Научная статья
УДК 33
https://doi.org/10.24412/2073-0454-2023-7-237-241
EDN: https://elibrary.ru/idluut
NIION: 2003-0059-7/23-927
MOSURED: 77/27-003-2023-07-126

# Особенности защиты от угроз социальной инженерии

**Артем Витальевич Иванов**
Московский университет МВД России имени В.Я. Кикотя, Москва, Россия, ivanof91@mail.ru

**Аннотация.** Социальные сети занимают все большее место в жизни каждого. Низкий уровень осведомленности пользователей информационных систем об угрозах информационной безопасности повышает риск стать жертвой социальных инженеров. Для противодействия атакам социальных инженеров, необходимо научиться распознавать методы воздействия социальных инженеров, правильно на них реагировать.

**Ключевые слова:** цифровая трансформация, цифровая экономика, информационная безопасность, информационное общество, цифровое развитие

**Для цитирования:** Иванов А. В. Особенности защиты от угроз социальной инженерии // Вестник Московского университета МВД России. 2023. № 7. С. 237–241. https://doi.org/10.24412/2073-0454-2023-7-237-241. EDN: IDLUUT.

Original article

# Features of protection against threats of social engineering

**Artem V. Ivanov**
Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia, ivanof91@mail.ru

**Abstract.** Social networks are taking an increasingly important place in everyone's life. The low level of awareness of information system users about information security threats increases the risk of becoming a victim of social engineers. To counteract the attacks of social engineers, it is necessary to learn how to recognize the methods of influence of social engineers and respond to them correctly.

**Keywords:** digital transformation, digital economy, information security, information society, digital development

**For citation:** Ivanov A. V. Features of protection against threats of social engineering. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2023;(7):237–241. (In Russ.). https://doi.org/10.24412/2073-0454-2023-7-237-241. EDN: IDLUUT.

На рынке информационных услуг существуют компании, оказывающие услуги по обеспечению информационной безопасности путем оценки осведомленности сотрудников, имитации действий нарушителя, направленных на несанкционированное проникновение в информационную систему организаций без нанесения им ущерба. Примером такой компании является Positive Technologies. Они не только оценивают техническую защищенность информационных систем, но и занимаются вопросами осведомленности пользователей информационных систем в вопросах информационной безопасности. Компания-заказчик с помощью услуг Positive Technologies может оценить надежность своих сотрудников, а также степень защищенности своей информационной системы от воздействия злоумышленников, использующих методы и приемы социальной инженерии.

Имитация действия нарушителя без нанесения ущерба — один из самых эффективных способов, позволяющий оценить степень защищенности системы. Если пентест (тестирование на проникновение в систему) позволяет обнаружить недостатки в работе программно-аппаратной стороны системы, то имитация действия нарушителя помогает узнать, насколько подготовлены сотрудники организации в сфере информационной безопасности. Этот метод набирает популярность, поскольку киберпреступники постепенно начинают применять приемы и методы социальной инженерии.

По итогу проведения таких работ, руководители компании или главы отделов внутренней безопасности могут выявить потребность в обучении сотрудников или необходимости использования более усовершенствованного программного обеспечения.

Этапы.

1. Сбор данных, формирование фокус-групп. Первоначально проводится сбор данных об организации. В определенных случая заказчик сам предоставляет все необходимые данные о сотрудниках, адресах их электронных почт, адреса страниц в социальных сетях.

2. Создание сценариев атаки. Все условия работы изначально обсуждаются персональные условия с заказчиком. Сценарий любой атаки формируется непосредственно под заказчика и его компанию.

3. «Доставка». В большинстве случаев хватает доставки фишинговых писем на рабочие или персональные электронные адреса сотрудников.

4. Сбор статистических данных. Суть схемы заключается в следующем: во вложениях писем прикреплены безопасные ссылки. В системе фиксируется: кто и когда перешел по указанному адресу, какие действия он выполнял, вводил ли пароль, скачал и запустил файл или нет. Все эти данные необходимы для получения объективной оценки осведомленности пользователя.

