ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2022-49-4-85-96 Обзорная статья / Review article

Защита от атак с применением средств и методов социальной инженерии

В.А. Репенко,[1] С.А.Резниченко[1,2,3,4]
[1]Национальный исследовательский ядерный университет «МИФИ»,
[1]115409, г. Москва, Каширское шоссе, 31, Россия,
[2]Финансовый университет при Правительстве РФ,
[2]125993, г.Москва, Ленинградский пр–кт, 49, Россия,
[3]Российский государственный университет нефти и газа
(национальный исследовательский университет) им. И.М. Губкина,
[3]119991, г. Москва, Ленинский пр-кт, 65, корпус 1, Россия,
[4]Российский государственный гуманитарный университет,
[4]125047, г. Москва, Миусская площадь, д. 6, Россия

Резюме. Цель. В современном мире активно развиваются инновационные технологии, коммуникации переходят в интернет-пространство. Тем не менее новые технологии оказались востребованными и в сегменте организаций, физических лиц, кибер-мошенников и хакеров. Цель исследования заключается в анализе сущности и структуры современной социальной инженерии, в том числе, обратного социального инжиниринга в условиях цифровизации общества. **Метод.** Адаптируя исследование к текущему моменту, уточняется, что технологии, разработки и манипулятивные социологические тактики подхватываются не просто хакерами, но и последователями радикальных идей. **Результат.** Предложено оптимальное определение термина «социальная инженерия» – выявление и эксплуатация некомпетентности, недостаточного профессионального уровня или халатности сотрудников организации или частных лиц для получения несанкционированного доступа к конфиденциальным данным; совокупность технологий, базирующихся на использовании психологической специфики человека. **Вывод.** Новизна исследования состоит в углубленном исследовании классификации видов атак с использованием методов социальной инженерии и рекомендациях по противодействию и профилактике им.

Ключевые слова: социальная инженерия, обратная социальная инженерия, киберпреступник, информационные системы, интернет, техники манипуляции, пользователи, программное обеспечение

Для цитирования: В.А. Репенко, С.А. Резниченко. Защита от атак с применением средств и методов социальной инженерии. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(4):85-96. DOI:10.21822/2073-6185-2022-49-4-85-96

Protection against attacks using social engineering tools and methods

V.A. Repenko[1], S.A. Reznichenko[1,2,3,4]
[1] National Research Nuclear University "MEPhI", (Moscow Engineering Physics Institute),
[1]31, Kashirskoe Highway, Moscow 115409, Russia,
[2] Financial University under the Government of the Russian Federation,
[2]49, Leningradsky Ave., Moscow 125993, Russia,
[3] Gubkin Russian State University of Oil and Gas (National Research University),
[3]65, Leninsky Ave., building 1, Moscow 119991, Russia,
[4] Russian State University for the Humanities,
[4]6, Miusskaya Square, Moscow 125047, Russia

Abstract. Objective. In the modern world, innovative technologies are actively developing,

communications are moving into the Internet space. Nevertheless, new technologies turned out to be in demand in the segment of organizations, individuals, cyber fraudsters and hackers. The purpose of the study is to analyze the essence and structure of modern social engineering, including reverse social engineering in the context of the digitalization of society. **Method.** Adapting the study to the current moment, it is clarified that technologies, developments and manipulative sociological tactics are picked up not just by hackers, but also by followers of radical ideas. **Result.** The optimal definition of the term "social engineering" is proposed - the identification and exploitation of incompetence, insufficient professional level or negligence of employees of an organization or individuals to obtain unauthorized access to confidential data; a set of technologies based on the use of the psychological specifics of a person. **Conclusion.** The novelty of the study lies in an in-depth study of the classification of types of attacks using social engineering methods and recommendations for countering and preventing them.

Keywords: social engineering, reverse social engineering, cyber criminal, sociology, digitalization, information systems, Internet, manipulation techniques, users, software

For citation: V.A. Repenko, S.A. Reznichenko. Protection against attacks using social engineering tools and methods. Herald of the Daghestan State Technical University. Technical Science. 2022; 49 (4): 85-96. DOI: 10.21822 /2073-6185-2022-49-4-85-96

Введение. Сведения, которые обеспечивают их собственнику конкретную выгоду, помогают избежать чрезмерных затрат, а также обеспечить устойчивое рыночное положение, являются предметом повышенного интереса кибер-преступников и должны быть надежно защищены. По мнению экспертов, самым незащищенным и уязвимым сектором системы обработки данных является персонал компании и физические лица [1-4].

Для оказания нужного кибер-мошеннику воздействия на потенциальную жертву приходится использовать все более изощренные способы и методы атак. В частности, для проведения несанкционированных действий по получению доступа к конфиденциальной информации особый упор ставится на специфику человеческого фактора.

Цель социальной инженерии заключается в обеспечении таких действий человека, которые бы он никогда не совершил в обычных условиях: разглашение данных конфиденциального характера; переходы на сомнительные сайты; добровольное согласие на скачивание и установление вредоносного программного обеспечения [5-16].

Социальный инжиниринг является достаточно молодой наукой. Автором первого научного обоснования выступил австрийский ученый К. Поппер в собственных исследованиях «Открытое общество» и «Нищета историцизма». В частности, в трактовке К. Поппера, социальная инженерия представляет собой «совокупность походов прикладной социологии, направленных на рациональное изменение социальных систем на основе фундаментальных знаний об обществе и предсказании возможных результатов преобразований» [17].

Отметим, что в той или иной форме человечество на протяжении тысячелетий использовало методы социального инжиниринга. Еще во времена Древнего Рима и Древней Греции был большой спрос на тех, кто мог ввести в заблуждение вторую сторону и обманом добиться ложной убежденности собеседника и нужных результатов. В частности, прямое использование таких людей много раз предотвращало вооруженные конфликты и находило дипломатический выход из крайне сложных положений.

