



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
(ШКОЛА)

Департамент информационной безопасности

О Т Ч Е Т

о прохождении научно-исследовательской работы (производственной
практики)

Выполнил студент
гр. С9117-10.05.01 ммзи

Д.С. Левчук
(И.О. Фамилия)

Отчет защищен с оценкой

Руководитель практики
Доцент департамента
информационной безопасности
ИМиКТ

Е.П. Кутикова
(подпись) (И.О. Фамилия)
« 19 » _____ ноября 2022 г.

Е.П. Кутикова
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 19 » _____ ноября 2022 г.

Практика пройдена в срок
с « 07 » _____ ноября 2022 г.
по « 19 » _____ ноября 2022 г.
на предприятии

Е.В. Третьяк
(подпись) (И.О. Фамилия)

ПАО
«Ростелеком»

г. Владивосток
2022 г.

Оглавление

Характеристика.....	2
Дневник студента	3
Введение	4
Текст статьи.....	7
Заключение.....	17
Список используемых источников	18

Характеристика

Выдана студенту 6 курса, специальности «Компьютерная безопасность», специализация «Математические методы защиты информации», Левчуку Денису Сергеевичу

Левчук Денис Сергеевич, в период с 07.11.2022 по 19.11.2022 года, проходил научно-исследовательскую работу (производственную практику) на предприятии ПАО «Ростелеком».

За время прохождения практики Денис проявил усердие, тягу к знаниям, огромное желание и трудолюбие, а также неподдельный интерес к изучению материала. Приходил на консультацию вовремя с перечнем вопросов, с подробным и исчерпывающим описанием о текущем состоянии практики, со списком отмеченных задач. Внимательно изучал предложенные материалы и литературу на интересующую тематику.

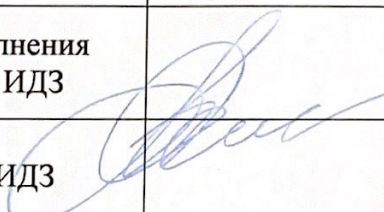
Левчук Д.С. полностью выполнил предусмотренную программу практики, продемонстрировал умения самостоятельно решать практические вопросы, применяя теоретическую базу, полученную в учебный период, а также при самостоятельном обучении.

При выполнении поставленных задач Левчук Д.С. характеризуется инициативностью, сообразительностью и ответственностью.

Директора по работе с массовым
сегментом Макрорегионального
филиала «Дальний Восток»
ПАО «Ростелеком»



Аюшеев Б.В.
подпись Ф.И.О.
М.П. 

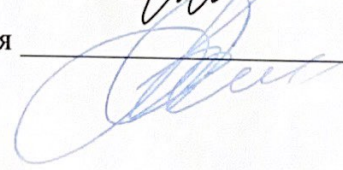
ДНЕВНИК СТУДЕНТА

Дата	Рабочее место	Краткое содержание выполняемых работ	Отметки руководителя
07.11.22 – 07.11.22	ПАО «Ростелеком»	Знакомство с коллегами, прохождение вводных инструктажей по прибытию на предприятие	
08.11.22 – 11.11.22	ПАО «Ростелеком»	Сбор материала для выполнения практических заданий и ИДЗ	
14.11.22 – 16.11.22	ПАО «Ростелеком»	Выполнение заданий и ИДЗ	
17.11.22 – 19.11.22	ПАО «Ростелеком»	Написание отчёта по проделанной работе	

Студент _____

Руководитель практики от предприятия _____

 – Левчук Д.С.
подпись Ф.И.О.

 Аюшеев Б.В.
подпись Ф.И.О.

Введение

С 07.11.2022 по 19.11.2022 проходил производственную практику на предприятии ПАО «Ростелеком». В рамках данной практики мне была предоставлена свобода действий при написании научно-исследовательской работы, приуроченной к моей выпускной квалификационной работе.

Целью данной практики были метаанализ утечек данных в социальных сетях и вынесение рекомендаций по защите данных от них.

Задачами практики являлись:

- Сбор данных для проведения анализа угроз данных социальных сетей;
- Работа с данными по написанию научно-исследовательской работы;
- Написание рекомендаций по сохранению данных пользователей в секретности;
- Публикация научно-исследовательской работы.

Статья получила название «Защита данных в социальных сетях» и была опубликована в журнале «Прикладная информатика» [26]. ВАК: 020306. «Методы и системы защиты информации, информационная безопасность».

