УДК 004.056
ББК 32.841

**Р. А. Файрузов,**
**А. Ю. Сорокин**

# Социотехническое тестирование компании, как средство определения уровня осведомлённости сотрудников компании

*Национальный Ядерный Исследовательский Университет МИФИ*
*Российский Государственный Социальный Университет*
*г. Москва*

***Аннотация**: В настоящей статье, рассмотрена проблема осведомлённости сотрудников компании в сфере информационной безопасности. Рассматривается социотехническое тестирование компании, как средство для определения уровня осведомлённости персонала в области информационной безопасности для своевременного выявления пробелов в этой области и планирования мероприятия по повышению уровня осведомлённости сотрудников.*

***Ключевые слова**: Информационная безопасность, осведомлённость сотрудников, социотехническое тестирование персонала.*

## Введение

На сегодня технический прогресс продвинулся далеко вперёд. Организации, заинтересованные в обеспечении информационной безопасности, зачастую стараются обойтись техническими, программными и организационными мерами, забывая про самое слабое звено, которым всегда были и являются люди, а именно персонал компании. Компании ежегодно инвестируют миллионы долларов в новейшие продукты безопасности, от межсетевых экранов до систем контроля доступа, но они забывают или не в состоянии инвестировать в свои самые ценные ресурсы для обеспечения своей безопасности — в частности, в своих сотрудников. Слишком часто обучение вопросам информационной безопасности — это событие бывает раз в год и связанно с незанятым и устаревшим материалом, который в значительной степени игнорируется. В результате сотрудники не понимают современных атак и их последствий. Этот пробел в знаниях предоставляет бесконечные возможности для злоумышленников.

Технологии безопасности, используемые в организациях и в которые вкладываются большие деньги, — межсетевые экраны, устройства идентификации, средства шифрования, системы обнаружения сетевых атак и другие — малоэффективны в противостоянии хакерам, использующим методы социальной инженерии. Социальная инженерия при рассмотрении информационной безопасности означает психологическое манипулирование сотрудником с целью заставить его выполнять действия, необходимые для социального инженера или для получения доступа к конфиденциальной информации. В связи с этим в основе методов и техник социальных инженеров заложено использование слабых сторон человеческой психики, что является крайне разрушительным в рамках организации.

На сегодня одной из наиболее распространённых видов такого рода атак является *фишинг*. Согласно [4] ущерб от фишинга, только на 2016–2017 годы в мире, оценивается в миллиарды долларов США. А также, согласно статистике, каждый год число фишинговых атак увеличивается примерно в полтора раза. По данным [2], на компьютерах пользователей было зарегистрировано 39,23 миллиона

срабатываний системы антифишинга против 42,2 миллиона по итогам предыдущего квартала, сказал представитель «Лаборатории Касперского». По его словам, в России число таких попыток увеличилось за квартал на 23,5% с 5,4 миллиона до 6,67 миллионов. В квартале 8,26% пользователей продуктов Kaspersky Internet в мире были атакованы фишерами. В то же время, если раньше их атаки были основаны на невнимательности пользователя, а также на низкой интернет—грамотности, то с ростом осведомлённости пользователей в сфере информационной безопасности фишеры должны придумывать новые уловки. Сумма ущерба, причинённого фишингом, не была оценена аналитиками «Лаборатории Касперского».

Возрастает процент целевых фишинговых атак, организованных путём распространения писем по электронной почте, в которых можно выделить конкретную организацию или группу лиц. Целевые пользователи получают тщательно разработанные фишинговые сообщения, заставляющие человека вводить конфиденциальные персональные сведения, такие как логин и пароль, которые дают доступ к корпоративным сетям или базам данных с важной информацией. Помимо запроса учётных данных, целевые фишинговые письма также могут содержать вредоносное программное обеспечение.

Причиной данной проблемы является низкий уровень осведомлённости сотрудников в вопросах противодействия фишинговым атакам. В целях снижения вышеперечисленных рисков, компании могут оценить уровень осведомлённости персонала компании в области информационной безопасности, который позволит своевременно выявлять пробелы в данной области и планировать мероприятия (тренинги и обучение персонала) по повышению уровня осведомлённости сотрудников в вопросах, связанных с противодействием фишингу. Планомерное многократное проведения социотехнического тестирования компании для определения и повышения уровня осведомлённости сотрудников об угрозах информационной безопасности позволит сократить негативные последствия, которые связанны с деятельностью организации: финансовые, технические, операционные и т. д.

## Социотехнический тест на проникновение

«Тест на проникновение проводится с использованием методов социальной инженерии. Основная цель теста –– определить уровень осведомлённости сотрудников в вопросах информационной безопасности. В процессе тестирования определяется реакция пользователей и сотрудников, ответственных за информационную безопасность, на организационные методы проникновения, используемые злоумышленниками» [3]. Организационные аспекты информационной безопасности является важной частью системы защиты, и чаще всего обычные пользователи являются самым слабым звеном. Результаты социотехнического

тестирования будут определять те организационные аспекты информационной безопасности, на которые, в первую очередь, следует обратить внимание Заказчику.

Результаты, полученные в ходе выполнения работ, могут стать основой для разработки программы повышения осведомлённости о безопасности, которая максимально ориентирована на проблемные области, выявленные во время проведения тестирования, а также может быть полезна для проверки эффективности текущей программы осведомлённости Заказчика.

