

(СЛАЙД 1) Уважаемый председатель, уважаемые члены государственной аттестационной комиссии! Вашему вниманию предлагается дипломная работа на тему «Информационная безопасность личности в условиях сетевой коммуникации (на примере соц.сетей Вконтакте,Facebook,Instagram)».

(Слайд 2) Цель данной работы - изучить способы обеспечения информационной безопасности в условиях сетевой коммуникации в социальных сетях. Для достижения цели необходимо решение следующих задач.

(Слайд 3) Из анализа рисунка можно сделать вывод о том, что ВКонтакте является самой популярной социальной сетью для авторов контента, хотя проигрывает социальной сети Instagram по количеству пользователей примерно в 1,5 раза. Сама же социальная сеть Instagram является самой популярной социальной сетью в России. Третья социальная сеть, которая будет проанализирована в рамках выпускной квалификационной работы, - Facebook, занимает 4 место, уступая Одноклассникам по количеству создаваемого пользователями контента и предпоследнее место по количеству пользователей, опережая только Twitter. Направленность социальных сетей на молодёжь является ключевой причиной того, почему одни социальные сети популярнее других. Так, например, социальная сеть ВКонтакте, является исторически «молодой», в которой основное количество пользователи представители до 35 лет. Перейдём к более детальному анализу трёх социальных сетей от самой крупной по количеству пользователей-авторов, которые находятся на территории Российской Федерации, до более мелких.

(Слайд 4) Социальная сеть Instagram набирает популярность на территории Российской Федерации, постоянно расширяя количество аудитории. Так, например, в 2019 году социальная сеть насчитывала 27,7 млн пользователей, а за год возросла более, чем на 50% до 42,8 млн публичных авторов на территории РФ. Сравнивая её с социальной сетью ВКонтакте, Instagram ещё пока проигрывает ВКонтакте по количеству контента, который производит аудитория. В Инстаграме показатель публикации на одного автора равен 6,2 публикациям в месяц. В социальной сети ВКонтакте данный показатель превышает в три раза. В общем, за один месяц в социальной сети Instagram производят 265,2 млн публикаций. Однако, социальная сеть не разглашает данные о возрасте аудиторий, что усложняет анализ. Однако,

социальная сеть считается молодёжной, и её главная аудитория является представителю молодёжи.

(Слайд 5) Социальная сеть ВКонтакте исторически считалась «молодёжной» социальной сетью, которая создаёт больше всего контента – почти 500 млн сообщений, постов, комментариев производят авторы платформы в месяц. В отличие от Instagram, ВКонтакте раскрывает информацию о возрастах пользователей, что позволяет проанализировать долю пользователей, которая относится к молодёжи. Поскольку в соответствии с новым Федеральным законом молодёжью считаются граждане до 35 лет, можно сделать вывод, что на платформе ВКонтакте более 66,6% молодёжи. То есть из трёх людей, два точно будут представителями молодого поколения. Также стоит отметить, что из почти 29 млн пользователей аудитория разделилась пополам между мужчинами и женщинами. Мужчин чуть более 45%, а женщин почти 55%. А сами молодые авторы публикуют каждый почти по 17 единиц контента (посты, комментарии и т.д.) в месяц.

(Слайд 6) Социальная сеть Facebook не так популярна на территории Российской Федерации, как её аналог, ВКонтакте. Однако, возраст пользователей также является публичной информацией, что позволяет сделать некоторые выводы. В отличие от молодёжной сети ВКонтакте, Facebook является более возрастной социальной сетью. Всего лишь 33% аудитории являются молодёжью, то есть из трёх человек всего один. Здесь свою роль играет позиционирование социальной сети, как место «для профессионалов», что является непривлекательным для молодой аудитории. По соотношению мужчин и женщин, здесь также выигрывают женщины, опережая мужчин почти на 20%.

(Слайд 7) Все виды информационных угроз, связанных с совокупностью информационнотехнических и информационно-технических способов атаки, можно обозначить таким понятием, как спам. По мнению О.В. Лутовиновой, спамом является анонимная рассылка сообщений пользователям, не дававшим на это согласие и не выражавшим желание ее получить. Автор предлагает собственную классификацию спам-сообщений среди которых: коммерческий спам, целью которого является получение какой-либо коммерческой выгоды; спам для раскрутки ресурса, посредством которого владельцы сайта накручивают трафик и увеличивают посещаемость; мошеннический спам, направленный на кражу личных данных или денег, в том числе спам с рассылкой вредоносных программ;

спам для сбора необходимых данных, который маскируется под вид опросников и анкет; религиозный спам; «письма счастья» или сообщения, которые с помощью тех или иных методов убеждают пользователя продолжать участвовать в рассылке сообщений.

(Слайд 8) Специалисты информационной безопасности компаний, которые занимаются развитием онлайн-платформ и различных ресурсов, регулярно повышают уровень информационной безопасности, блокируют миллионы попыток вторжения. Однако, многие пользователи всё равно становятся жертвами хакеров. Этому есть несколько причин.

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

(Слайд 9) 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..

(Слайд 10) Таким образом, цель работы достигнута. Доклад окончен!