Однако настоящий рассвет науки социальной инженерии пришелся на 50-60-е гг. XX в. в США и Великобритании. Например, приемы социнжиниринга широко задействовали спецслужбы перечисленных государств, которые и обеспечили социальной инженерии как научному направлению социологии глобальный практический характер. В данном случае, целью американских и британских спецслужб выступало создание и апробация технологий манипулирования человеческим сознанием [10].

70-е годы XX в. отметились стремительным развитием фрикинга – технологии, пред-

ставляющей собой набор методов и приемов по взлому уличных телефонных аппаратов, после чего методы социальной инженерии позволяли осуществлять управление телефонными сетями. К концу десятилетия фрикинг-мошенники стали настолько изощренными при использовании техник манипулирования операторами телефонных линий, что могли получить любые сведения.

Наиболее квалифицированные специалисты в области социальной инженерии всегда предпочитали работать экспромтом, основываясь на собственной интуиции, пользуясь практикой наводящих вопросов. Применяя определенные интонации голоса, такие люди могли выявить все страхи и комплексы конкретного лица и моментально выработать правильную стратегию их эксплуатации для достижения личного результата. Другими словами, использовался строго индивидуализированный подход.

Постановка задачи. В области информационных технологий социальный инжиниринг возник в качестве практической области обнаружения уязвимостей. Именно после того, как эксперты информационной безопасности стали едины во мнении, что максимальные риски информационных систем и технологий относятся к человеческому фактору, было принято решение использовать психологию влияния, манипулятивные технологии и тактику социальной инженерии.

Цифровизация же общества и перенос коммуникативных связей в интернет обусловил переход в цифровую сферу и практической социальной среды.

Цель исследования заключается в анализе сущности и структуры современной социальной инженерии, в том числе, обратного социального инжиниринга в условиях цифровизации общества.

Методы исследования. ИТ-системы пребывают в динамичном состоянии, оборудование и программные продукты непрерывно совершенствуются и усложняются. Для того, чтобы владеть ситуацией не только в рамках атаки, но и при защите, принципиально важно отслеживать новые тренды отрасли и просто быть в теме ИТ-бекграунда в принципе. Это и есть дорога развития классического хакера, который сегодня максимально романтизирован.

В настоящее время в хакерской группе присутствуют несколько узких специалистов, досконально владеющими конкретными технологиями конечной цели. Тем не менее, практически всегда главная задача состоит во взломе периметра защиты.

Рис. 1 демонстрируют объекты хакерских атак в 2021 г.

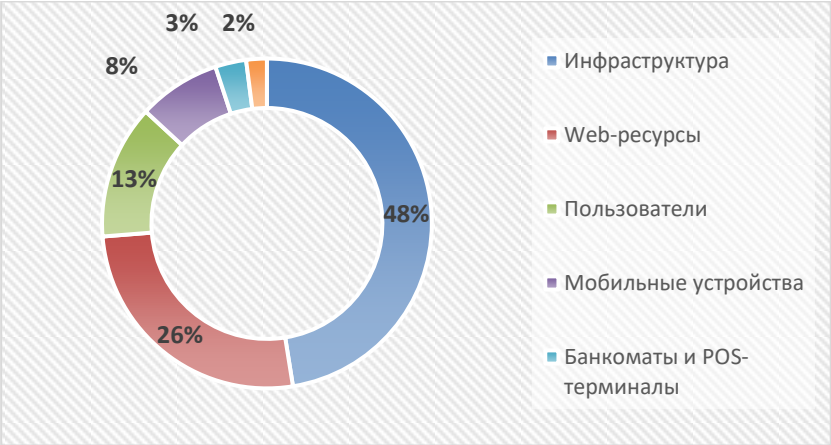

Рис. 1. Объекты хакерских атак в 2021 г. [7]
Fig. 1. Objects of hacker attacks in 2021

Рис. 2, в свою очередь, конкретизирует методы атак и место социальной инженерии в общей структуре киберпреступлений. Именно это и обуславливает актуальность социнжиниринга, который обязательно будет востребован.

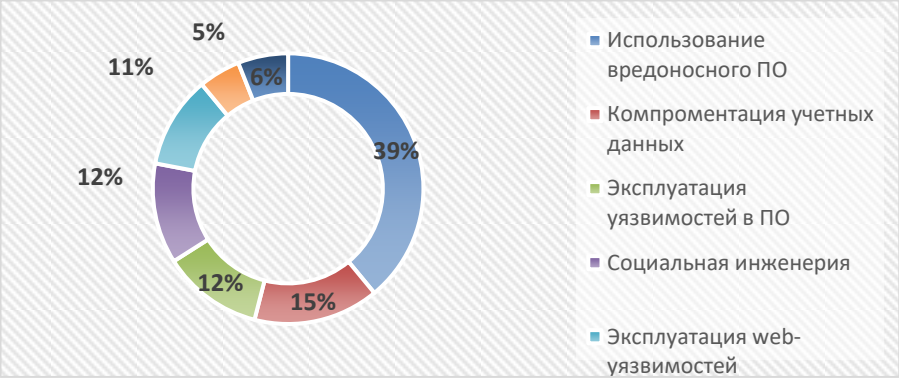

Рис.2. Методы хакерских атак в 2021 г. [7]
Fig. 2. Methods of hacker attacks in 2021

На первой стадии осуществляется сбор данных и подготовка, а уже на втором этапе сверху накладываются технологии и углубленное знание ИТ-систем.

