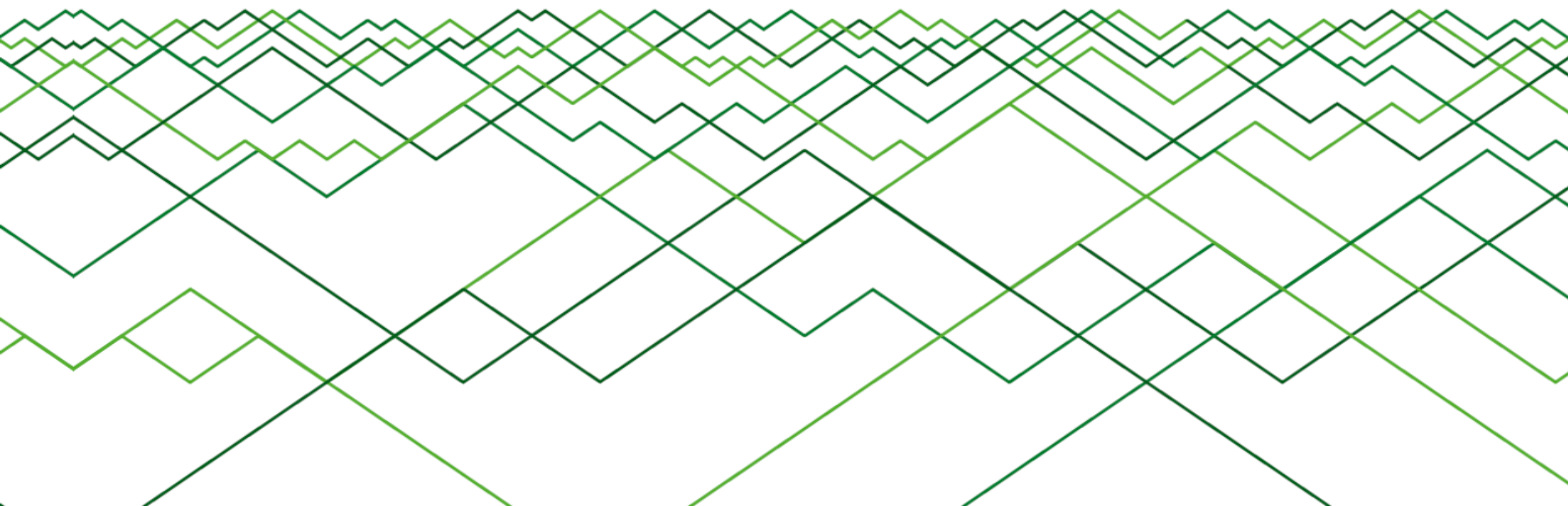
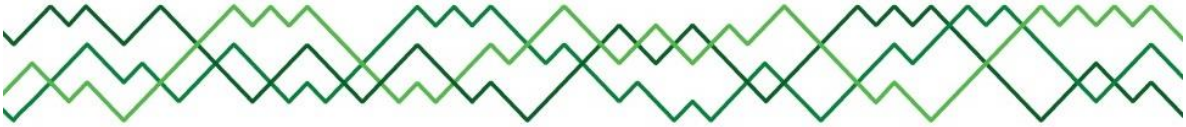
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Аналитический центр InfoWatch
www.infowatch.ru/analytics

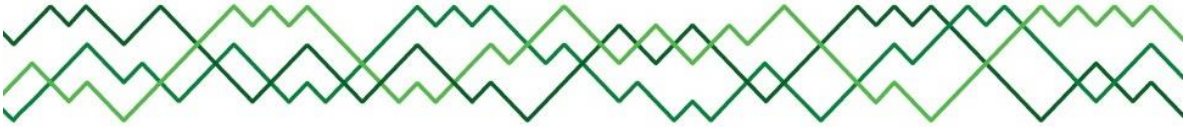
Исследование утечек конфиденциальной информации из медицинских учреждений в 2017 году





INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

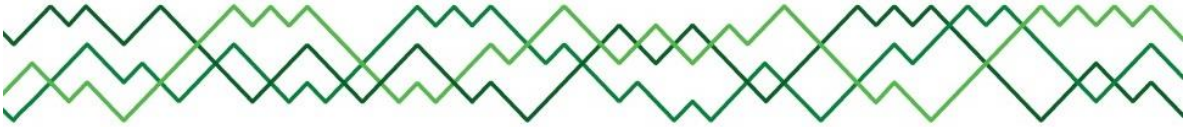
Оглавление



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Только цифры

- ✓ В 2017 году во всем мире зарегистрировано **370** утечек данных из медицинских учреждений, что на **7,7%** меньше, чем в 2016 году.
- ✓ Объем записей, скомпрометированных медицинскими учреждениями, за год упал на **47%**.
- ✓ Доля утечек информации из медицинских организаций в отраслевом распределении составила **17,4%**.
- ✓ **Четверть** всех случаев компрометации данных сопряжена с мошенническими действиями и неправомерным доступом.
- ✓ В России случайный характер носят **60%** инцидентов с утечками медицинских данных, в мире — **48%**.



