DOI 10.17150/2411-6262.2021.12(2).14 http://brj-bguep.ru

УДК 338

Л.В. Санина
Байкальский государственный университет, г. Иркутск, Российская Федерация
О.А. Чепинога
Байкальский государственный университет, г. Иркутск, Российская Федерация
Э.А. Ржепка
Байкальский государственный университет, г. Иркутск, Российская Федерация
О.Ю. Палкин
Байкальский государственный университет, г. Иркутск, Российская Федерация

ДЕСТРУКТИВНАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ: ИСПОЛЬЗУЕМЫЕ МЕТОДЫ И МАСШТАБЫ ЯВЛЕНИЯ

АННОТАЦИЯ. Нарастающий интерес к исследованию темы определения сущности социальной инженерии как угрозы экономической безопасности обусловлен усложнением информационной и технической составляющих жизни современного общества. Одновременно, с усложнением всех существующих в обществе процессов, усложняются и увеличиваются информационные угрозы. Информационные угрозы, возникающие извне, имеют возможность проникать в самые защищенные системы организаций различного уровня, реализуя цели субъектов проникновения. Ситуация с каждым годом усложняется и потому, что, как правило, цели подобных вторжений в сферу информационной безопасности носят исключительно деструктивный характер.

В ходе проведения исследования были рассмотрены шесть методов социальной инженерии, сочетающие в себе мошеннические схемы разного уровня сложности, которые в настоящее время применяются в деструктивном плане и негативно отражаются на экономической безопасности. Показаны масштабы утечек информации в финансовом секторе в 2019–2020 гг. по типам данных, умыслу, виновнику и типу инцидентов.

В результате исследования было выявлено, что методы социальной инженерии являются адаптивными, они видоизменяются в соответствии с изменяющимися условиями среды, в связи с чем, сотрудникам службы безопасности необходимо постоянно обновлять информацию об актуальных методах и схемах с целью увеличения эффективности предупреждения их применения.

КЛЮЧЕВЫЕ СЛОВА. Социальная инженерия, экономическая безопасность, информационная безопасность.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 21 мая 2021 г.; дата принятия к печати 21 июня 2021 г.; дата онлайн-размещения 13 июля 2021 г.

L.V. Sanina
Baikal State University, Irkutsk, Russian Federation
O.A. Chepinoga
Baikal State University, Irkutsk, Russian Federation
E.A. Rzhepka
Baikal State University, Irkutsk, Russian Federation

O.Yu. Palkin
Baikal State University,
Irkutsk, Russian Federation

DESTRUCTIVE SOCIAL ENGINEERING AS A THREAT TO ECONOMIC SECURITY: METHODS USED AND THE SCALE OF THE PHENOMENON

ABSTRACT. The growing interest in researching the topic of defining the essence of social engineering as a threat to economic security is due to the increasing complexity of the information and technical components of the life of modern society. At the same time, with the complication of all processes existing in society, information threats are becoming more complex and increasing. Information threats arising from the outside have the ability to penetrate the most protected systems of organizations of various levels, realizing the goals of the subjects of hacking. The situation is getting more complicated every year also because, as a rule, the goals of such incursions into the sphere of information security are extremely destructive. In the course of the study, we analyzed six methods of social engineering combining fraudulent schemes of different levels of complexity, which are currently used in a destructive manner and negatively affect economic security. The scale of information leaks in the financial sector in 2019–2020 is illustrated by data type, intent, culprit, and type of incident. We found that social engineering methods are adaptive, they change in accordance with fluid environmental conditions, and therefore, security personnel need to stay up-to-date on current methods and schemes to prevent hacking activities.

KEYWORDS. Social engineering, economic security, information security.

ARTICLE INFO. Received May 21, 2021; accepted June 21, 2021; available online July 13, 2021.

Деструктивная социальная инженерия является на сегодняшний день актуальной угрозой практически на всех уровнях управления. Из-за угроз экономической безопасности, согласно статистических данных в сеть Интернет каждый год уходит до 14 млрд конфиденциальных записей крупных корпораций и организаций, представляющих крупный и средний бизнес. Если рост числа «информационных утечек» во всем мире увеличивается на 10 %, то в России данный показатель равняется 40 %[1].

Согласно данным аналитического центра Национального агентства финансовых исследований (НАФИ) средняя сумма убытков одной крупной российской компании от применения мошенниками распространенных схем деструктивной социальной инженерии составляет до 299,9 тыс. р. в год[2]. Экономические убытки из-за кибератак признает каждая пятая российская компания, в связи с чем аналитический центр подсчитал примерную сумму общих для российского бизнеса экономических потерь — около 100 млрд р. в год и эта сумма с каждым годом растет.

Социальная инженерия является сравнительно молодой наукой о преобразовании окружающей социальной реальности. Научное обоснование социальной инженерии впервые дал австрийский философ и социолог К. Поппер. В своем научном труде «Нищета историзма» [1, с. 29] К. Поппер рассмотрел социальную инженерию как совокупность неких подходов из области прикладной социологии, которые направлены на рационализированное изменение социальных систем на

[1] Утечки данных 2019: статистика и масштабы // Известия. URL: https://iz.ru/958561/anna-urmantceva/perekhod-na-lichnoe-v-2019-godu-uteklo-vdvoe-bolshe-personalnykh-dannykh (дата обращения 01.04.2020).

[2] Российские компании за год потеряли более 100 млрд р. из-за кибератак // РБК Новости. URL: https://www.rbc.ru/technology_and_media/19/12/2017/5a38f3749a794710aa15581 b (дата обращения 31.03.2020).

основе знаний об обществе и экстраполяции существующих данных с целью предсказания потенциальных результатов проводимых преобразований.

Рассмотрим основные подходы к определению термина «Социальная инженерия» (табл. 1).

