

# СИСТЕМА ПРОТИВОДЕЙСТВИЯ МЕТОДАМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<sup>1</sup>

*Цифровая эволюция и связанное с ней распространение гаджетов, повсеместное использование глобальной сети Интернет с каждым днём облегчают жизнь человека и создают множество путей для развития. Но, чем больше сфер жизни переходят в мир нулей и единиц, тем больше и правонарушений осуществляются в этом же контексте. Согласно исследованию Управления правовой статистики и информационных технологий Генпрокуратуры 25% от всех правонарушений составляют киберпреступления [1].*

*Определенную часть киберпреступлений занимают атаки с помощью методов социальной инженерии. Один из самых простых способов взлома в реалиях роста защищенности электронно-вычислительных машин и доступности антивирусного и иного подобного рода программного обеспечения — «взломать» человека.*

*В данной статье были рассмотрены основные понятия в области социальной инженерии, схема атаки, а также основные техники социальной инженерии и рекомендации по защите от них. В результате авторами статьи был разработан веб-сервис для поиска адресов электронных почт, номеров телефонов и ссылок в базах данных фишинговых адресов.*

**Ключевые слова:** социальная инженерия, информационная безопасность, фишинг.

**Khalilaeva E.I., Maslova M.A., Gerasimov V.M.**

# THE SYSTEM OF COUNTERING THE METHODS OF SOCIAL ENGINEERING IN THE FIELD OF INFORMATION SECURITY

*Digital evolution and the associated spread of gadgets, the widespread use of the global Internet make human life easier every day and create many ways for development. But, the*

<sup>1</sup> Работа выполнена в рамках Соглашения от 30.06.2022 г. № 40469-21/2022-к.

more spheres of life move into the world of zeros and ones, the more offenses are carried out in the same context. The Department of Legal Statistics and Information Technologies of the Prosecutor General's Office claims that one of the four crimes falls on "cyber" offenses [1].

A certain part of cybercrimes is occupied by attacks using social engineering methods. One of the simplest ways of hacking in the realities of the growing security of electronic computers and the availability of antivirus and other similar software is to "hack" a person.

So, in this article, the basic concepts in the social field of engineering, attack schemes, as well as the main technologies of social engineering and recommendations for protecting against them were considered. As a result, the authors of the article developed a website to search for email addresses, phone numbers and links in databases of phishing addresses.

**Keywords:** social engineering, information security, phishing.

**Введение.** В контексте информационной безопасности социальная инженерия — это вид обмана и (или) мошенничества с целью получения различного рода конфиденциальных данных [2]. Такой информацией могут выступать: персональные данные пользователей, пароли, в том числе к банковским картам; личная информация: фото или видеоматериалы. Это всё может быть использовано для дальнейшего получения злоумышленником материальной или иной выгоды.

Российская компания Positive Technologies провела собственное исследование в области

социальной инженерии. Эксперты компании имитировали деятельность хакеров и отправляли пользователям, сотрудникам компаний, которые были инициаторами данного исследования, вредоносные письма. Например, по фишинговым ссылкам в сообщения перешло 27% получателей. Из них 88% пользователей работники, не связанные с информационными технологиями (юристы, менеджеры и т.д.) [3].

Представим схему Шейнова, адаптировав ее для техник атак социальной инженерии. Схема содержит шесть этапов (рис. 1).

