

Всероссийская академия внешней
торговли



Школа правовых знаний

Персональные данные: проблемы использования и защиты

Вологдин Александр Анатольевич
к.и.н., зав.кафедрой ТИГП

Барковская Полина, Доброгост Ольга, Прокудина Татьяна
студенты МПФ

Что из перечисленного относится к персональным данным?

- Илья Арнольдович Ильф
- +7(916) 322-45-67
- 09.11.1970 – дата рождения
- Адрес дачи Ильи Арнольдовича
- lev.kusnetsov@gggg.ru
- Альяма – кличка собаки Ильи Арнольдовича
- IP- адрес
- ID Ильи Арнольдовича в Инстаграме
- Номер заказа в ресторане быстрого питания
- Гражданин А. - католик
- Цвет глаз – голубой
- Температура тела – 36.5
- Отпечатки пальцев





Что из перечисленного относится к персональным данным?

- **Илья Арнольдович Ильф**
- **+7(916) 322-45-67**
- **09.11.1970 – дата рождения**
- Адрес дачи Ильи Арнольдовича
- lev.kusnetsov@gggg.ru
- Альма – кличка собаки Ильи Арнольдовича
- **IP- адрес**
- **ID Ильи Арнольдовича в Инстаграме**
- Номер заказа в ресторане быстрого питания
- **Гражданин А. - католик**
- **Цвет глаз – голубой**
- **Температура тела – 36.5**
- **Отпечатки пальцев**

Законодательство о персональных данных

Конвенция о защите физических лиц
при автоматизированной обработке
персональных данных
(Заключена в г. Страсбурге
28.01.1981)

Федеральный закон от 27.07.2006 №
152-ФЗ "О персональных данных"

Кодекс Российской Федерации об
административных
правонарушениях от 30.12.2001 №
195-ФЗ

Трудовой кодекс Российской
Федерации от 30.12.2001 № 197-ФЗ

Уголовный кодекс Российской
Федерации от 13.06.1996 № 63-ФЗ

Постановление Правительства
Российской Федерации от 01.11.2012
г. № 1119 «Об утверждении
требований к защите персональных
данных при их обработке в
информационных системах
персональных данных»



Что такое персональные данные?

