ТЕХНИЧЕСКИЕ НАУКИ TECHNICAL SCIENCES

Научная статья

УДК 004.032.26

ББК 32.818.1

Ч 48

doi: 10.53598 / 2410-3225-2021-2-281-47-55

Разработка модели обеспечения безопасности аккаунта социальной сети на основе нейросетевого алгоритма (Рецензирована)

Александр Николаевич Черкасов¹, Алена Валерьевна Сивенко²

^{1,2} Кубанский государственный технологический университет, Краснодар, Россия

¹ cherk@mail.ru

² sivenkoalena99@mail.ru

Аннотация. Проведен анализ текущей статистики взлома учетных записей в социальных сетях. Построена архитектура нейронной сети, позволяющая классифицировать учетные записи пользователей на «безопасные» и «в зоне риска». Разработано программное обеспечение, позволяющее оценить надежность учетной записи пользователя в социальной сети «ВКонтакте».

Ключевые слова: социальная сеть, безопасность учетной записи, нейронная сеть

Original Research Paper

Development of a model for ensuring the security of a social network account based on a neural network algorithm

Aleksandr N. Cherkasov¹, Alena V. Sivenko²

^{1,2} Kuban State University of Technology, Krasnodar, Russia

¹ cherk@mail.ru

² sivenkoalena99@mail.ru

Abstract. An analysis is made of the current statistics of hacking accounts in social networks. The architecture of a neural network has been built, which makes it possible to classify user accounts into “safe” and “at risk”. Software has been developed to assess the reliability of a user's account on the “VKontakte” social network.

Keywords: social network, account security, neural network

Появление социальных сетей существенно упростило жизнь людей, так как они позволяют обмениваться сообщениями в режиме реального времени, читать последние новости, прослушивать музыку, загружать фото и видео, писать комментарии, участвовать в различных голосованиях, играть в игры и много чего другого. Согласно отчету Global Digital 2021, представленному We Are Social и Hootsuite [1], социальными сетями в 2021 году пользуются 53,6% мирового населения.

Анализ текущей статистики

Каждый человек тем или иным образом сталкивался со взломом аккаунта в социальной сети, возможно, была взломана учетная запись непосредственно пользователя, кого-либо из членов его семьи, друзей, коллег и т.д. Одной из главных причин взлома учетной записи в социальной сети по-прежнему остается фишинг. Согласно отчету, представленному Лабораторией Касперского о спаме и фишинге за 2020 год [2], социальные сети стоят на 4 месте по распределению организаций, чьи пользователи были атакованы фишерами (10,02%).

В результате проведенного нами анализа статистики взлома аккаунтов в социальной сети «ВКонтакте» было установлено, что в среднем в час взламывается 53 учетные записи. Пример сравнения количества взломанных учетных записей за два дня в промежуток с 13:00 до 24:00 представлен на рисунке 1.

Рис. 1. Сравнение количества взломанных учетных записей

Анализ существующих подходов

Развитие технологий машинного обучения привело к их активному применению в различных областях. В социальных сетях уже активно применяются различные нейронные сети (НС), которые успешно решают разные задачи. Более подробно о нейронных сетях в социальных сетях можно узнать в работе [3].

В ходе исследования были проанализированы существующие подходы, применяемые для обеспечения безопасности в социальных сетях [4–13]. Результаты приведены в таблице 1.

Таблица 1

Подходы, применяемые для обеспечения безопасности в социальных сетях

Подход	Пользователь	Деструктивный контент	Манипулятивные воздействия
Графовый	Да	Да	Да
Теоретико-множественный	Нет	Да	Да
Нейронная сеть	Да	Да	Да
Оценка тональности	Нет	Да	Нет
Системно-динамическое моделирование	Нет	Да	Да

В данной таблице строки – применяемые подходы, столбцы – в отношении чего применялся метод. На пересечении соответственно обозначено, применялся ли данный подход к сущности. Стоит отметить, что в отношении пользователей применялось два метода, однако они ориентированы на опасность, исходящую непосредственно от пользователя, а не на обеспечение безопасности учетной записи, поэтому было принято решение разработать нейронную сеть, которая позволила бы определять пользователей, находящихся в зоне риска.

Согласно статистике [1], самой популярной социальной сетью в России является «ВКонтакте», поэтому для работы была выбрана именно она.

Получение набора данных для обучения нейронной сети

Исходного набора данных в сети Интернет авторами не было обнаружено, поэтому на языке программирования высокого уровня Python были написаны два кода, позволяющие сформировать необходимые данные. Для этого применялась библиотека `vk_api`, а полученные данные сохранялись в `.csv` файл.

Согласно Федеральному закону N 152 «О персональных данных» [14], проводилось обязательное обезличивание персональных данных: информация о фамилии, имени и `id` пользователей. Пример сформированного набора данных представлен в таблице 2. Отметим, что в представленной таблице отображены не все полученные столбцы.