Аннотация

Проведен метаанализ угроз безопасности персональных данных пользователей социальных сетей в рамках изучения каналов утечки данных в социальных сетях. Рассмотрены уязвимости интернет-ресурсов, с помощью которых злоумышленники имеют возможность кражи данных с аккаунтов пользователей без разрешения вторых. Были вынесены ряд способов сохранения в секрете и защиты конфиденциальных данных пользователей, представленных в статье.

Annotation

A meta-analysis of threats to the security of personal data of users of social networks was carried out. The research is to study the channels of data leakage in social networks. The vulnerabilities of Internet resources are considered, with the help of which attackers can steal data from user accounts without the permission of the second. Several ways to keep confidential and protect confidential user data presented in the article were made.

Ключевые слова

социальные сети, угрозы персональных данных, конфиденциальность данных, кража данных, рекомендации по защите данных пользователей

Keywords

social networks, threats to personal data, data privacy, data leak, recommendations for user data protection

Текст статьи

«12,5 триллионов часов, проведенных в Интернете, новая веха в распространении Интернета и новые рекорды для социальных сетей» - об этом говорит Саймон Кемп, основатель «Kerios» [8]. Согласно данным ежегодного отчета об интернете и социальных сетях «Digital 2022 Global Overview Report» агентства «We Are Social» [8] 58,4% населения планеты имеет хотя бы один профиль в какой-либо социальной сети. На примере исследования среди студентов Ибадана и Политехнического института Ибадана [9] выяснилось, что с помощью аккаунтов в социальных сетях пользователи делятся с другими как текстовыми, так и фото- аудио- видеоматериалами как в личных сообщениях, так и в новостной ленте, тем самым, не осознавая, предоставляют ей свои персональные данные (ПД) в число которых могут входить такие данные, как ФИО пользователей, их дата рождения, адреса локации, данные документов.

С каждым годом количество случаев кражи персональных данных становится больше. Согласно документу «Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года» [10], представленного экспертно-аналитическим центром InfoWatch по итогам первой половины 2022 года была зарегистрирована 2101 утечка информации ограниченного доступа. Вполне ожидаемо, что на фоне повышения ценности конфиденциальной информации в цифровую эпоху, а также на новом витке кибератак продолжается рост многочисленных взломов как в Рунете, так и в международном пространстве. Становится наиболее актуальным вопрос защиты своих ПД от утечки, в том числе, и в социальных сетях.

Чтобы предпринятые меры по защите ПД решали вопрос сохранения конфиденциальности, пользователю социальной сети нужно понимать от каких угроз их следует защищать. Согласно методическому документу, утвержденному ФСТЭК России от 05.02.2021 г. в список угроз должны быть включены описание ИС, ее характеристики, а также описание угроз безопасности информации.

Следом важно дать краткую характеристику социальной сети, для которой будет составляться список угроз. Объектом исследования возьмем популярную социальную сеть Tik-Tok. Сервера социальной сети физически расположены более чем в 300 разных локациях. В разных случаях защита персональных данных регулируется своими нормативными актами: В Евросоюзе – Общий регламент по защите данных (GDPR), в России – ФЗ № 152 ФЗ «О персональных данных», в Америке - Закон о конфиденциальности электронных сообщений (ЕСРА) и закон о защите конфиденциальности детей в Интернете (COPPA). Приложения для IOS и Андроид написаны на стандартных для данных ОС языках Objective-C, SWIFT, C++, C# и Java. Само же приложение, построенное в формате «клиент-сервер», с возможностью догружать в себя модули в виде обфусцированного кода и держать целые функциональные модули в кеше. Схему работы приложения сами разработчики представили следующим образом (Рисунок 1):