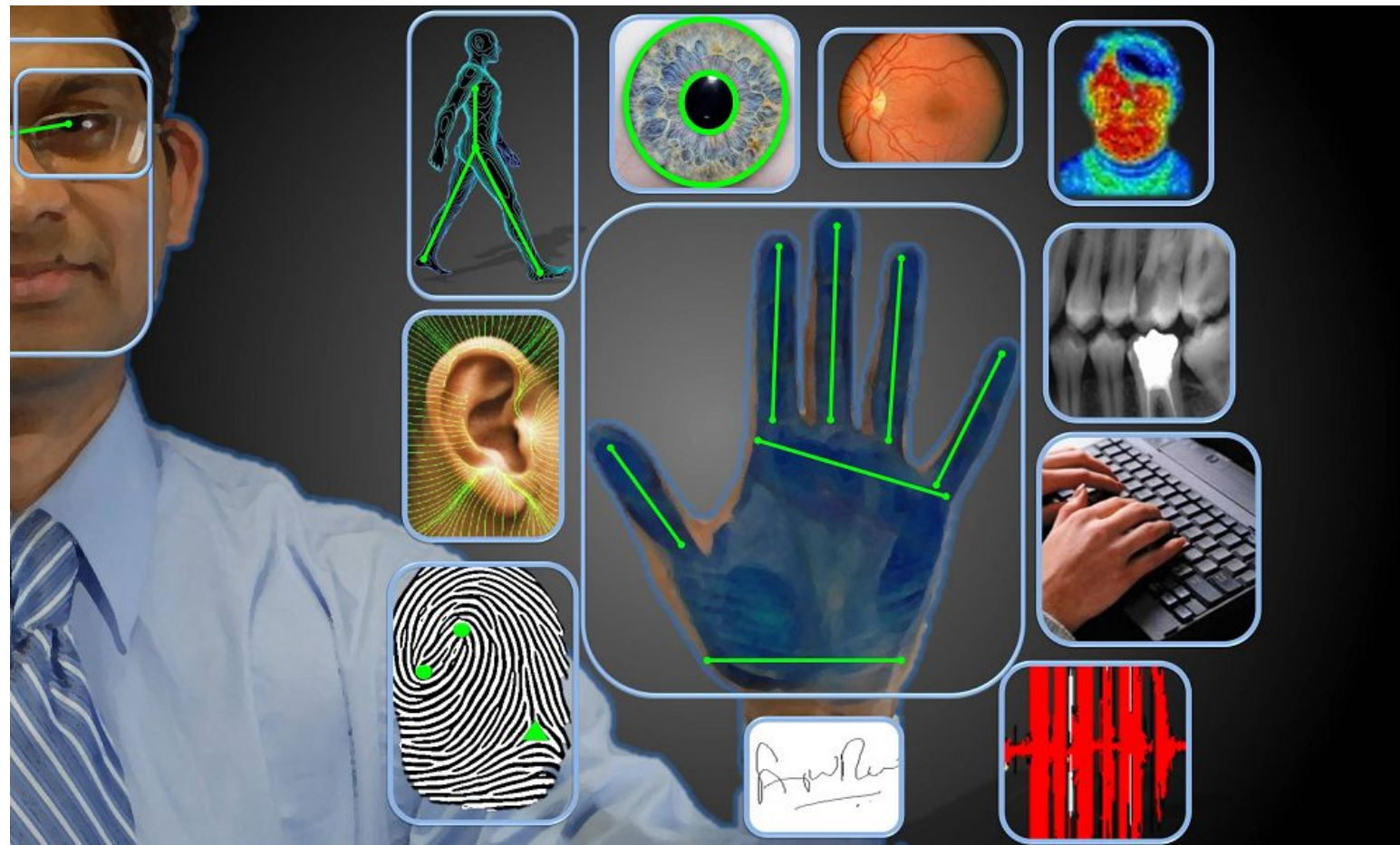
Персональные данные

- любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) – статья 3 ФЗ №152 «О персональных данных».



Биометрические персональные данные

- сведения, которые характеризуют **физиологические и биологические особенности человека**, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных,
- могут обрабатываться только при наличии **согласия в письменной форме** субъекта персональных данных, за исключением случаев, предусмотренных **частью 2**.
(статья 11 ФЗ №152).



Примеры использования биометрических персональных данных:

- Единая биометрическая система;
- Приложение «Социальный мониторинг».



Специальные категории персональны х данных

Специальные категории персональных данных, касающиеся:

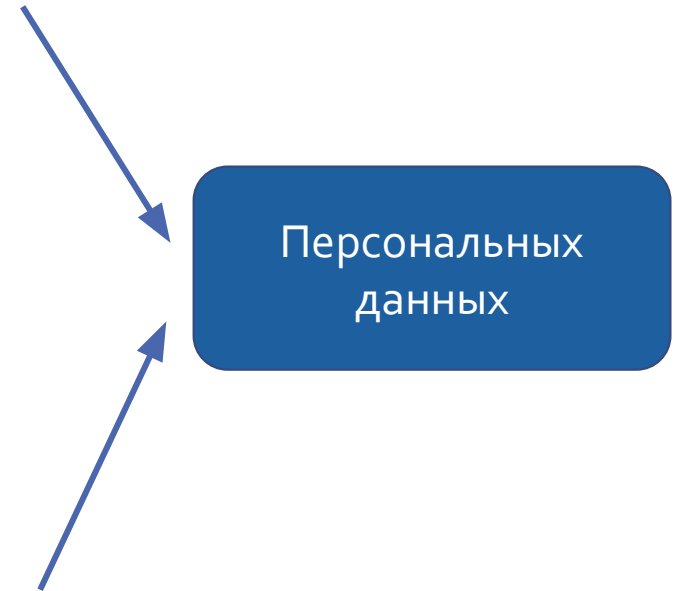
- расовой, национальной принадлежности,
- политических взглядов,
- религиозных или философских убеждений,
- состояния здоровья,
- интимной жизни.

Их обработка не допускается, за исключением случаев, предусмотренных законом.



Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, **включая:**

- сбор,
- запись,
- систематизацию,
- накопление,
- хранение,
- уточнение (обновление, изменение),
- извлечение,
- использование,
- передачу (распространение, предоставление, доступ),
- обезличивание,
- блокирование,
- удаление,
- уничтожение



Персональных
данных



Основания обработки персональны х данных (ч.1 ст.6 152-ФЗ)

- **Согласие субъекта персональных данных**
- **Достижение целей, предусмотренных международным договором РФ или законом РФ**
- Участие лица в судопроизводстве
- Исполнительное производство
- Предоставление государственных и муниципальных услуг
- **Исполнение договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных**
- Защита жизни и здоровья
- Законный интерес оператора
- Деятельность журналиста, СМИ, научная, литературная или иной творческая деятельность
- Исследовательские цели
- Эффективность государственного или муниципального управления
- Обязательное опубликование или раскрытие по закону





Оператор персональных данных

data controller

Оператор

- государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.





Обработчик персональных данных

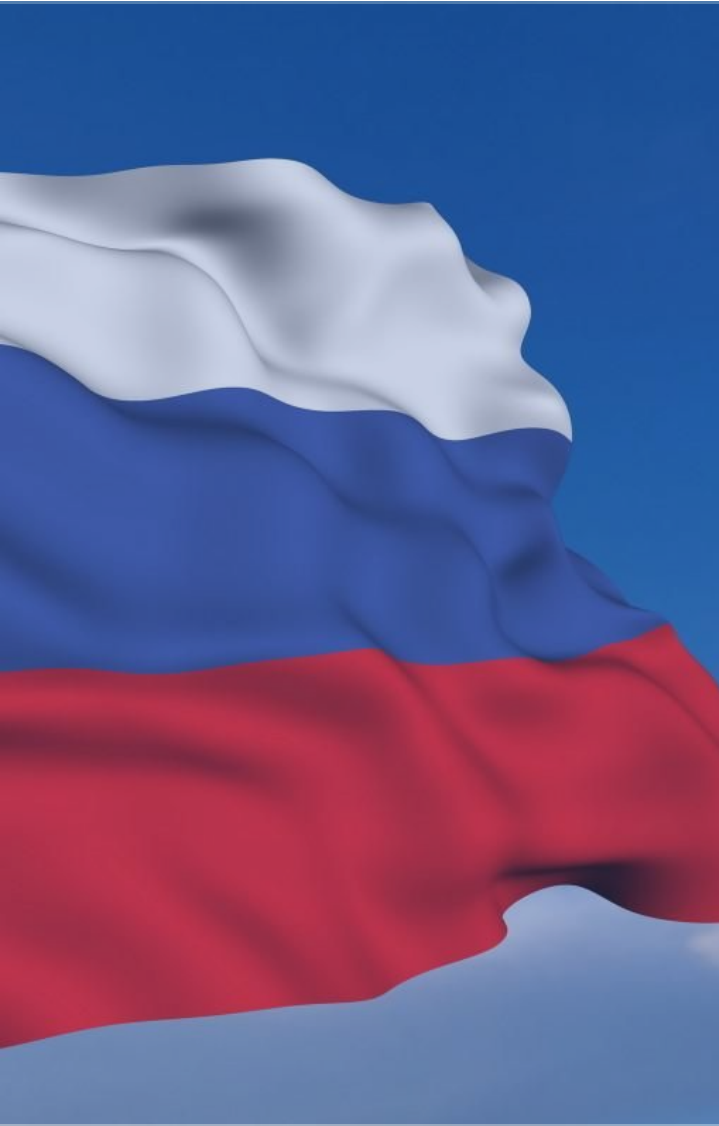
data processor

Обработчик персональных данных

В российском законодательстве такой термин специально не выделен, однако в ч. 3 ст. 6 Закона о персональных данных упоминается "лицо, осуществляющее обработку персональных данных по поручению оператора".