Таблица 2

Фрагмент сформированного набора данных

	is_closed	sex	verified	bdate	city	country	has_photo	has_mobile	wall_default
1	False	2	1.0	10.10.1984	'id': 2, 'title': 'Санкт-Петербург'	'id': 1, 'title': 'Россия'	1	1.0	owner
2	True	2	0.0				1	1.0	all
3	False	2	0.0	31.8.1988	'id': 2, 'title': 'Санкт-Петербург'	'id': 1, 'title': 'Россия'	1	1.0	all
4	False	2	0.0		'id': 2, 'title': 'Санкт-Петербург'	'id': 1, 'title': 'Россия'	1	1.0	all
5	False	1	0.0	19.12.1985	{'id': 1, 'title': 'Москва'}	'id': 1, 'title': 'Россия'	1	1.0	all
6	False	1	0.0	18.7	'id': 2, 'title': 'Санкт-Петербург'	'id': 1, 'title': 'Россия'	1	1.0	owner

В результате был сформирован набор данных, включающий в себя 109069 строк, из которых 52312 – данные о взломанных учетных записях.

Разработка архитектуры нейронной сети

Для анализа сформированного набора данных реализована модель нейронной сети. Реализация архитектуры нейронной сети выполнена при помощи языка программирования Python с использованием библиотеки Keras.

Разработанная архитектура нейронной сети включает в себя входной слой, четыре промежуточных слоя и выходной слой. Архитектура нейронной сети представляет собой обычный персептрон. Входные данные – параметры учетной записи. Первыми слоями являются три слоя по 35 нейронов с функцией активации `relu`, затем идет слой,

содержащий 25 нейронов с функцией активации `relu`, и 1 нейрон на выходном. Для предотвращения явления переобучения использовались слои Dropout. Структура сформированной нейронной сети представлена на рисунке 2.

В качестве метрики для оценки качества обучения была выбрана `precision`, точность которой вычисляется по формуле 1.

$$precision = \frac{TP}{TP + FP} . \quad (1)$$

В формуле (1) TP (True Positive) обозначает количество предсказаний классификатора, при которых он правильно отнес образ к классу «в зоне риска», а FP (False Positive) – количество предсказаний классификатора, при которых он неверно отнес образ к классу «в зоне риска».

Рис. 2. Схема нейронной сети

Метрика “`precision`” была выбрана, поскольку она показывает долю объектов, названных классификатором положительными и при этом действительно являющимися

положительными, а в решаемой задаче наибольшим приоритетом является выявление учетных записей, находящихся в зоне риска.

По результатам обучения классификатор показал следующие характеристики: $\text{accuracy}=86,5\%$, $\text{precision}=80\%$. Для оценки качества обученного классификатора проанализируем матрицу ошибок. Полученная по результатам эксперимента матрица ошибок представлена на рисунке 3.

Рис. 3. Матрица ошибок

Из матрицы видно, что общее количество ошибок классификации на тестовой выборке равняется 2945, из них 445 ошибок – ошибки второго рода (False Negative) и 2500 случаев – ошибки первого рода (False Positive). Данные результаты показывают, что модель успешно справляется с поставленной задачей.

Разработка программного обеспечения

На основании разработанной нейронной сети разработан программный продукт, позволяющий оценить учетную запись пользователя на подверженность взлому. Главное окно представлено на рисунке 4.

Рис. 4. Главное окно ПО

Для проверки пользователю достаточно ввести id учетной записи. Стоит обратить внимание на поля «Учетная запись относится к классу:» и «Уверенность нейронной сети в результате:». Данные поля выводят подробную информацию о полученном нейронной сетью результате. Так, в первом поле выводится присвоенный класс, а во втором поле выводится анализ присвоенного нейросетью процента. Для удобства было введено две шкалы – позитивная и негативная.

Если учетная запись отнесена к классу «безопасный», то отображается позитивная шкала. Рисунок шкалы представлен на рисунке 5.

Рис. 5. Позитивная шкала

В данной шкале баллы имеют следующее значение:

5 баллов – НС уверена, что учетная запись безопасна;

4 балла – НС менее уверена, что учетная запись безопасна;

3 балла – НС более-менее уверена, что учетная запись безопасна;

2 балла – НС не уверена, что учетная запись безопасна;

1 балл – НС могла ошибиться.

Если учетная запись отнесена к классу «в зоне риска», то отображается негативная шкала. Изображение шкалы представлено на рисунке 6.

Рис. 6. Негативная шкала

В данной шкале баллы имеют следующее значение:

5 – НС уверена, что учетная запись не безопасна;

4 – НС менее уверена, что учетная запись не безопасна;

3 – НС более-менее уверена, что учетная запись не безопасна;

2 – НС не уверена, что учетная запись не безопасна;

1 – НС могла ошибиться.

