Интеграл

Всероссийская видеоконференция «Вместе за семейный интернет: роль и возможности библиотек» 12 февраля

Кибербезопасность: как защитить персональные данные в интернете

Интеграл

Личные данные — это любая информация, которая может прямо или косвенно идентифицировать вас как конкретного человека. К персональным данным относятся не только очевидные сведения вроде имени, фамилии, адреса или номера телефона, но и гораздо больший объём информации.

Основные идентификаторы. Имя, фамилия, отчество, дата и место рождения, номера документов (паспорт, студенческий билет), адрес проживания и регистрации.

- **Контактная информация**. Номера телефонов, адреса электронной почты, аккаунты в социальных сетях, никнеймы в играх и на форумах.
- **Биометрические данные**. Отпечатки пальцев, сканы сетчатки глаза, голос, фотографии лица, генетическая информация.
- **Цифровые следы**. IP-адреса, данные о геолокации, история посещения сайтов, поисковые запросы, покупки в интернет-магазинах, переписка в мессенджерах.
- **Финансовая информация**. Номера банковских карт, счетов, данные о доходах, кредитная история.
- **Медицинские данные**. Результаты анализов, диагнозы, информация о принимаемых лекарствах, данные фитнес-трекеров о физической активности.

Важно понимать, что даже комбинация безобидных данных может раскрыть вашу личность.

Интеграл

Кто и зачем собирает данные о вас?

Сбором пользовательских данных занимаются не только злоумышленники, но и легальные маркетинговые структуры. Их цель — точечная реклама, основанная на ваших интересах. Зачем рекламировать продукт миллионам людей, если можно предложить его только тому, кто уже интересовался им?

Наиболее распространённые инструменты — **Google Analytics, Яндекс.Метрика, Adobe Analytics** и другие системы аналитики. Они отслеживают:

- что вы ищете;
- какие сайты посещаете;
- как долго остаетесь на страницах;
- на какие элементы кликаете;
- как перемещаете курсор мыши;
- какие действия совершаете (комментарии, лайки и прочее).

Собранная информация часто не содержит имени или e-mail, но в умелых руках из набора анонимных данных можно воссоздать полный психологический портрет пользователя: пол, возраст, уровень дохода, политические взгляды, состояние здоровья и даже место проживания.

Интеграл

Как работают технологии слежения?

1. Cookie-файлы (куки)
Cookie — небольшие фрагменты текста, сохраняемые в браузере. Они могут быть полезными — например, для сохранения логина или содержимого корзины.

2. Веб-маяки и пиксели
Невидимые изображения или скрипты, встроенные в сайты и электронные письма.

3. Цифровые отпечатки браузера
Даже без cookies сайты получают данные о вашем устройстве: язык системы, тип браузера, операционная система, список плагинов, шрифты и даже уровень заряда батареи.

4. Слежка через мобильные устройства
Мобильные телефоны стали полноценными источниками персональных данных. На смартфоне установлены десятки приложений с доступом к:

- геолокации (GPS, Wi-Fi, сотовые вышки);
- камере и микрофону;
- контактам и журналам звонков;
- датчикам движения и ориентации (акселерометр, гироскоп);
- Bluetooth и ближайшим устройствам.

Даже если приложение не активно, оно может отправлять данные на свои серверы в фоновом режиме.

Интеграл

Чем грозит утечка данных?

- **Брокеры данных.** Идеально подобранная реклама — результат работы брокеров данных, которые тщательно просмотрели всю доступную информацию о вас и продали эти данные компаниям.
- **Финансовое мошенничество.** Злоумышленники могут снять деньги с банковских карт, совершить покупки в интернет-магазинах.
- **Кража личности и личных данных.** Украденные персональные данные могут использоваться в самых разных целях: для создания поддельных документов, регистрации на различных сервисах, получения государственных услуг, оформление кредитной карты, попытки мошенника выдать себя за жертву, шантажировать знакомых и самой жертвы для обратного выкупа. Серьёзные юридические проблемы.
- **Шантаж и вымогательство.** Личная переписка, фотографии, информация о ваших привычках и предпочтениях может быть использована для психологического давления и требований денег.
- **Физическая опасность**. Данные о местоположении, распорядке дня, финансовом положении могут быть использованы для планирования преступлений против вас или членов вашей семьи.

Интеграл

Самая желанная цель злоумышленника — это реквизиты банковской карты.
Как правило, мошенники используют стандартные схемы для похищения информации.

