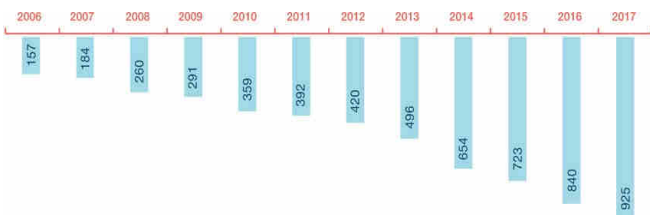
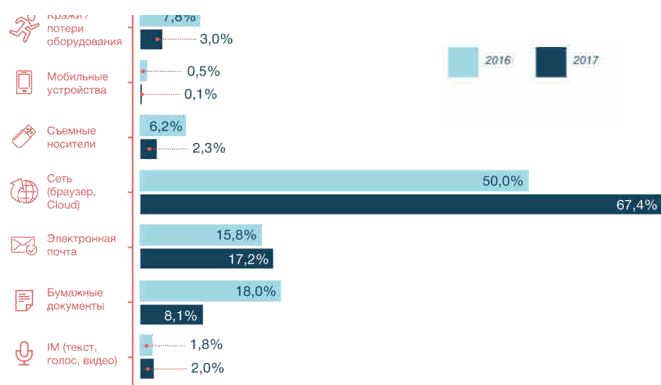


## Поговорим о цифрах



В первом полугодии 2017 г. InfoWatch зарегистрировал 925 случаев утечек конфиденциальной информации – на 10% больше, чем за аналогичный период 2016 г.



Увеличилась доля утечек по сетевому каналу и электронной почте. Снизилась доля утечек в результате кражи/потери оборудования, через съемные носители и бумажные документы.

## ЧЕМ ГРОЗИТ УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ?

Завладев паспортными или другими персональными данными, мошенники могут:

- оформить кредит в банке;
- «повесить» долги или фирму;
- совершить незаконные действия с вашей недвижимостью;
- распорядиться средствами с банковских карт;
- открыть электронный кошелек;
- зарегистрироваться на сайтах знакомств, онлайн-игр и казино;
- шантажировать вас или ваших родственников;
- использовать вашу личность как «подменную» для мошеннических действий;
- использовать ваши данные в собственных интересах, например, навязывать услуги, распространять противоправный контент.

## ИНФОРМАЦИЯ ДЛЯ РОДИТЕЛЕЙ

Если на все 4 вопроса, Вы ответили «Да», то Ваш ребенок в безопасности и Вам не о чем беспокоится.

Соблюдает ли ваш ребенок правила конфиденциальности в отношении своих персональных данных?

1

2

Безопасный ли доступ установлен к его профилю в целом и к отдельным категориям личной информации в социальной сети?

Следите ли Вы за информацией, которую Ваш ребенок отправляет/ вводит в Интернете?

3

4

Осведомлены ли Вы о проблемах своего ребенка, связанных с последствиями неосторожного отношения к персональным данным?

Если же в Ваших ответах присутствует «Нет», то Вам стоит обратить внимание на информационную защищенность Вашего ребенка.

В помощь родителям и детям :  
<http://персональныеданные.дети/>

Самая большая утечка 2017 года в России зафиксирована в сентябре, когда в Сети были обнаружены базы данных с информацией о более чем 5,6 млн клиентов страховых компаний. Большинство баз содержали не только персональные сведения, но также данные об автомобилях застрахованных лиц, историю сделок и копии документов.

ИСТОЧНИК: INFOWATCH

**Интересный факт**

## ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ЗЛОУМЫШЛЕННИКОВ В СЕТИ ИНТЕРНЕТ



Авторы :  
Алиев А.М, Жученко В.С, Саенко Д.А.

Национальный Центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет



## Что включают в себя персональные данные?

**Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

фамилия, имя и отчество, дата и место рождения, адрес, семейное положение, паспортные данные, профессия, доходы и другая информация.

## Нормативно-правовая база по защите персональных данных:

ЗАКОНЫ

Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»

Постановления  
Правительства

№781 от  
17.11.2007

№687 от  
15.09.2008

Приказы  
и иные  
документы

«Приказ трех»  
от 13.02.2008

Методические  
материалы  
ФСТЭК

Приказ ФСТЭК  
№17



## Где существует наибольший риск потери персональных данных ?



Социальные сети и мессенджеры



Цифровая кража смартфона

Аккаунты в игровых сервисах



Электронная почта



Банковские данные



Мобильные приложения и игры



Незащищённая

## ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ОБНАРУЖИЛИ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ИНТЕРНЕТЕ?

Написать жалобу



Владелец аккаунта

Тех.поддержка сайта



Администрация сайта

Когда невозможно установить источник распространения персональных данных или связаться с ним напрямую

Нужно обратиться в прокуратуру или Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций



Подкрепите требования ссылками на нормы закона № 152 «О персональных данных», который запрещает использовать информацию без разрешения субъекта данных. Предупредите, что в случае отказа вы вправе обратиться в суд согласно статье 24 закона (ответственность за нарушение требований ФЗ № 152).

## ТОП-4 ОСНОВНЫХ СПОСОБОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1

Пароль

\*\*\*\*\*

+



Используйте двухфакторную аутентификацию

2



Контролируйте доступ приложений к вашим данным

3



Пользуйтесь менеджерами паролей

4

<https://>

Используйте только защищённое соединение