Управление Роскомнадзора по Ростовской области

РКН

Новые формы угроз безопасности в пространстве современных цифровых технологий и пути решения проблемы

Зотова Ольга Григорьевна
Главный специалист – эксперт
отдела по защите прав субъектов персональных данных

Понятие персональных данных



Персональные данные – любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

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

Значительный объем персональных данных в интернете содержат:

- ✓ **Видеохостинги**
- ✓ **Игровые серверы**
- ✓ **Блоги**

Наибольший объем персональных данных содержат **социальные сети:**



veoh
Dailymotion
RuTube
Всё видео
vimeo
YouTube
GUILD WARS 2
WORLD of WARCRAFT
WORLD of TANKS
LINEAGE II
AION
LiVEJOURNAL

Угроза конфиденциальности пароля аккаунта

Нарушение конфиденциальности влечет:

- взлом профилей
- кража персональных данных
- мошенничество и обман в сети
- кибербуллинг



Примерно у **трети** пользователей установлен свободный доступ к общей информации (она может включать в себя такие сведения, как **возраст, учебное заведение, интересы, хобби и т.д.**), **каждый шестой** ребенок открывает косвенную контактную информацию (**ссылку на свой сайт, скайп, аккаунты в других социальных сетях и т.д.**).



Пути решения угроз в СОЦИАЛЬНЫХ СЕТЯХ при обработке персональных данных

Социальная сеть - это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями



Огранить список друзей. В друзьях не должно быть случайных и незнакомых людей

Не передавать пароли в адрес третьих лиц, не указывать: телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как пользователи проводят отпуска, выходные, каникулы

Необходимо защитить репутацию – перед размещением задавать себе вопрос: хотел бы я, чтобы другие пользователи видели, что я загружаю?

Пути решения угроз в СОЦИАЛЬНЫХ СЕТЯХ при обработке персональных данных

Социальная сеть - это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями



При общении с людьми, которых пользователь не знает, ему не рекомендуется использовать свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее

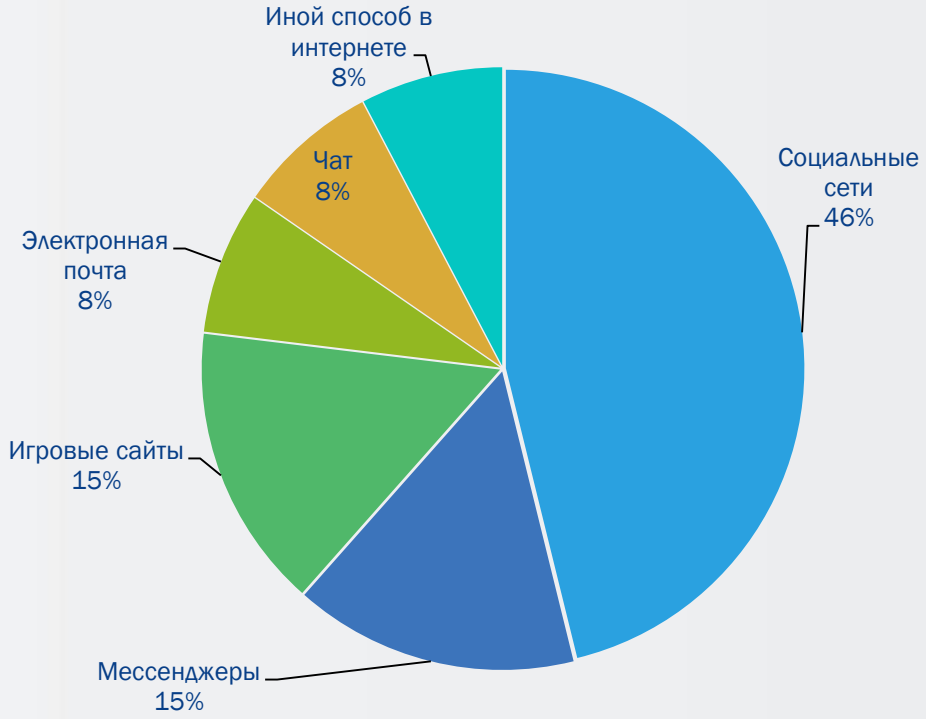
Необходимо избегать размещения фотографий в Интернете, где пользователь изображен на местности, по которой можно определить его местоположение

При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8

Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если пользователя взломают, то злоумышленники получат доступ только к одному месту, а не ко всем сразу

Угроза Кибербулинга при размещении персональных данных в **социальных сетях**

- Санкт-Петербург и Ростов-на-Дону – лидеры по кибербуллингу в России
- Жертвой буллинга становится **каждый 6-й пользователь социальной сети (14%)**