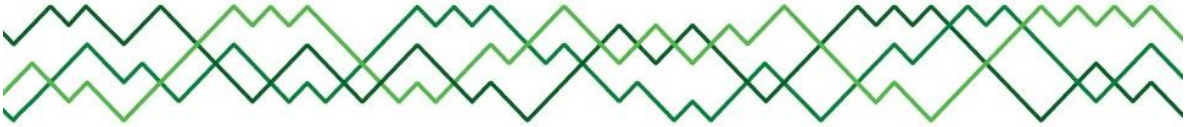
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Аннотация

Аналитический центр компании InfoWatch представляет отчет об исследовании утечек конфиденциальной информации из учреждений сферы здравоохранения (сети клиник, медицинские научные центры, лаборатории и т.д.), а также из страховых компаний, оперирующих медицинскими данными пациентов.

Цена, которую медицинская отрасль вынуждена платить, ликвидируя последствия инцидентов, постоянно возрастает. Согласно отчету Ponemon Institute, одна утечка, случившаяся в результате действий внутренних злоумышленников, обходится компании в среднем в $8,72 млн – в 2,2 раза выше, чем два года назад. Этим, во многом, обусловлен особый интерес исследователей к вопросу защиты медицинских данных во всем мире.

Авторы настоящего отчета считают, что его результаты будут полезны различным категориям читателей: практикующим специалистам в области информационной и экономической безопасности; собственникам и руководителям медицинских организаций, заинтересованным в обеспечении контроля над всем спектром конфиденциальной информации: персональными данными пациентов и сотрудников, медицинской информацией (история болезни, результаты исследований), платежными сведениями, иными ценными информационными активами; журналистам и аналитикам в области ИБ; всем, кто интересуется темой защиты информации и предотвращения утечек конфиденциальных данных в медучреждениях.



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Методология

Исследование основывается на собственной базе данных Аналитического центра InfoWatch, пополняемой с 2004 года. В базу включаются публичные сообщения[1] о случаях утечки[2] информации из коммерческих и некоммерческих (государственных, муниципальных) организаций вследствие злонамеренных или неосторожных действий[3] сотрудников, внешних нарушителей[4].

База утечек InfoWatch насчитывает несколько тысяч инцидентов. В ходе наполнения базы каждая утечка (если возможно и такая информация есть в сообщении об утечке) классифицируется по ряду критериев: размер организации[5], сфера деятельности (отрасль), размер ущерба[6], тип утечки (по умыслу), канал утечки[7], типы утекших данных.

По оценке авторов, исследование охватывает не более 1% случаев от предполагаемого совокупного количества произошедших утечек. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества (категории) содержали достаточное или избыточное число элементов (фактических случаев утечки). Такой подход к формированию поля исследования позволяет считать получившуюся выборку достаточной для выявления и прогнозирования закономерностей на всей совокупности утечек.

Случаи нарушения конфиденциальности информации (обнаруженные уязвимости), иные инциденты (DDoS-атаки), не повлекшие утечек данных, а также утечки с неясным источником (когда неизвестно, какой компании принадлежали скомпрометированные данные) в выборку не попадают.

---

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

[2] Утечка информации (данных) - действие или бездействие легитимного пользователя информации (физического лица), которое повлекло потерю контроля над информацией или нарушение конфиденциальности этой информации, а также потеря контроля над информацией (компрометация информации) вследствие внешней атаки.

[3] Утечки данных разделяются на умышленные (злонамеренные) и неумышленные (случайные) в зависимости от наличия или отсутствия умысла у физического лица, которое спровоцировало утечку данных. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

[4] В данном исследовании авторы представляют картину утечек в разрезе виновных лиц. Наряду с внутренними нарушителями, в данную классификацию попадает внешний нарушитель.

[5] Аналитики Центра InfoWatch классифицируют организации по размеру в зависимости от известного либо предполагаемого парка персональных компьютеров (ПК). Небольшие компании – до 50 ПК, средние - от 50 до 500 ПК, крупные – свыше 500 ПК.

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

[7] Под каналом утечки мы понимаем такой сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. Классификация каналов утечек приведена в глоссарии.

Результаты исследования

На основе глобальной выборки в 2017 году Аналитическим центром InfoWatch зарегистрировано 370 случаев утечек конфиденциальной информации из медицинских организаций (Рисунок 1). В результате утечек было скомпрометировано 14,2 млн записей персональных и связанных с персональными данных (например, платежная информация) — в том числе имена, фамилии, почтовые и электронные адреса, номера социального страхования, реквизиты платежных карт, специфические медицинские записи о состоянии здоровья, истории болезни субъектов данных.

