Тема: Защита персональных данных в сети Интернет

Содержание

Персональные данные

Нормативная база

Угрозы в сети Интернет

Советы

Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Законы в сфере защиты данных

Федеральный закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ.

Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» указ Президента РФ от 6 марта 1997 г. № 188.

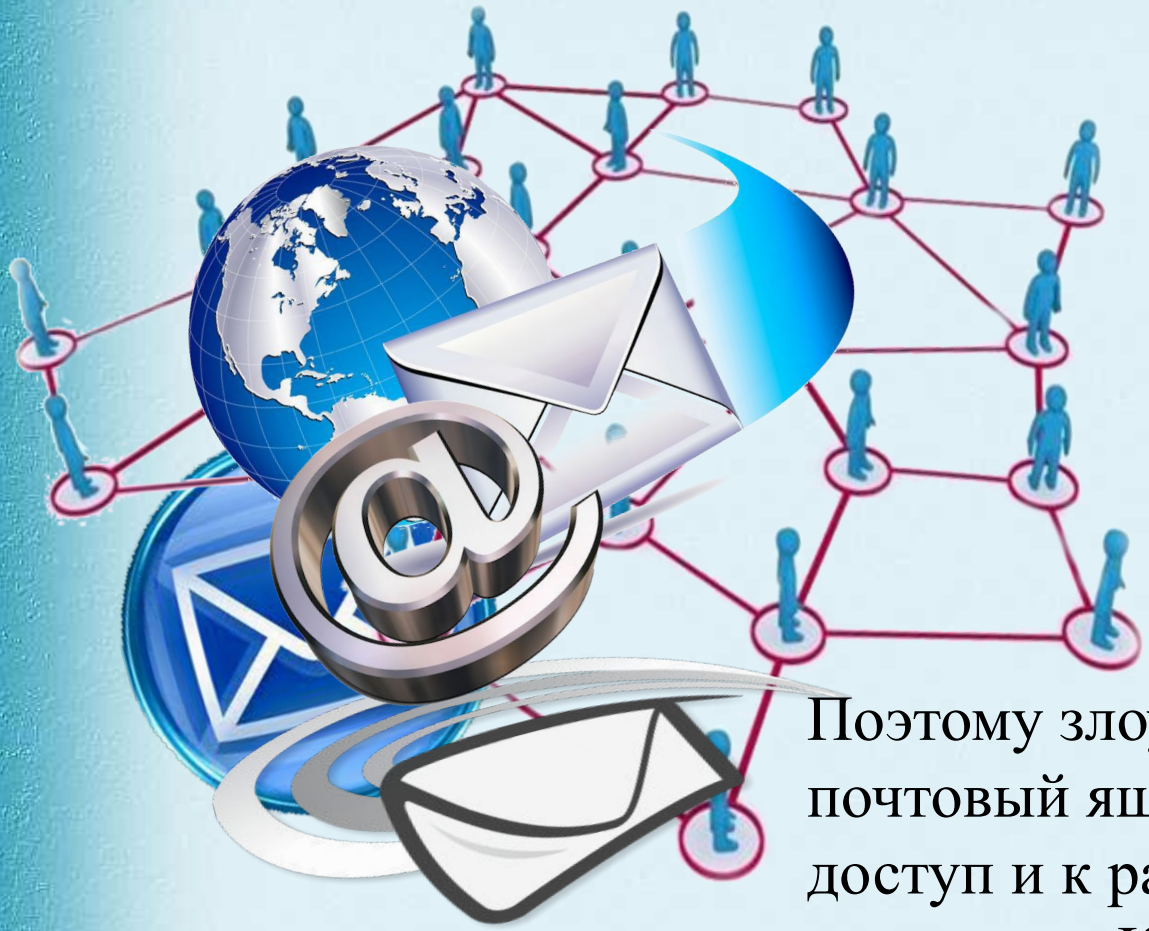
Постановления Правительства РФ от 06.07.2008 № 512; от 15.09.2008 № 687; от 01.11.2012 № 1119.

