Обзорная статья
УДК 004.056; DOI: 10.61260/2218-13X-2025-4-94-106

ОБЗОР НАУЧНЫХ РАБОТ ПО СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

✉**Кюнер Андрей Павлович;**
Чечулин Андрей Алексеевич.
Санкт-Петербургский Федеральный исследовательский центр
Российской академии наук, Санкт-Петербург, Россия
✉***kunerandrey@mail.ru***

Аннотация. Различные информационные источники акцентируют внимание на методах социальной инженерии как наиболее значимых угрозах нарушения информационной безопасности организаций и финансового сектора. Несмотря на развитие технических, организационных, законодательных и других мер защиты, угроза, исходящая от социо-инженерных атак, остается актуальной. В целях разработки методики противодействия подобным угрозам необходимо рассмотреть существующие подходы к обеспечению защиты информации от данного рода атак. В статье представлен обзор опубликованных диссертационных работ и научных статей, в которых проводилось исследование механизмов проведения атак с использованием социальной инженерии и мер противодействия. Также приводится описание основных идей по разработке новых способов защиты, области применения данных инструментов, возможностей и ограничений. В ходе анализа предлагаемых в научных работах методик защиты от социоинженерных атак представлен перечень сходства и полноты описания нарушителя информационной безопасности, каналов осуществления атак, основных этапов совершения воздействия, предлагаемых защитных мер, научной новизны.

Ключевые слова: социальная инженерия, информационная безопасности, обзор научных работ, литературный анализ

Для цитирования: Кюнер А.П., Чечулин А.А. Обзор научных работ по социальной инженерии // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 4. С. 94–106. DOI: 10.61260/2218-13X-2025-4-94-106.

Review article

OVERVIEW OF SCIENTIFIC WORKS ON SOCIAL ENGINEERING

✉**Kyuner Andrey P.;**
Chechulin Andrey A.
St. Petersburg Federal Research Center of the Russian Academy of Sciences,
Saint-Petersburg, Russia
✉***kunerandrey@mail.ru***

Abstract. Various information resources focus on social engineering methods as the most significant threats to the information security of organizations and the financial sector. Despite the development of technical, organizational, lawmaking and other security measures, the threats caused by social engineering attacks remain relevant. This article describes an overview of published dissertations and research articles that have investigated the mechanisms of social engineering attacks and defensive mechanisms. The article also provides a description of the ideas for developing new protection methods, the scope of application of these instruments, capabilities and limitations. In the course of the analysis of the defensive methods against social engineering attacks proposed in scientific works, a list of similarities and completeness of the description of the information security violator, attack channels, the main stages of the impact, the proposed protective measures is presented, and also a scientific novelty.

Keywords: social engineering, information security, intruder model, review of scientific works, literary analysis

For citation: Kyuner A.P., Chechulin A.A. Overview of scientific works on social engineering // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 4. P. 94–106. DOI: 10.61260/2218-13X-2025-4-94-106.

Введение

В контексте кибербезопасности важную роль играет разработка технических и организационных мер защиты от атак с применением методов социальной инженерии. Предотвращение подобного типа атак является сложной задачей по ряду причин: пренебрежение пользователями политик информационной безопасности, стремительное развитие информационно-коммуникационных технологий (ИКТ) и запаздывающее внедрение средств безопасности, недостаточное внимание руководства организации по защите сотрудников, умышленное и непреднамеренное распространение информации о себе в открытых источниках и утечка персональных данных. Сценарии атаки зачастую основываются на знании атакующим личной жизни человека или событиях в обществе, также в основе могут быть использованы некоторые события в компании, ставшие известными другим лицам. Помимо вышеизложенных причин стоит отметить, что одной из причин применения злоумышленниками приемов социальной инженерии является возможность обходить существующие средства защиты информации.