Считается, что в отделе кибербезопасности компании все сотрудники делятся на две группы:

1) параноиков, которые в полной мере осознают, каким количеством ценной информации владеет персонал;

2) циников, у которых совершенно нет веры в благоразумие и осторожность остальных сотрудников.

Именно специалисты отдела кибербезопасности занимаются разграничением прав пользователей, разрабатывает инструкции и регламенты, а также осуществляют обработку критических ситуаций в реальности.

Все перечисленное дает возможность сформировать у сотрудников компании определенному иммунитет к интернет-мошенническим проявлениям, тем не менее, не гарантирует высокого уровня защиты. Главным недостатком выступает тот факт, что социнжиниринг не позволяет «поставить патч» и больше не контролировать процессы – однажды доказавшая свою эффективность киберпреступникам механика будет эффективна и вероятна всегда, поскольку поведение индивидов, в принципе, не претерпевает радикальных изменений.

Обсуждение результатов. Данные Центрального банка России свидетельствуют, что социальная инженерия является основным способом хищений со счетов в учреждениях банков и темп роста таких преступлений в данной сфере только возрастает (рис. 3).

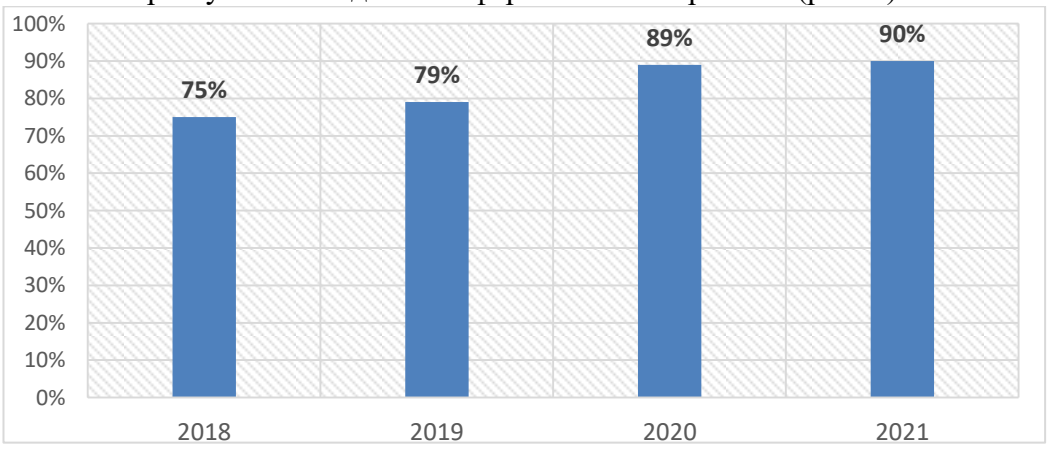

Рис. 3.Динамика количества хищений с банковских счетов, осуществленных методами социальной инженерии в 2019-2021 гг. [16]
Fig. 3. Dynamics of the number of thefts from bank accounts carried out by social engineering methods in 2019-2021

Также Центральный Банк России считает, что в ближайшем будущем острая ситуация вряд ли поменяется кардинальным образом и кибер-мошенники продолжат эксплуатировать феномен кибернеграмотности граждан России.

Поэтому регулятор предлагает криминализировать в Уголовном кодексе Российской Федерации нормы, предусматривающие уголовную ответственность за социальную инженерию и фишинг. В свою очередь, Министерство внутренних дел РФ категорически против того, чтобы вводить в УК РФ дополнительное количество статей. Аргументом служит тот факт, что действующие нормы уже предусматривает ответственность за следующие деяния [1]:

1) «ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации»;

2) ст. 1593 УК РФ «Мошенничество с использованием электронных средств платежа»;

3) ст. 158 «Мошенничество».

Существует значительное количество разновидностей атак с использованием социальной инженерии, по состоянию на сентябрь 2022 г. классифицируют не менее 10 разновидностей. Если принимать во внимание и комбинированные способы, то общее количество видов атак достигает нескольких десятков. Именно поэтому принципиально важно не просто знать о ее существовании, но и детально разобраться в том, как она работает. Именно получив навык идентифицировать главный механизм действия, появляется возможность повысить эффективность распознавания атак такого типа:

1. Фишинг. Термин происходит от английского слова «fishing» – рыбалка, выуживание. Данный тип атаки представляет собой интернет-мошенничество, осуществляемое ради того, чтобы заполучить доступ к конфиденциальной информации пользователей. Как правило, первоочередной интерес представляют собой сетевые учетные данные, данные банковских карт, логины и пароли, которые добываются у доверчивых пользователей с помощью предложных сайтов и web-страниц.

Акцентируем внимание на том, что иногда кибер-преступнику достаточно данных или других личных сведений о пользователе-жертве. Но иногда фишинговые письма своей целью имею получение регистрационных данных конкретного работника или прочих сведений, которые будут использованы при расширенной атаки на определенную компанию.

В том числе фишинговая атака может проводиться так, что после перенаправления пользователя на ложный сайт появится еще ряд проблем:

а) на ПК будет автоматически установлено вредоносное программное обеспечение;

б) система откажется функционировать из-за атаки софта-вымогателя.

2. Ловля на «живца». В рамках данного типа атак злоумышленник, ловец, оставляет приманку, которая может представлять собой флешку, зараженную вирусом. Обнаруживший ее пользователь, движимый чувством любопытства, наверняка вставит флешку в свой ПК, после чего вирус уничтожает систему. Утоним, что есть флешки, которые могут повредить ПК – зарядка такого ИТ-аксессуара производится USB-порт, после чего происходит высвобождение сверхмощного заряда посредством устройства ввода. По состоянию на начало 2022 г. стоимость такой флешки в Даркнете составляла всего 54 доллара [14].