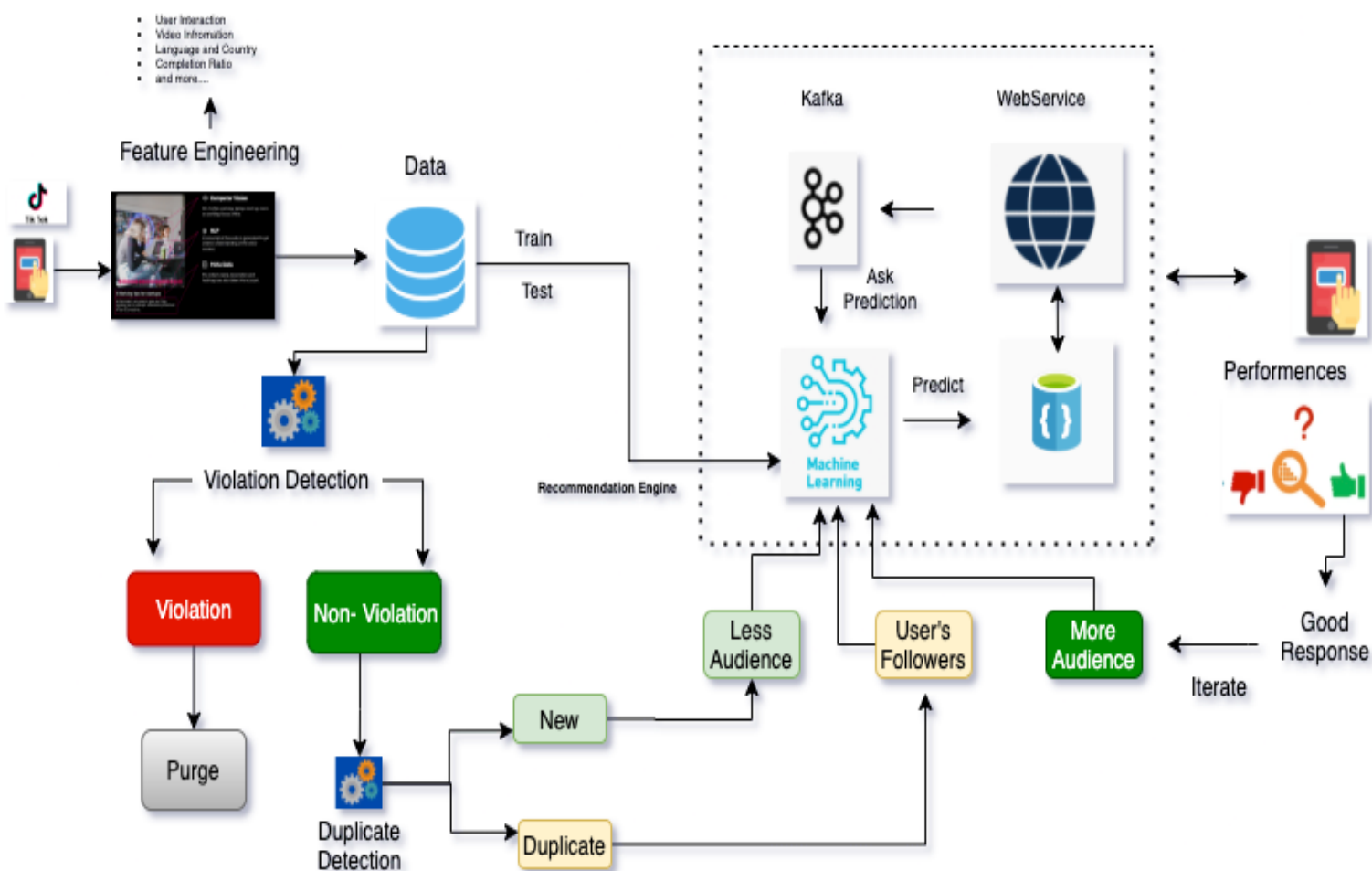


Рисунок 1. Поток контента Tik-Tok [15]

Среди уязвимостей системы, на основании исследования компании Postuf, опубликованном на сайте Habr.com [11], а также на основании отчетов с сайта HackerOne [16], можно выделить следующие примеры:

- SMS-спуфинг;
- Межсайтовый скриптинг;
- Управление аккаунтом пользователя Tik-Tok;
- Обнаружение контента через поисковую строку.

На официальном сайте создателями социальной сети была реализована функция создания SMS, которое будет выступать приглашением к скачиванию и регистрации в приложении. Это может стать причиной SMS-спуфинга. Если немного скорректировать сам URL-адрес, который отправляется в сообщении, то возможно в текст сообщения вписать свой URL-адрес, который будет использован для атаки пользователя.

Домен «ads.tiktok.com» уязвим для атак типа XSS, при которых вредоносные скрипты периодически внедряются в другие безопасные и надежные веб-сайты. Часть уязвимостей ранее была решена [17][18][19], но с постоянным обновлением приложения появляются новые ошибки и уязвимости. В справочном центре, с доменом «https://ads.tiktok.com/help/», содержится информация о создании и публикации объявлений в социальной сети. Здесь также была обнаружена точка внедрения XSS-атаки в функцию поиска. Когда злоумышленник пытается выполнить поиск, на сервер веб-сайта выполняется запрос HTTP GET с параметром q и искомой строкой в качестве значения для поиска.

При управлении аккаунтом пользователя Tik-Tok злоумышленник может управлять аккаунтом пользователя.