Что делать:

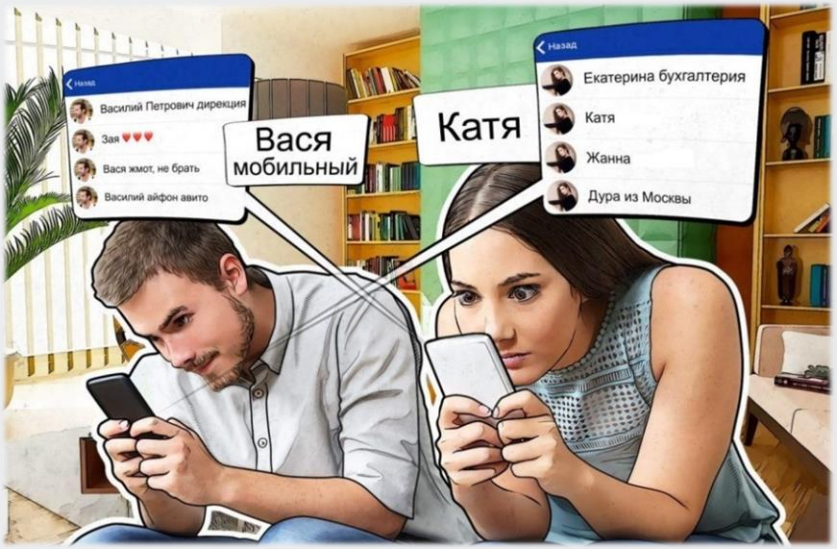
- Обратиться в компетентные органы
- Сохранять доказательства (снимки экранов, с датой и временем сообщений, аудио и видео информацию при наличии)
- Настроить приватность страниц

Угроза Интернет сервисов **(например GetContact)**

Пользователь предоставляет доступ **ко всем** своим данным и данным третьих лиц



- Контакты
- E-mail
- Аккаунты соцсетей
- Записи разговоров
- Фото
- Ip адреса



Угрозы сбора персональных данных с использованием КОМПЬЮТЕРНЫХ ВИРУСОВ и пути их решения

Компьютерный вирус - разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию).
В дополнение к этому, вирусы могут повредить, скопировать, предоставить доступ к персональным данным или полностью уничтожить все файлы и персональные данные. А также повредить или даже уничтожить операционную систему со всеми файлами в целом.



Использовать современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ

Постоянно устанавливать патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления операционной системы. Скачивать приложения только с официального сайта разработчика ОС.

Работать на компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на персональном компьютере.

Угрозы сбора персональных данных с использованием КОМПЬЮТЕРНЫХ ВИРУСОВ и пути их решения

Методы защиты от вредоносных программ



- Использовать антивирусные программные продукты известных производителей, с автоматическим обновлением баз
- Ограничить физический доступ к компьютеру для посторонних лиц
- Использовать внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников
- Не открывать компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые присылают знакомые.

Угроза безопасности ПД при ИСПОЛЬЗОВАНИИ СЕТЕЙ WI-FI

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Это является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.



Не передавать свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-либо номера телефонов

- Использовать и обновлять антивирусные программы и брандмауэр.

- Не использовать публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту

Использовать только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводить именно «https://»

- В мобильном телефоне отключить функцию «Подключение к Wi-Fi автоматически». Не допускать автоматического подключения

Угроза ФИШИНГА ИЛИ КРАЖА персональных данных и пути решения

Главная цель фишинг - вида Интернет-мошенничества, состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль)



Следить за своим аккаунтом. Если есть подозрение, что страница была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее

Использовать безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем

Использовать сложные и разные пароли. Таким образом, если будет осуществлен взлом, то злоумышленники получат доступ только к одному профилю в сети, а не ко всем

ФИШИНГ ИЛИ КРАЖА ЛИЧНЫХ ДАННЫХ



Если осуществлен взлом страницы, то необходимо предупредить всех своих знакомых, которые добавлены в друзьях, о взломе личной страницы так как , возможно, от Вашего имени будет рассылаться спам и ссылки на фишинговые сайты

Установить надежный пароль (PIN) на мобильный телефон

Отключить сохранение паролей в браузере

Не открывать файлы и другие вложения в письмах даже если они пришли от друзей. Лучше уточни у них, отправляли ли они тебе эти файлы

Спасибо за внимание!

РКН

(863) 285-08-67
61.роскомнадзор.рф
61.rkn.gov.ru