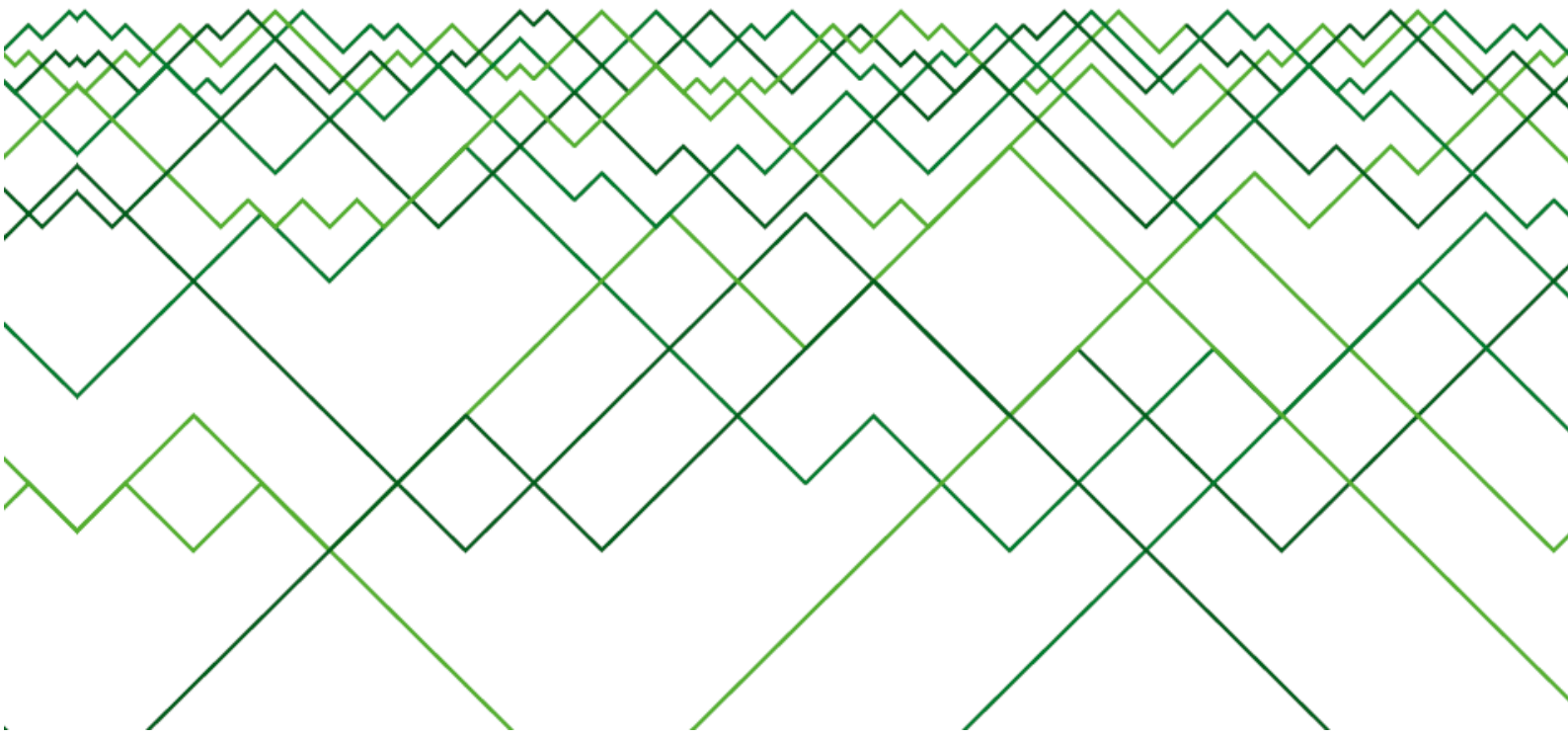
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический Центр InfoWatch

10 самых распространенных ошибок сотрудников, приводящих к утечке информации

Составитель: Прозоров Андрей, ведущий эксперт по информационной безопасности



INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Оглавление

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Введение

Аналитический Центр компании InfoWatch регулярно разрабатывает отчеты об исследовании утечек информации ограниченного доступа в России и Мире, а также другие аналитические материалы и рекомендации по защите от утечек информации.

Одним из важных выводов, которые можно увидеть в наших отчетах, является тот факт, что **количество случайных утечек приблизительно равно количеству умышленных**. При этом подходы к защите от умышленных и случайных утечек довольно сильно отличаются. Так, в первом случае, организациям стоит сфокусироваться на повышении осведомленности и обучении персонала, внедрить средства, позволяющие уведомлять пользователей о попытках нарушения ими политик безопасности. Во втором случае важно минимизировать права пользователей, сократить количество возможных каналов утечки информации, использовать средства мониторинга и контроля передачи информации, сохранять архив событий безопасности.