Различные информационные ресурсы предлагают ряд однотипных подходов в решении задач противодействия социальной инженерии. При анализе интернет-порталов можно выделить следующие направления защиты: обновление программного обеспечения, использование антивирусных средств и спам-фильтров, проведение инструктажей и киберучений, усиленная аутентификация. В качестве причин успеха атаки выделяются человеческие черты: любопытство, страх, алчность и др. В научных статьях, посвященных изучению проблемы защиты финансовой и информационной сферы от угрозы социальной инженерии, немногие авторы уделяют внимание всестороннему изучению характеристик объекта атаки: демографических показателей, автобиографии, занимаемой должности и полномочий в информационной системе, применяемых политик безопасности, «пентеста» сотрудников. На основании полученных сведений проводится анализ возможности совершения атаки с использованием методов социальной инженерии и оценка рисков в случае результативной атаки.

На основании вышеизложенного можно сделать вывод, что применение методов социальной инженерии представляет высокую угрозу нарушения информационной безопасности, а злоумышленники оперативно находят способ снижения эффективности защитных мер пользователя, основываясь на психологических особенностях человека. Для исследования эффективности применяемых мер защиты требуется проанализировать существующие подходы по обеспечению информационной безопасности, в частности противодействия социальной инженерии, выделить преимущества и ограничения применения тех или иных механизмов защиты, выявить нерешенные вопросы в опубликованных работах и провести систематизацию данной области.

Основными целями данной научной статьи являются:

– выделение наиболее информативных научных работ, описывающих атаки с применением методов социальной инженерии;

– разделение области защиты от социоинженерных атак на составные элементы (атакующий, атакуемый, этапы атаки);

– обзор предлагаемых мер противодействия;

– выделение достоинств и недостатков в описании элементов атак.

Анализ научных работ

Для анализа изложенных подходов по обеспечению защиты от методов социальной инженерии в данном обзоре отражены имеющие высокую (по сравнению с другими) степень информативности статьи российских журналов и англоязычные работы, диссертационные исследования, находящиеся в открытом доступе. Работы, имеющие значительное сходство, не включены в данный обзор. Тактики проведения атаки, такие как «дорожное яблоко», фишинг (всех видов) и др., определяются каналом связи и описывают модель злоумышленника, поэтому не включены в текущий обзор. В табл. 1 приведены диссертационные работы по тематике социальной инженерии, включающие технические (компьютерные), гуманитарные и юридические науки. В табл. 1 и 2 представлена оценка объема описания элементов социоинженерной атаки: характеристик нарушителя, параметров жертвы, каналов осуществления атаки, основных этапов, описание защиты. Табл. 1 содержит российские и зарубежные диссертационные работы с 2013 по 2025 г. В табл. 2 представлены публикации из научной электронной библиотеки, а также зарубежные статьи, опубликованные в период с 2011 по 2025 г. Основным критерием оценки научных работ является полнота описания элементов атаки. На основе анализа представленных в научных работах примеров описания элементов социоинженерной атаки были выделены следующие характеристики и составлена следующая классификация.

Описание нарушителя

1. Цели атаки:
– финансовая выгода;
– получение конфиденциальной информации;
– репутационная;
– другие.
2. Возможности атакующего:
– психологический портрет (описание и квалификация);
– ресурсы (технические средства, сведения о жертве, численность).
3. Объекты атаки:
– организации;
– частные лица.
4. Местонахождение:
– территория страны;
– за границей.
5. Сценарии атаки:
– метод установления контакта (претекстинг, вишинг и пр.);
– способ имперсонализации.
6. Характер атаки:
– целевой;
– массовый.

Описание жертвы

1. Уровень доступа:
– в информационной системе;
– к конфиденциальной информации;
– прочие люди и сведения.
2. Психологический портрет:
– демографические показатели;
– психологические качества и профессиональные навыки;
– опыт противодействия атакам.

3. Наличие средств защиты информации:
– формальные;
– неформальные.

Каналы осуществления атаки

1. Физические:
– вербальный контакт;
– машинный носитель информации;
– бумажный носитель информации.
2. Дистанционные:
– средства мгновенного обмена сообщениями;
– телефонная связь (сообщение и звонок, стационарные и мобильные);
– социальные сети;
– точки доступа к сети (в том числе в киберфизических системах);
– электронная почта (корпоративная и личная);
– интернет-ресурс (сайт, файловое хранилище, магазин приложений).

