

ВУЗ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему:

«Информационная безопасность личности в условиях сетевой коммуникации (на примере соц.сетей Вконтакте, Facebook, Instagram)»

Выполнил:

Научный руководитель:

Цель и задачи исследования

Цель исследования - изучить способы обеспечения информационной безопасности в условиях сетевой коммуникации в социальных сетях.

Задачи:

1. Изучить молодёжную аудиторию социальных сетей и дать им общую характеристику
2. Проанализировать угрозы и способы защиты от них контексте коммуникативных практик молодёжной аудитории социальных сетей
3. Предложить план по обеспечению комплексной защиты личности от информационных угроз, а также выявить основные способы защиты от информационных угроз в сетевой коммуникации.

Исследование Brand Analytics по количеству пользователей-авторов социальных сетей и количеству опубликованного контента

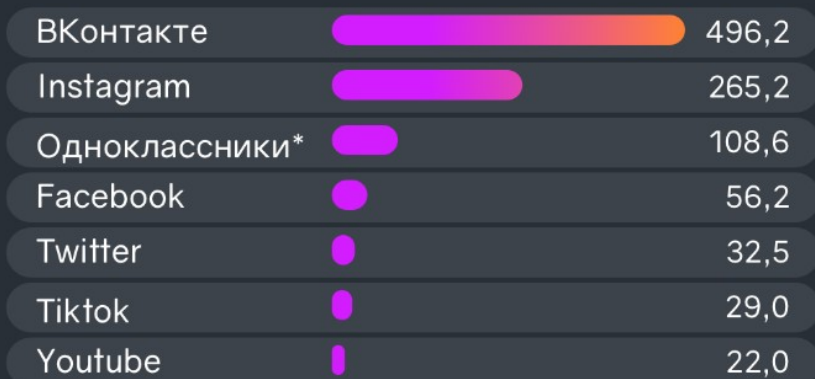


Социальные медиа в России

Сообщений в месяц

1,2 млрд

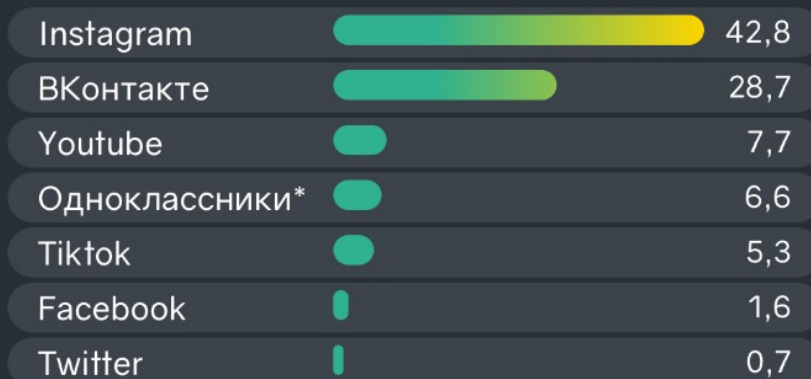
Сообщений в месяц, млн.



Авторов в месяц

64 млн

Авторов в месяц, млн.



Основные термины исследования

Автор – пользователь, написавший хотя бы 1 публичное сообщение за месяц.

Сообщение – любой открытый (публичный) пост, включая комментарии.

Россия, октябрь 2020

Подготовлено Brand Analytics,
системой анализа соцмедиа и СМИ

Instagram, данные по России

Авторов

42 841 400

Возраст

В Instagram данные о возрасте авторов отсутствуют

Сообщений

265 157 600

Пол

 22,9%  77,1%

Россия, октябрь 2020

ВКонтакте, данные по России

Авторов

28 663 700

Сообщений

496 156 200

Пол



45,3%



54,7%

Возраст

(указан у 43,5% авторов)

до 18 лет



15,0%

18-24 лет



20,8%

25-34 лет



30,8%

35-44 лет



19,0%

45-54 лет



7,9%

55 и старше



6,5%

Россия, октябрь 2020

Facebook, данные по России



Авторов

1 587 300

Сообщений

56 176 700

Пол



40,2%



59,8%

Возраст

(указан у 3,3% авторов)

до 18 лет 0,1%

18-24 лет 6,4%

25-34 лет 26,6%

35-44 лет 33,0%

45-54 лет 22,1%

55 и старше 11,6%

Россия, октябрь 2020

Классификация спам-сообщений

коммерческий спам, целью которого является получение какой-либо коммерческой выгоды;

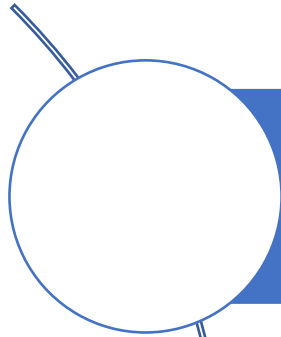
спам для раскрутки ресурса, посредством которого владельцы сайта накручивают трафик и увеличивают посещаемость;

направленный на кражу личных данных или денег, в том числе спам с рассылкой вредоносных программ;
спам для сбора необходимых данных, который маскируется под

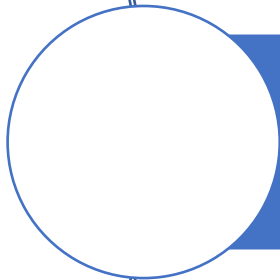
религиозный спам;

«письма счастья» или сообщения, которые с помощью тех или иных методов убеждают пользователя продолжать участвовать в рассылке сообщений

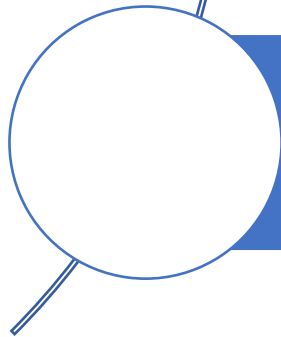
Причины становления жертвой хакера



Злоумышленники действуют на шаг впереди, а сторона защиты в многих случаях должна реагировать на новые вызовы, которые предлагают им хакеры



Пользователи слабо информировано о том, какими возможностями обладают хакеры, также у них нет навыков, которые необходимы для надежной защиты своих собственных данных.



Злоумышленникам проще действовать, видя те механизмы защиты, которые применены в системе. Хакеры подбирают нужные ключи и обладают преимуществом перед слабыми системами

Выводы

В рамках исследования изучены реальные ситуации хакерских нападений на пользователей и связанные с ними судебные прецеденты. В результате анализа представленных кейсов сделаны значимые выводы о необходимости комплексной защиты личности, базирующейся на совокупности технических, психологических, правовых методов и определенном алгоритме действий.

В ходе работы доказано, что разрозненные способы защиты могут не только не привести к необходимому результату, но и повлечь за собой более серьезные негативные последствия для пользователя.

На основании теоретических и практических данных описаны основные элементы комплексной модели защиты, обозначена последовательность действий для обеспечения личной безопасности: идентификация угрозы, описание и анализ особенностей реальной или потенциальной опасности, выбор подходящих методов защиты, разработка плана действий и его реализация. Под идентификацией в рамках данной модели понимается распознавание негативного воздействия техническими и/или психологическими способами. Описание и анализ реальной или потенциальной опасности определены как совокупность процессов соотнесения обнаруженной угрозы с определенной группой на основе классификации, обозначения основных характеристик, источников воздействия, цели атаки, используемых методов, установления количества нападающих злоумышленников и их личностные особенности.

СПАСИБО ЗА ВНИМАНИЕ!