Пример тестирования учетной записи приведен на рисунке 7.

Рис. 7. Проверка учетной записи пользователя

Проведено тестирование точности нейронной сети в определении аккаунтов, находящихся в зоне риска. В рамках часового промежутка в течение суток проверено разработанное программное обеспечение (ПО) через соответствующие аккаунты: протестированы 38 учетных записей, которые в течение заданного промежутка времени публиковали сообщения о взломе. В результате все 38 были отнесены ПО к классу «в

зоне риска». Предложенная система представляет систему поддержки принятия решений, которая может быть использована как для рядового пользователя, так и для реализации других задач [15].

Выводы

1. Проведен анализ текущей статистики взломов в социальных сетях. В результате было установлено, что в среднем в час взламывается 53 учетные записи.
2. Разработана архитектура нейронной сети, позволяющая определять учетные записи, находящиеся в зоне риска. Полученная модель успешно справляется со своей задачей.
3. Разработано программное обеспечение, позволяющее пользователю проверить учетную запись на основании ее id. Программа является интуитивно понятной, поэтому проста в использовании.

Список литературы:

1. Digital 2021: главная статистика по России и всему миру. URL: <https://exlibris.ru/news/digital-2021-glavnaya-statistika-po-rossii-i-vsemu-miru/>
2. Куликова Т. Спам и фишинг в 2020 году. URL: <https://securelist.ru/spam-and-phishing-in-2020/100408/>
3. Сивенко А.В., Корх И.А. Применение нейронных сетей в обеспечении информационной безопасности социальных сетей // Машины. Люди. Ценности: когнитивные и социокультурные системы в потоке времени: материалы II междунар. науч. конф., посвященной 100-летию со дня рождения доктора философских наук, профессора С.М. Шалютина (г. Курган, 22–23 апреля 2021 г.). Курган, 2021. С. 75–79.
4. Социальные сети: моделирование динамики распространения манипулятивных воздействий / В.А. Минаев, Е.В. Вайц, А.Э. Киракосян, В.В. Умеренков // Информация и безопасность. 2018. Т. 21, № 4. С. 594–599.
5. Еременко В.Т., Сазонов М.А., Шекшуев С.В. Исследование подходов к созданию информационных моделей для сбора и обработки данных социальных сетей // Информация и безопасность. 2019. Т. 22, № 1. С. 118–129.
6. Основы метрологии контентов для мониторинга социальных сетей на предмет обеспечения информационной безопасности (часть 1) / А.Г. Остапенко, Е.С. Соколова, А.В. Ещенко, А.А. Остапенко, Т.Ю. Чапурина // Информация и безопасность. 2019. Т. 22, № 2. С. 170–180.
7. Основы метрологии контентов для мониторинга социальных сетей на предмет обеспечения информационной безопасности (часть 2) / А.Г. Остапенко, Е.С. Соколова, А.В. Ещенко, А.А. Остапенко, Т.Ю. Чапурина // Информация и безопасность. 2019. Т. 22, № 2. С. 181–187.
8. Методы тематического моделирования, их развитие и применение для контента, циркулирующего в региональных онлайн-сообществах / Е.Н. Телегин, Е.Ю. Чапурин, К.А. Разинкин, Д.Г. Плотников, А.В. Попов // Информация и безопасность. 2019. Т. 22, № 3. С. 325–344.
9. Использование и развитие методик оценки тональности контентов социальных сетей в целях обеспечения информационной безопасности пользователей / Е.А. Москалева, Е.Р. Нежелский, М.Е. Волкова, К.В. Сибирко, В.В. Сафронова // Информация и безопасность. 2019. Т. 22, № 3. С. 433–444.
10. Моделирование манипулятивных воздействий в социальных сетях / В.А. Минаев, М.П. Сычев, Л.С. Куликов, Е.В. Вайц // Моделирование, оптимизация и информационные технологии. 2019. Т. 7, № 1 (24). С. 494–510.
11. Программно-технический комплекс для риск-анализа деструктивных контентов социальных сетей: структура, внешний вид и базы данных / Е.Ю. Чапурин, А.Е. Гусянников, Л.В. Парина, В.Г. Юрасов, Ю.Г. Пастернак // Информация и безопасность. 2020. Т. 23, № 3 (4). С. 389–398.

12. Минаев В.А. Информационное противоборство в социальных сетях: модели и методы исследования // *Информация и безопасность*. 2020. Т. 23, № 4. С. 477–496.