Этапы атаки

1. Подготовка:
– постановка целей атаки;
– подготовка технических средств;
– подготовка сценария;
– поиск информации о жертве;
– выбор категорий жертв.
2. Установление доверия:
– обход спам-фильтров (при наличии);
– установление связи с жертвой;
– психологическое воздействие;
– получение контроля над жертвой.
3. Выполнение действий:
– обход средств защиты;
– нарушение безопасности объекта атаки.
4. Завершающий этап:
– сокрытие следов;
– достижение целей;
– анализ результатов.

Для заполнения содержимого табл. 1 и 2 на основании представленной выше классификации введена шкала оценки полноты описания элементов социоинженерной атаки. Степень полноты описания можно разделить на отсутствие описания (–), высокую (В), среднюю (С) и низкую (Н). Высокая степень соответствует наличию не менее 80 % характеристик в научных работах, средняя – 50–79 %. Следует отметить, что многие диссертационные работы подробно описывают только определенные аспекты элементов социальной инженерии.

Таблица 1

Анализ диссертационных работ

Автор	Описание нарушителя	Описание жертвы	Каналы	Этапы	Предлагаемые защитные меры
Российские работы					
Азаров [1]	С	С	Н	Н	Оценка вероятности утраты конфиденциального документа на основе уязвимостей пользователя
Абрамов [2]	В	С	В	Н	Расчет вероятности успеха многоходовой атаки на основе профиля пользователя в социальной сети
Старостенко [3]	С	С	С	С	Методика расследований преступлений в сфере ИКТ
Зотина [4]	В	С	С	Н	Оперативно-розыскные мероприятия, портрет мошенника, законодательные меры, профилактика населения
Зарубежные работы					
Hussain [5]	С	С	В	С	Программы повышения осведомленности и проведения киберучений по каждой тактике атаки
Alharthi [6]	–	В	В	–	Оценка осведомленности сотрудников для создания модели политик безопасности
Algarni [7]	Н	С	Н	–	Оценка уязвимостей пользователя на основе данных из социальной сети и обзора литературы по социальной инженерии
Albladi [8]	С	С	Н	С	Расчет вероятности успеха различных техник атаки в зависимости от полученных в ходе опроса сведений
Bulle [9]	–	Н	С	–	Практическая проверка подверженности различным техникам в зависимости от возраста
Heartfield [10]	С	Н	В	С	Разработка соответствующих каждому типу атаки обучающих методик
Mouton [11]	В	С	В	В	Модель выявления атак на основе примеров техник, целей нарушителя и каналов
Kikerpill [12]	Н	Н	Н	–	Диагностика защитных рефлексов при вербальном воздействии
Jacob [13]	Н	Н	С	–	Анализ техник мошенничества и оценка влияния на различные категории граждан

Таблица 2

Анализ научных статей

Автор (один из авторов)	Описание нарушителя	Описание жертвы	Каналы	Этапы	Предлагаемые защитные меры
Российские работы					
Neumeier [14]	Н	–	С	В	Частные случаи организационных, программных и психологических мер
Санина [15]	С	–	С	С	Обзор причин утечек данных по сферам деятельности
Журин [16]	С	Н	Н	В	Сравнительные анализ технических средств
Федосенко [17]	С	Н	С	С	Повышение грамотности населения на основе реальных сценариев атак
Наумова [18]	В	–	В	–	Программные средства для каждого типа устройств и каналов
Путято [19]	Н	–	В	–	Антивирусные и антифишинговые программы
Воробьева [20]	С	–	С	С	Внутренняя безопасность, обучение, контроль и запрет доступа
Полянская [21]	С	Н	Н	С	Регулярное информирование населения
Максименко [22]	С	–	Н	С	Обучение и обновление политик информационной безопасности
Зарубежные работы					
Rao [23]	В	С	В	–	Расширенные рекомендации для политики организаций и частных лиц
Krombholz [24]	В	–	В	–	Внедрение политик использования сервисов передачи данных на предприятии
Foozy [25]	В	–	В	–	Описание сценариев атак
Naz [26]	С	–	Н	С	Обзор возможностей и недостатков различных методов защиты
Salahdine [27]	В	Н	В	С	Обзор достоинств и недостатков мер против каждого вида атак
Chapagain [28]	С	–	Н	–	Комплекс организационных и технических мер
Alnusif [29]	С	–	Н	С	Анализ сетевого трафика
Huseinov [30]	Н	В	С	–	Выявление подверженных атакам лиц на основе демографических данных и машинного обучения