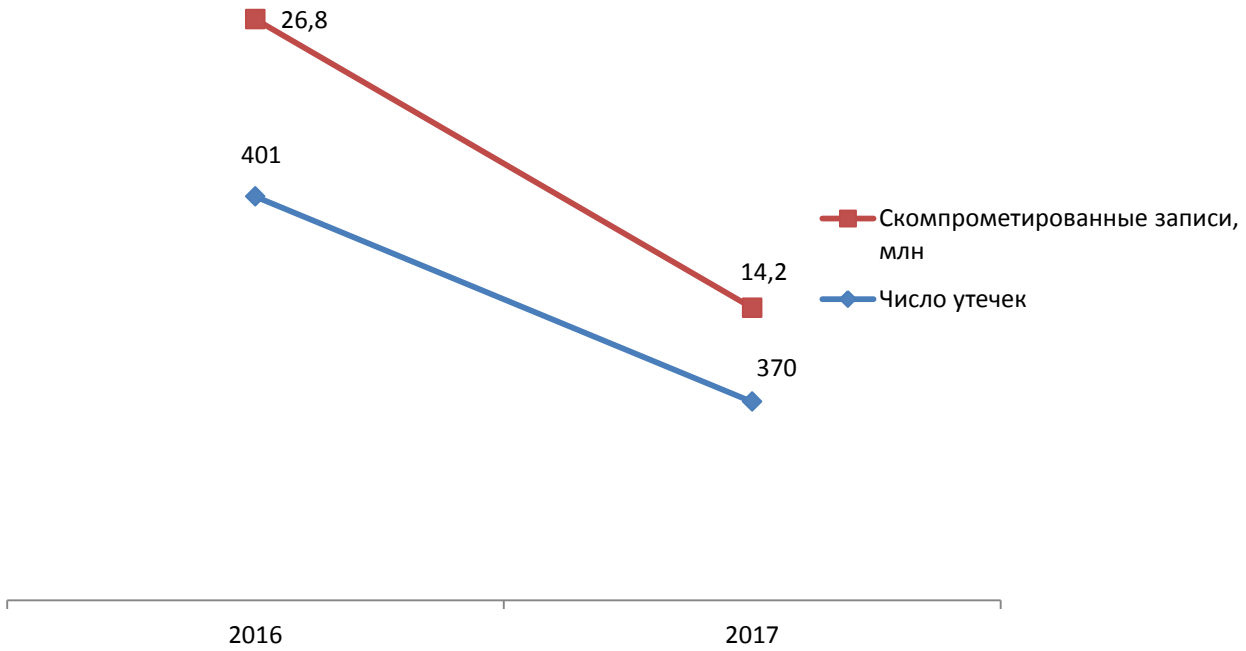


Рисунок 1. Число утечек информации и объем персональных данных, скомпрометированных в сфере здравоохранения, 2016-2017 гг.

По сравнению с 2016 годом число утечек в медицинской отрасли снизилось на 7,7%, объем скомпрометированных записей сократился на 47%. Доля утечек из учреждений здравоохранения в общем мировом распределении инцидентов по отраслям сократилась с 25,8% в 2016 году до 17,4% в 2017 году.

Снижение числа инцидентов и объема утекших записей предположительно было обеспечено за счет повышения уровня защиты медицинских данных в США. После того, как в 2015-2016 гг. американские медучреждения обновляли печальные рекорды по числу утечек и объему скомпрометированных данных, руководство многих клиник всерьез задумалось об укреплении систем информационной безопасности. По данным Thales, в 2017 г. более 80% организаций сферы здравоохранения США увеличили расходы на ИБ. Все это позволяет с осторожным оптимизмом говорить о наметившемся позитивном сдвиге в системе борьбы с утечками самой большой системы здравоохранения мира.

> *Philly.com: В Филадельфии сеть клиник женского здоровья пострадала в результате хакерской атаки. Злоумышленники взломали информационные системы организации и похитили персональные данные 300 тыс. пациентов.*

В России, напротив, в 2017 году отмечено резкое увеличение – более чем в два раза – числа утечек конфиденциальной информации из организаций медицинской сферы. В результате существенно (до 9%) выросла доля России в мировом распределении «медицинских» утечек (Рисунок 2).

Вероятно, это связано с тем, что внутренние злоумышленники в отечественных клиниках почувствовали «вкус» к данным, поняли, что информацию пациентов и коллег, находящуюся без должного контроля, относительно несложно использовать для извлечения выгоды.