Каждое видео имеет свой ID номер. Получив его, можно создать ссылку, конечным результатом которой будет удаление видео из профиля. Пример ссылки:

«api-t.tiktok.com/aweme/v1/aweme/delete/?aweme_id=«ID_видео»

Создается JavaScript запрос, за которым следует HTTP GET запрос на удаление по идентификатору, видео.

Обнаружение контента через поисковую строку дает возможность найти данные пользователей, которые они сами размещают внутри социальной сети. Примером данной угрозы являются отметки электронной почты на видео и фото данных, которые пользователи выкладывают у себя на странице (рисунок 2).

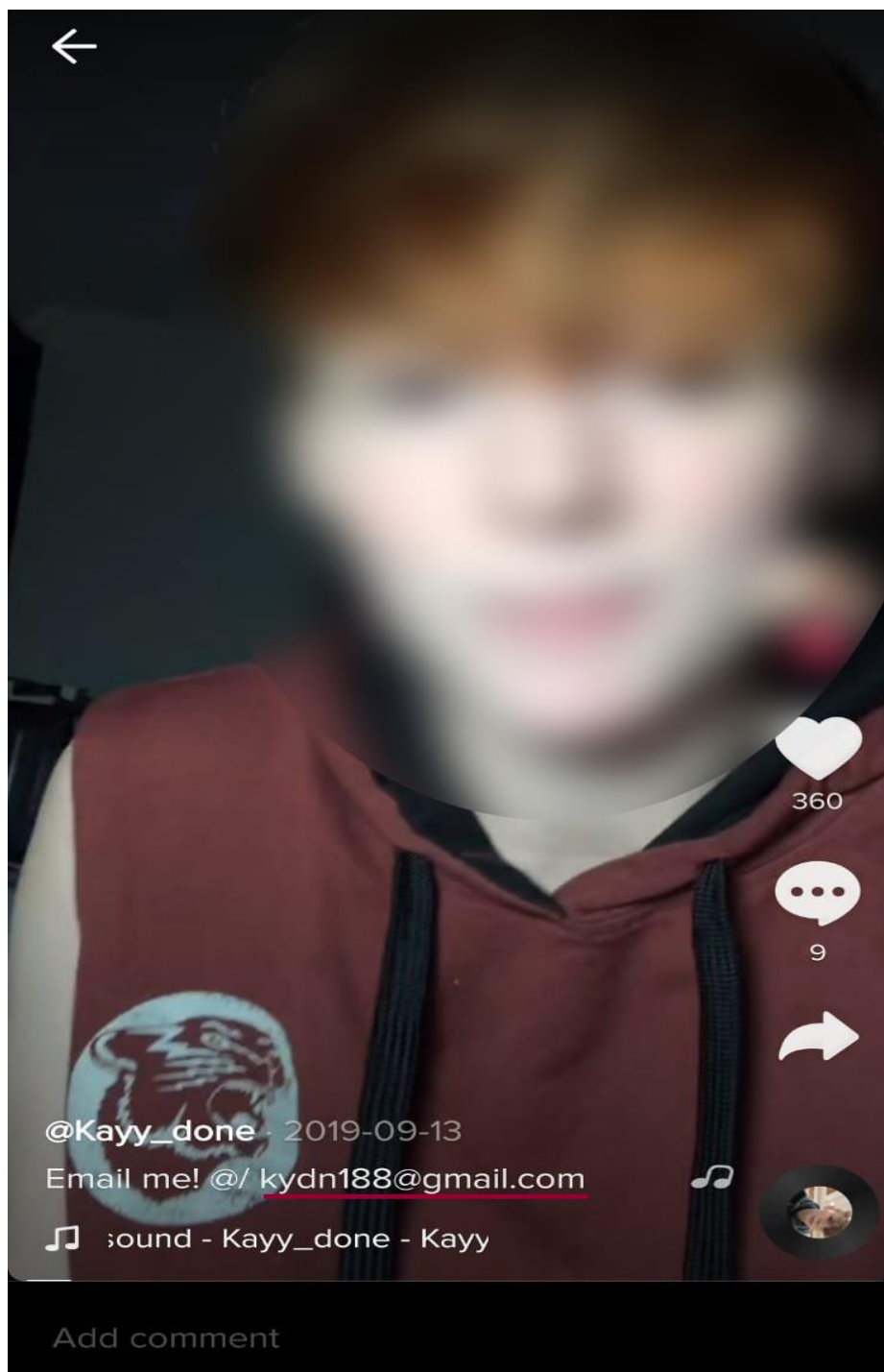


Рисунок 2. Размещение адреса электронной почты в подписи к видео

В данном случае пользователь разместил домен почты под видео, раскрывая свои персональные данные. Участвуя в разного рода «челленджах» пользователи могут раскрыть, сами о том не задумываясь, например, свои номера телефонов, свою геолокацию и прочие данные, которые являются личными и большая часть пользователей желают оставить в секрете. Вследствие этого злоумышленники могут собирать эти данные. Так 6 сентября

2022 года появилась запись в Forbes, в которой указано о краже 2-ух миллиардов записей пользователей социальной сети [12]. В 2014 году актриса Джанна Джеймсон с помощью «челендажда» на платформе 4chan смогла через пользователей найти ее бывшего помощника, который сливал ее данные с социальных сетей [20].

