# Методы защиты пользовательских данных в социальной сети «ВКонтакте»

**Елюбаева К.С. , ЮР-418, 2 курс, СПО**

**научные руководители Мальгин Е.Л., к.п.н., доцент, Шеметова Е.Г., к.т.н., доцент**

**Сибирский университет потребительской кооперации, г. Новосибирск**

**Цель**:

•Предоставление методов защиты пользовательских данных социальной сети **«ВКонтакте»** и анализ основных угроз безопасности в **«ВКонтакте».**

•Выявление проблемных аспектов и рисков для пользователей.

**Задачи:**

•Проанализировать основные угрозы безопасности в социальной сети **«ВКонтакте».**

•Ознакомиться с методами защиты пользовательских данных в социальной сети.

•Подвести итог.

**Актуальность**:

Необходимость защиты личной информации пользователей социальных сетей в условиях увеличения числа киберугроз и кибератак.

## История возникновения социальной сети «ВКонтакте»

Создателем «ВКонтакте» считается Павел Дуров. Идея сайта для переписок, который бы работал по всему миру, появилась после того, как он понял, насколько сложно ему поддерживать связь с друзьями, которые живут далеко.

В 2008 году, менее чем через полтора года с момента запуска, «Вконтакте» становится самым популярным интернет-ресурсом в России.

## Как не попасться на мошенничество?

**1. Друг, выручи деньгами!**

Если Вам поступило подобное сообщение, следует прежде всего позвонить другу на мобильный номер и узнать правда ли нужна такая помощь. Если это не так, сообщить о взломе его аккаунта.

**2. Опросы, тесты и конкурсы**

Не открывайте подозрительные ссылки от своих друзей и знакомых, прежде наберите по обычной связи своему товарищу и спросите, что за ссылка. Если он опровергает отправление сообщения, значит ссылку отправил мошенник, которая может нести в себе большую опасность

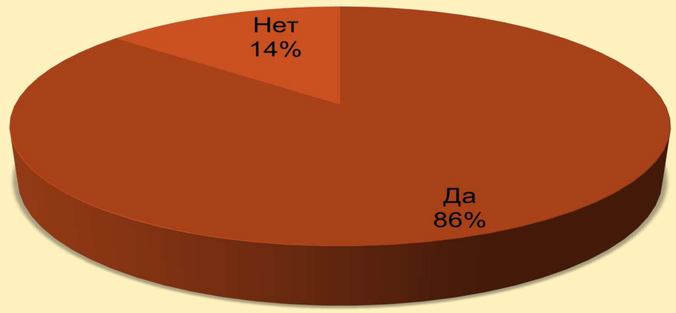
**3. Вымогание денег, угрозы о продаже или организации утечки ваших личных данных**

Вам стоит не вестись на провокации, следует отказаться от оплаты, а также обратиться с заявлением в правоохранительные органы. Заявление Вы можете подать через официальный сайт МВД.

**4. Взлом аккаунта**

При взломе аккаунта поменяйте пароль от страницы. Желательно также сменить пароль от почтового ящика, который был привязан к аккаунту.

**Сталкивались ли студенты СибУПК с мошенничеством в социальной сети "ВКонтакте"**




**Вывод:**

Основные угрозы включают в себя **утечку личной информации, фишинг, мошенничество и кибербуллинг.**

Для обеспечения безопасности необходимо принимать меры, такие как использование **надежных паролей, ограничение доступа к личной информации и осознанное поведение в сети.**

Соблюдение этих рекомендаций поможет защитить личные данные и сохранить безопасность в социальных сетях.

## Методы защиты пользователей в социальных сетях:

***Пароли:*** Используйте сложные, уникальные пароли для каждого аккаунта и регулярно меняйте их.

***Двухфакторная аутентификация:*** Включите её для дополнительной защиты.

***Личная информация:*** Ограничьте доступ к ней, не публикуйте конфиденциальные данные.

***Запросы в друзья*:** Отклоняйте запросы от незнакомцев и подозрительных аккаунтов.

***Настройки приватности*:** Регулярно проверяйте и настраивайте их, чтобы контролировать видимость ваших данных.

***Ссылки и файлы*:** Не переходите по подозрительным ссылкам и не загружайте файлы из ненадежных источников.

**Социальные сети — удобная платформа для общения и обмена информацией, но они также источник угроз информационной безопасности:**

***Фишинг:***
выманивание личных данных под видом официального запроса.

***Вредоносные программы:***
внедрение вредоносного ПО в систему.

***Нарушение конфиденциальности*:**
публикация личных данных (фото, адреса, телефоны).

***Кибербуллинг:***
оскорбления, угрозы, шантаж онлайн.

***Социальная инженерия*:**
манипулирование людьми для получения доступа к информации.