Таблица 1

Подходы к определению термина «социальная инженерия»

Наименование подхода	Представители подхода	Основная суть подхода
Институциональный	К. Поппер, Н.А. Фомина, А.В. Веселов, А.М. Сычев.	Создание и управление социальными институтами и значимыми социальными процессами (например, реорганизация системы образования), при которых происходит качественная модификация общественной системы в целом. Институциональный подход социальной инженерии имеет практически необратимый или слабо обратимый эффект.
Управленческий	П.В. Равенков, А.А. Бердюгин, Ю.М. Резник, Г.А. Антонюк.	Методы стимулирования и управления поведением общества, включающие в себя политическое воздействие при коррекции социальных установок при формировании общественного мнения, воздействие на трудовую мотивацию в рамках определенной организационной структуры, а также воздействие на потенциальных клиентов и конкурентов в бизнес среде.
Функциональный	В.А. Сухомлинский, Л.И. Новикова, В.А. Караковский, А.Н. Тубельский.	Целенаправленное воздействие на изменение частной функции социальной среды в процессе социализации индивидов. Применение данного подхода может быть организованным (через СМИ, школу, семью) или стихийным (реклама, улица, Интернет). Внедрение нового социального опыта через частные функциональные преобразования при формировании поведенческих моделей.
Манипуляционный	К. Митник, А.А. Сиротский, Т.Ф. Байрушин, А.А. Казыханов.	Целенаправленное воздействие с целью получения определенного социального действия. Характеризуется психологическим внедрением информации и изменения посредством данного внедрения определенных психологических реакций людей, таких как привычка, интерес, доверие и т.д. Чаще всего манипуляции направлены на достижение ожидаемой материальной или нематериальной выгоды, которая, как правило, оказывается очевидной для субъекта манипулятивного воздействия.

Институциональный подход к определению социальной инженерии характеризуется процессом создания и управления социальными институтами и значимыми социальными процессами, при которых происходит качественная модификация общественной системы в целом. Представителями подхода (К. Поппер [1], Н.А. Фомина [2], А.В. Веселов [3], А.М. Сычев [4]) социальная инженерия рассматривается как процесс формирования социальных систем и институтов. Отметим, что данный подход характеризуется довольно сильным воздействием, которое оказывает качественное влияние на самые сложные социальные структуры. Можно сказать, что институциональный подход социальной инженерии имеет практически необратимый или слабо обратимый эффект, так как последствия от такого вмешательства имеют пролонгированный во времени эффект.

С позиции управленческого подхода (представители П.В. Равенков и А.А. Бердюгин [5], Ю.М. Резник [6], Г.А. Антонюк [7]) социальная инженерия рассматривается как совокупность методов стимулирования и управления поведением общества. Совокупность указанных методов включает в себя воздействие при коррекции социальных установок при формировании общественного мнения, в том числе воздействие на трудовую мотивацию в рамках определенной организационной структуры или воздействие на потенциальных клиентов и конкурентов в бизнес среде. Применяются данные методы с целью управления поведенческими характеристиками объекта управления с конкретной и определенной для субъекта целью. П.В. Равенков и А.А. Бердюгин рассматривают социальную инженерию как разновидность управления процессами хищения конфиденциальной информации. Социальная инженерия одновременно может быть управлением различными системами общества, в том числе и деструктивными. Основным направлением изучения социальной инженерии перечисленных ученых является кибербезопасность.

Со стороны функционального подхода (В.А. Сухомлинский [8], Л.И. Новикова [9], В.А. Караковский [10], А.Н. Тубельский [11]) определение социальной инженерии сводится к целенаправленному воздействию на изменение частной функции социальной среды в процессе социализации индивидов. Причем, применение данного подхода может быть организованным (через СМИ, школу, семью) или стихийным (реклама, улица, Интернет).

Как видно из описания, любой подход к определению социальной инженерии содержит в себе манипулятивную составляющую по причине неизбежного вмешательства в социальные структуры и социальное поведение с целью изменения психологических характеристик общества с целью реализации определенных идей. Чаще всего манипуляции направлены на достижение ожидаемой материальной или нематериальной выгоды. С помощью методов социальной инженерии возможно обойти любые, даже самые сложные системы информационной безопасности, что дает злоумышленникам возможности для получения выгоды.

Ученые отмечают, что использование социальной инженерии при несанкционированном получении информации становится все более выгодным способом деструктивного воздействия с целью получения выгоды в связи со следующими факторами: 1) простота получения интересующей информации по сравнению с прямым взломом информационных систем; 2) атаки очень сложно вычистить с помощью автоматизированных защитных систем; 3) минимальные финансовые вложения; 4) минимальный риск; 5) большая вероятность положительного (для субъекта воздействия) эффекта. Цели и задачи социальной инженерии во взаимодействии с физической, экономической и информационной безопасностью показаны в табл. 2.

На наш взгляд, изучение темы социальной инженерии в современном обществе является достаточно актуальным на протяжении нескольких последних десятилетий, а все рассмотренные подходы позволяют описать социальную инженерию как определенную совокупность приемов, методов и различных технологий, позволяющих создавать информационное пространство, состоящее из условий и обстоятельств, способных привести субъекта воздействия к получению конкретного результата. На сегодняшний день можно выделить шесть основных методов социальной инженерии, в деструктивном ее аспекте (рис. 1).

Дадим краткую характеристику, указанным на рис. 1 методам.