Основываясь на приведенных выше данных, а также дополнительно на отчетах программ по поиску уязвимостей [25] следует, что существует множество способов кражи данных, с учетом временной задержки с момента регистрации уязвимости до фактического её устранения, что дает возможность совершить атаку на архитектуру или отдельных пользователей.

Так как внутри социальной сети данные проходят через пользователя и через систему, созданную разработчиками, следует разделить меры безопасности по сохранению данных на две группы:

- Регулируемые разработчиками социальной сети;
- Регулируемые пользователями сети.

Первая группа представляет собой использование качественных методов шифрования данных пользователей, установки разграничения доступов внутри социальной сети.

Например, в социальной сети Telegram используется протокол шифрования MTProto 2.0 (рисунок 3) [13]. Как отмечал специалист по Криптографии Мэтт Грин [21]: «Telegram имеет 10 миллионов деталей, которые поддерживают единичный неавторизованный обмен ключами по методу Диффи-Хеллмана». Это и создают одну из уязвимостей в работе протокола шифрования, при которой с помощью MITM-атаки, как писали исследователи Х. Сарибекян и А. Маргвелашвили [22] можно выкрасть данные пользователей. Как писали исследователи: «Атака связана с генерированием общих секретов по методу Диффи-Хеллмана для двух жертв, имеющих одинаковый 128-битный визуальный отпечаток, и пользователи, которые сравнивают отпечатки, не смогут обнаружить атаку»

MTProto 2.0, part I

Cloud chats (server-client encryption)

