Федерации
НПД	Неправомерный доступ
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ТК РФ	Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ
УК РФ	Уголовный кодекс Российской Федерации от 13.06.2009 г. № 63-ФЗ

Глоссарий

Атака – см. компьютерная атака, сетевая атака, вторжение.

Вторжение (атака) – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам [Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ. Утвержден ФСТЭК России. 3 февраля 2012 г.].

Вектор воздействия – критерий классификации в отношении действий лиц, спровоцировавших утечку (в рамках данного отчетов InfoWatch).
Различаются действия внешних нарушителей (злоумышленников) (хакеров и других лиц) – внешние атаки, направленные против компании, воздействующие на веб-ресурсы, информационную инфраструктуру, носители корпоративной информации с целью компрометации информации, и действия внутренних нарушителей, (сотрудники компании и подрядчики, получившие права доступа к ресурсам компании) атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.).

Внешняя атака – атака, совершенная внешним нарушителем.

Внутренний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Внешний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Деструктивные действия сотрудников – в рамках данного отчета об утечках информации аналитики InfoWatch к таким действиям относят действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, в том числе сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными] разведками и другими заинтересованными субъектами [ГОСТ Р 50922-2006, статья 2.3.2].

Примечание – Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Инцидент – см. инцидент безопасности, инцидент информационной безопасности, компьютерный инцидент.

Инцидент безопасности (Security incident) – неблагоприятное событие в системе или сети, а также угроза такого события.

Примечание – Иногда используется термин ≪несостоявшийся инцидент≫ для описания события, которое могло обернуться инцидентом при несколько других обстоятельствах [ГОСТ 56205-2014, статья 3.2.106]

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [ГОСТ Р 53114-2008, статья 3.2.7. ГОСТ Р ИСО/МЭК 27001-2006, статья 3.6].

Примечание – Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Канал утечки информации – способ утечки информации; предполагает сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность.

На данный момент аналитики InfoWatch выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

- «Оборудование (сервер, СХД, ноутбук, ПК)», – компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
- «Мобильные устройства» – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
- «Съемные носители» – потеря/кража съемных носителей (CD, USB, карты памяти и др.).
- «Сеть (сетевой канал)» – утечка через браузер (отправка данных через веб-интерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.
- «Электронная почта» – утечка данных через корпоративную электронную почту.
- «Бумажные документы» – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).
- «IM –сервисы мгновенных сообщений» - утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.
- «Не определено» - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, п.7 ст.2].

Конфиденциальная информация – сведения конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997 г. №188.
В данном отчете (исследовании) авторы относят к таким сведениям информацию, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. Помимо персональных данных, это платежная информация, коммерческие секреты и ноу-хау, а также государственные и военные секреты. В некоторых случаях при анализе полученных сведений определить тип конфиденциальной информации не представляется возможным, поэтому она относится в категории «не определено».

Нарушитель информационной безопасности организации (нарушитель) – физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации [ГОСТ Р 53114-2008, статья 3.3.5].
В БДУ ФСТЭК России bdu.fstec.ru приведены следующие виды нарушителей/ источников угроз:

- внутренний нарушитель (потенциал низкий, средний, высокий);
- внешний нарушитель (потенциал низкий, средний, высокий).

В данном отчете (исследовании) к категории «нарушитель» авторы относят лицо, которое по ошибке или осознанно (с умыслом – злоумышленник) совершило определенные запрещенные действия, повлекшие утечку информации.

InfoWatch различает два вида нарушителей – «внешний нарушитель» и **«внутренний нарушитель»,** а также **шесть категорий нарушителей:**

- *Внешний нарушитель – Хакер/неизвестное лицо: взломщики компьютерных сетей, в том числе представляющие организованную киберпреступность; владельцы хакерского инструментация (библиотек); взломщики, действующие в политических и социальных целях, - хактивисты; сотрудники иностранных разведок и армий; похитители оборудования с конфиденциальной информацией.*
- *Рядовой сотрудник*.
- *Топ-менеджер (руководитель).*
- *Системный администратор.*
- *Подрядчик: сторонние исполнители работ по заказу компании, партнеры и внештатные сотрудники.*
- *Бывший сотрудник*.

В рамках исследования топ-менеджеров, системных администраторов, а в отдельных случаях и подрядчиков авторы включают в категорию привилегированных пользователей, то есть пользователей, наделенных повышенными правами доступа к информации. Как правило, действия таких пользователей в информационной системе службами информационной безопасности контролируются слабо либо не контролируются.
Иных пользователей корпоративной информационной системы (рядовых сотрудников) авторы относят к непривилегированным, обычным пользователям.

Неправомерный доступ – см. несанкционированный доступ.

Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа [ГОСТ Р 53114-2008, статья 3.3.6].

Примечания:

1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.
2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

В данном отчете (исследовании) авторы используют также словосочетание «нелегитимный доступ».

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию

доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [ГОСТ Р 50922-2006, статья 2.6.6]

Правонарушение – неправомерное поведение, запрещенное законом под угрозой наступления ответственности общественно вредное или опасное деяние.

Выделяют: преступление (в рамках УК РФ и УПК РФ), административное правонарушение (в рамках КОАП РФ), налоговое правонарушение (в рамках НК РФ).
В данном отчете (исследовании) авторы используют понятие «правонарушение» как родовое (общее) по отношению к преступлению и административному правонарушению.

Привилегированный пользователь – к таким пользователям InfoWatch относит категории лиц, имеющие расширенные права доступа в информационные системы, полномочия по изменению конфигураций и назначения прав администраторов другим пользователям. К привилегированным пользователям относятся руководители различного уровня, системные администраторы, в некоторых случаях подрядчики и другие категории.

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации [ГОСТ Р 53114-2008, статья 3.3.11].

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [98-ФЗ «О коммерческой тайне» п.9 ст.3]

Событие: Возникновение или наличие определенной совокупности обстоятельств [ГОСТ Р 53114-2008, статья 3.2.8].

Примечания:

1. Характер, вероятность и последствия события могут быть не полностью известны.
2. Событие может возникать один или несколько раз.
3. Вероятность, связанная с событием, может быть оценена.
4. Событие может состоять из невозникновения одного или нескольких обстоятельств.
5. Непредсказуемое событие иногда называют «инцидентом».
6. Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию [инциденту], опасным состоянием, опасным стечением обстоятельств и т.д.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа

к информации и получения защищаемой информации иностранными разведками [ГОСТ Р 53114-2008, статья 3.3.10].

В данном отчете (исследовании) InfoWatch к категории «утечка информации» относится событие, когда в результате умышленных или неумышленных действий внутреннего или внешнего нарушителя обладатель информации ограниченного доступа (компания) утрачивает контроль над этой информацией.

Умышленная (злонамеренная) утечка информации – InfoWatch понимает под ней такую утечку, когда пользователь, работающий с информацией ограниченного доступа, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду, или руководствовался иными мотивами (месть, зависть, личная неприязнь и т.д.). При этом в результате таких действий контроль над информацией со стороны ее обладателя был утрачен. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Также к умышленным утечкам относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей компании.

Неумышленная (случайная) утечка информации – под такой утечкой InfoWatch понимает ту, когда пользователь не предполагал наступления возможных негативных последствий своих действий, не преследовал личной выгоды и не руководствовался иными мотивами. При этом не важно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.