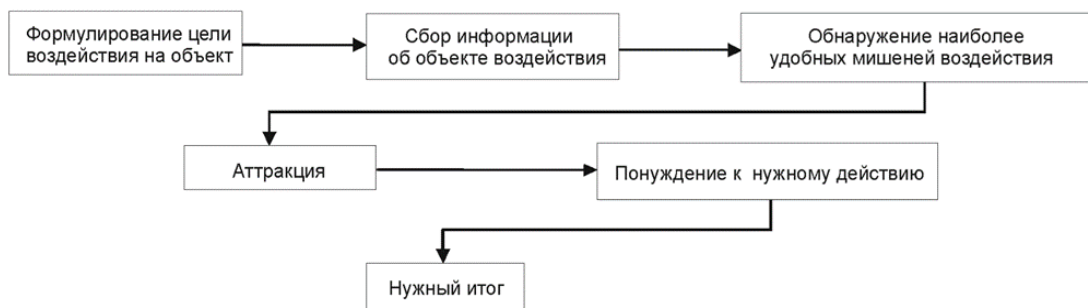


Рис. 1. Общая схема атаки социальной инженерии

Первый этап атаки — это формулирование цели воздействия на объект. Например, получение персональных данных, личных материалов пользователя, шантаж и др.

За первым этапом следует процесс сбора информации об объекте воздействия. Источников информации неограниченное количество: открытые ресурсы, социальные сети, базы данных и пр. В случае, если целью становится реальный человек, с которым есть возможность установить прямой личный контакт, злоумышленник может так же этим воспользоваться.

Далее злоумышленник изучает и определяет наиболее удобные мишени воздействия

на выбранный объект, например, персональные данные человека.

Следующий этап называется аттракцией. Он дает возможность создавать необходимые условия для воздействия киберпреступника на выбранный им объект.

Этапа понуждения злоумышленники обычно не достигают, т.к. в основном жертва уже компрометирует себя на одном из предыдущих шагов [4].

Стоит отметить, что схемой Шейнова преимущественно пользуются опытные социальные инженеры, ориентированные на узкий круг пользователей или одного человека с четко поставленной целью. В настоящее же

время с ростом доли Интернета и иных средств коммуникации в жизни обычного человека большую часть атак социальной инженерии осуществляют дилетанты путём массовых рассылок фишинговых писем, звонков и т.д. в надежде, что определенная часть пользователей откликнется на отправленную ими «приманку».

Техники атак социальной инженерии могут быть самые различные. Фишинговые атаки (от англ. «phishing» – рыбная ловля) – одни из самых распространенных, где акцент, зачастую, направлен на получение конфиденциальных данных пользователя. Тут может быть любая ценная информация: логины и пароли, данные, удостоверяющие личность и т.п. [5]. Выбрав средством осуществления цели фишинг, злоумышленник может отправить жертве на первый взгляд безобидную картинку или гиперссылку с привлекательным текстом. Пользователь, ничего не подозревая, кликает на вложение и в этот момент уже себя компрометирует.

Основные рекомендации по защите от фишинговых атак:

- не открывать вложения и не переходить по ссылкам, содержащимся в письмах или сообщениях от неизвестных отправителей;
- если отправитель письма или сообщения известен, необходимо сначала убедиться в корректности и правильности ссылки;
- внимательно проверять электронные письма от легитимных лиц: письма или уведомления от банка или банковских служащих, сервисов, предоставляющих государственные услуги («Госуслуги», например) и т.д.;
- использовать, а затем своевременно обновлять эффективное антивирусное программное обеспечение.

Quid pro quo (лат. «услуга за услугу», или «то за это» – ещё один распространённый тип атаки социальной инженерии. Злоумышленник может представиться легитимным лицом: сотрудником технической поддержки, или банковским служащим. Далее он внушает объекту воздействия, что возникли какие-то неполадки: заблокирован банковский счёт, неизвестный списал со счёта круглую сумму или компьютер подвергся хакерской атаке. Затем киберпреступник обычно предлагает различные варианты действий для устранения данной проблемы. Он обманным путем пытается вынудить жертву выдать ему пароли от своих счетов или от аккаунтов в соци-

альных сетях, перейти по ссылке для установки мошеннических программ на ПК жертвы и т.д. [6].

Ещё одна из самых распространенных техник атак – троянский конь или троян. Киберпреступник отправляет жертве любой контент, который может ее заинтересовать: безобидная картинка, открытка, смешное видео и др. Пользователь переходит по ссылке, тем самым скачивая вредоносные файлы на устройство. Троянские кони могут содержаться в ссылках, подозрительных и поддельных веб-сайтах, рекламных баннерах и всплывающих окнах [7, 8].