1. Фишинг — это вид мошенничества, при котором основной целью злоумышленников является получение персональных данных клиентов или работникам организации, в частности, мобильным номерам, электронным почтам, данным

Таблица 2

Цели и задачи социальной инженерии во взаимодействии с физической, экономической и информационной безопасностью

Социальная инженерия и	Цель применения	Задачи, необходимые для выполнения
Физическая безопасность	Анализ физической защищенности	Анализ контроля доступа Анализ технических средств (СКУД, видеонаблюдение, сигнализация) Анализ физической охраны
Экономическая безопасность	Мошенническая деятельность	Контрольная закупка Контрольная поставка Тайный покупатель
	Получение конкурентного преимущества	Конкурентная разведка
Информационная безопасность	Получение доступа к информации атакуемого объекта	Проверка возможности получения доступа к информационным системам и к конфиденциальной информации Проверка эффективности работы СЗИ и работы служб ИБ Проверка осведомленности сотрудников в вопросах ИБ

[*] Составлена по данным: Информационная безопасность современного преподавателя : программа повышения квалификации // Национальный исследовательский ядерный университет «МИФИ» : офиц. сайт. URL: https://vector.mephi.ru/ (дата обращения: 20.03.2021).

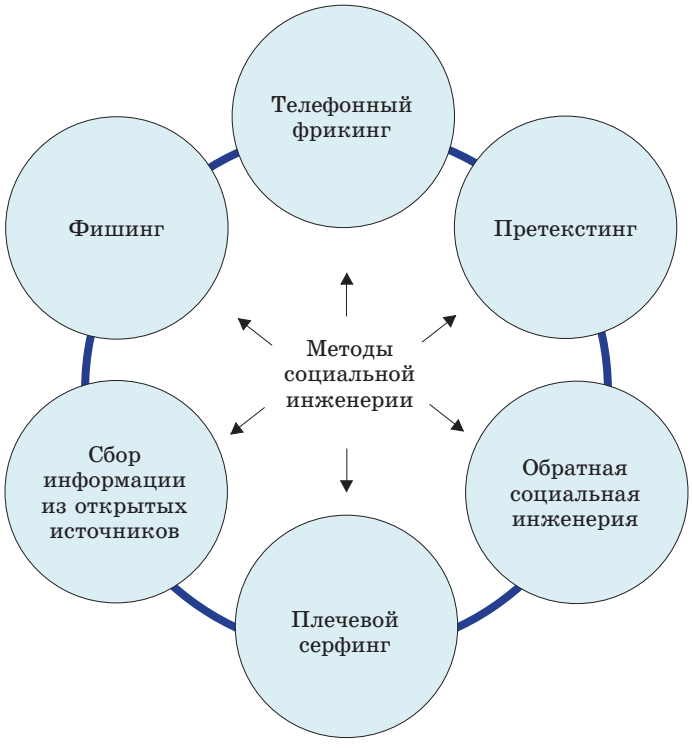

Рис. 1. Методы социальной инженерии, имеющие деструктивный характер и представляющие угрозу экономической безопасности

Составлен по [10].

банковских карт, логинам, паролям и т.д.[3]. Фишинг, являясь реальной угрозой для организаций, их клиентов и работников, пользуется популярностью в Интернете злоумышленниками различного уровня: от мелких Интернет-мошенников, преследующих свою финансовую выгоду, до специализированных крупных группировок, целью которых может быть уничтожение информационных систем и репутации целый корпораций и государственных институтов. Первые фишинговые атаки были отмечены в конце XX в., на сегодняшний день, по оценке Google каждый год от фишинга страдают до 12,4 млн. пользователей сети Интернет. Данный вид мошенничества опасен тем, что он постоянно модифицируется исходя из условий, которые меняются практически сиюминутно и подстраивается под актуальные информационные условия. Среди популярных фишинговых схем можно выделить следующие [10]:

– переход по несуществующим ссылкам, который выглядит как письмо с причиной посетить подложный сайт, который имеет сходство с привычными сайтами на которых оставляются персональные данные (например, PayPal);

– использование узнаваемых брендов, например, при объявлении победы в конкурсах или при требовании изменить логин и пароль (подложное предостережение о том, что персональным данным угрожает опасность);

– подложные лотереи используются для перевода взносов, чтобы получить выигрыш;

– ложные антивирусные системы и программы для обеспечения безопасности генерируют ложные уведомления на компьютерах об информационных угрозах с целью получения персональных данных;

– IVR или телефонный фишинг выражается в использовании заранее записанных официальных звонков крупных организаций с целью «обновления» персональной информации.

Все вышеперечисленные методики характеризуются тем, что информация «выуживается» посредством подлога, который имитирует официальные источники. Сходство порой бывает настолько разительно, что потенциальная жертва даже после совершенной операции не понимает, что стала жертвой обмана.

2. Телефонный фрикинг. Похож на IVR или телефонный фишинг. Метод телефонного фрикинга осуществляется с помощью звуковых манипуляций (самое простое проявление: звонки сотрудникам компании, представляясь другими сотрудниками с созданием похожих голосов и манеры общения с просьбой срочного предоставления каких-либо данных). Отличается от телефонного фишинга тем, что взлом происходит при помощи манипуляций с телефонным тоновым набором. Многие злоумышленники таким образом получают доступ к созданию целых телефонных конференций, во время которого на жертву воздействует не один абонент, что значительно ослабляет ее бдительность [5].

Данный способ мошенничества был популярен еще в «доцифровую» эру, когда звонки переадресовывались на подложные номера в процессе набора телефонного номера. Сегодня технологии шагнули дальше и даже с определителем телефонного номера абонент может не понимать, что его переадресовали на подложный канал связи, так как номер не меняется. Злоумышленникам необходимо лишь дождаться сигнала «занято» и тогда можно не только переадресовать абонента, но и прослушивать его последующие звонки.

3. Претекстинг — является настоящей атакой, при которой злоумышленник выдает себя полностью за другого человека по сценарию, досконально подготовленному заранее. В данный сценарий входит практически вся информация объек-

[3] Что такое фишинг и как от него защититься / Rusbase : офиц. сайт. URL: https://rb.ru/sto6:39 ry/what-is-fishing/html (дата обращения 12.02.2020).