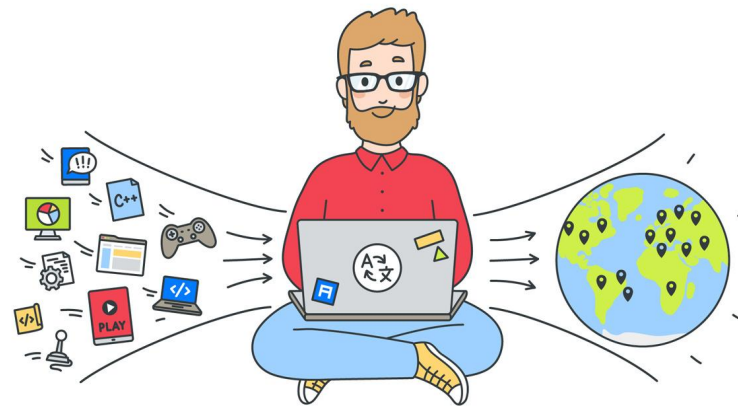
- Ключевыми характеристиками такого лица являются:
 1. наличие самостоятельной правосубъектности, т.е. это лицо должно быть юридически самостоятельным по отношению к оператору, что позволяет исключить из сферы его работников оператора и обособленные подразделения организации;
 2. обработка данных осуществляется таким лицом в интересах оператора.





Локализация персональных данных

— При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.





Сбор персональных данных

- Согласно разъяснениям (далее – «Разъяснения») Министерства связи и массовых коммуникаций Российской Федерации под сбором следует понимать:

"целенаправленный процесс получения персональных данных оператором непосредственно от субъекта персональных данных либо через специально привлеченных для этого третьих лиц".

- Если персональные данные собрало иное лицо (например, работодатель), а в дальнейшем передало их для обработки иностранному лицу, у такого иностранного лица отсутствует обязанность локализовать базы данных, так как он не осуществлял сбор персональных данных.





Распространение требований локализации на иностранные компании

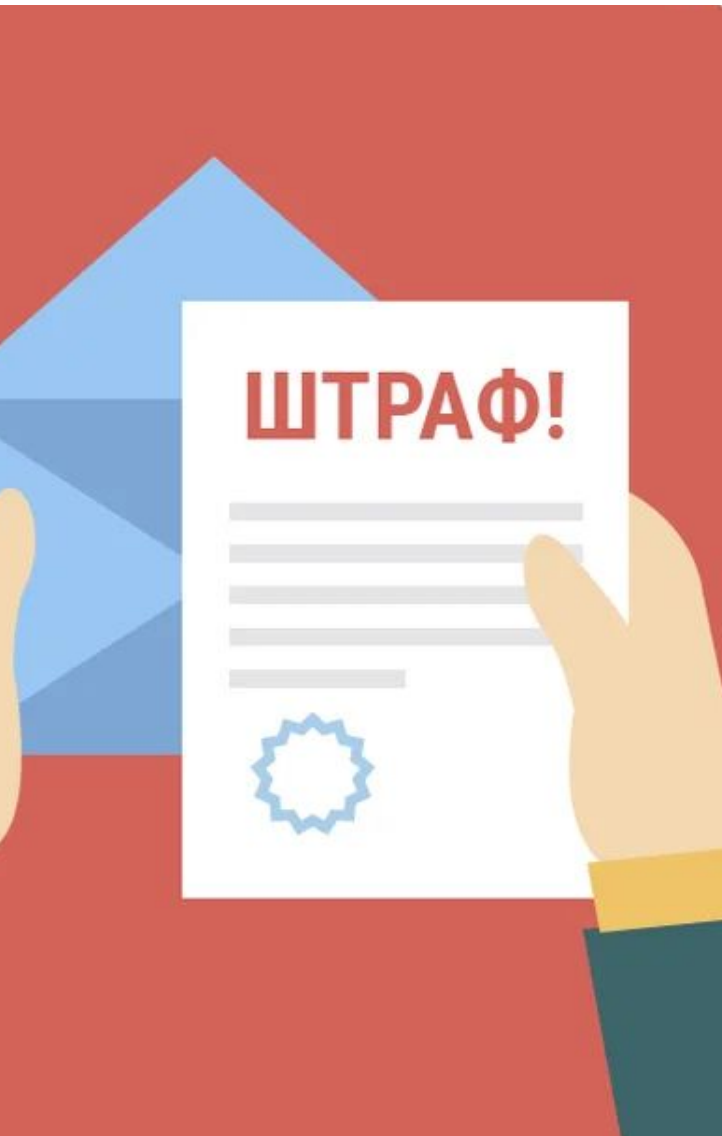
О направленности деятельности на территорию России, по мнению Минкомсвязи России, могут свидетельствовать:

– использование доменного имени, связанного с Российской Федерацией (.ru, .рф., .su, .москва., .moscow и т.п.);

– наличие русскоязычной версии интернет-сайта, созданной владельцем такого сайта или по его поручению иным лицом, за исключением функции автоматизированного переводчика, в сочетании со следующими условиями (одним их них):

- а) возможность производить расчеты в российских рублях;
- б) возможность доставки товара, оказания услуги или пользования цифровым контентом на территории России, а также иные случаи исполнения договора на территории Российской Федерации;
- с) использование рекламы на русском языке, отсылающей к соответствующему интернет-сайту;
- д) иные обстоятельства, явно свидетельствующие о намерении владельца интернет-сайта включить российский рынок в свою бизнес-стратегию.





Штраф за отказ от локализации

- За нарушение закона в части локализации предусмотрено наказание в виде штрафа для юридических лиц в размере до 6 млн руб. (ч. 8 ст. 13.11 КоАП), в случае повторного нарушения – до 18 млн руб. (ч. 9 ст. 13.11 КоАП).

Facebook, Twitter и WhatsApp оштрафовали за отказ локализации. Общая сумма штрафа составила 36 млн руб.

- Суд впервые оштрафовал WhatsApp на 4 млн руб. за отказ локализовать базы данных российских пользователей. Это первый штраф для мессенджера. Американские соцсети Facebook и Twitter получили штрафы в размере 15 млн и 17 млн руб. соответственно за повторные нарушения, сообщили в Роскомнадзоре.
- В 2020 году Facebook и Twitter уже привлекались к ответственности по ч. 8 ст. 13.11 КоАП («Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)»). Компании тогда были оштрафованы судом на 4 млн руб. каждая. Facebook оплатил штраф, Twitter – нет.



Роскомнадзор и защита прав субъектов персональных данных



Роль Роскомнадзора* - контроль и надзор за соответствием обработки персональных данных требованиям законодательства РФ.

*Роскомнадзор - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

- проводит проверки в компаниях, обрабатывающих персональные данные;
- разъясняет нормы действующего законодательства;
- отвечает на жалобы и вопросы граждан.



Общедоступные персональные данные

- Из части 1 статьи 6 152-ФЗ **исключается** пункт 10 — важное условие обработки персональных данных без согласия:
- «10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);»



Понятия общедоступных
персональных данных
больше нет

Любые данные о человеке
можно публиковать только с
его прямого согласия



Ответственность на нарушение законодательства о персональных данных

- **Административные штрафы** (штрафы за обработку по 13.11 КоАП до 500 000 рублей, штрафы за локализацию до 18 млн рублей, до 500 000 рублей за маркетинг без согласия).
- **Блокировка сайта** (самый известный пример – LinkedIn)
- **Принудительное прекращение незаконной обработки ПД** по соответствующему запросу РКН
- **Уголовная ответственность**, такая как уголовные штрафы.



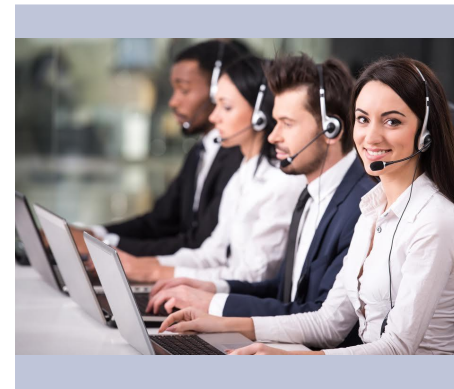


Почему
персональные
данные это важно?

Риски для приватности:



Личности сложнее
скрыться от
нежелательного внимания
со стороны



Информация о человеке может
быть использована в
коммерческих целях, в
дальнейшем заинтересованные
лица могут целенаправленно
нарушать автономию личности