5. Анализ результатов. Завершающий этап проверки. Проводится оценка полученных данных. Учитывается, какой процент сотрудников совершил то или иное потенциально опасное действие, по какому сценарию удалось достичь лучших результатов, какая фокус-группа себя лучше проявила, а какая фокус-группа менее подготовлена в сфере защиты от угроз информационной безопасности. В соответствии с итогами работы сотрудники Positive Technologies выставляют рекомендации, направленные на повышение все уровней информационной безопасности. Заказчику поступает документ с исчерпывающей информацией о ходе и результатах проверки.

Примеры атаки.

Перед тем, как начать атаку на сотрудников организации проводится тестовая рассылка с целью вступить в контакт с сотрудниками. Собирается информация об электронных адресах, стиле общения, подписях к сообщениям, чтобы позже в таком же стиле проводить уже финальную рассылку. Допустим, в компании все внутренние сообщения отправляются с использованием синего шрифта Arial 16 размера, а подпись отделена знаком «-------». Соответственно, получив письмо в таком же стиле, сотрудник с большей вероятностью воспримет его как обычное письмо, полученное от начальника своего отдела, к примеру.

Статистика показывает, что IT-специалисты и даже специалисты в области обеспечения информационной безопасности вступают в диалог с сотрудниками Positive Technologies, выдавая им информацию о компании, свои данные. Риску стать жертвой атаки социальных инженеров подвержены даже самые опытные и осведомленные сотрудники организаций (рис. 1).

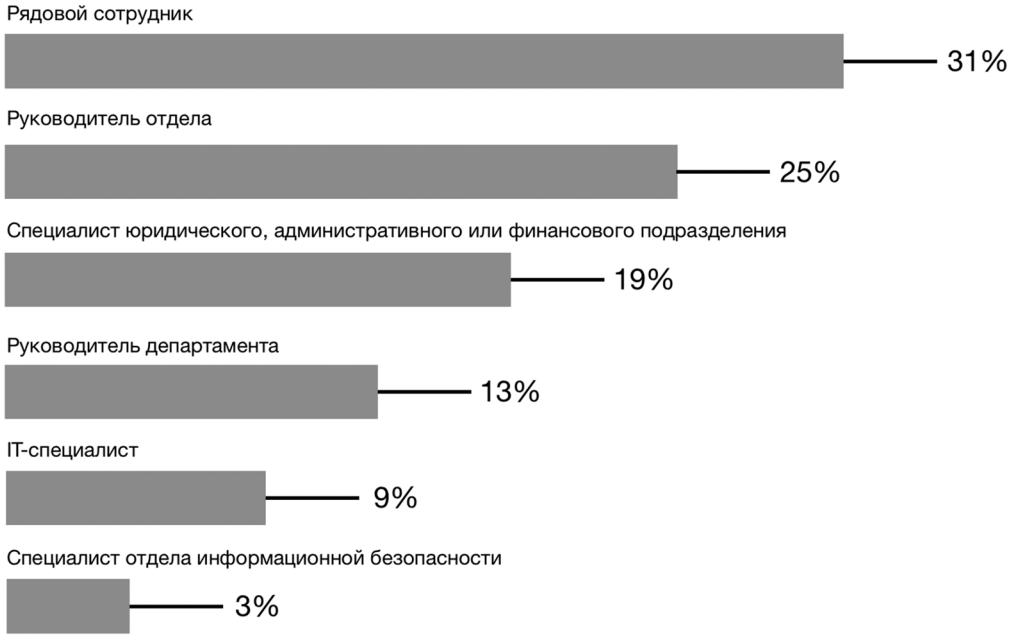


*Рис. 1. Должности сотрудников, вступивших в переписку*

Пример № 1.

Сотруднику на служебную или личную почту приходит письмо (рис. 2) со знакомого электронного адреса, в котором указана цепляющая тема, как правило, касающаяся рабочего процесса, само письмо оформлено в привычном деловом стиле.

В письме размещена ссылка, по которой сотрудника просят перейти и сделать необходимые операции.