В рамках данного документа представлены типовые сценарии утечки информации, происходящие из-за ошибок персонала организаций и/или небрежного отношения с носителями информации, системами и средствами обработки, примеры инцидентов, рекомендации по применению мер защиты.

10 самыми распространенными ошибками сотрудников, приводящими к утечке информации, являются:

- ✓ Потеря съемных носителей
- ✓ Потеря мобильных устройств (в т.ч. в результате кражи)
- ✓ Небрежное обращение с бумажными документами (в т.ч. потеря)
- ✓ Ошибочная пересылка электронных сообщений
- ✓ Ошибочная пересылка почтовых отправлений и факсов
- ✓ Ошибочное предоставление прав доступа, выкладывание закрытой информации в общий доступ
- ✓ Небрежная утилизация бумажных документов
- ✓ Небрежная утилизация оборудования
- ✓ Передача оборудования, содержащего информацию ограниченного доступа, на техническое обслуживание третьим лицам
- ✓ Нарушение политики безопасности (нелегитимная пересылка, копирование информации) по просьбе других сотрудников и прочих лиц (социальная инженерия)

Сценарии утечки и инциденты

1. Потеря съемных носителей

Съемные носители (например, USB-флешки, CD/DVD-диски, карты памяти, ленточные накопители) являются популярным и общедоступным средством для транспортировки (обмена) информации, а также хранения резервных копий. Их достаточно просто вынести за пределы контролируемой зоны, а их небольшие размеры способствуют повышению вероятности потери носителя.

Пример инцидента:

> [1] *Сотрудник госучреждения Колорадо (Governor's Office of Information Technology) потерял USB-накопитель, на котором хранились личные данные почти 19 000 работников госучреждения. Электронный документ, записанный на флешке, содержал имена, фамилии, номера социального страхования (SSN), как нынешних, так и бывших сотрудников. Не смотря на наличие соответствующих требований в организации, съемный диск зашифрован не был.*

Еще ссылки и примеры утечек: [1], [2], [3]

2. Потеря мобильных устройств (в т.ч. в результате кражи)

В настоящее время все больше сотрудников организаций используют корпоративные и личные мобильные устройства (ноутбуки, планшетные компьютеры, смартфоны и прочее) для обработки информации ограниченного доступа. Их так же, как и съемные носители, достаточно просто вынести за пределы контролируемой зоны (для этого они обычно и используются). Отдельно стоит отметить, что сами по себе мобильные устройства являются желанной целью для грабителей и воров. Потери, а скорее даже кражи, ноутбуков и других устройств являются очень распространенным инцидентом.

Пример инцидента:

> [4] *У шерифа округа Кинг (Вашингтон, США) из автомобиля был похищен корпоративный ноутбук, где находились персональные данные нескольких тысяч американцев (включая номера соцстрахования и водительских удостоверений). Данные были не зашифрованы.*
>
> [5] *Исследование Sony's VAIO Digital Business показало, что за последние 12 месяцев было потеряно более 1 млн ноутбуков, содержащих ценные корпоративные данные организаций. В опросе приняли участие представители 600 компаний Великобритании.*
>
> [6] *Компания Credant Technologies провела исследование в аэропортах 7 городов Америки: Чикаго, Сан-Франциско, Дугласе, Майами, Орландо, Миннеаполис, Денвер. Собранная информация оказалась удручающей: в период с июня 2011 по июнь 2012 года пассажиры оставили в аэропортах 8016 девайсов, среди них смартфоны, планшеты, ноутбуки, флеш-накопители.*

Еще ссылки и примеры утечек: [4], [5], [6], [7], [8], [9], [10], [11]

3. Небрежное обращение с бумажными документами (в т.ч. потеря)

Очень часто распечатанные документы, содержащие информацию ограниченного доступа, бесконтрольно складируют, оставляют рядом с принтерами, теряют за пределами организации.

Пример инцидента:

> [12] *Сотрудники стоматологической клиники г. Лангепаса (Тюменская область) выносили за пределы лечебного учреждения амбулаторные карты пациентов. Одна из историй болезни была оставлена в такси работником клиники, после чего информация о здоровье пациентки стала достоянием общественности.*

Еще ссылки и примеры утечек: [12], [13], [14], [15]

4. Ошибочная пересылка электронных сообщений

Ошибочная пересылка электронных сообщений обычно происходит из-за невнимательности сотрудников при выборе/наборе адресата или желания упростить себе задачу отправкой единой информационной базы сразу всем участникам переписки.