Методические материалы Роскомнадзора «Об утверждении требований и методов по обезличиванию персональных данных», «Об утверждении требований и методов по обезличиванию персональных данных».

Угрозы в сети Интернет

- электронная почта
- аккаунты в игровых сервисах
- социальные сети и мессенджеры
- цифровая кража смартфона
- мобильные приложения и игры
- банковские данные
- незащищённая Wi-Fi-точка

Электронная почта



Электронная почта является не только услугой, но и средством для регистрации на различных сайтах и сервисах.

Поэтому злоумышленник взломав ваш почтовый ящик, может легко получить доступ и к различным вашим аккаунтам. Кроме того, ваша личная переписка может стать обнародованной.

Аккаунты в игровых сервисах

Множество людей играют в сетевые игры, такие как World of Tanks, DOTA 2, Counter Strike: Global Offensive, FIFA и другие. Пользователи зарабатывают баллы, благодаря чему, выстраивается рейтинг, за реальные деньги приобретают экипировку, оружие, внутриигровую валюту.

Взломанный аккаунт опасен кражей купленных лицензионных игр, игрового инвентаря и предметов, которые мошенник затем продаёт за реальные деньги.

Социальные сети и мессенджеры

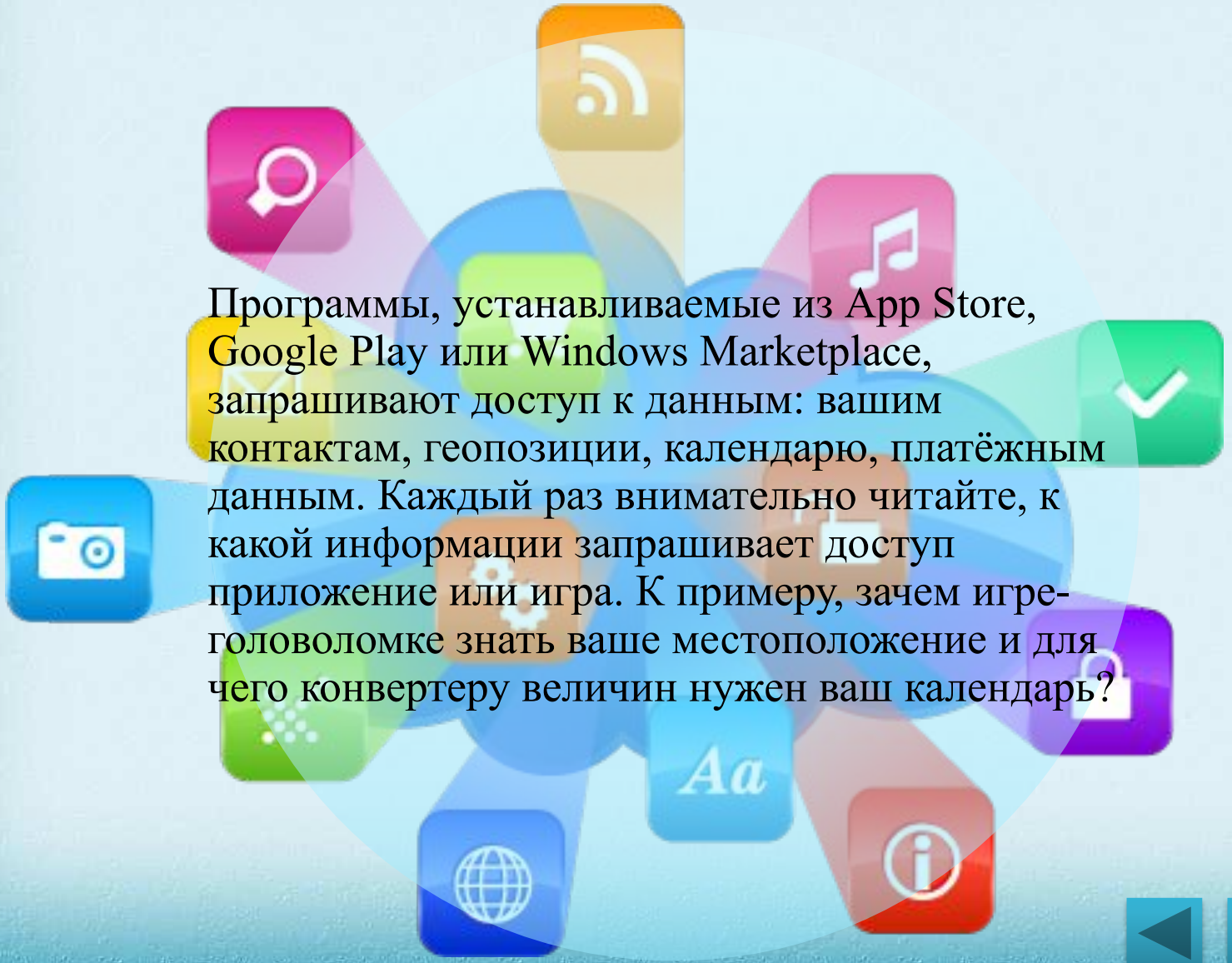
Социальные сети и мессенджеры привлекают злоумышленников подробностями вашей личной жизни. И если у вас есть «скелеты» мошенники не прочь шантажировать вас.