те подлога: паспортные данные, история жизни (если это необходимо), банковские реквизиты и т.д. Отличается от фрикинговых схем тем, что каналы атак не ограничиваются телефонной связи, а подготовка осуществляется досконально [12].

Претекстинг является сложным методом социальной инженерии, и поэтому, применяется в работе с крупными организациями и корпорациями. Метод включает в себя две основные схемы [11]:

– «квид про кво» (услуга за услугу) — схема, при которой актер обращается на корпоративный номер телефона или почту, представляясь сотрудником технической поддержки и запускает на компьютер жертвы специальное программное обеспечение, без труда собирающее информацию;

– «дорожное яблоко» или схема «троянского коня», заключается в подлоге физического носителя в места корпоративного пользования (обычно надпись на носителе вызывает интерес к просмотру и когда он оказывается в компьютере, на него записывается вредоносное программное обеспечение).

В обоих случаях происходит внедрение программного обеспечения практически руками ни о чем не подозревающих работников организации, именно поэтому сфера информационной безопасности не ограничивается работой одного человека, отдела или специальной службы, а должна распространяться на весь коллектив.

4. Сбор информации из открытых источников является методом, который обычно недооценивают в силу его кажущейся простоты. Однако это не так. Этот метод сочетает в себе знания из области психологии и информационной безопасности. Основа метода состоит в сборе и анализе информации об объекте из открытых источников. Работники организации, зачастую, не задумываются о том, сколько конфиденциальной информации они выдают в социальных сетях: маршруты, конференции, деловые переговоры, распорядок дня того или иного работника и т.д. Все это помогает злоумышленникам завладеть информацией, которая, впоследствии оказывается частью иных мошеннических схем [4].

Стоит отметить, что данный метод доступен в силу информационной открытости и сложно контролируем сотрудниками службы информационной безопасности.

5. Плечевой серфинг — это своеобразное наблюдение за информацией «через плечо жертвы». Множество работников видят информацию, которую они не должны видеть (курьеры, водители, доставляющие важные документы и т.п.). Также данную информацию можно отследить в общественных местах: аэропортах, деловых центрах, торговых центрах. Злоумышленникам остается выследить сотрудника и выбрать способ получения информации: посмотреть, стоя рядом, выспросить в процессе разговора, подменить папку с документами и т.д. Метод является достаточно доступным и распространенным не одно десятилетие.

6. Обратная социальная инженерия. Данный метод предполагает вариант, при котором жертва сама выходит на злоумышленников и предлагает информацию. В ситуациях, когда жертве нужно оперативно решить рабочую проблему, она добровольно выходит на подложную службу поддержки и говорит персональные данные. Одним словом, жертва делает все что надо и даже сверх того, только чтобы решить сложившуюся проблему. Итогом становится «слив» конфиденциальной информации без каких-либо усилий со стороны злоумышленников [11].

Стоит отметить, что та или иная схема не применяется мошенниками в чистом виде, чаще имеет место комбинация методов и/или схем, которые в совокупности позволяют злоумышленникам осуществить свои планы. Наиболее популярный способ использования мошеннических схем деструктивной социальной инженерии — это кибератаки, число которых сегодня достигло «беспрецедентных масштабов», они стали одними из главных глобальных рисков после экологических и геополитических проблем. Пока кибератакам отведено шестое место в десятке

технологических рисков, но, по мнению экспертов, к 2023 г. эта угроза может занять первую строчку[4]. При этом ученые говорят о том, что развитие преступности в ближайшем будущем будет иметь следующие характерные черты: а) растущая виртуализация; б) снижение эффективности (результативности) некоторых форм криминального насилия; в) повышение законспирированности преступной деятельности; г) рост показателей «преступности без жертв». Поэтому актуальным является вопрос системной и комплексной оценки ожидаемых интернет-угроз, в том числе от деструктивной социальной инженерии, сравнительного исследования методов обнаружения и противодействия [13; 14; 15].

Многие кибератаки проводятся при комбинации схем применения социальной инженерии, которые описываются схемой Шейнова [16] (рис. 2).

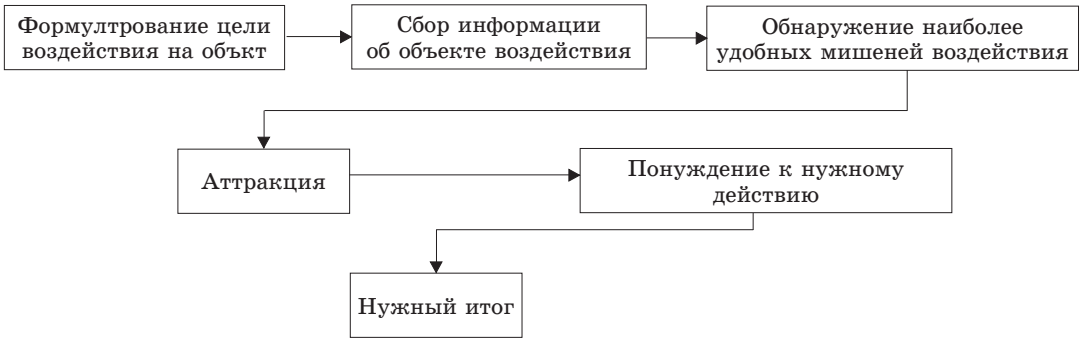

Рис. 2. Схема Шейнова

Составлен по [16].