Для возможного предотвращения атак социальной инженерии (преимущественно фишинга) авторами статьи был разработан веб-сервис, который дает возможность анализа почтовых электронных адресов, URL-ссылок, номеров мобильных телефонов на возможное наличие их в предварительно собранной и регулярно обновляемой базе данных подозрительных адресов и тех адресов, с которых уже были совершены атаки социальной инженерии. Это позволит пользователям более предусмотрительно относиться к входящим звонкам, сообщениям или письмам с подозрительным содержанием.

Главным аргументом в пользу выбора веб-приложения, а не мобильного или десктопного приложения, например, послужила кроссплатформенность такого сервиса. Сервис может быть доступен с любого устройства, имеющего выход в Интернет. В дальнейшем в рамках развития проекта может быть осуществлена возможность сохранять базу на устройство: ПК, смартфон или планшет, к примеру, для пользования в режиме «оффлайн». Кроме того, возможна интеграция с системами мобильных операторов, почтовых серверов, с внутренними системами защиты в браузерах и, соответственно, подключение монетизации.

Для реализации сервиса был использован следующий стек технологий: Python 3.10, Django Rest Framework, React.JS, PostgreSQL версии 10.23. Из библиотек, не включенных в стандартную базу для языка Python, были применены beautifulsoup4, lxml.

В данном проекте есть четыре модуля, которые разделены на сбор данных, базу данных, бэк-энд приложения и фронт-энд приложения.

Парсинг данных запускается ежедневно в 00:00. В настройки приложения внесено бо-

более двадцати различных ресурсов, которые представляют собой сервисы для жалоб пользователей на адреса электронных почт, ссылки, номера телефонов. Написанный скрипт проходит по каждому из ресурсов, парсит веб-страницы, конвертирует данные в модели и обновляет информацию в базе.

Представим ER-диаграмму базы данных (рис. 2).