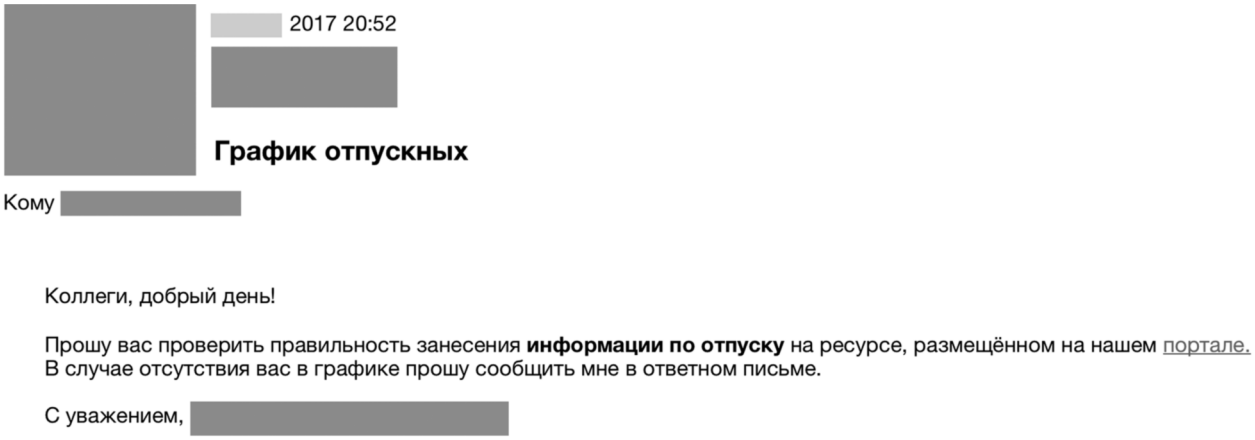


*Рис. 2. Письмо с вредоносной ссылкой*

Сама ссылка ведет на ресурс, оформленный в стиле компании сотрудника или другого известного сервиса. Когда пользователь переходит по ссылке, перед ним открывается окно авторизации, и очень часто пользователи спокойно вводят свои персональные учетные данные, после чего сайт перестает отвечать.

Пример № 2.

Сотруднику организации на почту пришло письмо (рис. 3) с вложенным файлом.

Скачав файл, открыв его, пользователь запускает у себя на рабочей станции вредоносную программу. В случае Positive Technologies во вложенном файле размещена программа, которая после запуска отправляет в аналитический центр компании информацию о запуске вложенного файла. Никакого вреда эта программа не несет.

Результаты, отраженные на диаграмме (рис. 4), дают понять, что каждый шестой сотрудник совершает действие, которое предоставляет доступ третьим лицам к его персональным данным, личной учетной записи, а если рабочие станции организации связаны локальной сетью, то действие пользователя может заразить и другие компьютеры сети. Если атака совершается на крупные компании, то счет идет на сотни или даже тысячи зараженных компьютеров.

Выбор темы письма.

Результативность рассылки очень часто зависит от выбранной темы. Поскольку тема, это первое,