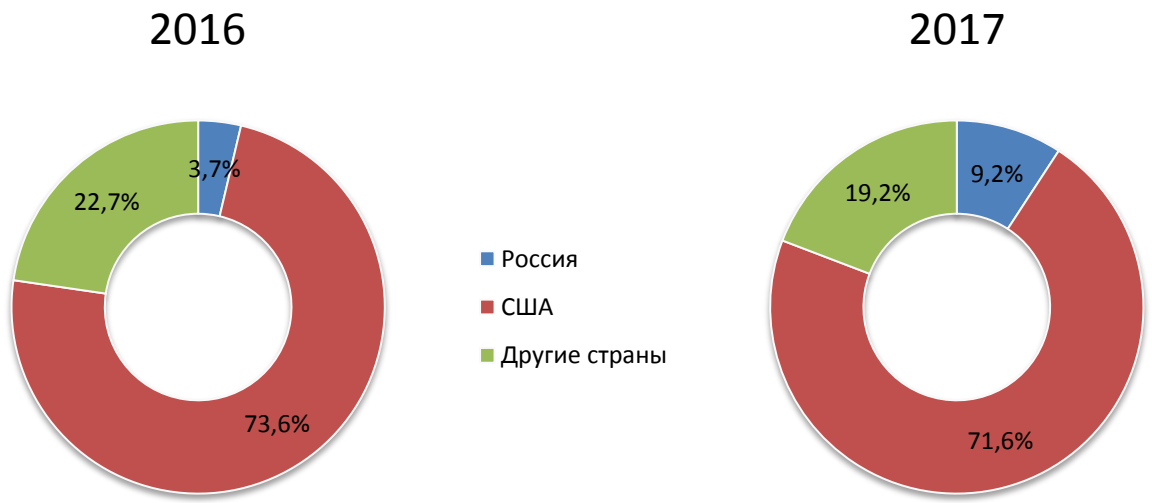


Рисунок 2. Распределение долей утечек: Россия, США, другие страны, 2016-2017 гг.

Классический для России пример «медицинской утечки» – это «слив» сотрудниками учреждений здравоохранения данных о тяжелобольных и умерших пациентах ритуальным агентам. При этом, скорее всего, достоянием общественности становится лишь малая толика подобных инцидентов.

> *«Эхо Москвы» в Саратове: Фигурантом уголовного дела стала фельдшер – руководитель бригады городской скорой помощи. Установлено, что около года женщина передавала представителям похоронных бюро сведения, представляющие категорию врачебной тайны. Получив данные умерших лиц, ритуальные агенты выезжали по указанным адресам и навязывали родственникам свои услуги».*

С другой стороны, сравнительно невысокие темпы информатизации российской медицины, лоскутный, зачастую несистемный характер развития медицинских информационных систем, большие массивы информации в бумажном виде – все это пока делает отечественные учреждения здравоохранения не слишком привлекательными целями для организованной киберпреступности. На 100% российскую картину утечек в медицине составляют внутренние утечки. В то же время

в мире, прежде всего в США, в медицинской сфере растет доля внешних инцидентов (Рисунок 3). В 2017 г. на глобальной выборке она увеличилась на 5 процентных пунктов – с 25,5% до 30,5%.

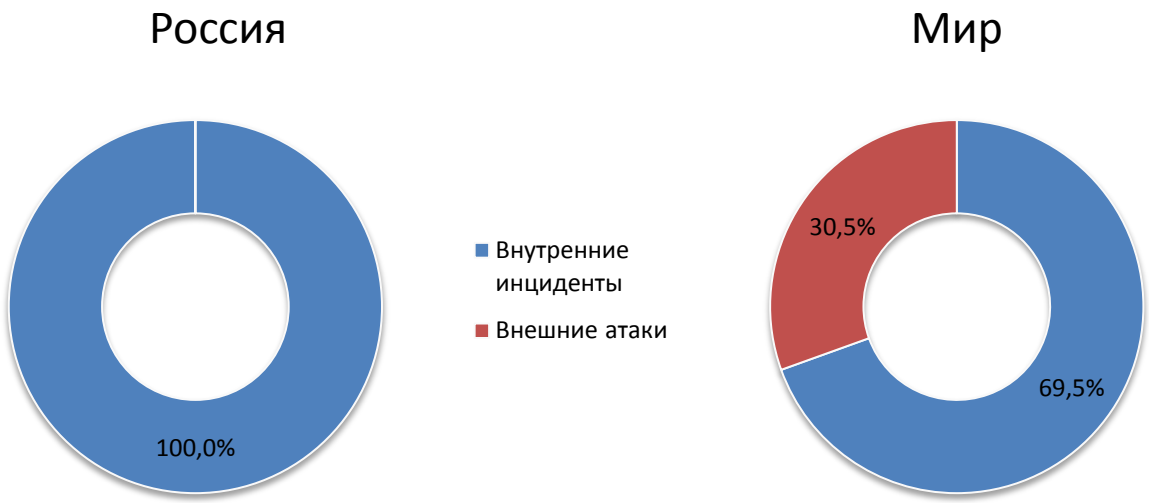


Рисунок 3. Распределение утечек по вектору воздействия: Россия - Мир, 2017 г.

В российский медицине почти две трети утечек носят случайный характер. В мире более половины инцидентов связаны с умышленными нарушениями (Рисунок 4).