Кроме того, ваши личные фотографии могут быть использованы для корыстных целей.

Цифровая кража смартфона

Все современные сматфоны имеют основную учетную запись: для iOS это Apple ID, для Android — аккаунт Google. Если злоумышленники получат к ним доступ, ценная информация о вас и вашем смартфоне окажется в их руках.

Мобильные приложения и игры

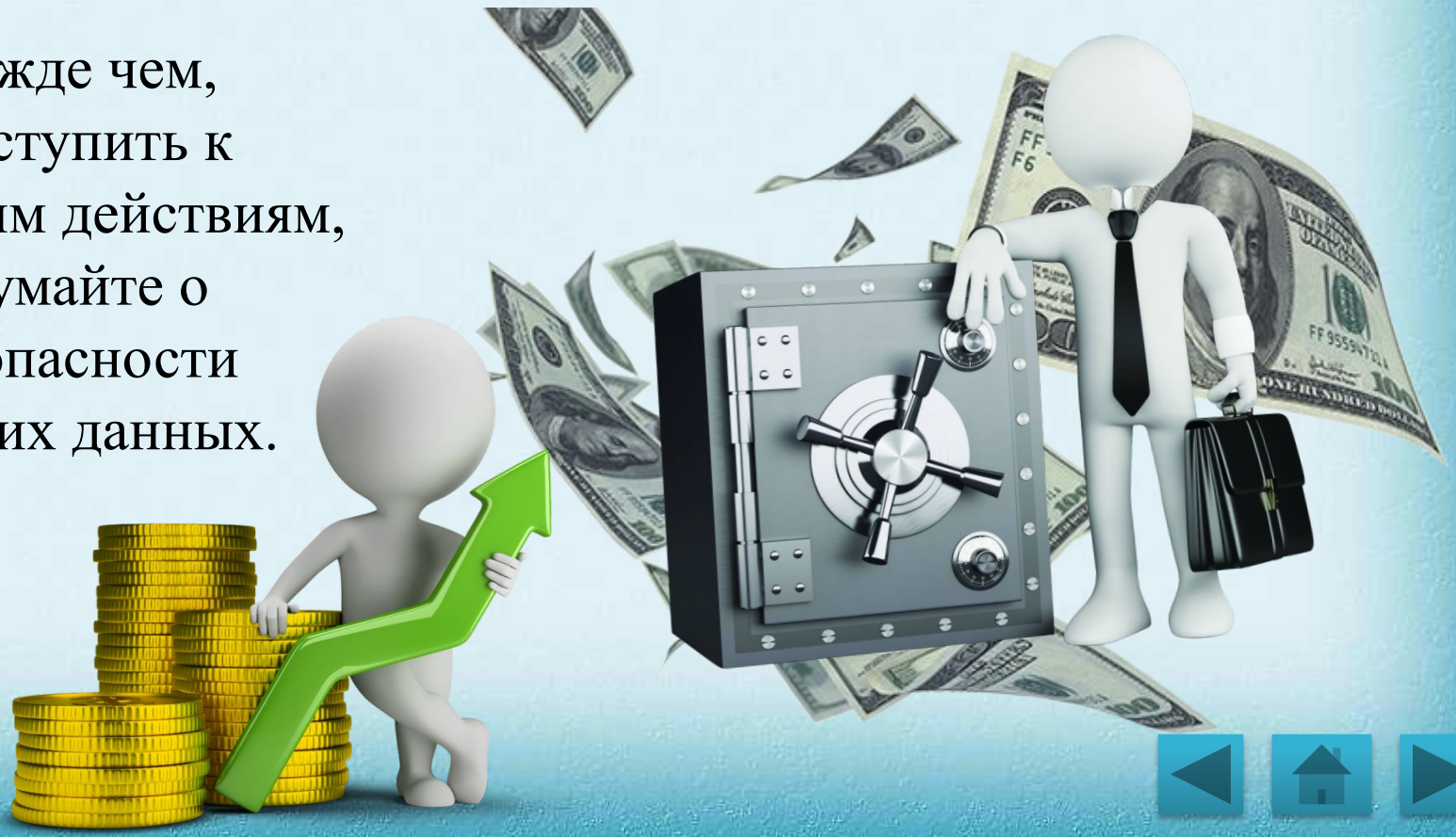


Программы, устанавливаемые из App Store, Google Play или Windows Marketplace, запрашивают доступ к данным: вашим контактам, геопозиции, календарю, платёжным данным. Каждый раз внимательно читайте, к какой информации запрашивает доступ приложение или игра. К примеру, зачем игре-головоломке знать ваше местоположение и для чего конвертеру величин нужен ваш календарь?

Банковские данные

Множество людей оплачивает коммунальные услуги, делает покупки, приобретает авиа-, железнодорожные билеты через интернет-банки и он-лайн сервисы.

Прежде чем, приступить к таким действиям, подумайте о безопасности ваших данных.



Незащищённая Wi-Fi-точка

Хакеры пользуются незащищённостью открытых точек доступа и неосторожностью пользователей. Кроме того, злоумышленники могут получить доступ и к запаролленным точкам. Подключившись к Wi-Fi они видят всё, что вы делаете на экране и вводите на клавиатуре.

Как защитить личные данные в сети?

Включите двухфакторную авторизацию на всех сайтах и сервисах.

Пользуйтесь VPN, работая с открытыми Wi-Fi-точками.

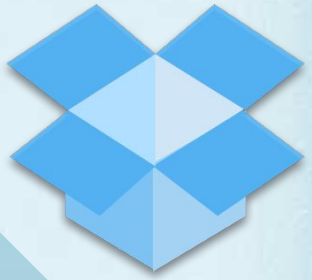
Работайте с защищённым соединением или пользуйтесь программами для шифрования трафика.

Следите, как мобильные приложения используют личные данные.

Используйте менеджеры паролей. Не меняйте пароль слишком часто.

Двухфакторная аутентификация (двойная защита):