Способ	Уязвимость
Взлом аккаунта	Ненадежный пароль — это самый простой путь к утечке, так как существуют специальные программы, способные подобрать комбинацию методом перебора. Чем меньше в пароле символов, чем они однообразнее, тем быстрее злоумышленники получат доступ к данным.
Фишинговая ссылка	Преступники копируют целые сайты или отдельные страницы, чтобы украсть реквизиты банковской карты. Посетитель думает, что оплачивает заказ в интернет-магазине, но по факту он отдает данные карты прямиком мошенникам.
Незащищенные страницы	Если в адресной строке в браузере нет символа с замочком, на этом сайте не действует защита. Любая внесенная информация может быть легко похищена.
Обман и вымогательство	Для кражи информации или денег мошенники прибегают к обману. Например, представляются сотрудниками банка или сообщают о трагедии в семье.

Интеграл

Способы защиты личных данных в Интернете:

1. Сложные пароли.
2. Подключите двухфакторную аутентификацию в соцсетях.
3. Не переходите по подозрительным ссылкам, используйте сайты только с защищенным соединением (с замочком в адресной строке).
4. Используйте разные почтовые ящики для личной переписки и для регистрации в интернет-магазинах.
5. Используйте последнюю модель антивируса, чтобы проверять ПК на уязвимости.
6. Очищайте куки в настройках браузера время от времени.
7. В целях безопасности минимизируйте информацию о себе в открытых ресурсах.
8. Осторожное использование открытых WI-FI сетей.
9. Обезопасьте свой гаджет и компьютер.
10. Защитите себя от слежки.
11. Настройки браузера.
12. Не скачивайте файлы на ненадежных сайтах.
13. Установка лицензионного программного обеспечения.
14. Выключайте компьютер.

Интеграл

Главное!!!

- Чтобы личные данные оставались личными, не пренебрегайте основными правилами безопасности, которые используете и вне интернета. Закрывайте доступ к своим постам и фотографиям, как закрываете дверь в квартиру. Внимательно читайте условия конфиденциальности, как и любой другой документ.
- Не стоит также уповать на то, что никому ваша жизнь не интересна и вообще денег и особняков у вас нет. Часто наши персональные данные нужны мошенникам не меньше, чем банковский счет и недвижимость.
- Главное в интернете — сохранять бдительность.

Интеграл

Что делать, если личные данные все же украли?

- **Если вы обнаружили в интернете свои логины и пароли, в первую очередь необходимо сменить их.**
- **В случае попадания в сеть данных банковской карты нужно оперативно заблокировать ее.**
- **Если в открытом доступе оказалось ваше имя или номер телефона, необходимо связаться с администрацией ресурса, на котором они опубликованы, или владельцем ресурса, разместившего ваши данные. (Ссылайтесь в подобных ситуациях на нормы Федерального закона № 152-ФЗ «О персональных данных».)**
- **Если ваши данные появляются в результатах выдачи, обратитесь в техподдержку поисковика или заполните специальную форму «Сообщить о нарушении». Такая есть, например, у «Яндекса» и Google.**
- **Если вы не знаете, кто распространяет ваши персональные данные, не можете связаться с нарушителем или получили отказ на просьбу удалить информацию о вас из сети, обратитесь в прокуратуру или Роскомнадзор.**

Интеграл

Согласие на обработку ПДн: новые требования с 1 сентября 2025 года

- В России действует Федеральный закон № 152-ФЗ «О персональных данных». Согласно ст. 3 Закона № 152-ФЗ под персональными данными следует понимать любую информацию, которая прямо или косвенно относится к определенному или определяемому физическому лицу (субъекту персональных данных).
- Обновленная статья 9 №152-ФЗ фиксирует, что документ должен быть действительно добровольным и осознанным — с понятной формулировкой. Согласие должно быть оформлено отдельно. Распространенная практика включения согласия в договор, оферту или заявление теперь не допускается. Это должен быть самостоятельный документ, не объединенный ни с какими другими.