3. Кви про кво. Термин происходит от латинского «Quid pro quo», что в переводе означает «то за это». В соответствии с данным методом проведения кибератаки преступник звонит в компанию по корпоративному телефону. Как правило, он называет себя специалистов технической поддержки компании, который интересуется наличием проблем, которые должны быть срочно исправлены. Под легендой решения озвученных пользователем проблем преступник мотивирует сотрудника ввести конкретный набор команд, предоставляющих в будущем удаленный доступ к его рабочему месту.

4. Троян или вирус «Троянский конь». Представляет собой вредоносный код, который проникает в ПК сотрудника, полагающего, что идет установка или обновление программных продуктов.

5. Претекстинг. Метод заключается в применении интернет-мошенником предлога, который заставляет жертву предоставить конфиденциальные данные. В частности, банальный интернет-опрос может привести к выведыванию финансовых или банковских данных.

Важность более детального исследования фишинга подтверждается статистикой отчета о

киберпреступности, проведенного США, в котором указывается, что именно фишинговые атаки стали причиной потери частными лицами и организациями не менее 58 млн. долл. Общая численность жертв фишинга составила 115 тысяч [15]. Подчеркнем, что эти данные касаются только США, глобальная статистика же многократно выше.

Известны следующие виды фишинговых кибератак:

- **целевой или Spear Phishing** – с первого взгляда может напоминать стандартный фишинг, однако целью выступает конкретный человек или компания. Поэтому на первоначальном этапе злоумышленники осуществляют сбор детальной информации о том, кто является целью, после чего идет рассылка электронных писем, правдоподобно адаптированных под интересы конкретизированной жертвы. Эксперты, как правило, называют данную разновидность фишинга самой продвинутой, поскольку при его реализации следует серьезная проработка цели. Именно поэтому так сложно выстроить эффективную защиту против целевой фишинговой атаки. Уточним, что обычно лицо, которое выбрано объектом такой атаки – не конечная реальная цель кибер-мошенников. Обычно реальной целью является корпоративная сетевая инфраструктура, контроль над которой даст возможность осуществить промышленный шпионаж или получить финансовую выгоду;
- **голосовой или Voice Phishing** – предполагает использование телефонной связи для доступа к личным данным или финансовой информации о пользователе-жертве. Механика реализации такого вида фишинга следующая – преступник под видом работника страховой фирмы или банковского учреждения, рекламируя очень выгодную услугу, выуживает из жертвы необходимые личные сведения. В частности, среди «вишеров» считается эффективным уловка с предложением кредита на максимально выгодных для жертвы условиях. Однако в рамках обсуждения условий кредита всегда требуются личные данные пользователя и сведения финансового характера. Поэтому жертва совершенно искренне предоставляет кибер-мошеннику конфиденциальные данные. Наиболее аморальным видом голосового фишинга выступает «работа» с больными или пожилыми людьми. Преступник совершенно цинично и бесчеловечно использует уязвимое психическое или физическое состояние жертвы, чтобы получить доступ к его личным данным. Наживкой в данном случае выступают посулы оказания финансовой помощи сразу после предоставления персональных данных. Также часто встречается разновидность вишинг-атак, в ходе которых жертву информируют об ужасном происшествии, которое произошло с родственниками или близкими. Причем дается обещание решить проблему после оперативного перевода денежных средств;
- **«китобойный» или Whake Phishing** – представляет собой атаку, целью которой является топ-менеджер большой компании, что и предполагает собой такое название. Жертва такой атаки, как и потенциальная выгода, крайне велики, полученная конфиденциальная информация будет такого уровня, который недоступен, в случае если жертвой выступает рядовой сотрудник компании. Именно поэтому и фишинговый текст должен быть соответствующего уровня: юридические сообщения или предложения финансового характера. Самой значительной успешно реализованной «китобойной» атакой является совершенная хакерской группой Эвалдаса Римаскаускаса (Литва) атака на Facebook и Google. В рамках коммуникации с указанными гигантами хакерами была создана фальшивая компания, которая представлялась производителями ПК и уже имела опыт сотрудничества. Общие убытки от «китобойной» фишинговой атаки составили свыше 120 млн. долл. США [19];
- **СМС-фишинг или Smishing** – подразумевает использование мобильных гаджетов. Цель получает сообщение якобы с номера банка, содержание которого должно напугать человека, после чего ему предлагается вариант решения проблемы. Приведем пример такого вида фишингового мошенничества: с лицевого счета человека якобы были списаны средства нецелевым способом, поэтому клиенту банка предлагается перейти по ссылке

на официальную (на самом деле, поддельную) страницу банка или перезвонить по конкретному номеру телефона, контроль за которым осуществляется также злоумышленниками. Если жертва попадает в руки изощренных преступников, ее могут обманывать продолжительное время, на протяжении целых месяцев, снимая небольшие суммы, чтобы не насторожить жертву;