В общем виде описание комбинированной схемы Шейнова выглядит так: сначала формулируется цель воздействия на тот или иной объект. Под объектом имеется ввиду потенциальная жертва (персона или организация), на которую планируется социоинженерная кибератака. Следующим этапом является сбор информации из всех доступных источников с целью обнаружения слабых сторон и основных мишеней воздействия. Затем следует аттракция, этап который характеризуется созданием условий для потенциальной атаки мошенников. Следующий этап описывает применение распространенных мошеннических схем, которые характеризуются различными способами формирования решения для принуждения жертвы к необходимому для хакера действию. Необходимые обстоятельства, приводящие к программируемому итогу, приводят социального хакера к ожидаемому итогу. Весь процесс может сопровождаться приманкой (по схеме «Дорожное яблоко»), подкупом или внедрением работы вредоносного программного обеспечения (по схеме «Копье фишинга»).

Целью хакерского взлома, как правило, является кража базы данных для ее перепродажи или шантажа обладателя. Причем, канал кражи имеет больше социальный, чем технический характер, что значительно усложняет процесс защиты от хакерских атак.

Во избежание подобных ситуаций, многие организации стремятся к минимизации человеческого фактора при обеспечении информационной и экономической

[4] В группе риска: почему кибератаки скоро возглавят мировой рейтинг угроз // РБК : офиц. сайт. — URL: https://www.rbc.ru/opinions/technology_and_media/15/03/2018/5aaa58b29a7947a6994c650d (дата обращения 31.05.2020).

безопасности организации. Но пока сложно утверждать возможно ли заменить человеческий фактор при принятии решений на искусственный интеллект. Согласно статистике при атаках на юридические лица основным мотивом злоумышленников выступает получение данных, а в атаках на физические лица — получение выгоды, что иллюстрирует рис. 3.

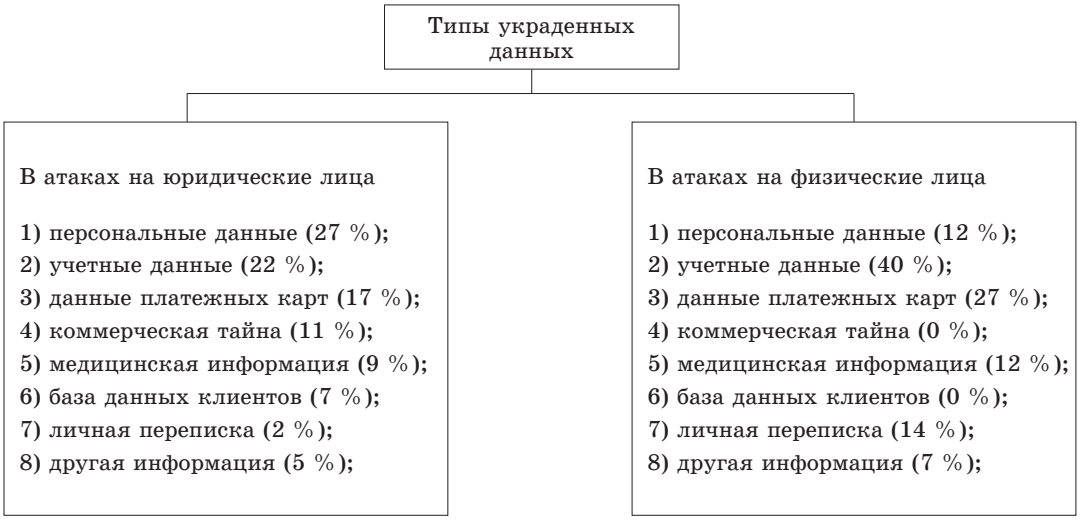

Рис. 3. Типы украденных данных у юридических и физических лиц

Составлен по данным: Актуальные киберугрозы: итоги 2019 г. // Positive technologies : офиц. сайт. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/ (дата обращения 30.05.2021).

Пути получения информации мошенниками являются достаточно простыми. Как правило, проводится анализ вебархивов, использования парсеров (языков программирования), компрометации мобильных устройств и применении современных социально-психологических методов воздействия. Методы атак представлены на рис. 4.

Рассмотрим масштабы утечек информации в организациях финансового сектора (банков, финансовых, инвестиционных и страховых компаний, криптовалютных бирж) России в 2019 и 2020 гг. в сравнении с мировыми значениями. За 2020 г. экспертно-аналитический центр InfoWatch зарегистрировал в мире 202 утечки конфиденциальной информации из финансовой сферы, что на 7,3 % меньше, чем в 2019 г.[5]. В России количество известных утечек в финансовом сегменте возросло на 36,5 % с 52 до 71. Среди причин называют и пандемию, поскольку произошла трансформация сферы предоставления финансовых услуг в сторону дистанционного обслуживания, участники рынка на новые вызовы реагировали неоперативно. Доля утечек конфиденциальных данных составила 8,4 % в мире и 17,6 % в России (рис. 5), при этом большая доля этих утечек не была обнаружена.

[5] Утечки данных. Россия. 2020 г. // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_финансы_2020_отчет.pdf (дата обращения: 28.05.2021).