На основе анализа сведений, представленных в табл. 1 и 2, на рисунке отражено соотношение полноты описания элементов социоинженерных атак. Представленные диаграммы позволяют сделать следующие выводы:

1. Описанию нарушителя уделяется недостаточно внимания;

2. Характеристики защитных механизмов пользователя и уровень доступа в системах почти не рассматриваются в контексте социоинженерных атак;

3. Не приводится описания задач мониторинга информационной безопасности, сбора сведений от сотрудников, обзора информационных ресурсов в целях определения сценариев атак;

4. Описание этапов социоинженерной атаки проводится шаблонно, не разрабатываются защитные механизмы для каждой стадии атаки.

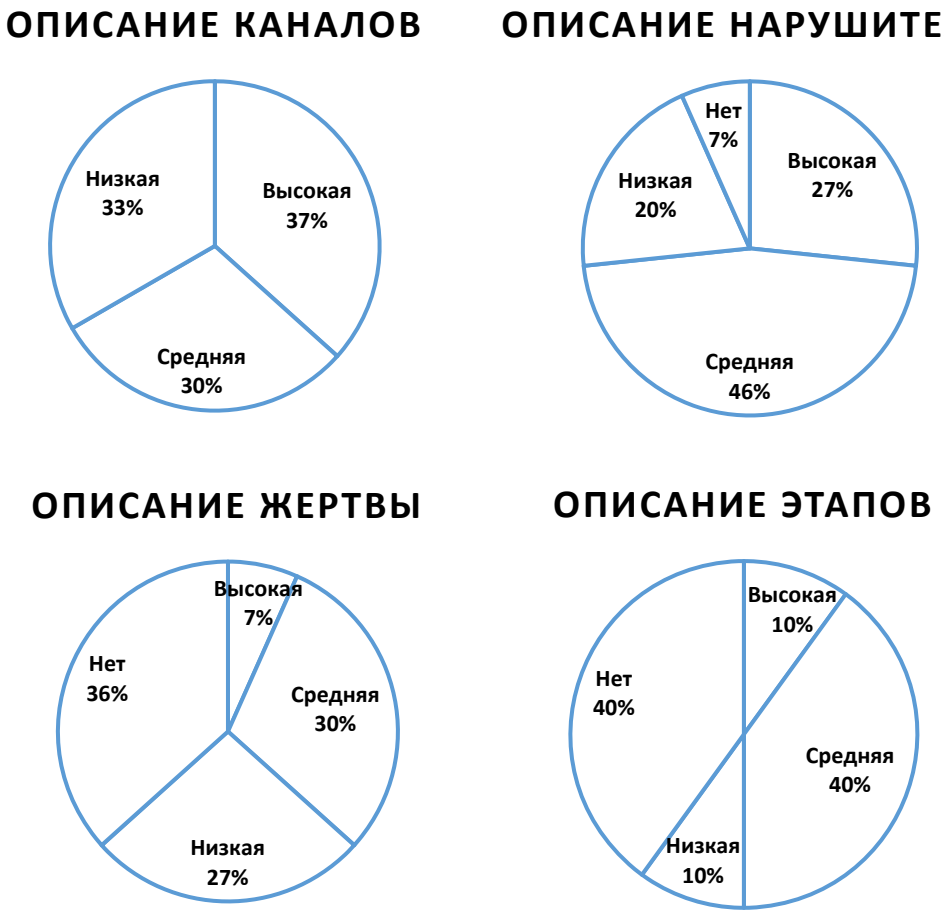

Рис. **Полнота нарушителя, жертвы, каналов и этапов атаки в научных работах**

Исходя из представленных на рисунке сведений можно сделать выводы: в половине работ полнота описания этапов атаки не позволяет оценить возможные варианты внедрения защитных мер; описание характеристик потенциальной жертвы в большинстве работ сводится к психологическим и демографическим показателям без учета уровня доступа в системе и оценки устойчивости к атакам; описание нарушителя информационной безопасности приводится на удовлетворительном уровне за счет детального разбора в ряде работ тактик атаки; распределение полноты описания каналов атаки имеет близкие значения.

Также следует отметить, что в ряде зарубежных работ по данной тематике представлено более подробное описание нарушителя информационной безопасности и этапов социоинженерной атаки, нежели в отечественных сборниках статей. При этом в ряде российских работ приведены примеры программных средств защиты и организационных мер в зависимости от канала атаки. Иностранные работы в основном описывают разработку защитных мер на основе известных тактик атаки. Наиболее подробное описание представлено в диссертационной работе Mouton [11] и научной публикации Salahdine [27], при этом работа Mouton [11] описывает применение защитных мер на основе общепринятых тактик социальной инженерии, не закладывается возможность модернизации мер в зависимости от реальных атак и не рассматривает выработку защитных мер на каждом этапе атаки. В тоже время статьи Neumeier [14], Воробьевой [20]