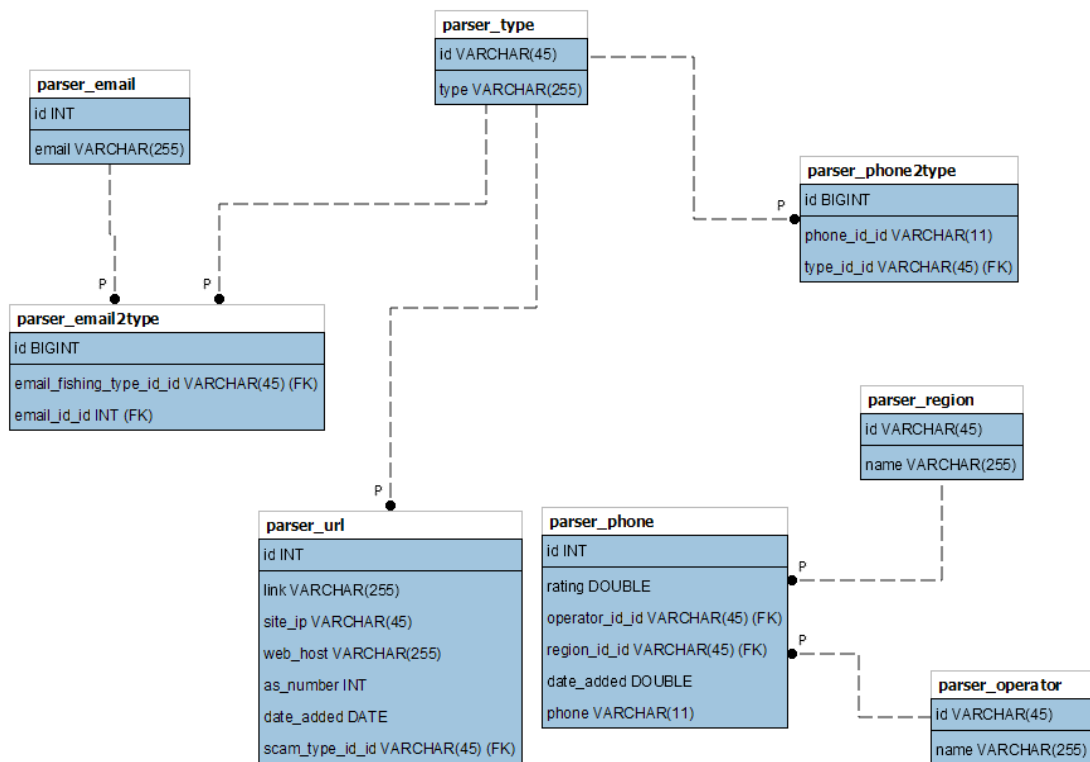


Рис. 2. ER-диаграмма базы данных проекта

тронную почту) для того, чтобы узнать, есть ли в базе искомый им адрес. Результат поиска в базе URL-ссылки, номера телефона и адреса электронной почты приведены на рис. 3–5.

Дополнительно по различным адресам можно узнать тип мошенничества, в котором они были уличены или подозреваемы. Для номеров телефонов также можно узнать регион, оператора мобильной связи и общий рейтинг номера, основанный на средней арифметической оценок номера для различных ресурсов. Для ссылок выводится так же информация о внешнем IP-адресе, веб-хосте, номере автономной системы и дата добавления в базу.

В случае, если адреса нет в базе, пользователю выводится соответствующее уведомление (рис. 6).

Перечислим основные используемые сущности — это url, emails, phone. Они предназначены для хранения основных данных, таких, как ссылки, e-mail, мобильные телефоны.

Взаимодействует с бек-эндом приложения и базой данных пользователь через фронт-энд. На экранной форме он может ввести адрес (ссылку, номер телефона или элек-

Неявным направлением работы над проектом является обеспечение его целостности, конфиденциальности и доступности. Необходимо максимизировать защиту и минимизировать возможность получения злоумышленником доступа к базе. В таком случае злоумышленники могут добавить в неё легитимных пользователей, исключить себя и все свои адреса или в целом нарушить целостность базы данных.

Один из столпов обеспечения защиты проекта — использование CSRF-токена (ключа) для построения запросов с клиентской стороны. CSRF-токен представляет собой токен для защиты сервиса от межсайтовой подделки запроса. Происходит эта генерация случайного токена на сервере, после чего она отправляется клиенту. Проверка ключа

Введите e-mail для проверки:

xiakifoni@vodafone.net.gr

Проверить

Адрес электронной почты: xiakifoni@vodafone.net.gr  
Тип мошенничества: Нигерийские письма

Рис. 3. Результат поиска подозрительного адреса электронной почты

Введите URL-ссылку для проверки:

http://www.gscuk.net

Проверить

URL-адрес: http://www.gscuk.net  
Внешний IP-адрес сайта: 0.0.0.0  
Веб-хост: 205.209.105.47  
Номер автономной системы: 0  
Дата добавления в базу данных: 1.2.2007 г.  
Вид мошенничества: Мошенничество с законом

Рис. 4. Результат поиска подозрительного адреса URL

Введите номер телефона для проверки:

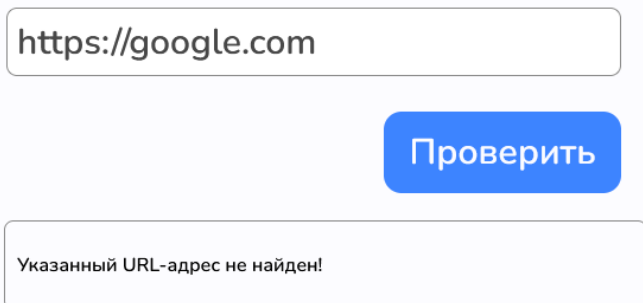
+74950693894

Проверить

Номер телефона: 4950693894  
Регион: г. Москва и Московская область  
Оператор: ООО "КОРДИС ТЕЛЕКОМ"  
Рейтинг: 1.43  
Виды мошенничества: Колл-центры

Рис. 5. Результат поиска подозрительного номера мобильного телефона

## Введите URL-ссылку для проверки:



https://google.com

Проверить

Указанный URL-адрес не найден!