Запрещены заранее проставленные галочки. Пользователь должен самостоятельно поставить отметку, подтверждающую согласие. В документе нужно четко указать:

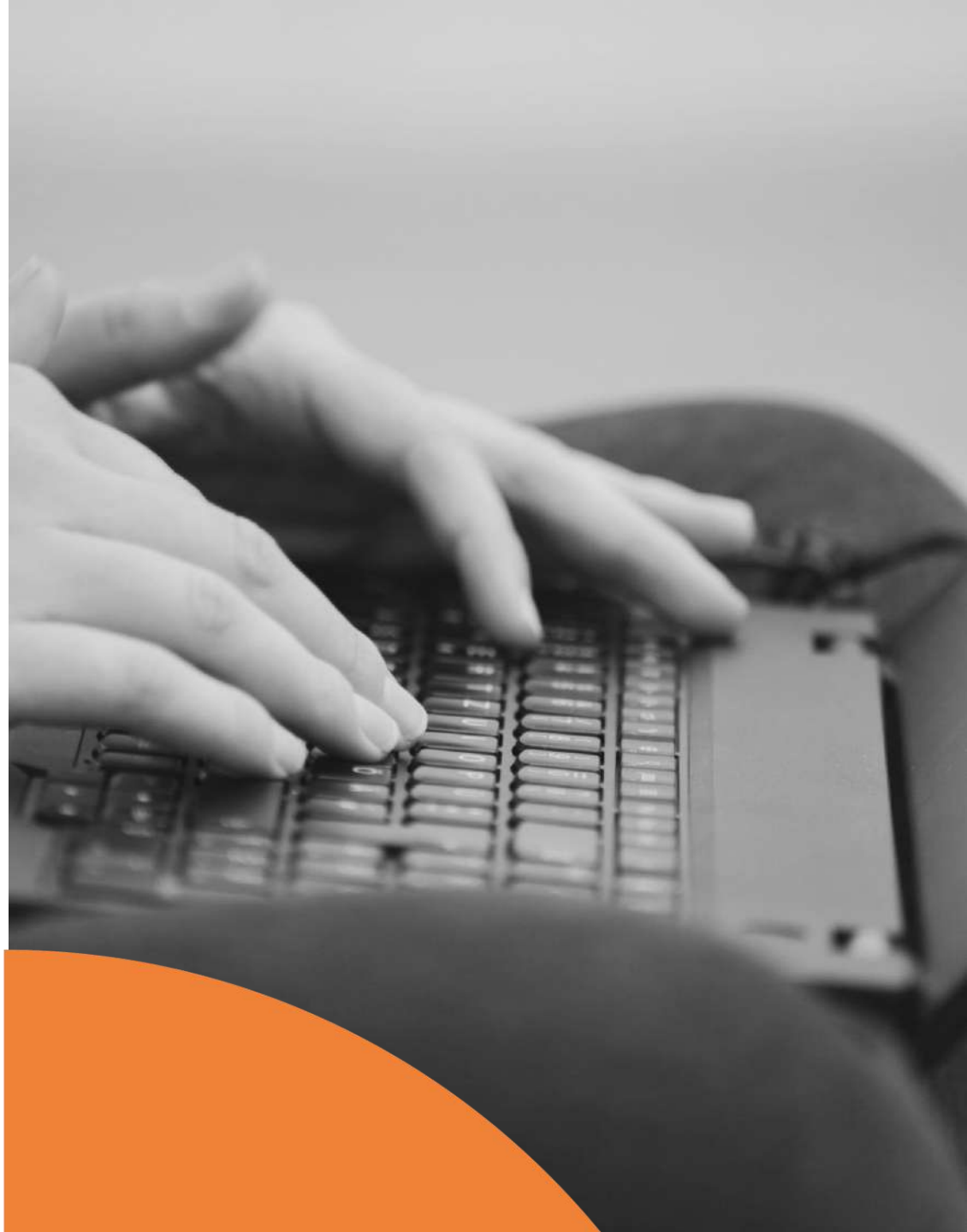
- Цель обработки.
- Конкретный список обрабатываемых сведений.
- Перечень организаций и партнеров, которые получат доступ к информации.
- Подробное описание операций с данными.
- Период действия документа и понятная процедура отмены.

Организациям запрещено использовать «скрытые» или обезличенные согласия.

Интеграл

Заключение

Защита персональных данных при использовании онлайн-сервисов требует комплексного подхода, включающего в себя как технические, так и организационные меры. Следование рекомендациям и использование современных средств защиты поможет существенно снизить риск компрометации данных и защитить вашу конфиденциальную информацию. Помните, что защита данных – это непрерывный процесс, требующий постоянного внимания и обновления знаний.



Интеграл

Спасибо за внимание!