и Chapagain [28] описывают общепринятые меры защиты от атак. В диссертациях Старостенко [3] и Зотина [4] представлено информативное описание нарушителя, использующего социальную инженерию исключительно в целях получения денежных средств физических лиц, что позволяет применять данные исследования в расследованиях преступлений, совершаемых дистанционно, при этом ни одна из представленных в обзоре работ не описывает действия специалистов по информационной безопасности организаций по повышению защищенности сотрудников от социоинженерных атак. В научных работах Зотиной [4], Федосенко [17], Полянской [21] предлагается мера противодействия, основанная на информировании населения за счет средств массовой информации, эффективная против нецелевых атак. На практике данная мера реализуется недостаточно оперативно и не учитывает возможность предотвращения предпосылок к совершению кибермошенничества.

Оригинальный подход к противодействию атакам представлен в работах Наумовой [18], Krombholz [24] и Alnusif [29], где предлагаются способы повышения защищенности каналов связи между злоумышленником и потенциальной жертвой путем внедрения организационных и программных мер защиты и анализа трафика. Исследовательские работы Hussain [5] и Heartfield [10] описывают выработку методики противодействия социальной инженерии путем проведения основанных на различных видах атак киберучений, основной проблемой данного подхода является недостаточный охват обучающейся аудитории. В исследованиях Абрамова [2] и Algarni [7] информация из профиля в социальной сети может быть недостаточной для оценки уязвимостей, особенно при отсутствии или сокрытии профиля от посторонних. Подробное описание этапов социоинженерной атаки, изложенное в работах Mouton [11] и Журина [16], позволяет выстраивать систему защиты на разных стадиях, однако в работах не описано применение мероприятий на каждой стадии.

В работах Азарова [1], Абрамова [2], Alharthi [6], Algarni [7], Albladi [8], Bulle [9], Kikerpill [12], Huseynov [30] построение защиты основывается на исследовании параметров потенциальной жертвы. Исследования Hussain [5], Heartfield [10], Mouton [11], Jacob [13] Федосенко [17], Foozy [25] и Комашинского [31] акцентируют внимание на построении системы защиты на основе общеизвестных тактик и характеристик злоумышленника.