Рис. 6. Поиск по базе данных адреса Google

происходит благодаря генерации случайного ключа и далее отправки его браузеру клиента. После запроса браузером информации сервера он, в свою очередь, первый делом требует предоставление ключа и производит его проверку. После проверки, если она положительная, сессия продолжается, в противном же случае нет. При этом токен действует только на одну секцию, с каждой новой он обновляется [9].

На клиентской стороне этот процесс незаметен, т.к. все происходит автоматически на серверной.

Другой распространённый тип угроз — SQL-инъекции. Данный вид атаки происходит благодаря действиям злоумышленника, который может выполнить произвольный SQL-скрипт в базе данных. Это может быть запрос на SELECT (чтение данных), UPDATE (их обновление) или даже DELETE (удаление данных). Такие скрипты обычно передаются злоумышленниками через поля ввода на форме.

Запросы, которые строятся с помощью параметризации, а именно SQL-запросы, обрабатываются с применением Django и име-

ют защиту от такого рода атак. Тут имеющийся код запроса будет обрабатываться отдельно от имеющихся параметров. Данные параметры при передаче их в базу данных экранируются.

Также в рамках данной работы был разработан API для доступа к базе данных. Это позволит создать различные пути для интеграции с почтовыми сервисами, операторами мобильной связи и т.д.

Таким образом, важно постоянно повышать уровень знаний в информационной сфере, чтобы предотвращать инциденты, вызванные атаками социальной инженерии. Это относится не только к обычным, но и к корпоративным пользователям. В заключение стоит отметить, что разработанный веб-сервис позволяет проверять пользователям нежелательные адреса электронных почт, номеров телефонов и ссылок в базах данных фишинговых адресов, что поможет обезопасить себя от злоумышленников в информационном пространстве, что и было основной целью разработки.

### Литература

1. Генпрокуратура: в 2020 году число зарегистрированных киберпреступлений выросло более чем на 76% // D-Russia.ru: ежедн. интернет-изд. 2020. 30 дек. URL: <https://d-russia.ru/genprokuratura-v-2020-godu-chislo-zaregistrirovannyh-kiberprestuplenij-vyroslo-bolee-chem-na-76.html> (дата обращения: 19.03.2022).
2. Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов // Банк России, 2021. – 107 с.
3. PositiveTechnologies: Как социальная инженерия открывает хакеру двери в вашу организацию // [www.ptsecurity.com](http://www.ptsecurity.com): сайт компании PositiveTechnologies. 2018. URL: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf> (дата обращения: 20.03.2022).

4. Шейнов В. П. Психология обмана и мошенничества. – М.: Харвест, 2010. – 464 с.
5. Хэднэги К. Искусство обмана. Социальная инженерия в мошеннических схемах. – М.: Альпина Паблшер, 2020 г. – 430 с.
6. Чалдини Р. Психология влияния. 5-е изд. / Р. Чалдини. – СПб.: Питер, 2014.
7. Коллеров А.С., Синадский Н.И., Хорьков Д.А. Системы обнаружения компьютерных атак / А.С. Колеров. – Горячая Линия-Телеком, 2021. – 124 с.
8. URL: [https://www.gazeta.ru/techzone/2011/10/21\\_a\\_3808934.shtml](https://www.gazeta.ru/techzone/2011/10/21_a_3808934.shtml) (дата обращения: 21.03.2023).
9. URL: <https://www.securitylab.ru/analytics/292473.php> (дата обращения: 30.03.2023).