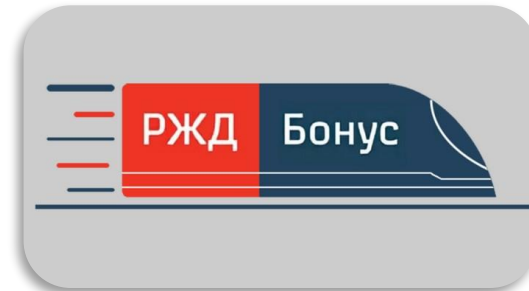


Существуют риски утечки
данных и их
несанкционированного
оборота



Недавние утечки персональных данных

Косметическая компания	допущена утечка 1,5 млн паспортов российских граждан
«Мосгортранс»	Данные пользователей » украдены и выложены в открытый доступ
Одна из крупнейших компаний сотовой связи	Данные 70% абонентов попали в публичный доступ
Российская службы электронной почты	Утечка данных 5 тысяч почтовых пользовательских ящиков
Корейская автомобильная компания	На продажу выставлены данные 1,3 млн российских владельцев авто
Программа «РЖД Бонус»	Утечка данных 1,36 млн участников программы





Недавние утечки персональных данных



РЖД

ФИО, даты рождения, адреса, номера СНИЛС, должности, фотографии и номера телефонов

700 тыс.
сотрудников



ВТБ

ФИО, домашний адрес и индекс, номер телефона (в некоторых записях — мобильный и домашний) и сумма вклада, которая начинается от 1 млн рублей

5 тыс.
клиентов

ГИБДД

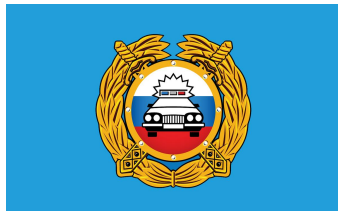
Номера телефонов, марки, модели и годы выпуска транспортных средств, коды VIN, имена и фамилии владельцев

1 136 601
запись
регистрацион
ных действий
в Москве и
МО

**Red Wings
Airlines**

паспортные данные (ФИО, номер загранпаспорта, пол, гражданство, дата рождения)

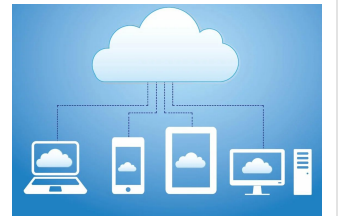
пассажиры
рейса Москва
— Анталья





Как происходят утечки? (1)

- Отправка конфиденциальной информации сотрудником на личный адрес электронной почты (*Определение КС РФ от 28.02.2019 N 457-О*)
- Обсуждение размеров заработной платы работников, изучение и фотографирование документов на чужих столах в отсутствие на рабочих местах соответствующих работников, запись разговора между сотрудниками (*Апел. опред. Мосгорсуда от 18 апреля 2016 г. по делу N 33-10533/2016*)
- Загрузка служебной и конфиденциальной информации, включая ФИО клиентов, номера договоров, контактные данные клиентов во внешние Интернет-ресурсы (*Апел. опред. Мосгорсуда от 14 декабря 2018 г. по делу N 33-55813/2018*)





Как происходят утечки? (2)

Передача зарплатных карт клиентов третьему лицу (Апел. опред. Мосгорсуда от 6 июня 2017 г. по делу N 33-21192)

Фотографирование данных клиентов на телефон и продажа третьему лицу (ИА REGNUM <https://regnum.ru/news/2784184.html>)

Изучение и фотографирование документов на чужих столах, запись разговоров, обсуждение в личной беседе (Апел. опред. Мосгорсуда от 18 апреля 2016 г. по делу N 33-10533/2016)

Запрос сведений о соединениях абонентов на основании поддельных заявлений абонентов и копирование полученных сведений на внешний носитель (Приговор Муромского городского суда Владимирской области от 09.07.2019 по делу N 1-40/2019)



10 правил цифровой гигиены, которые снизят риски кражи персональных данных

1. Внимательно относитесь к письмам и сайтам, которые требуют ввода данных о пользователе

2. Оперативно устанавливайте обновления ПО

3. Не загружайте ПО и другие файлы из непроверенных источников

4. Остерегайтесь публичных сетей Wi-Fi

5. Читайте пользовательские соглашения

6. Проверьте и настройте доступ приложений к камере, микрофону, геолокации, галерее, файлам

7. Используйте сложные пароли

8. Используйте разные пароли к учетным записям

9. Пользуйтесь антивирусным ПО

10. Настройте автоматическое резервное копирование данных



Спасибо за внимание!

*Университетские
субботы в*



https://vk.com/us_vavt