Пример инцидента:

> [16] *Сотрудники отдела бухгалтерского учёта центра Миссисипского Университета (The University of Mississippi) в ходе массовой рассылки письма, информирующего об изменениях в программе медицинского страхования, допустили ошибку. Во вложении была отправлена таблица, содержащая персональные данные 2281 студента: номера социального страхования, средний балл аттестатов, пол, расовая принадлежность, дни рождения, адреса, номера телефонов и другие персональные данные студента.*

Еще ссылки и примеры утечек: [16], [17], [18], [19], [20]

5. Ошибочная пересылка почтовых отправлений и факсов

Здесь все происходит аналогично предыдущему пункту с отличием только в способе отправки.

Пример инцидента:

> [21] *Британская Информационная комиссия (Information Commissioner's Office) оштрафовала Банк Шотландии (Bank of Scotland) на 75 тысяч фунтов стерлингов за рассылку факсов с конфиденциальной информацией по неправильным номерам. Установлено, что сотрудники банка ошибались номерами с февраля 2009 по 2012 годы. По неверным номерам направлялись*

платежные ведомости, банковские выписки и ипотечные заявки. В документах содержались имена и контактные данные клиентов.

Еще ссылки и примеры утечек: [21], [22]

6. Ошибочное предоставление прав доступа, выкладывание закрытой информации в общий доступ

Данный вид ошибки является обобщающим для такого рода действий как: предоставление излишних прав доступа к информации и сервисам, случайные ошибки при настройке прав доступа, разглашение информации из-за не понимания требований по защите ее конфиденциальности, превышение служебных полномочий при раскрытии информации и другие аналогичные.

Пример инцидента:

[23] *Проводя проверку, прокуратура Тамбовской области установила, что на официальном сайте региональной Госинспекции труда с 1 декабря 2012-го по 6 августа 2013 года чиновники разместили план проверок юридических лиц и индивидуальных предпринимателей на 2013 год, содержащий поля с данными об ИНН и адресах проживания ряда предпринимателей.*

[24] *Мировой суд Тюмени оштрафовал «Тюменское центральное агентство воздушных сообщений» (ТЦАВС) за публикацию персональных данных пассажиров на собственном сайте. На одной из страниц сайта ТЦАВС публиковались персональные данные пассажиров с указанием их фамилии, имени, отчества, даты рождения, места проживания, паспортных данных, маршрутов полетов и др. Любой посетитель ресурса мог беспрепятственно их просмотреть.*

Еще ссылки и примеры утечек: [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]

7. Небрежная утилизация бумажных документов

Небрежная утилизация бумажных документов, на удивление, является довольно распространенным инцидентом. Документы, содержащие информацию ограниченного доступа, просто выбрасывают, не заботясь об их правильном уничтожении.

Пример инцидента:

[34] *Жительница г. Абакан (Республика Хакассия) обнаружила три мешка бумаг, содержащих персональные данные клиентов банка "Кедр", около мусорного бака у себя во дворе. Среди персональных данных числились: фамилии, имена людей, паспортные данные и даже наличие иждивенцев.*

[35] *Главврач, он же владелец, одной из клиник Канзаса вынужден прекратить врачебную практику из-за безалаберного отношения к конфиденциальным документам, касающихся его клиентов – женщин, сделавших аборт. В середине марта в мусорном баке на территории школы, находящейся рядом с домом главврача, прохожие обнаружили тысячи историй болезни, в которых*

можно без труда найти имена, адреса, телефоны, номера социального страхования, а также медицинские сведения о пациентах.

Еще ссылки и примеры утечек: [34], [35], [36], [37], [38]

8. Небрежная утилизация оборудования

Помимо непосредственного выбрасывания средств обработки и хранения информации, содержащих информацию ограниченного доступа, без ее удаления, к такому рода ошибкам относится и передача (а также перепродажа) таких средств другим лицам для повторного использования.