- **клон-фишинг** (от англ. Clone Phishing) состоит в том, что кибер-преступник готовит и направляет ложное электронное письмо, которое внешне сложно отличить от стандартного письма, отправляемого надежными и широко известными источниками. В частности, может быть указано, что отправитель Mail.crop вместо Mail.corp, как пишется в оригинале. Другими словами, электронное фишинговое письмо очень похоже на то, которое может прийти от банковского учреждения или вашей телекоммуникационной компании. В таком письме жертве поступает просьба от сотрудников соответствующего учреждения предоставить сведения личного характера. В рамках данного типа фишинговой атаки кибер-преступники подделывают форму корпоративного электронного письма, получая в результате очень похожий образец. Однако отправка данного письма осуществляется не с реального, а похожего адреса. Ссылки в теле письма являются опасными и вредоносными. Также текст содержит убедительное пояснение того, почему пришло данное сообщение и по какой причине запрашиваются личные данные. Одним из наиболее показательных примеров клон-фишинга является глобальная атака, имевшая место в январе 2022 г., в ходе которой кибер-преступники очень убедительно представили сообщения от Министерства труда Соединенных Штатов (DoL), в результате чего был получен доступ к учетным данным с сервиса Office 365 [23];
- **кража с диверсией**, второе название Diversion Theft, представляет собой еще один способ мошенничества «социальных инженеров», в рамках которого ничего не подозревающие курьерские службы доставляют заказчикам фейковые товары. При этом дорогостоящие оригиналы становятся добычей самих кибер-преступников. Механика преступления такова: в компанию по оказанию услуг курьерской доставки внедряется сообщник, вследствие чего у мошенников появляется непосредственный доступ к перечню товаров для доставки. В результате они будут срочно заменяться на копии. Время появления данного метода мошенничества относится еще к временам до внедрения интернета, родиной является Лондон, район Ист-Энд. Тем не менее, именно Всемирная Паутина дала толчок стремительному развитию кражи с диверсией, поскольку манипуляция сведениями максимально упрощена;
- **мошенническая атака**, также называется Rogue Attack, фактически является одним из видов Scareware-атак. ПК будущей жертвы оснащается шпионским программным обеспечением, мотивируя это соображениями безопасности. При этом владелец компьютера убежден, что устанавливаемый софт полностью безопасен и находится в правовом поле. Вредоносное ПО после его активации формирует оповещения и всплывающие окна, рекомендующие устанавливать дополнительный «полностью безопасный и законный» софт. Как правило, во всплывающих окнах пользователь получается разные варианты сценария соглашений. Тем не менее, при нажатии на «да» любого из предлагаемых вариантов жертва устанавливает на своем ПК вредоносную программу, отдавая свою компьютер в полное распоряжение кибер-преступника;
- **«водопой»** или Water-Holing. Сущность атаки данного типа полностью отражается в самом термине «водопоя». С помощью существующих уязвимостей сети кибер-преступник осуществляет компрометирующие действия в отношении группы лиц. Для этого происходит заражение сайтов, на которые они ходят и которым привыкли полностью доверять. Мошенники могут выбирать востребованные сайты, которые в их среде носят название «целевой группы». Благодаря встроенному в уязвимости сайта вредоносному ПО в виде HTML-кодов или Java Script происходит массовое перенаправление «це-

левой добычи» на другой сайт, который и внедряет вредоносное ПО. Как правило, целевой добычей выступает персонал государственных учреждений или крупных компаний;

- **оригинальнейшие методики «катания на спине» или «задняя дверь»** (Tailgating или Piggy back) представляет собой метод получения доступа в закрытое или охраняемое помещение, просто следуя за кем-то, у кого есть карта доступа. При этом кибер-преступник позиционирует себя как «друг» человека, обладающего привилегированным доступом, что делает для него возможным доступ в зону ограниченного доступа;
- **«медовая ловушка»**, еще называющаяся Honey Trap, Honey Pot, действует по принципу, описанному в басне про ворону и лисицу. Принцип действия таков – кибер-преступник знакомится с будущей жертвой и очень достоверно имитирует формирования влечения или романтического чувства. Довольно быстро развиваются виртуальные личные отношения, в искренности которых жертва не сомневаемся. В это время кибер-мошенник, обладающий серьезным обаянием, осуществляет усиленный сбор личных данных, которые впоследствии используются для взлома аккаунтов в социальных сетях или электронной почты жертвы. В случае необходимости жертва может передать и удаленный доступ к своему ПК;
- **методика «услуги за услугу»** или второе название Quid pro quo, как правило, используется кибер-преступниками, которые не располагают инновационными инструментами взлома, тем не менее, осуществляют предварительную разведку будущей цели. В частности, в рамках данного вида атак преступник создает иллюзию, что жертве была оказана очень серьезная услуга. Например, кибер-мошенник выбирает жертву из числа лиц с привилегированным доступом, совершает ей звонок от лица представителя технической поддержки. После проведения конструктивного диалога жертва соглашается принять «помощь» от преступника в ликвидации якобы выявленных проблем и уязвимостей. Для этого жертва выполняет все рекомендуемые мошенником последовательности действий. В результате на компьютер жертвы устанавливается вредоносное программное обеспечение или же утекают регистрационные данные;
- **атака с предлогом**, также носящая название Pretexting attack, представляет собой ложь со стороны кибер-мошенника, который таким образом, пытается заполучить доступ к информации высокого уровня. Инициатором такого типа мошенничеств зачастую выступает недобросовестный работник компании-жертвы, который имитирует срочную необходимость получить данные конфиденциального характера, что позволит ему решить срочную и важную задачу. В данном случае, прямой взлом отсутствует, имеет место сугубо психологическое воздействие, которое со стороны выглядит очень естественным и не вызывает, на первый взгляд, никаких опасений и подозрений;
- **атака по методу «пугалка»** или Scareware заключается в угрозах и испуге потенциальной жертвы в том, что ПК уже заражено шпионским программным обеспечением или жертва сама загрузила нелегальный контент. Как правило, такие угрозы поступают через всплывающие окна, после того как пользователь побывал на взломанных хакерами сайтах. После того, как предполагаемая жертва, скажем так, достигла определенной стадии отчаяния, кибер-преступник сам предлагает решение проблемы – вредоносное ПО, позиционируемое как эффективный антивирус.

Целью данной акции является получение несанкционированного доступа к личным данным выбранной жертвы. Анализируя механику атаки «пугалки», можно выделить главный прием – технология внушения, которая формирует страх у пользователя и мотивирует его согласиться на установку ложного антивирусного ПО [13].