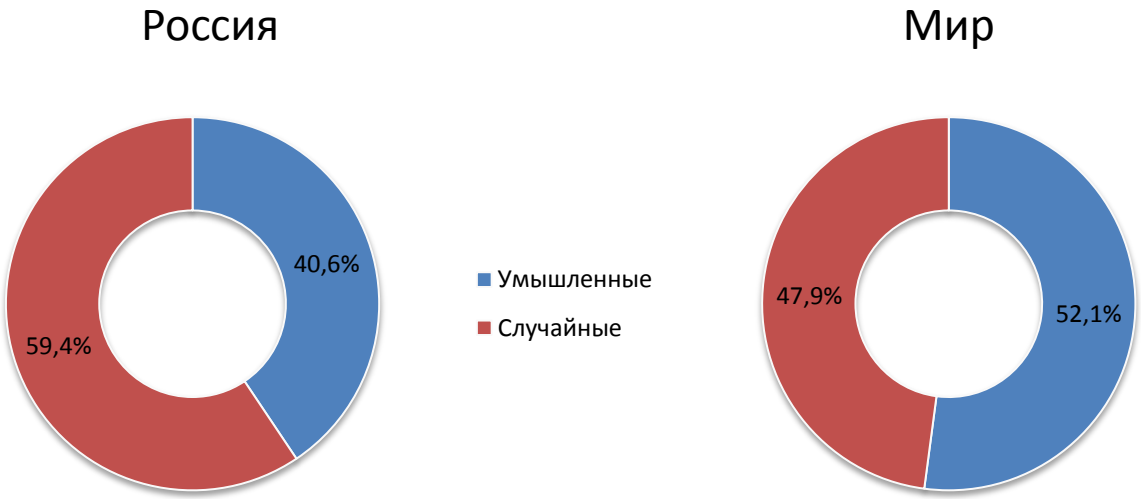


Рисунок 4. Распределение утечек по умыслу: Россия - Мир, 2017 г.

Daily News: Бывший сотрудник сети Med Centre Health из американского штата Кентукки обвиняется в том, что похитил информацию порядка 160 тыс. пациентов: номера, адреса, SSN, информация о страховании, процедурные коды и др.

Доля умышленных утечек из медицинских организаций в России по вине внутреннего нарушителя существенно выше, чем в целом по миру (Рисунок 5).

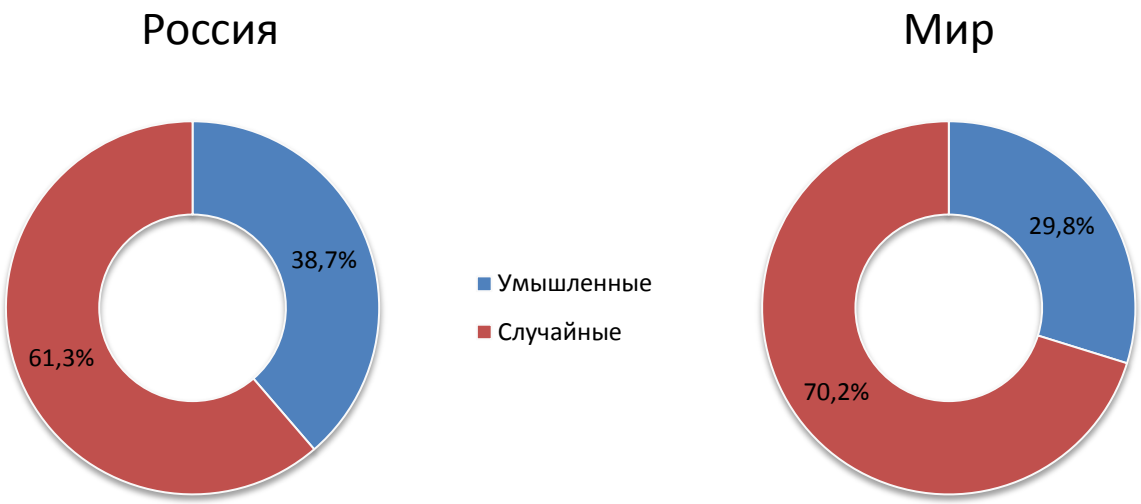


Рисунок 5. Внутренние утечки по типу умысла: Россия - Мир, 2017 г.

НТВ: Директор клиники в Калуге по договору делилась личными данными пациентов с фирмой, которая проводит бизнес-тренинги. Как выяснилось, фирма занимается пропагандой одной из нетрадиционных религий. Таким образом сектанты получали персональные данные посетителей клиники, а также их родственников и коллег.

Отдельно отметим, что в медицинской сфере наблюдается один из самых высоких среди различных отраслей мирового хозяйства уровень утечек по вине внутреннего злоумышленника (Рисунок 6).