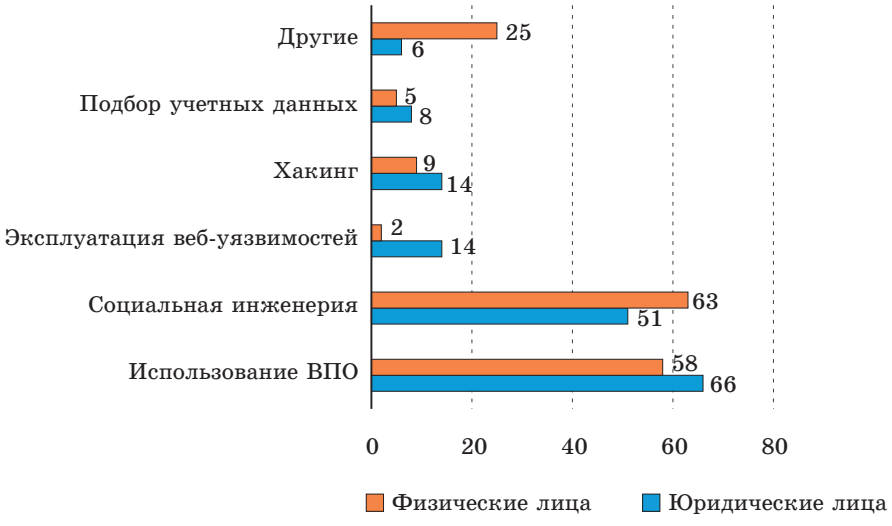

Рис. 4. Методы атак на физических и юридических лиц в 2019 г., %

Составлен по данным: Актуальные киберугрозы: итоги 2019 г. // Positive technologies : офиц. сайт. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/ (дата обращения 30.05.2021).

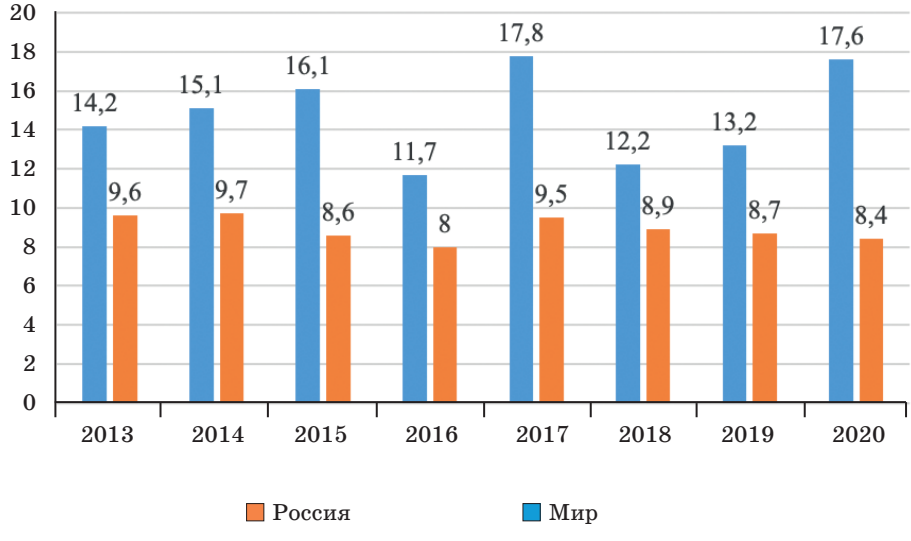

Рис. 5. Доля утечек конфиденциальных данных к их общему количеству в организациях финансового сектора в России и мире в 2013–2020 гг.

Составлен по данным: Утечки данных. Россия. 2020 г. // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_финансы_2020_отчет.pdf (дата обращения: 28.05.2021).

Существенный разрыв (в 2 раза) между количеством утечек в России и мире эксперты связывают с деятельностью внешних нарушителей, к которым относят хакеров или неизвестных лиц (взломщики компьютерных сетей, в том числе пред-

ставляющие организованную киберпреступность; владельцы хакерского инструментария (библиотек); взломщики, действующие в политических и социальных целях, хактивисты; сотрудники иностранных разведок и армий; похитители оборудования с конфиденциальной информацией). При этом в России информация об утечках из финансовых организаций охотно тиражируется СМИ, западные журналисты

Рассматривая распределение утечек ви В России финансовый сектор пока по-прежнему, в основном, страдает от утечек по вине внутренних нарушителей. Случаи краж конфиденциальной информации хакерами в публичном поле встречаются сравнительно редко. По результатам проведенных в конце 2020 г. учений Центробанк отметил, что готовность отечественных банков к отражению киберугроз оказалась лучше ожиданий. Тем не менее с учетом принятых мер, доля утечек в результате действий внешних сил в России выросла с 8,7 % до 17,9 %, а в мировом финансовом сегменте — с 37,4 % до 49 % (рис. 6).

Приходится констатировать, что для отечественных предприятий внешние угрозы становятся все более опасными, хотя доминирующими нарушителями все равно пока остаются сотрудники.

Из организаций финансовой сферы в 2020 г. стали реже утекать платежные данные и сведения, относящиеся к категории «коммерческая тайна», при этом возросла доля утечек персональных данных (рис. 7). Данные платежных карт имеют ценность у злоумышленников в течение ограниченного периода времени, поскольку банки оперативно блокируют скомпрометированные карты, выпускают новые, предлагают клиентам различные страховые продукты для защиты от мошенничества. Стоит отметить, что персональные данные заемщиков и кредиторов являются ликвидным товаром на черном рынке, его можно конвертировать в денежные средства посредством оформления кредитов или выплат, использовать

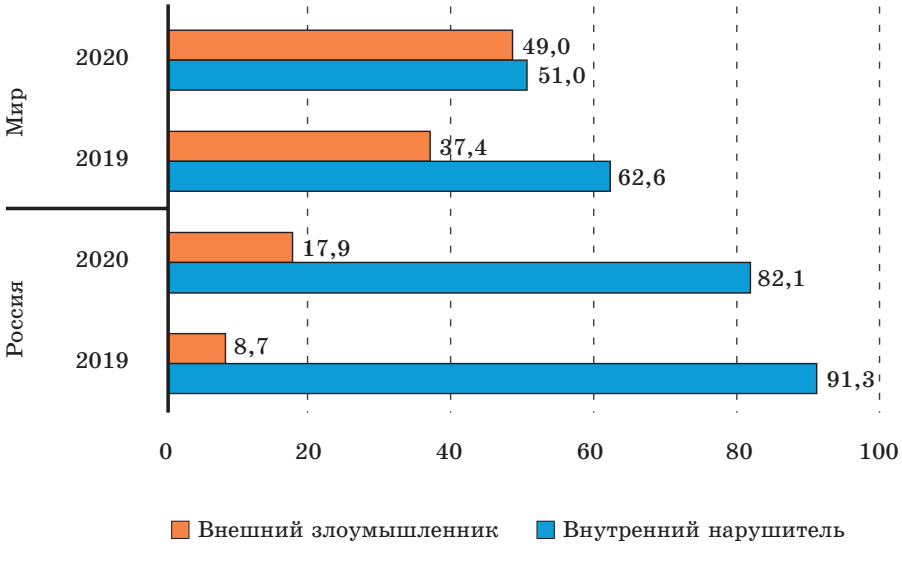

Рис. 6. Распределение утечек в организациях финансового сектора в России и в мире в 2019–2020 гг.