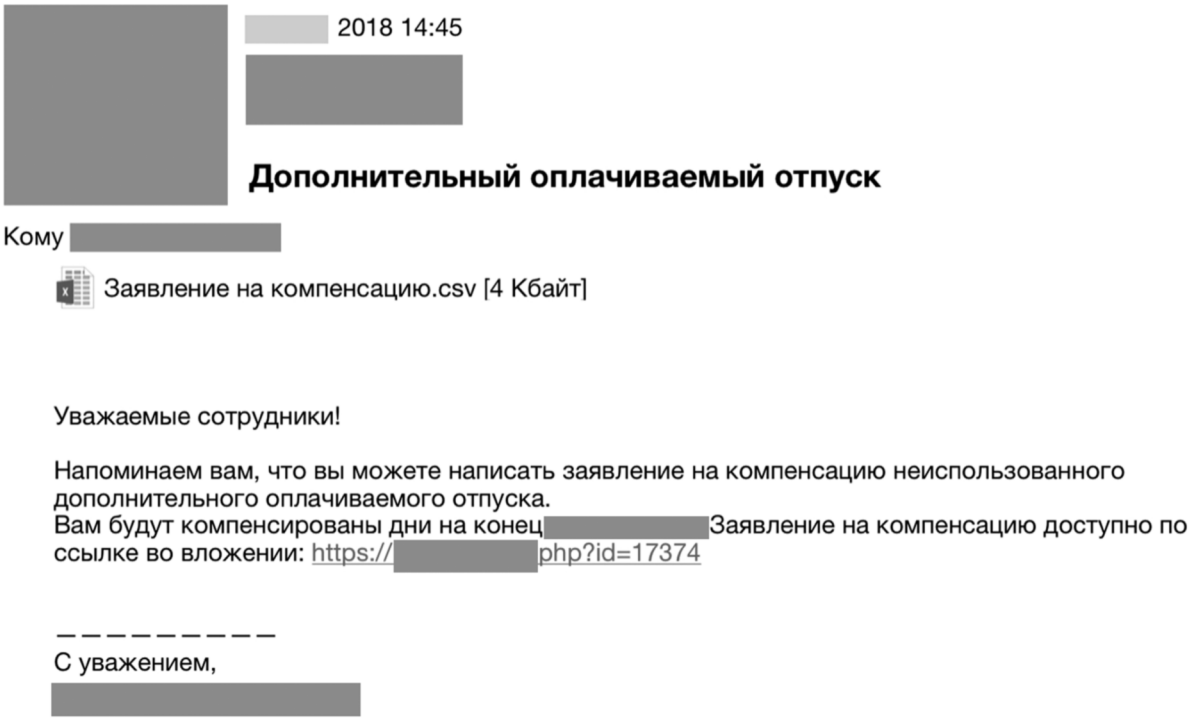


*Рис. 3. Письмо с вложенным файлом*


*Рис. 4. Результаты тестирования*

что увидит пользователь, получивший новое сообщение. Самые распространенные варианты тем представлены на рис. 5.

Сотрудники Positive Technologies при выборе сценария атаки стараются подходить к жертвам индивидуально и персонализировать выбранную тему под каждую компанию. Проводится анализ прошедших мероприятий, актуальных событий: различные корпоративы, акции.

Что предлагает Positive Technologies в качестве защиты от утечки конфиденциальной информации:

1) использовать антивирусное ПО с «песочницей»;

2) проверять предлагаемые ссылки из писем;

3) блокировка вложений по почте с расширениями для исполняемых, системных, скриптов и других файлов.

Рассмотренные методы и приемы психологического воздействия на людей являются актуальными угрозами в настоящее время. Информация приобрела колоссальную важность. Доступ к интересующей информации злоумышленникам становится получать намного проще с развитием социальных сетей, поскольку жертвы их атак сами выкладывают в сеть все свои данные. Социальная инженерия может стать опасным оружием в руках злоумышленников.

Не повышая свой уровень информационной осведомленности в соответствии с современными требованиями информационной безопасности, пользователи информационных систем рискуют стать жертвами атак социальных инженеров. На сегодняшний день история насчитывает множество громких примеров атак злоумышленников на крупные корпора-