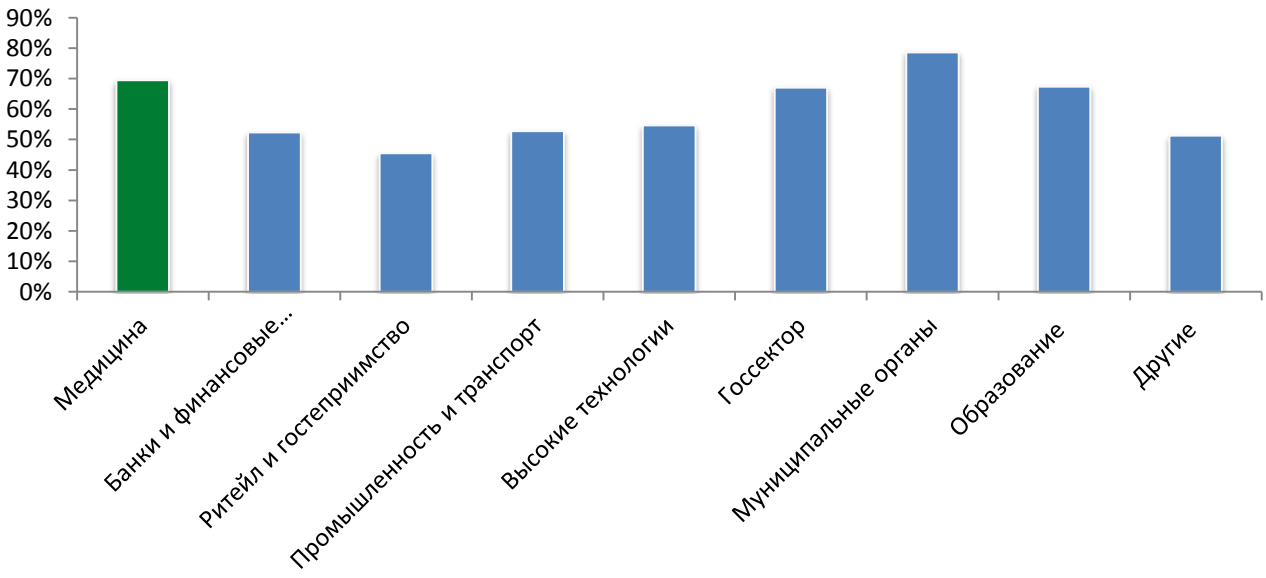


Рисунок 6. Доля внутренних утечек в различных отраслях. Мир, 2017 г.

Это может свидетельствовать о слабости систем ИБ в медучреждениях от действий рядового персонала и привилегированных пользователей — руководителей, системных администраторов, дежурного персонала. Что касается распределения утечек по типам пострадавшей информации, то в 2017 году в российских медучреждениях были скомпрометированы только персональные данные клиентов и персонала, в то время как в мире медучреждения также теряли платежную информацию и данные из категории коммерческой тайны и ноу-хау (Рисунок 7).

Рисунок 7. Распределение утечек по типу информации: Россия – Мир, 2017 г.

Медицинские учреждения обрабатывают и хранят большой спектр информации о пациентах: классические персональные данные и данные, относящиеся к категории врачебной тайны (результаты исследований, диагнозы, ход течения болезни, рецептурные назначения и т.д.). Нулевая доля компрометации платежных данных в России объясняется относительно невысоким уровнем развития коммерческой медицины и низким интересом злоумышленников к получению этой информации.

Как в России, так и в мире доля квалифицированных утечек, то есть сопряженных с мошенническими действиями или превышением прав доступа в информационные системы медицинских учреждений, составляет около 25%. (Рисунок 8). При этом в России доля таких утечек за 2017 год выросла вдвое, в то время как на мировой выборке этот показатель изменился не значительно. По мере роста ценности информации, которой располагают организации медицинской сферы в нашей стране, продолжит расти и число злоумышленников, стремящихся ей завладеть.

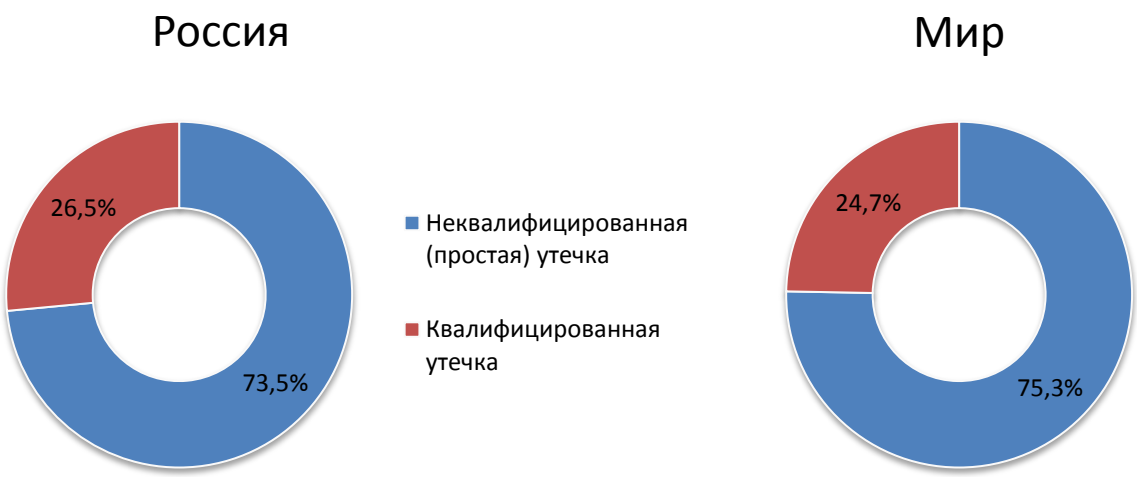


Рисунок 8. Доли инцидентов по характеру: Россия – Мир, 2017 г.