13. Титов Н.Г. Методы мониторинга социальных сетей, их развитие и применение в контексте обеспечения их информационной безопасности / Н.Г. Титов, Е.Ю. Чапурин, Е.А. Москалева, М.И. Бочаров, В.И. Борисов // *Информация и безопасность*. 2019. Т. 22, № 3. С. 305–324.

14. О персональных данных: Федеральный закон от 27.07.2006 N 152-ФЗ (редакция от 30 декабря 2020). URL: http://www.consultant.ru/document/cons_doc_LAW_61801

15. Черкасов А.Н. Разработка математического и алгоритмического обеспечения адаптивных систем поддержки принятия решений в ситуационных центрах: дис. ... канд. техн. наук / Кубанский государственный технологический университет. Краснодар, 2011. 152 с.

References:

1. Digital 2021: главная статистика по России и всему миру. URL: <https://exlibris.ru/news/digital-2021-glavnaya-statistika-po-rossii-i-vsemu-miru/>

2. Kulikova T. Spam and phishing in 2020. URL: <https://securelist.ru/spam-and-phishing-in-2020/100408/>

3. Sivenko A.V., Korkh I.A. The use of neural networks in providing information security of social networks // *Cars. People. Values: cognitive and sociocultural systems in the flow of time: materials of the 2nd International Scientific Conference dedicated to the 100th anniversary of the birth of Doctor of Philosophy, Professor S.M. Shalyutin (Kurgan, April 22–23, 2021)*. Kurgan, 2021. P. 75–79.

4. Social networks: modeling the dynamics of the spread of manipulative influences / V.A. Minaev, E.V. Vayts, A.E. Kirakosyan, V.V. Umerenkov // *Information and Security*. 2018. Vol. 21, No. 4. P. 594–599.

5. Eremenko V.T., Sazonov M.A., Shekshuev S.V. Investigation of approaches to the creation of information models for collecting and processing data from social networks // *Information and Security*. 2019. Vol. 22, No. 1. P. 118–129.

6. Basics of content metrology for monitoring social networks for information security (Part 1) / A.G. Ostapenko, E.S. Sokolova, A.V. Eshchenko, A.A. Ostapenko, T.Yu. Chapurina // *Information and Security*. 2019. Vol. 22, No. 2. P. 170–180.

7. Ostapenko A.G. Basics of content metrology for monitoring social networks for information security (Part 2) / A.G. Ostapenko, E.S. Sokolova, A.V. Eshchenko, A.A. Ostapenko, T.Yu. Chapurina // *Information and Security*. Voronezh: 2019. Vol. 22, No. 2. P. 181–187.

8. Methods of thematic modeling, their development and application for content circulating in regional online communities / E.N. Telegin, E.Yu. Chapurin, K.A. Razinkin, D.G. Plotnikov, A.V. Popov // *Information and Security*. 2019. Vol. 22, No. 3. P. 325–344.

9. The use and development of methods for assessing the sentiment of the content of social networks in order to ensure the information security of users / E.A. Moskaleva, E.R. Nezhelsky, M.E. Volkova, K.V. Sibirko, V.V. Safronova // *Information and Security*. 2019. Vol. 22, No. 3. P. 433–444.

10. Modeling of manipulative influences in social networks / V.A. Minaev, M.P. Sychev, L.S. Kulikov, E.V. Vayts // *Modeling, Optimization and Information Technology*. 2019. Vol. 7, No. 1 (24). P. 494–510.

11. Software and hardware complex for risk analysis of the descriptive content of social networks: structure, appearance and databases / E.Yu. Chapurin, A.E. Guslyannikov, L.V. Parinova, V.G. Yurasov, Yu.G. Pasternak // *Information and Security*. 2020. Vol. 23, No. 3 (4). P. 389–398.

12. Minaev V.A. Information confrontation in social networks: models and research methods // *Information and Security*. 2020. Vol. 23, No. 4. P. 477–496.

13. Titov N.G. Methods for monitoring social networks, their development and application in the context of ensuring their information security / N.G. Titov, E.Yu. Chapurin, E.A. Moskaleva, M.I. Bocharov, V.I. Borisov // *Information and Security*. 2019. Vol. 22, No. 3. P. 305–324.

14. On Personal Data: Federal Law of July 27, 2006 N 152-FZ (as amended on December 30, 2020). URL: http://www.consultant.ru/document/cons_doc_LAW_61801

15. Cherkasov A.N. Development of mathematical and algorithmic support for adaptive decision support systems in situational centers: Diss. for the Cand. of Techn. Sciences degree / Kuban State University of Technology. Krasnodar, 2011. 152 p.

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Статья поступила в редакцию 08.04.2021; одобрена после рецензирования 10.05.2021; принята к публикации 15.05.2021.

The article was submitted 08.04.2021; approved after reviewing 10.05.2021; accepted for publication 15.05.2021.

© А.Н. Черкасов, А.В. Сивенко, 2021