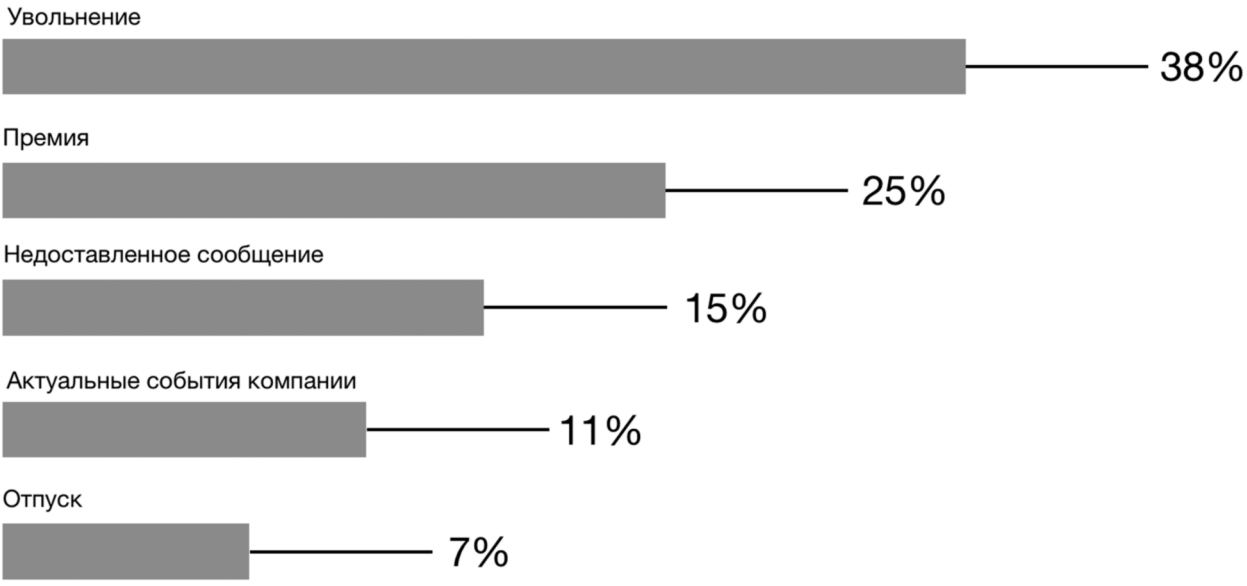


*Рис. 5. Темы тестовых писем*

ции, когда по вине всего одного или нескольких человек компании несли миллиардные убытки, преступники получали доступ к конфиденциальной информации. Необходимо тщательно анализировать совершенные ошибки и на основании их создавать методы защиты от воздействия социальных инженеров, обучать этим навыкам пользователей. Но полностью избавиться от данной проблемы невозможно до тех пор, пока у человека есть доступ к информационным системам, конфиденциальной информации.


**Библиографический список**

1. Ассанж Дж., Мюллер-Магун Э., Аппельбаум Дж., Циммерман Ж. Шифропанки. Свобода и будущее Интернета. М. : Азбука, 2015.

2. Касперски К. Секретное оружие социальной инженерии // URL://http://citforum.ru/security/articles/soc_eng/

3. Лобель Т. Теплая чашка в холодный день. Как физические ощущения влияют на наши решения. М. : Альпина Паблишер, 2016.

4. Попов А. А. Эргономика пользовательских интерфейсов в информационных системах: учеб. пособие. М. : РУСАЙНС, 2016.

5. Фейнман Р. Радость познания (The pleasure of finding things out). М. : АСТ, 2013.

6. Шишкова С. Социальная инженерия // URL://http://www.executive.ru/knowledge/announcement/345004/

7. Christopher Hadnagy, Paul Ekman. Unmasking the Social Engineer: The Human Element of Security. San-Francisco : Wiley, 2014.

8. Peter Kim. The Hacker Playbook: Practical Guide to Penetration Testing. New York : Kindle Edition, 2014.

**Bibliographic list**

1. Assange J., Muller-Magun E., Appelbaum J., Zimmerman J. Cipherpunk. Freedom and the future of the Internet. M. : ABC, 2015.

2. Kaspersky K. The secret weapon of social engineering // URL://http://citforum.ru/security/articles/soc_eng/

3. Lobel T. A warm cup on a cold day. How physical sensations affect our decisions. M. : Alpina Publisher, 2016.

4. Popov A. A. Ergonomics of user interfaces in information systems: textbook. the manual. M. : RUSAINS, 2016.

5. Feynman R. The Joy Of knowing (The pleasure of finding things out)). M. : AST, 2013.

6. Shishkova S. Social engineering // URL://http://www.executive.ru/knowledge/announcement/345004/

7. Christopher Hadnagy, Paul Ekman. Unmasking the Social Engineer: The Human Element of Security. San-Francisco : Wiley, 2014.

8. Peter Kim. The Hacker Playbook: Practical Guide to Penetration Testing. New York : Kindle Edition, 2014.



**Информация об авторе**

**А. В. Иванов** — доцент кафедры экономической безопасности, финансов и экономического анализа Московского университета МВД России имени В.Я. Кикотя, кандидат экономических наук.

**Information about the author**

**A. V. Ivanov** — Associate Professor of the Department of Economic Security, Finance and Economic Analysis of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Candidate of Economic Sciences.



Статья поступила в редакцию 08.11.2023; одобрена после рецензирования 29.11.2023; принята к публикации 14.12.2023.

The article was submitted 30.11.2023; approved after reviewing 29.11.2023; accepted for publication 14.12.2023.