## References

1. Genprokuratura: v 2020 goduchislozaregistrovannykhkiberprestupleniyvyrosloboleyechemna 76% // D-Russia.ru: yezhedn. internet-izd. 2020. 30 dek. URL: <https://d-russia.ru/genprokuratura-v-2020-godu-chislo-zaregistrovannyh-kiberprestuplenij-vyroslo-bolee-chem-na-76.html> (data obrashcheniya: 19.03.2022).
2. OsnovnyuenapravleniyarazvitiyafinansovogorynkaRossiyskoyFederatsiina 2022 god i period 2023 i 2024 godov // Bank Rossii, 2021. – 107 s.
3. Positive Technologies: Kaksotsial'nayainzheneriyaotkryvayetkhakerudveri v vashuorganizatsiyu // www.ptsecurity.com: saytkompanii Positive Technologies. 2018. URL: <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf> (data obrashcheniya: 20.03.2022).
4. Sheynov V. P. Psikhologiyaobmanaimoshennichestva. – М.: Kharvest, 2010. – 464 s.
5. Khednegi K. Iskusstvoobmana. Sotsial'nayainzheneriya v moshennicheskikhskhemakh. – М.: Al'pinaPablisner, 2020 g. – 430 s.
6. Chaldini R. Psikhologiyavliyaniya. 5-ye izd. / R. Chaldini. – SPb.: Piter, 2014.
7. Kollerov A.S., Sinadskiy N.I., Khor'kov D.A. Sistemyobnaruzheniyakomp'yuternykhatak / A.S. Kolerov. – GoryachayaLiniya-Telekom, 2021. – 124 s.
8. URL: [https://www.gazeta.ru/techzone/2011/10/21\\_a\\_3808934.shtml](https://www.gazeta.ru/techzone/2011/10/21_a_3808934.shtml) (data obrashcheniya: 21.03.2023).
9. URL: <https://www.securitylab.ru/analytics/292473.php> (data obrashcheniya: 30.03.2023).

---

**ХАЛИЛАЕВА Эмине Илимдаровна**, студент 1-го курса магистратуры кафедры «Информационная безопасность» Института информационных технологий Севастопольский государственный университет. Россия, 299053, г. Севастополь, Университетская улица, дом 33. E-mail: emine.halilaeva@yandex.ru

**МАСЛОВА Мария Александровна**, старший преподаватель кафедры «Информационная безопасность» Севастопольский государственный университет. Россия, 299053, г. Севастополь, Университетская улица, дом 33.; аспирант, младший научный сотрудник, Федеральное государственное автономное образовательное учреждение высшего образования Ростовский государственный экономический университет (РИНХ). Россия, 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69. E-mail: mashechka-81@mail.ru

**ГЕРАСИМОВ Виктор Михайлович**, инженер, студент первого курса магистратуры направления «Безопасность систем искусственного интеллекта» факультета Безопасности Информационных Технологий (БИТ), Национального исследовательского университета ИТМО. Россия, 197101, г. Санкт-Петербург, Кронверкский проспект, д. 49. E-mail: my.virus.kaspersky@gmail.com

**KHALILAEVA Emine Ilimdarovna**, 1-year student of the Department "Information Security" Federal State Autonomous Educational Institution of Higher Education Sevastopol State University. Russia, 299053, Sevastopol, Universitetskaya street, 33. E-mail: emine.halilaeva@yandex.ru

**MASLOVA Maria Aleksandrovna**, Senior Lecturer, Department of Information Security, Sevastopol State University. Russia, 299053, Sevastopol, Universitetskaya street, 33.; PhD student, junior researcher Federal State Autonomous Educational Institution of Higher Education Rostov

State University of Economics (RINH). Russia, 344002, Rostov-on-Don, st. BolshayaSadovaya, 69.  
E-mail: mashechka-81@mail.ru

**GERASIMOV Viktor Mikhailovich**, engineer, first-year master's student in the field of "Security of artificial intelligence systems" of the Faculty of Security of Information Technologies (BIT), ITMO Research University. Russia, 197101, St. Petersburg, Kronverksky prospect, 49. E-mail: my.virus.kaspersky@gmail.com