Пример инцидента:

[39] *Один из жителей Великобритании (более точно - Уэльса) случайно выбросил жесткий диск, на котором содержался файл с записью о более чем 7500 биткоинов. На сегодняшний день стоимость одного биткоина составляет более тысячи долларов и, таким образом, несчастный потерял свыше $7,5 млн.*

Еще ссылки и примеры утечек: [39], [40]

9. Передача оборудования, содержащего информацию ограниченного доступа, на техническое обслуживание третьим лицам

Довольно часто организации не занимаются сложным ремонтом и техническим обслуживанием компьютерной техники самостоятельно, а передают ее в специализированные центры. При этом наличие информации ограниченного доступа на данных носителях не всегда проверяется (и не всегда возможно в связи с нарушением работоспособности устройства). В ходе ремонта/технического обслуживания персонал, проводящий его, может получить доступ ко всей хранимой на устройстве информации.

Пример инцидента:

[41] *Компания Virginia Tech допустила утечку персональных данных 145 000 человек, когда передала на техническое обслуживание сервер, на котором они хранились.*

Еще ссылки и примеры утечек: [41]

10. Нарушение политики безопасности (нелегитимная пересылка, копирование информации) по просьбе других сотрудников и прочих лиц (социальная инженерия)

Такого рода ошибки происходят, если сотрудника кто-то попросит (в том числе и неизвестный внешний человек, представившийся сотрудником компании) или даст прямое указание (если является его начальником) сохранить или переслать информацию ограниченного доступа каким-либо способом. При этом такая просьба может быть вызвана вполне осознанным желанием данную информацию похитить.

Пример инцидента:

> [42] *Из баз данных банков Standard Chartered Bank и Citi Bank Korea была допущена утечка конфиденциальной информации на 130 тысяч клиентов. Один из них (сотрудник "Сити Банка") распечатал личные и контактные данные на более чем 30 тысяч человек, а другой (сотрудник SC) скопировал информацию "по просьбе старшего товарища" на USB-носитель. Эти данные, которые содержали имена клиентов, их телефоны, адреса, а также сведения о финансовом положении, были переданы на сторону. За свою работу они получили в общей сложности около 300 миллионов вон (около 300 тысяч долларов). Сведения были использованы затем для рассылки по телефонам рекламы с предложениями о выдаче займов.*

Еще ссылки и примеры утечек: [42]

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Меры защиты

№	Ошибка сотрудников	Меры защиты
1.	Потеря съемных носителей	– Повышение осведомленности и обучение персонала – Принудительное шифрование носителей – Мониторинг и контроль подключаемых устройств, фильтрация информации, передаваемой на съемные устройства – DLP-системы – Использование средств гарантированного уничтожения информации – Маркирование съемных носителей – Использование наклеек на корпусе и/или записанных текстовых файлов, содержащих контактную информацию владельца
2.	Потеря мобильных устройств (в т.ч. в результате кражи)	– Повышение осведомленности и обучение персонала – Шифрование информации на мобильных устройствах – Запрет хранения информации на мобильных устройствах, терминальный доступ к информации – Замки и тросы для ноутбуков – Использования программных и/или аппаратных средств поиска (контроля перемещения) мобильных устройств – Использование средств удаленного уничтожения информации – Использование средств гарантированного уничтожения информации – Маркирование мобильных устройств; использование наклеек на корпусе и/или заставок, содержащих контактную информацию владельца
3.	Небрежное обращение с бумажными документами (в т.ч. потеря)	– Повышение осведомленности и обучение персонала – Маркирование документов – Использование папок и/или вложений, содержащих контактную информацию владельца – Контроль печати
4.	Ошибочная пересылка электронных сообщений	– Повышение осведомленности и обучение персонала – DLP-системы
5.	Ошибочная пересылка почтовых отправлений и факсов	– Повышение осведомленности и обучение персонала
6.	Ошибочное предоставление прав доступа, выкладывание в общий доступ закрытой информации	– Повышение осведомленности и обучение персонала – Усложнение процедуры предоставления прав доступа, введение дополнительных шагов по согласованию; регулярный анализ и пересмотр прав доступа – Использование средств мониторинга и контроля предоставления прав доступа

7.	Небрежная утилизация бумажных документов	– Повышение осведомленности и обучение персонала – Использование шредеров или других средств уничтожения бумажных документов – Контроль печати
8.	Небрежная утилизация оборудования	– Повышение осведомленности и обучение персонала – Использование средств гарантированного уничтожения информации и/или носителей информации
9.	Передача оборудования, содержащего информацию ограниченного доступа, на техническое обслуживание третьим лицам	– Повышение осведомленности и обучение персонала – Использование средств гарантированного уничтожения информации и/или носителей информации – Соглашение о неразглашении информации с третьими лицами
10.	Нарушение политики безопасности (нелегитимная пересылка, копирование информации) по просьбе других сотрудников и прочих лиц (социальная инженерия)	– Повышение осведомленности и обучение персонала

Вместо заключения

Неумышленные утечки информации в организациях могут произойти по различным сценариям. Единого и универсального подхода по защите от такого рода утечек не существует, к ней необходимо подходить системно и комплексно.