Составлен по данным: Утечки данных. Россия. 2020 г. // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_финансы_2020_отчет.pdf (дата обращения: 28.05.2021).

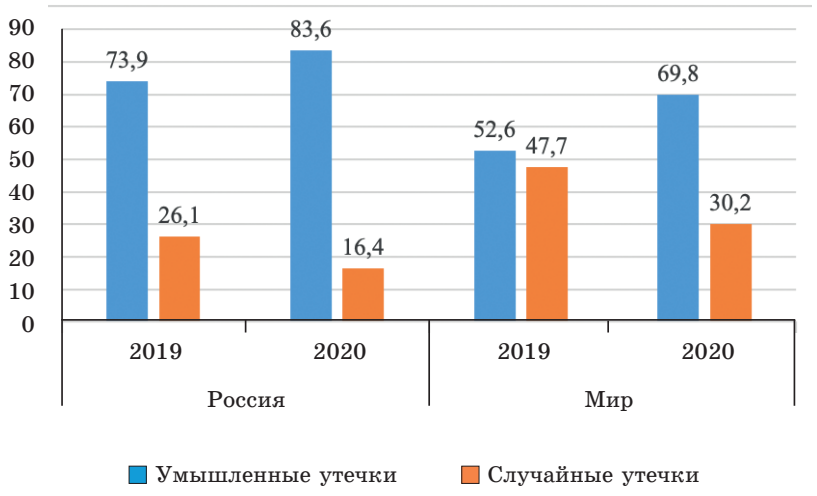

Рис. 7. Распределение утечек из организаций финансового сектора по типам данных в России и в мире в 2019–2020 гг.

Составлен по данным: Утечки данных. Россия. 2020 г. // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_финансы_2020_отчет.pdf (дата обращения: 28.05.2021).

в фишинговых атаках, продавать провайдерам различных услуг, повышать ценность существующих баз данных путем их обогащения новыми записями.

На рис. 8 проиллюстрировано, что 69,8 % утечек в мире и 83,6 % в России происходят по вине персонала, т.е. являются умышленными. В 2019 г. данные показатели составили 52,6 % и 74,0 % соответственно. Среди внутренних нарушителей также существует градация: рядовой сотрудник; топ-менеджер (руководитель); системный администратор; подрядчики (сторонние исполнители работ по заказу компании, партнеры и внештатные сотрудники); бывший сотрудник. Топ-менеджеры, системные администраторы, а в отдельных случаях и подрядчики включаются в категорию привилегированных пользователей, т.е. пользователей, наделенных повышенными правами доступа к информации. Как правило, действия таких пользователей в информационной системе службами информационной безопасности контролируются слабо либо не контролируются вовсе.

Рост доли умышленных инцидентов вызван повышением ликвидности на черном рынке конфиденциальной информации из организаций финансового сектора, а также пандемией, поскольку часть недобросовестных сотрудников, ища возможности дополнительного «заработка», встали на путь преступления. Вместе с тем, снижение доли случайных нарушений может быть связано с более широким проникновением в финансовую сферу DLP-систем и развитием уровня цифровой грамотности персонала.

В 2020 г. как в России, так и в мире стало намного больше утечек, где виновниками определены внешние злоумышленники. С одной стороны, такая статистка свидетельствует о том, что организация, допустившая утечку, не смогла определить, кто является виновником, или не захотела сообщить об этом. С другой стороны, это можно объяснить усложнением характера многих утечек, когда может иметь место сговор внутреннего и внешнего злоумышленника.

Доля квалифицированных утечек, когда компрометация данных сопряжена с мошенническими действиями или имеет место превышение прав доступа к ин-

Рис. 8. Распределение внутренних утечек (по вине внутреннего нарушителя) в организациях финансового сектора по умыслу в России и в мире в 2019–2020 гг.

Составлен по данным: Утечки данных. Россия. 2020 г. // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_финансы_2020_отчет.pdf (дата обращения: 28.05.2021).

формационным системам, в мировой финансовой сфере выросла на 4 % с 2019 по 2020 г., в России динамика роста незначительная (1,1 %), но само количество таких утечек в 2 раза выше, чем в мире[6].

Таким образом, на примере организаций финансового сектора можно констатировать рост числа факторов, с помощью которых осуществляется атаки на экономическую безопасность организации с применением современных информационных технологий. Подводя итоги рассмотрения сущности и методов деструктивной социальной инженерии отметим, что в ходе проведения исследования нами были рассмотрены шесть методов социальной инженерии, которые применяются в деструктивном плане и составляют угрозу экономической безопасности, прежде всего на уровне предприятия. Данные методы сочетают в себе различные мошеннические схемы различного уровня сложности. Безусловно сотрудникам службы безопасности организаций необходимо постоянно обновлять информацию о новых мошеннических методах и схемах с целью увеличения эффективности предупреждения их применения.

[6] Утечки данных. Россия. 2020 г. // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_финансы_2020_отчет.pdf (дата обращения: 28.05.2021).