Метод обратной социальной инженерии ориентирован на то, чтобы смодулировалась ситуация, когда потенциальная жертва принимает навязанное решение обратиться к инициатору за решением созданной им проблемы [8,18].

В частности, практическим примером данной механики выступают атаки с использова-

нием вируса-шифровальщика. При угрозах такого типа дешифровка собственными силами нереализуема. Поэтому вирусы-шифровальщики используют оболочку полезного программного обеспечения или ожидаемые файлы. Файлы могут маскироваться под стандартные для конкретного пользователя «договор», «судебное постановления», «заказ №» и т.д.

Сегодня обратная социальная инженерия использует методику информационного манипулирования тем, что та или иная проблема не имеет легального решения, происходит грамотная дискредитация общественных ценностей и явлений, в результате чего индивида или целевую группу людей подталкивают на вступление в радикальные группы, участие в антигосударственных несанкционированных мероприятиях.

Применение обратной социальной инженерии в качестве полноценного метода профилактики практически невозможно, потому что он предполагает деструктивные манипуляции и давление.

Эксперты считают, что самое главное в защите персонала и организации в целом – это постоянное информирование пользователей всех подразделений на каждом уровне управленческой иерархии об угрозах социальной инженерии, существующих и новых видах атак, о психологических технологиях, которые применяют хакеры при поиске доступа к конфиденциальной информации. Тем не менее, принципиально важна и профилактика:

1) постоянное тестирование на проникновение. Сотрудники IT-подразделений должны осуществлять постоянное тестирование на возможные атаки, в основе которых лежат технологии именно социальной инженерии. Благодаря этому у администраторов появится возможность классификации рисков для конкретных видов атак. Также периодическое тестирование позволяет выявить готовность персонала к противодействию кибер-мошенникам и спрогнозировать масштаб потенциальной утечки информации. Фишинговое тестирование, как правило, проводится с помощью специальных программ. Сущность такого тестирования состоит в рассылке персоналу фишинговых электронных писем и установление пользователей, которые поверили методам социальной инженерии. В дальнейшем эти работники направляются на переподготовку;

2) двухфакторная аутентификация, которая, в свою очередь, предполагает введение двух методов подтверждения личности: пароль при входе; код, отправляемый на номер телефон;

3) применение эффективной защиты от вредоносного софта. В рамках такой защиты важен принцип комплексности, предполагающий одновременное использование следующих тактических средств: почтового антивируса; противошпионского программного обеспечения (antimalvware); антивирусное программное обеспечение для обеспечения возможности безопасного веб-серфинга [21].

Отметим, что некоторые компании предлагают подобную защиту в пакетной версии, однако доказали свою эффективность и одновременное применение сразу нескольких хороших программ от разных разработчиков.

Едва ли не ключевой задачей в рамках данного профилактического мероприятия считается предотвращение угроз при переходе пользователя по ссылкам из мессенджеров и писем. В данном случае, должна быть предотвращена загрузка страницы с вредоносным контентом путем ее блокировки.

4) обязательные своевременные обновления операционной системы, поскольку компании-разработчики постоянно выпускают фиксы, которые устраняют выявленные уязвимости предыдущих версий;

5) грамотные пароли и их периодическая смены. Принципиально важной, считаем, является строгая политика управления паролями, которая выступает правильной профилактической мерой. Однако мало время от времени пользователю просто менять пароль, следует научиться составлять сложные, случайно сгенерированные их версии, которые не поддаются ни подбору, ни угадыванию. Все это требует проведения мероприятий по повышению квалификации персонала в соответствующей области;

6) обязательное использование брандмауэра, например, сетевого фаервола (WAF), кото-

рый блокирует любые шпионские запросы, включая и атаки с применением методов социальной инженерии. Следовательно, любой проход на интересующих пользователя сайт возможен только после того, как запрос отфильтрован WAF. Именно фаервол определяет безопасность подключения;

7) обеспечение положительного психологического климата в коллективе [11]. В данном случае персонал должен не стеснять информировать коллектив и IT-подразделение о появившихся подозрениях, в случае если они считают, что на них направлена атака с использованием тактики социальной инженерии. В случае, если соответствующая атмосфера доверия в коллективе отсутствует, сотрудник не поделится подозрениями, поскольку будет опасаться насмешек или ожидать возможное наказание.

Главным механизмом кибер-мошенников для хищения денежных средств у россиян является применение методов и инструментов социальной инженерии. В рамках использования данного метода человек самостоятельно передает кибер-преступникам огромные сумму или предоставляет личные сведения коммерческого и строго конфиденциального характера, что дает возможность похитить активы человека. В соответствии со статистикой ПАО «Сбербанк» 94% от преступлений, совершенных с помощью социальной инженерии, приходится на телефонное мошенничество.

Правоохранительные органы России и специалисты по кибербезопасности давно утверждают, что подавляющее большинство мошеннических звонков россиянам производится с территории Украины. Начиная с 2016 г., фактической «столицей» данного вида «бизнеса» является город Днепропетровск . Только в этом крупном городе функционировало не менее 150 криминальных колл-центров. Это огромный сектор теневого бизнеса, который взаимодействовал не только с международной преступностью, но и напрямую был связан с украинскими спецслужбами.

Информация о будущей жертве, как правило, приобретается в Даркнете, причем стоимость баз, например, сотовых операторов крайне демократична – порядка 20 тыс. руб. Поэтому мошенников не затрудняет приобрести сразу несколько таких баз, дополнить из сведениями из соцсетей и базами сервиса логистических компаний (например, сервиса по доставке готовой еды).