Специалисты компании InfoWatch в рамках консалтинговых услуг могут помочь в выборе необходимых мер защиты, разработке политик и процедур, проведении обучения персонала и многое другое.

Обращайтесь!

Тел./факс: +7 495 22-900-22

E-mails:

– Общие вопросы: info@infowatch.ru
– Отдел продаж: sales@infowatch.ru
– Служба поддержки: support@infowatch.ru
– Контакты для прессы: pr@infowatch.ru

Адрес: Российская Федерация, 123022, Москва, 2-ая Звенигородская ул., д.13, стр.41

Сайт компании: www.infowatch.ru

Мы в социальных сетях:

– https://www.facebook.com/InfoWatch
– https://twitter.com/InfoWatchNews

Приложение А.
Ссылки на инциденты, представленные в документе

[1] http://www.infowatch.ru/analytics/leaks_monitoring/5059
[2] http://www.infowatch.ru/analytics/leaks_monitoring/4040
[3] http://www.infowatch.ru/analytics/leaks_monitoring/2604
[4] http://www.infowatch.ru/analytics/leaks_monitoring/3129
[5] http://www.infowatch.ru/analytics/leaks_monitoring/3040
[6] http://www.infowatch.ru/analytics/leaks_monitoring/2704
[7] http://www.infowatch.ru/analytics/leaks_monitoring/2768
[8] http://www.infowatch.ru/analytics/leaks_monitoring/2747
[9] http://www.infowatch.ru/analytics/leaks_monitoring/2690
[10] http://www.infowatch.ru/analytics/leaks_monitoring/2682
[11] http://www.infowatch.ru/analytics/leaks_monitoring/2602
[12] http://www.infowatch.ru/analytics/leaks_monitoring/3601
[13] http://www.infowatch.ru/analytics/leaks_monitoring/3137
[14] http://www.infowatch.ru/analytics/leaks_monitoring/2862
[15] http://www.infowatch.ru/analytics/leaks_monitoring/2653
[16] http://www.infowatch.ru/analytics/leaks_monitoring/4026
[17] http://www.infowatch.ru/analytics/leaks_monitoring/4045
[18] http://www.infowatch.ru/analytics/leaks_monitoring/3053
[19] http://www.infowatch.ru/analytics/leaks_monitoring/2746
[20] http://www.infowatch.ru/analytics/leaks_monitoring/2589
[21] http://www.infowatch.ru/analytics/leaks_monitoring/3399
[22] http://www.databreaches.net/company-responsible-for-mps-social-security-mistake-explains/
[23] http://www.infowatch.ru/analytics/leaks_monitoring/3926
[24] http://www.infowatch.ru/analytics/leaks_monitoring/3439
[25] http://www.infowatch.ru/analytics/leaks_monitoring/5064
[26] http://www.infowatch.ru/analytics/leaks_monitoring/5012
[27] http://www.infowatch.ru/analytics/leaks_monitoring/4685
[28] http://www.infowatch.ru/analytics/leaks_monitoring/4044
[29] http://www.infowatch.ru/analytics/leaks_monitoring/3575
[30] http://www.infowatch.ru/analytics/leaks_monitoring/3306
[31] http://www.infowatch.ru/analytics/leaks_monitoring/3290
[32] http://www.infowatch.ru/analytics/leaks_monitoring/3150
[33] http://www.infowatch.ru/analytics/leaks_monitoring/3092
[34] http://www.infowatch.ru/analytics/leaks_monitoring/3086
[35] http://www.infowatch.ru/analytics/leaks_monitoring/2644
[36] http://www.infowatch.ru/analytics/leaks_monitoring/5208
[37] http://www.infowatch.ru/analytics/leaks_monitoring/2643
[38] http://www.infowatch.ru/analytics/leaks_monitoring/4686
[39] http://www.ichip.ru/novosti/internet-i-seti/2013/11/zhitel-velikobritanii-vybrosil-zhestkii-disk-s-7500-bitkoinov16
[40] http://rus.delfi.lv/news/daily/abroad/major-britanskoj-armii-vybrosil-v-more-noutbuk-s-sekretnoj-informaciej.d?id=43872606
[41] http://news.idg.no/cw/art.cfm?id=30A58A5E-F281-7C65-AB08CF33CE7C4D1C
[42] http://www.infowatch.ru/analytics/leaks_monitoring/5021