Список использованной литературы

1. Поппер К. Нищета историзма / К. Поппер // Вопросы философии. — 1992. — № 10. — С. 29.

2. Фомина Н.А. Использование методов социальной инженерии при мошенничестве в социальных сетях : учеб. пособие / Н.А. Фомина. — Москва : Изд-во Инфра-М, 2015. — 443 с.

3. Веселов А.В. Социальная инженерия: сущность и парадигмальная методология : учебник / А.В. Веселов. — Москва : Изд-во Моск. ун-та, 2016. — 196 с.

4. Сычев А.М. Кибератаки: миф или реальность / А.М. Сычев // Финансы. — 2017. — № 1. — С. 61–65.

5. Ревенков П.В. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания : учеб. пособие / П.В. Ревенков, А.А. Бердюгин. — Москва : Юрайт, 2017. — 1760 с.

6. Резник Ю.М. Социальная инженерия: предметная область и границы применения : учеб. пособие / Ю.М. Резник. — Москва : Изд-во Моск. ун-та, 2016. —95 с.

7. Антонюк Г.А. Социальное проектирование и управление общественным развитием : учеб. пособие / Г.А. Антонюк. — Москва : Инфра-М, 2018. — 167 с.

8. Сухомлинский В.А. О социализации : учеб. пособие / В.А. Сухомлинский. — Москва : Политиздат, 2018. — 272 с.

9. Новикова Л.И. Функция социальной инженерии : учеб. пособие / Л.И. Новикова. — Москва : Юрайт, 2019. — 346 с.

10. Караковский В.А. Социальные технологии : учеб. пособие / В.А. Караковский. — Москва : Инфра-М, 2017. — 556 с.

11. Тубельский А.Н. Технологии социального воздействия на функциональные системы : учеб. пособие / А.Н. Тубельский. — Москва : Юрайт, 2018. — 76 с.

12. Сиротский А.А. Технологии социальной инженерии как потенциальная угроза в социальной сфере : учеб. пособие / А.А. Сиротский. — Москва : Изд-во РГСУ, 2016. — 170 с.

13. Жмуров Д.В. Эра Милосердия. Пути развития преступности / Д.В. Жмуров, А.А. Протасевич, А.С. Костромина. — DOI 10.17150/2411-6262.2019.10(2).18 // Baikal Research Journal. — 2019. — Т. 10, № 2. — URL: http://brj-bguep.ru/reader/article.aspx?id=23010.

14. Судакова Т.М. Осмысление будущего криминологии: обзор современных тенденций / Т.М. Судакова, В.А. Номоконов. — DOI 10.17150/2500-4255.2018.12(4).531-540 // Всероссийский криминологический журнал. — 2018. — Т. 12, № 4. — С. 531–540.

15. Коломинов В.В. Мошенничество в сфере компьютерной информации: криминалистический аспект / В.В. Коломинов. — DOI 10.17150/2072-0904.2015.6(1).26 // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2015. — Т. 6, № 1. — URL: http://eizvestia.isea.ru/reader/article.aspx?id=19976.

16. Кузнецов М.В. Социальная инженерия и социальные хакеры : учеб. пособие / М.В. Кузнецов, И.В. Симдянов. — Санкт-Петербург : БХВ-Петергбург, 2017. — 368 с.

Информация об авторах

Санина Людмила Валерьевна — кандидат экономических наук, доцент, кафедра мировой экономики и экономической безопасности, Байкальский государственный университет, г. Иркутск, Российская Федерация, e-mail: glv2010@yandex.ru.

Чепинога Оксана Александровна — кандидат экономических наук, доцент, заведующий кафедрой мировой экономики и экономической безопасности, Байкальский государственный университет, г. Иркутск, Российская Федерация, e-mail: chepinoga@mail.ru.

Ржепка Элина Александровна — кандидат географических наук, доцент, кафедра мировой экономики и экономической безопасности, Байкальский государственный университет, г. Иркутск, Российская Федерация, e-mail: rjepka@yandex.ru.

Палкин Олег Юрьевич — кандидат географических наук, доцент, кафедра мировой экономики и экономической безопасности, Байкальский государственный университет, г. Иркутск, Российская Федерация, e-mail: o.palkin2017@yandex.ru.

Authors

Liudmila V. Sanina — PhD in Economics, Associate Professor, Department of World Economy and Economic Security, Baikal State University, Irkutsk, Russian Federation, e-mail: glv2010@yandex.ru.

Oksana A. Chepinoga — PhD in Economics, Associate Professor, Head of Department of World Economy and Economic Security, Baikal State University, Russian Federation, e-mail: chepinoga@mail.ru.

Elina A. Rzhepka — PhD in Geography, Associate Professor, Department of World Economy and Economic Security, Baikal State University, Russian Federation, e-mail: rjepka@yandex.ru.

Oleg Yu. Palkin — PhD in Geography, Associate Professor, Department of World Economy and Economic Security, Baikal State University, Irkutsk, Russian Federation, e-mail: o.palkin2017@yandex.ru.

Для цитирования

Санина Л.В. Деструктивная социальная инженерия как угроза экономической безопасности: масштабы явления и меры предотвращения / Л.В. Санина, О.А. Чепинога, Э.А. Ржепка, О.Ю. Палкин. — DOI 10.17150/2411-6262.2021.12(2).14 // Baikal Research Journal. — 2021. — Т. 12, № 2.

For Citation

Sanina L.V., Chepinoga O.A., Rzhepka E.A., Palkin O.Yu. Destructive Social Engineering as a Threat to Economic Security: Methods Used and the Scale of the Phenomenon. *Baikal Research Journal*, 2021, vol. 12, no. 2. DOI: 10.17150/2411-6262.2021.12(2).14. (In Russian).