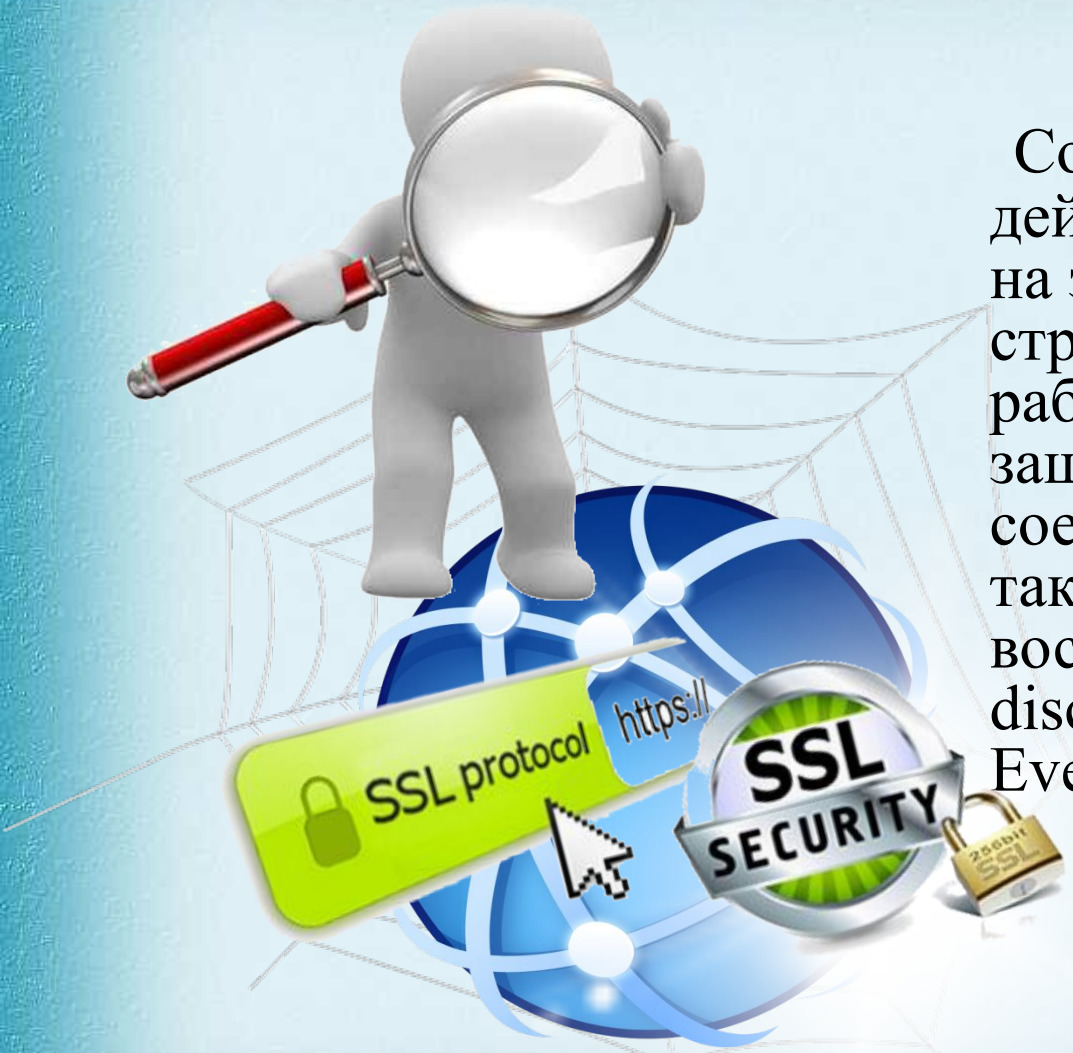
вход в аккаунт с помощью логина и пароля



подтверждение входа, например с помощью смс-сообщения

Сервисы поддерживающие двухфакторную аутентификацию: Google, Apple, Microsoft, Facebook, «ВКонтакте», Dropbox, Telegram и др.

Защищённое соединение



Совершая покупки и другие действия, обратите внимание на значок слева от адресной строки. Убедитесь, что работаете с сайтом по зашифрованному соединению https. Если нет такой возможности, воспользуйтесь сервисами disconnect.me и HTTPS Everywhere.

Менеджеры паролей

Даже, если вы придумаете сложный пароль, велика вероятность его забыть или если он записан, то велика вероятность доступа к нему третьих лиц.

Существуют специальные менеджеры паролей, которые хранят их в защищенном хранилище.

Доступ приложений к данным

Пользователи iOS, Android, могут управлять доступом приложений к различным данным. Если какие-то запросы на доступ вызывают подозрение — отключайте.

Пользуйтесь VPN, работая с публичными Wi-Fi-точками

Выходя в сеть с помощью открытого wi-fi, воспользуйтесь VPN-сервисом, который перенаправит трафик на собственный сервер, а вам отдаст тот, который не могут отслеживать злоумышленники.

Береги свои персональные данные