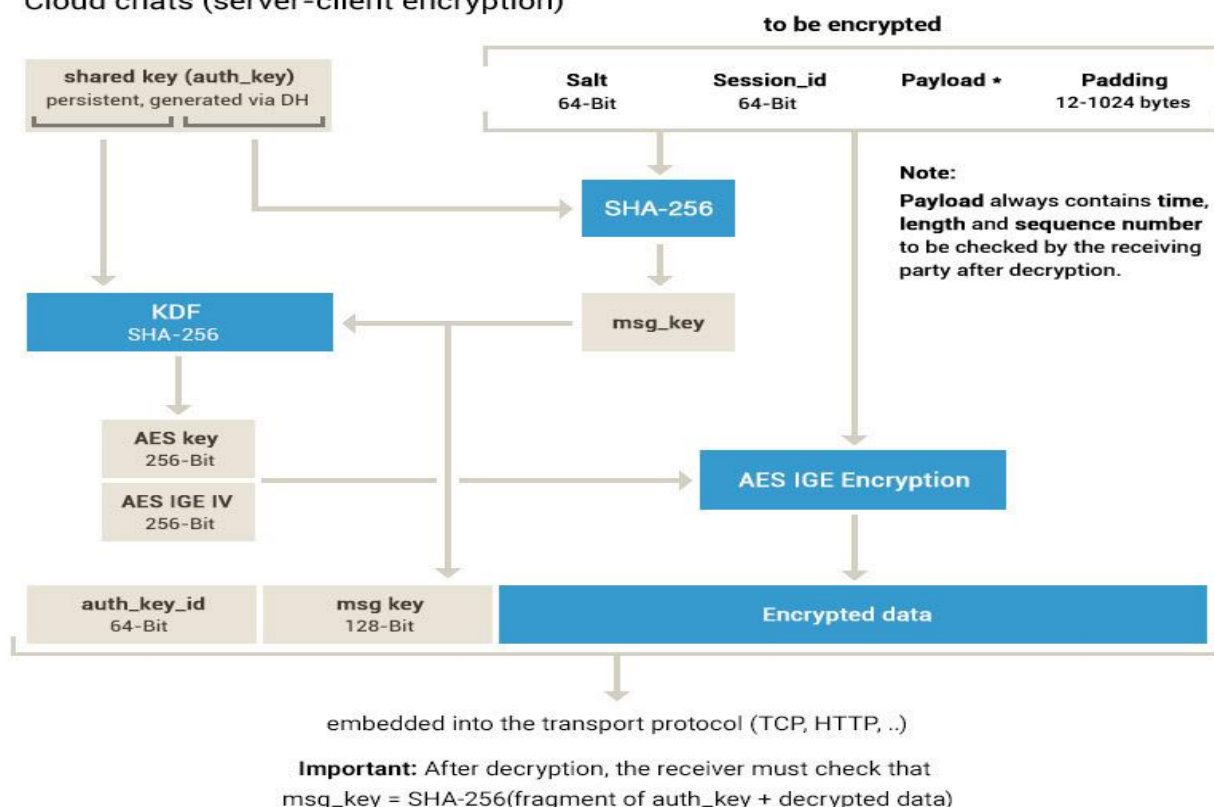


Рисунок 3. Схема протокола MTProto 2.0

Tik-Tok, напротив, использует более безопасные методы шифрования данных, в отличие от Telegram. Согласно исследованию Э. Алдерсона [23] от 2020 года данные, которые пересылает социальная сеть к себе на сервер. С помощью перехватчиков удалось уточнить несколько данных об устройстве, но не содержимое сообщения.

Установка разграничений доступов внутри социальной сети – довольно простой способ защиты данных от внешних пользователей. В настройках приватности профиля можно закрыть просмотр информации другим пользователям социальных сетей (рисунок 4), чтобы усложнить возможность кражи данных через поисковую строку. Например, здесь можно запретить просмотр личной информации страницы всем пользователям, социальной сети, выставив параметр «Только я».

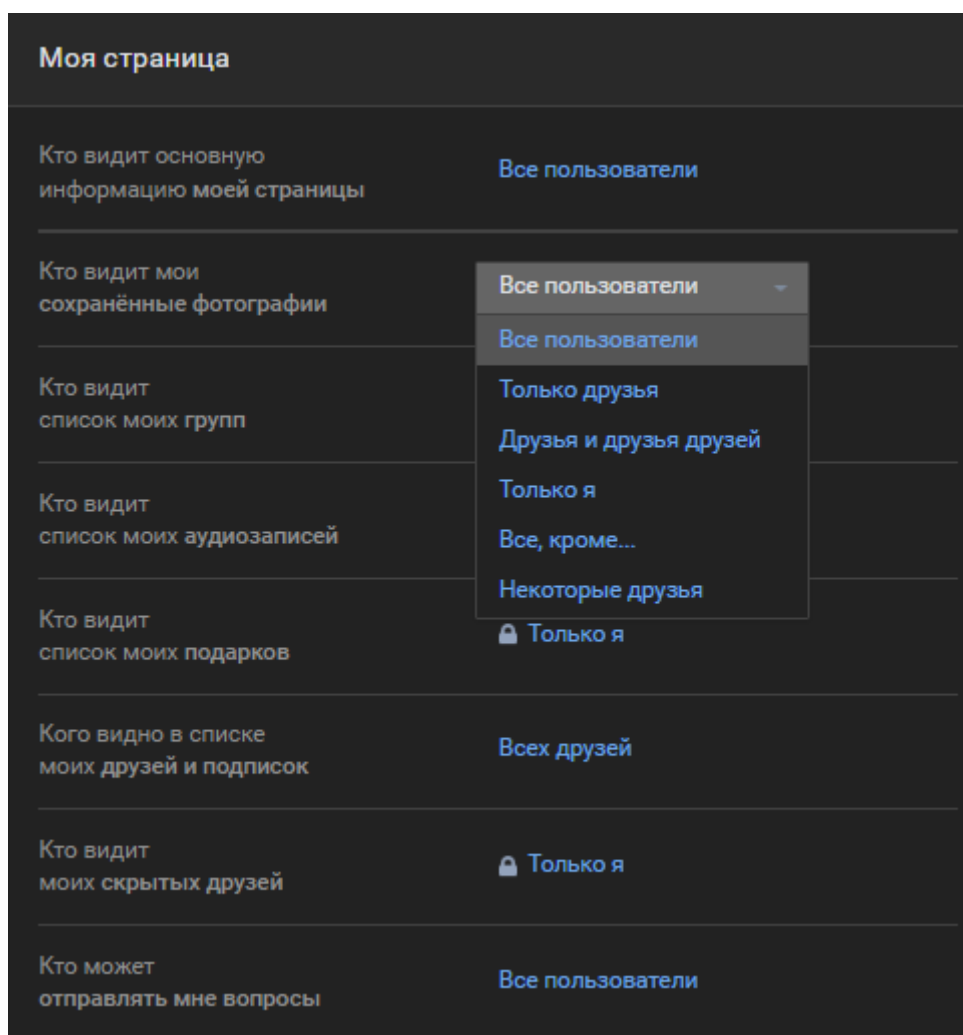


Рисунок 4. Настройки приватности социальной сети VK [5].