В общем случае порядок проведения работ делится на следующие категории:

*1. Внешний нарушитель;*

*2. Внутренний нарушитель;*

*3. Оценка осведомлённости.*

Разница между «Внутренним нарушителем» и «Внешним нарушителем» в том, что у первого изначально есть определённый набор знаний, сведения о компании (структура, новости, почта, инсайды, формат электронной почты, электронных сообщений, шаблоны документов и т. д.), сведения о сотрудниках (ФИО, должность, адрес электронной почты, номера телефонов), а у «Внешнего нарушителя» этого всего нет и ему требуется какое—то время, чтобы собрать эти данные, в большинстве случаев используется методы конкурентной разведки.

«Оценка осведомлённости» — процесс имитации угрозы на компанию, задачей «оценки осведомлённости» никогда не стоит получение доступа во внутреннюю сеть, проведение тестирования на проникновение с использованием человеческого фактора, этот процесс направлен на получение среза статистики компании о количестве успешных имитаций атак на сотрудников компании. С клиентом согласовываются методы социальной инженерии, которые будут использоваться во время теста. Например, отправка почтовых / мгновенных сообщений от имени анонимных пользователей и сотрудников Заказчика, содержащих ссылки на веб—ресурсы с исполняемым кодом, который содержится в теле письма, запрос на изменение пароля, отправку пароля или свою персональную информацию и пр.; От заказчика потребуется введения белого списка (антиспам и т. д.) для лучшего качества статистики [1].

План работы выглядит следующим образом:

*1. Сбор данных:*

А) Данные, списки сотрудников от заказчика;

Б) Google, Linkedin (FOCA, Maltego), Active Directory, Twitter, Facebook, Email Providers, etc;

В) SMTP: vrfy, expn;

Г) Bruteforce.

*2. Создание сценариев рассылки:*

А) Многолетние «best cases» с определённой поправкой относительно организации и фирменный стиль (известные фамилии, шаблоны писем);

Б) «Личные» пожелания заказчика.

3. *Создание нагрузок к сообщениям (Win oriented):*

А) Макросы (macro);

Б) mht / chm+ zip;

В) exe / bat / vbs / ps /;

Г) ExternalResourse;

Д) Вредоносная программа (malware);

Е) Фишинг.

4. *Процесс рассылки "Simple Mail Transfer Protocol" (SMTP):*

А) отправка электронной почты с использованием ptsecurity.ru / DigitalOcean;

Б) зарегистрировать собственный фишинговый домен: Например news.c0mpany.com;

В) XSS on company.com;

Г) Учётная запись AD + outlook web access (OWA).

*5. Сбор и обработка статистических данных:*

А) HTTP / DNS;

Б) IntranetHTTP;

В) Разница между целями социотехнического тестирования и оценки осведомлённости.

*6. Интерпретация полученных данных;*

Результатом работы будет являться отчёт, содержащий:

- Выводы для руководства, содержащие общую оценку уровня осведомлённости персонала.
- Методику проведения теста.

Список основных проблемных областей (включая информацию обо всех действиях пользователя в каждой целевой группе).

Рекомендации по устранению выявленных проблемных областей. Проверки в области социальной инженерии осуществляются с использованием одного или нескольких каналов взаимодействия с сотрудниками: электронная почта, личное

общение, социальные сети, системы обмена мгновенными сообщениями. На практике специалисты используют специальные целенаправленные фишинговые атаки.

Совокупность методов социотехнического тестирования компании для определения уровня осведомлённости сотрудников об угрозах информационной безопасности с использованием методов обучения в конечном итоге позволит сократить негативные последствия, которые связанны с деятельностью организации: финансовые, технические, операционные и т. д.

Так же стоит отметить направление создания механизма, способного совмещать социотехническое тестирование с элементами обучения сотрудников, в автоматизированном режиме позволит снизить стоимость обучения и повысить эффективность обучения за счёт многократных проверок и оценок уровня осведомлённости сотрудников, а это поможет избежать высоких издержек для компании.

## Заключение

Подводя итоги вышеописанного, стоит сказать, что использование социотехнического тестирования компании с целью определения и дальнейшего повышения уровня осведомлённости сотрудников в сфере информационной безопасности и дальнейшего повышения поможет многим компаниям избежать больших убытков и негативных последствий как финансовом плане, так и в операционном.

## Литература

1. Астахова Л. В., Н. Л. Ульянов. Модель политики управления осведомленностью сотрудников организации в области информационной безопасности. // Наука ЮУрГУ: материалы 67–й научной конференции. Секция технических наук. – С. 678–681.
2. Гудкова Д. Н., Демидова Н. Т., Вергелис М. И. Спам и фишинг в четвертом квартале 2017. [Электронный ресурс]. – Электронные текстовые данные – Москва, ноябрь 2, 2017. – Режим доступа: https://securelist.ru/spam–and–phishing–in–q4–2017/30565/ (Дата обращения 04.01.2018).
3. Романенко Е. А., Тимофеев Д. С. Методы обучения персонала по вопросам информационной безопасности. // Наука ЮУрГУ: материалы 67–й научной конференции. Секция технических наук. – С. 641–645.
4. Jonathan C.A. Phishing by the Numbers: Must–Know Phishing Statistics 2017 [Электронный ресурс]. – Электронные текстовые данные – New York, 2017. – Режим доступа: https://blog.barkly.com/phishing–statistics–2017 (Дата обращения 20.11.2017).