Российское и мировое распределение инцидентов в учреждениях здравоохранения по каналам утечек существенно отличается. Например, для России характерна высокая доля «бумажных» утечек и комментации данных по каналам мгновенных сообщений (Рисунок 9).

> *ГТРК "Вятка": В деревне Башарово Кировской области найдена свалка медицинских отходов. Помимо медицинских материалов для взятия анализов, одноразовых пеленок, перчаток и шприцев, обнаружены пакеты с данными пациентов. В региональный Минздрав направлено обращение о ненадлежащем обращении с персональными данными.*

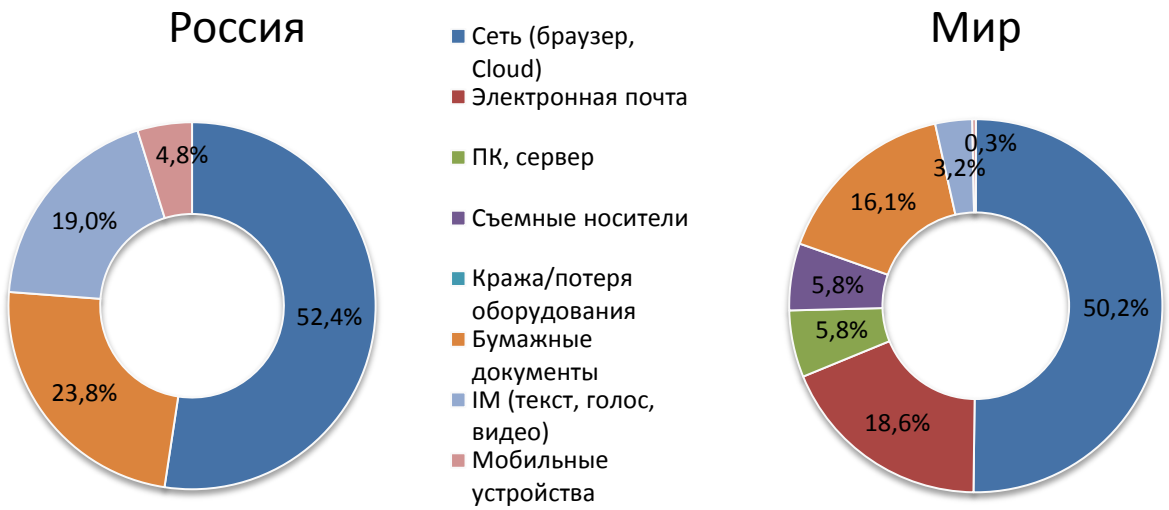
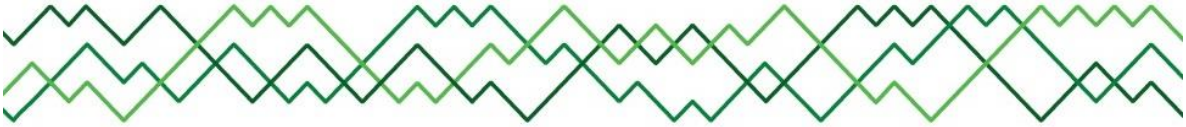


Рисунок 9. Каналы утечек: Россия – Мир, 2017 г.

В то же время в мире весьма распространены утечки информации по электронной почте, в России этот канал не представлен в публичных сообщениях.

TVNet: В Латвии семья получила по электронной почте результаты чужих анализов. Имя и фамилии были указаны верно, но персональный код и адрес относились к другому человеку. В лаборатории пояснили, что ошибка могла произойти по вине врача, который указал неправильный электронный адрес. Медики уверяли, что это единичный случай, однако в ходе уличного опроса журналистам не составило труда найти ряд людей, которые сталкивались с подобными утечками.



Заключение и выводы

В 2017 г. в мире отмечено снижение числа зарегистрированных утечек информации и практически двукратное падение объема скомпрометированных записей в медицинских организациях. Но значение этих показателей не следует переоценивать. Относительные успехи в глобальном масштабе во многом обеспечены благодаря активной позиции многих клиник и медицинских центров США, которые выделили дополнительные средства на укрепление ИБ. В частности, это позволило снизить долю внутренних инцидентов в американских медучреждениях.

К сожалению, примеру заокеанских коллег пока не в полной мере следуют медицинские организации в России. В отечественной медицине более чем вдвое выросло число утечек – как за счет умышленных, так и случайных действий внутренних нарушителей в организациях. Это связано с общим повышением ценности обрабатываемой медицинской информации и, следовательно, с ростом ее привлекательности в глазах злоумышленников.