Вторая группа относится к ответственности самого пользователя. Из статьи bankstoday.net [14] говорится, что пользователи, кто небрежно относится к разглашению своих личных данных (номера телефона, домена электронной почты и прочее), чаще попадают в ту группу людей, чьи данные будут опубликованы или проданы коммерческим компаниям, из-за чего им часто могут поступать рекламные звонки, с целью социальных опросов, а также спам-рассылки, чем те, кто относится в вопросу разглашения данных более ответственно. Данный вопрос также рассматривался студентами Калифорнийского и Флоридского университетов [24], который исследовали раскрытие конфиденциальных данных самими пользователями. При проведении небольших опросов выяснилось, что большая часть пользователей

не задумываются о сохранении в секретности своих данных, при проведении прямых трансляций внутри социальных сетей.

Обезопасить свои данные можно, например, созданием отдельной электронной почты, которая будет использоваться для регистрации в социальных сетях, чтобы обезопасить свою деловую почту от тех же спам-рассылок.

Подводя итоги, стоит сказать, что в связи с развитием мира социальных сетей список уязвимостей растет. В ходе анализа социальной сети Tik-Tok была описана лишь часть угроз, которые были ранее выявлены пользователями социальной сети и независимыми аудиторами. Социальные сети, вероятней всего, исходя из законопроекта о регистрации по паспорту, внесенного в недавно в ГД РФ [24], обяжут новых пользователей в России вносить данные документа, из-за чего кража персональных данных может стать еще более желанна для дальнейшего использования в личных целях. В связи с этим разработчикам соцсетей следует как проводить проверку запуска новых и действующих алгоритмов на предмет уязвимостей, так и прибегать к сторонним сервисам выявления угроз (DeteAct, BI.ZONE, Positive Technologies, Bug Bounty, HackerOne, BugCrowd, Synack Red Team). Самим пользователям социальных сетей следует, в первую очередь, вносить минимальное количество данных, достаточных для использования социальной сети, скрывать геолокации фото, которые выставляются в новостную ленту, либо ограничивать круг теми данными, что не нанесут вред самому пользователю. Во-вторых, стоит игнорировать подозрительные сообщения, в которых «собеседник» может запросить от обычных данных, до данных кредитной карты, что может привести к печальным последствиям. Перед регистрацией в социальной сети стоит прочитать «политику приватности», где может быть указано, что владелец социальной сети в праве использовать Ваши данные в социальных исследованиях. Также следует использовать защищенный SSL-доступ, чтобы шифровать сеансы связи между сетью и браузером. Если следовать вышесказанным рекомендациям обоим сторонам

обработки ПД, возможна минимизация рисков утечки информации пользователей социальных сетей в открытый доступ или на «черный рынок».

Заключение

В рамках написания научно-исследовательской работы (прохождения производственной практики) были рассмотрены уязвимости хранения данных в социальных сетях, приведены примеры использования данных уязвимостей, а также были вынесены рекомендации по сохранению в секрете своей личной информации.

В результате написания отчёта была получена и проанализирована информация, что помогает для написания выпускной квалификационной работы, задачи практики были выполнены, статья опубликована в журнале «Прикладная информатика» [26]. Цель практики была достигнута.

Список используемых источников

1. Федерального закона от 27.07.2006 № 152-ФЗ (ред. 01.03.2021) «О персональных данных»;
2. Федерального закона от 27.07.2006 №149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2022);
3. Протокол Signal // Свободная энциклопедия Wikipedia [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Протокол_Signal;
4. Tik-Tok: // Социальная сеть Tik-Tok [Электронный ресурс]. URL: <https://www.tiktok.com/>;
5. VK: // Социальная сеть VK [Электронный ресурс. URL: vk.com;
6. Заикин Р. «Кто и как атаковал Tik-Tok?»: //Сообщество по информационной безопасности и защите данных CiscoClub [Электронный ресурс]. URL: <https://cisoclub.ru/kto-i-kak-atakoval-tiktok>;
7. Мамедов Р. Защита персональных данных в социальных сетях // Information Security [Электронный ресурс]. URL: <http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah/>;
8. Кемп С. DIGITAL 2022: ANOTHER YEAR OF BUMPER GROWTH // WE ARE SOCIAL [Электронный ресурс]. URL: <https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/>;
9. Мобоаджи А. PRIVACY CONCERNS, SELF-DISCLOSURE AND SOCIAL MEDIA USERS" ONLINE BEHAVIOUR // DEPARTMENT OF COMMUNICATION AND LANGUAGE ARTS, UNIVERSITY OF IBADAN [Электронный ресурс]. URL: https://www.researchgate.net/publication/350890073_PRIVACY_CONCERNS_SELF-DISCLOSURE_AND_SOCIAL_MEDIA_USERS_ONLINE_BEHAVIOUR;

10. Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года // Экспертно-аналитический центр InfoWatch [Электронный ресурс]. URL: https://webcache.googleusercontent.com/search?q=cache:zFK3K9S35V0J:https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_0.pdf&cd=4&hl=ru&ct=clnk&gl=ru
11. «Ищем уязвимости в TikTok при помощи OSINT» // Сообщество IT-специалистов Хабр [Электронный ресурс]. URL: <https://habr.com/ru/company/postuf/blog/502966/>
12. Уиндер Д. «TikTok Denies Breach After Hacker Claims ‘2 Billion Data Records’ Stolen» // FORBES [Электронный ресурс]. URL: <https://www.forbes.com/sites/daveywinder/2022/09/06/has-tiktok-us-been-hacked-and-2-billion-database-records-stolen/?sh=71f25a5105d9>
13. Мобильный протокол MTProto 2.0 // Telegram [Электронный ресурс]. URL: <https://core.telegram.org/mtproto>
14. Кокош Е. «Подпись, утечка и навязчивые звонки: откуда мошенники берут номера телефонов жертв и как их используют?» // Информационно-аналитическое финансовое издание «Банки Сегодня» [Электронный ресурс]. URL: <https://bankstoday.net/last-articles/podpis-utechka-i-navyazchivye-zvonki-otkuda-moshenniki-berut-nomera-telefonov-zhertv-i-kak-ih-ispolzuyut#i>
15. «What Makes TikTok Algorithm So Powerful?» // DataSadak [Электронный ресурс]. URL: <http://datasadak.com/what-makes-tiktok-recommendation-system-so-powerful/>
16. Tik-Tok // Интернет-сообщество HackerOne [Электронный ресурс]. URL: <https://hackerone.com/tiktok?type=team>
17. Cross site scripting via file upload in subdomain ads.tiktok.com // Интернет-сообщество HackerOne [Электронный ресурс]. URL: <https://hackerone.com/reports/1433125>

- 18.DOM XSS on ads.tiktok.com // Интернет-сообщество HackerOne [Электронный ресурс]. URL: <https://hackerone.com/reports/1549451>;
- 19.Reflected xss on ads.tiktok.com using `from` parameter. // Интернет-сообщество HackerOne [Электронный ресурс]. URL: <https://hackerone.com/reports/1452375>;
- 20.Jenna Jameson just got 4chan to do her dirty work for her // Интернет-издание Daily Dot [Электронный ресурс]. URL: <https://www.dailydot.com/upstream/jenna-jameson-4chan/>;
- 21.Matthew Green // Социальная сеть Twitter [Электронный ресурс]. URL: https://twitter.com/matthew_d_green/status/582916365750669312;
- 22.Сарибемян Х., Маргвелашвили А. «Анализ безопасности Telegram» // Информационный портал SecurityLab.ru [Электронный ресурс]. URL: <https://www.securitylab.ru/analytics/490726.php>;
- 23.Андерсон Э. «ТикТок: Логи, логи, логи» // Информационный портал SecurityLab.ru [Электронный ресурс]. URL: <https://www.securitylab.ru/analytics/510846.php>;
- 24.Милонов В. // Сайт Государственной думы Федерального собрания Российской Федерации [Электронный ресурс]. URL: [http://asozd2.duma.gov.ru/main.nsf/\(ViewDoc\)?Openagent&addwork/scans.nsf/ID&CDE75DB8CA378E8D432580FE002C8A84](http://asozd2.duma.gov.ru/main.nsf/(ViewDoc)?Openagent&addwork/scans.nsf/ID&CDE75DB8CA378E8D432580FE002C8A84);
- 25.Tik-Tok Bug Bounty Program // Интернет-сообщество HackerOne [Электронный ресурс]. URL: <https://hackerone.com/tiktok?type=team>.
- 26.Научный журнал «Прикладная информатика» [Электронный ресурс]. URL: https://elibrary.ru/title_about_new.asp?id=25599.