В настоящее время с территории Украины поступают звонки следующего содержания:

1) радикальные призывы совершать акты гражданского неповиновения и участвовать в несанкционированных митингах;

2) звонки из военкомата по поводу мобилизации;

3) звонки из учреждений российских банков о совершении несанкционированных операций со счетами клиента.

Также следует отметить, что кибер-мошенники из Украины переместились в соцсети, где их потенциальными жертвами является молодежь 18-22 лет. Данные МВД РФ свидетельствуют о том, что в период с 2018 по октябрь 2022 г. граждане России были обмануты на сумму свыше 200 млрд. руб. Это не просто сухая статистика, за этим огромными цифрами стоят трагедии конкретных людей [5].

Вывод. В современных условиях геополитической напряженности и усиления киберпреступлений во всех областях применение технологий социальной инженерии оперативно подстраивается под текущую ситуацию и приобретает эффективность особенно в отношении тех пользователей, который недоинформированы о рисках и угрозы цифровой среды. В статье предлагается оптимальное определение термина «социальная инженерия» – это выявление и эксплуатация некомпетентности, недостаточного профессионального уровня или халатности сотрудников организации или частных лиц для получения несанкционированного доступа к конфиденциальным данным. Другими словами, это совокупность технологий, базирующихся на использовании психологической специфики человека.

В целом, вся система социальной инженерии базируется на том, что именно индивид

представляет собой самое уязвимое звено любой информационной системы, что активно используется кибер-преступниками. Современный социальный инжиниринг дает возможность корректировать социальную реальность, используя методы прогнозирования, планирования и программирования.

Библиографический список:

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 24.09.2022) // Электронно-правовая база «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 18.10.2020).
2. Кэррол Э. Изард. Психология эмоций / Изард Э. Кэролл. – СПб.:Питер. 1999. 357 с.
3. Ламинина О.Г. Возможности социальной инженерии в информационных технологиях / О.Г. Ламинина // Гуманитарные и общественные науки. – 2019. – №2. – С. 8-14.
4. Созаев С.С., Кунашев Д.А. Социальная инженерия, ее техники и методы ее противодействия / С.С. Созаев, Д.А. Кунашев // Вестник науки. – 2020. – Т.1. – №2(23). – С. 85-88.
5. Станислав Кузнецов: против России ведется необъявленная кибервойна / С. Кузнецов // РИА Новости. – 08.10.2022. – URL: https://ria.ru/20220418/kuznetsov-1784035779.html (дата обращения 16.10.2022).
6. Стеценко Ю.А., Холодковская Н.С. Мошенничество в сети Интернет / Ю.А. Стеценко, Н.С. Холодковская // Вестник Таганрогского института имени А.П. Чехова. – 2021. – №4. – С. 75-80.
7. Суворова В.В., Суворова Л.А. Совершение преступлений с использованием социальной инженерии: постановка проблемы. Теория и практика приоритетных научных исследований: сборник научных трудов по материалам VIII Международной научно-практической конференции. Изд. МНИЦ «Наукосфера», 2019. С. 71-74.
8. Тепляков С.П., Тимохович А.С. Социальная инженерия. Анализ и методы защиты / С.П. Тепляков, А.С. Тимохович // Academy. – 2018. – №11. – С. 26-27.
9. Титкова Е.В. Способы инициации атак с применение методов инженерии / Е.В. Титкова // Актуальные проблемы авиации и космонавтики. – 2020. – Т. 2. – С. 248-250.
10. Чеботарева С.С. Использование социоинженерного подхода в распространении и профилактике радикальных идей / С.С. Чеботарева // Обзор. НЦПТИ. – 2020. – №2 (21). – С. 57-66.
11. Чалдини Роберт Б. Психология влияния / Б. Роберт Чалдини. – СПб.: Изд-во «Питер», 2016. – 389 с.
12. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений / М.О. Янгаева // Вестник Сибирского юридического института МВД России. – 2021. – №1 (42). – С. 133-138.
13. Hadnagy Ch., Wilson P. Social Engineering: The Art of Human Hacking. Indianapolis: Wiley Publishing, Inc., 2020. 416 p.
14. Как избежать атаки с использованием социальной инженерии / Официальный сайт Лаборатории Kaspersky. – URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (дата обращения 10.10.2022).
15. Отчет о киберпреступности «Internet Crime Report 2019» // Federal Bureau of Investigation. – URL: https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf (дата обращения 14.10.2022).
16. Официальный сайт ежедневной деловой газеты РБК. – URL: https://www.rbc.ru/technology_and_media/17/04/2020/5e988cc29a7947ff6c7b4e6eПРО СБЕРБАНК (дата обращения: 18.10.2022).
17. Поппер К.Р. Открытое общество и его враги / К.Р. Поппер. – М.: Проспект, 1992. URL: https://gtmarket.ru/laboratory/basis/3912/3913 (дата обращения: 20.09.2022).
18. Социальная инженерия — как не стать жертвой. – URL: https://efsol. ru/articles/social-engineering.html (дата обращения: 06.05.2020).
19. Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme // The United States Department of Justice. – URL: https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business (дата обращения 09.10.2022).
20. Business Mobile Banking Rank. Markswebb. – URL: https://markswebb.ru/upload/iblock/255/2559c9b9ebc370b64a380c0af5135062.pdf (дата обращения 18.10.2022).
21. Krombholz K., Hobel H., Huber M., Weippl E. Advanced Social Engineering Attacks // Journal of Information Security and Applications. 2015. Vol. 22. P. 113–122. - URL: https://doi.org/10.1016/j.jisa.2014.09.005 (дата обращения 20.10.2022).
22. Safa N.S., von Solms R., Futcher L. Human Aspects of Information Security in Organizations // Computer Fraud & Security. 2016. Vol. 2016. Iss. 2. P. 15–18. URL: https://doi.org/10.1016/S1361-3723(16)30017-3 (дата обращения 18.10.2022).
23. Разнообразный арсенал социальной инженерии: виды атак и способы их предотвращения / Эксперт 1shaman // ХАБР. Блог компании FirstVDS Информационная безопасность. – URL: https://habr.com/ru/company/first/blog/670766/ (дата обращения 10.10.2022).