Оставляет желать лучшего культура обращения с информацией ограниченного доступа у медицинских работников в России. Об этом свидетельствует тот факт, что все утечки, зарегистрированные в российских медучреждениях, произошли по вине или неосторожности именно внутреннего нарушителя.

Внешние утечки медицинских данных, чрезвычайно распространенные в мире, в России не зафиксированы вовсе. Можно предположить, что их действительно статистически не было, и российские медицинские данные для хакеров не интересны в принципе (что в целом выглядит правдоподобно, поскольку в России медицинские данные не столь тесно связаны с платежной и иной ликвидной информацией через механизмы медицинского страхования). Либо (что также вполне вероятно), такие утечки все же имели место быть, однако происходили редко, и имеющихся в медучреждениях средств защиты сегодня оказалось просто недостаточно для того, чтоб их зафиксировать, установить каналы утечки, найти виновных.

Компании сферы здравоохранения занимают одно из первых мест среди всех отраслей мирового хозяйства по такому показателю, как воздействие на информационные активы со стороны внутренних злоумышленников. Именно по вине сотрудников, топ-менеджеров и системных администраторов здесь происходит подавляющее большинство инцидентов, утекает основной объем записей.

Стоит отметить, что почти половина внутренних утечек из медицинской сферы совершается в результате неумышленных действий, что во многом объясняется слабой подготовкой сотрудников в области защиты информации и тем, что мероприятия по ИБ в здравоохранении зачастую финансируются скудно, порой по остаточному принципу.

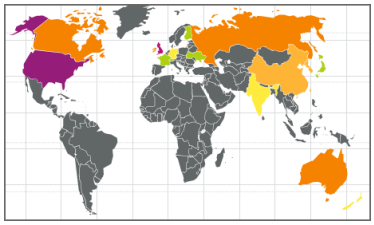
Из наиболее очевидных тенденций можно указать рост ценности медицинской информации во всем мире (в силу естественного развития технологий, в том числе телемедицины), а также большого разнообразия способов использования медицинских данных в электронном виде при оказании медицинских услуг. Отсюда следует, что число «медицинских» утечек и объем скомпрометированных данных в мире неизбежно будут расти.

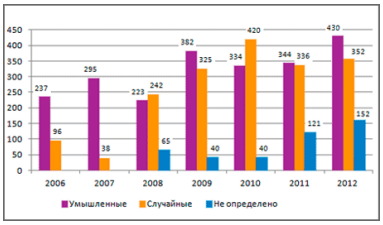
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Мониторинг утечек на сайте InfoWatch

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

Кроме того на сайте представлены статистические данные по утечкам информации за прошедшие годы, оформленные в виде динамических графиков.



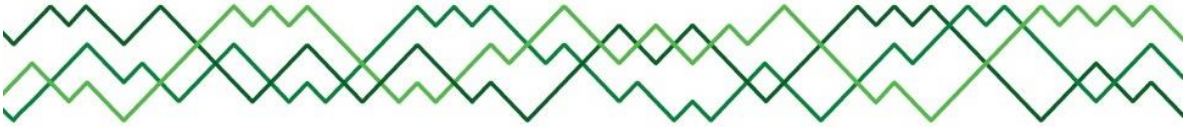


Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитический центр InfoWatch

www.infowatch.ru/analytics



INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Глоссарий

Инциденты информационной безопасности — *в данном исследовании к этой категории авторы относят случаи компрометации информации ограниченного доступа вследствие утечек данных и/или деструктивных действий сотрудников компании.*

Утечка данных — *под утечкой мы понимаем утрату контроля над информацией (данными) в результате внешнего воздействия (атаки) а также действий лица, имеющего легитимный доступ к информации или действий лица, получившего неправомерный доступ к такой информации.*

Деструктивные действия сотрудников — *действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).*

Конфиденциальная информация — *(здесь) информация, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. В данном отчете в категорию КИ мы включаем информацию, подпадающую под определение персональных данных.*

Умышленные/неумышленные утечки — *к умышленным относятся такие утечки, когда пользователь, работающий с информацией, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду. В результате создались условия для утраты контроля над информацией и/или нарушения конфиденциальности информации. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.*

К неумышленным относятся утечки информации, когда пользователь не предполагал наступления возможных негативных последствий своих действий и не преследовал личной выгоды. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

Вектор воздействия — *критерий классификации в отношении действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников – (Внешние атаки), направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников – (Внутренний нарушитель), атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.)*

Канал передачи данных — *сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. На данный момент мы различаем 8 самостоятельных каналов:*

- ✓ *Кража/потеря оборудования (сервер, СХД, ноутбук, ПК), – компрометация информации в ходе обслуживания 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, флеш-карты).*
- ✓ *Сеть – утечка через браузер (отправка данных 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).*
- ✓ *IM – мессенджеры, сервисы мгновенных сообщений (утечка информации при передаче голосом, текстом, видео при использовании сервисов мгновенных сообщений).*
- ✓ *Не определено - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки».*