References:

1. Criminal Code of the Russian Federation dated 13.06.1996 n c 63-FZ (ed. dated 24.09.2022) // Electronic legal base "ConsultantPlus". – URL: http://www.consultant.ru/document/cons_doc_LAW_10699 / (accessed 18.10.2020).
2. Carroll E. Izard. Psychology of emotions. St. Petersburg:Peter. 1999; 357.
3. Laminina O.G. Possibilities of social engineering in information technologies. *Humanities and social sciences*. 2019; 2: 8-14.
4. Sozaev S.S., Kunashev D.A. Social engineering, its techniques and methods of its counteraction. *Bulletin of Science*. 2020; 1(2(23): 85-88.
5. Stanislav Kuznetsov: an undeclared cyber war is being waged against Russia. S. Kuznetsov. RIA Novosti. 08.10.2022. – URL: https://ria.ru/20220418/kuznetsov-1784035779.html (accessed 16.10.2022).
6. Stetsenko Yu.A., Kholodkovskaya N.S. Fraud on the Internet / Yu.A. Stetsenko, N.S. Kholodkovskaya. *Bulletin of the Taganrog Institute named after A.P. Chekhov*. 2021; 4: 75-80.
7. V.V. Suvorova, L.A. Suvorova. Committing crimes using social engineering: problem statement. Theory and practice of priority scientific research: a collection of scientific papers based on materials from the VIII International Scientific and Practical Conference. Izd. MNITS "Naukosphere", 2019; 71-74.

8. Teplyakov S.P., Timokhovich A.S. Social engineering. Analysis and methods of protection. *Academy.* 2018; 11: 26-27.
9. Titkova E.V. Methods of initiating attacks with the use of engineering methods. *Actual problems of aviation and cosmonautics*. 2020; 2: 248-250.
10. Chebotareva S.S. The use of a socio-engineering approach in the dissemination and prevention of radical ideas Review. NCPTI. 2020; (21): 57-66.
11. Cialdini Robert B. Psychology of influence. St. Petersburg: *Publishing house "Peter"*, 2016; 389.
12. Yangaeva M.O. Social engineering as a way of committing cybercrimes / M.O. Yangaeva. *Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia.* 2021; 1(42): 133-138.
13. Hadnaghi Ch., Wilson P. Social engineering: the art of hacking people. Indianapolis: Wiley Publishing, Inc., 2020; 416.
14. How to avoid an attack using social engineering. Kaspersky Lab official website. – URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (accessed 10.10.2022).
15. Report on cybercrime "Report on crimes on the Internet for 2019" // Federal Bureau of Investigation. – URL: https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf (accessed 14.10.2022).
16. The official website of the daily business newspaper RBC. – URL: https://www.rbc.ru/technology_and_media/17/04 /2020/5e988cc29a7947ff6c7b4e6ePRO SBERBANK (publication date: 10/18/2022).
17. Popper K.R. Open Society and its enemies / K.R. Popper. – Moscow: Prospect, 1992. URL: https://gtmarket.ru/laboratory / basis/3912/3913 (accessed: 09/20/2022).
18. Social engineering — how not to become a victim. URL: https://efsol . ru/articles/social-engineering.html (date of appeal: 06.05.2020).
19. Lithuanian Sentenced To 5 Years In Prison For Stealing More Than $ 120 Million In A Fraudulent Scheme Of Compromising Business Email. United States Department Of Justice. URL: https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business (accessed 09.10.2022).
20. Rating of mobile banking for business. Markswebb. URL: https://markswebb.ru/upload/iblock/255/2559c9b9ebc370b64a380c0af5135062.pdf (accessed 18.10.2022).
21. Krombholz K., Hobel H., Huber M., Weippl E. Advanced attacks of social engineering // Journal of Information Security and Applications. 2015;22:113-122. URL: https://doi.org/10.1016/j.jisa.2014.09.005 (accessed 20.10.2022).
22. Safa N.S., von Solms R., Futcher L. Human aspects of information security in organizations. *Computer fraud and security.* 2016; 2: 15-18. URL: https://doi.org/10.1016/S1361-3723 (16)30017-3 (accessed 18.10.2022).
23. Diverse arsenal of social engineering: types of attacks and ways to prevent them / Expert 1shaman // HABR. Blog of the company FirstVDS Information security. – URL: https://habr.com/ru/company/first/blog/670766/ (accessed 10.10.2022).

Сведения об авторах:
Репенко Виктор Андреевич, магистр; repenkovic@yandex.ru, ORCID.0000-0001-8783-6975
Резниченко Сергей Анатольевич, кандидат технических наук, доцент; rsa_5@bk.ru, ORCID.0000-0002-539-0457
Information about authors:
Viktor A. Repenko**,** master; repenkovic@yandex.ru, ORCID.0000-0001-8783-6975
Sergey A. Reznichenko, Cand.Sci. (Eng.), Assoc. Prof.; rsa_5@bk.ru, ORCID.0000-0002-539-0457
Конфликт интересов/Conflict of interest.
Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.
Поступила в редакцию/Received 01.11.2022.
Одобрена после рецензирования/ Reviced 26.11.2022.
Принята в печать/Accepted for publication 26.11.2022.