В последние годы наблюдается тенденция всестороннего внедрения технологий машинного обучения в информационную сферу, в частности для задач информационной безопасности. Разрабатываются методы оценки уязвимостей на основе демографических и автобиографических сведений (Huseynov [30]) с применением алгоритмов машинного обучения взамен методик расчета вероятности, представленных в исследованиях Азарова [1] и Абрамова [2]. Дальнейшим развитием алгоритмов может послужить автоматизация сбора сведений о злоумышленнике и выявление потенциальных жертв, что повысит эффективность центров мониторинга и реагирования по предотвращению кибератак, в частности социо-инженерных. Публикации методов защиты от социальной инженерии последних лет акцентируют внимание на внедрении алгоритмов машинного обучения для распознавания атак. При исследовании зависимости полноты описания социальной инженерии от даты публикации работы наблюдается незначительное увеличение, связанное с применением новых средств передачи данных (мессенджеров) и QR-кодов для осуществления атак. В наиболее поздних работах рассматривается поиск корреляции статистики атак с демографическими показателями.

Заключение

При изучении проблемы разработки мер противодействия методам социальной инженерии в контексте кибербезопасности были рассмотрены 30 научных работ, из которых: 9 российских научных статей и 8 зарубежных, 4 российские диссертационные работы и 9 зарубежных. Рассмотрены различные подходы по обеспечению информационной безопасности сотрудников и частных лиц перед угрозой социоинженерных атак,

предлагаемые в научных работах. Представлено краткое изложение предлагаемых в работах мер противодействия социоинженерным атакам, проанализированы сходства и различия подходов. Обзор научных статей и диссертационных работ позволяет сделать выводы о том, что основные направления изучения проблемы защиты пользователей от кибератак фокусируют внимание на анализе уязвимостей человека, разработке политик доступа к информационным ресурсам и каналам, создании обучающих программ, всестороннем внедрении технических решений. С учетом существующих наработок в области описания элементов социоинженерной атаки разработана схема, представленная в работе [32], позволяющая рассмотреть возможность внедрения защитных механизмов на разных стадиях атаки в зависимости от характеристик атакующего и атакуемого.

В результате рассмотрения научных подходов по разработке методик защиты от социальной инженерии были выявлены следующие особенности: не изучены возможности подразделений центров мониторинга и реагирования по сбору данных о нарушителях и построении стратегии защиты на основании этих сведений; предпосылки к осуществлению атак рассматриваются кратко или не изложены; противодействия социальной инженерии представлено на последних этапах атаки. Существующие подходы по защите пользователей от угрозы социальной инженерии (если не рассматривать вопросы защиты населения в целом) нацелены на внедрение организационных и технических мер защиты, которые не всегда могут быть реализованы не только ввиду технической сложности, неудобства, финансовых издержек, но и из-за психологических особенностей самого сотрудника. При этом наиболее целесообразным решением будет повысить возможность специалистов по информационной безопасности по оперативному и заблаговременному выявлению векторов атаки. В данном случае возникают две важные задачи: недопущение установления контакта злоумышленника с потенциальной жертвой, а вследствие построения доверия; оперативный сбор сведений об атаках.

Социоинженерные атаки развиваются с появлением новых технологий и сценариев, при этом существуют определенные сходства. Первые научные работы по социальной инженерии изучали целевые атаки для получения конфиденциальной информации, последние – сосредоточены на противодействии дистанционному мошенничеству. Задача специалистов по информационной безопасности – оперативно выявить новые сценарии атак и принять соответствующие меры, важную роль при этом будет играть автоматизация процесса с использованием передовых инструментов и технологий. При глубоком изучении реальных сценариев социоинженерных атак однотипные и менее техничные атаки перестают представлять угрозу для большинства потенциальных жертв ввиду своего устаревания. Последние исследования в области социальной инженерии показывают тенденцию постепенного внедрения технологий искусственного интеллекта для оценки уязвимостей пользователя и распознавания фишинговых атак.

Работа выполнена при поддержке гранта Российского научного фонда и Санкт-Петербургского научного фонда № 25-11-20028 (https://rscf.ru/project/25-11-20028/) в СПб ФИЦ РАН.

Список источников

1. Азаров А.А. Вероятностно-реляционные модели и алгоритмы обработки профиля уязвимостей пользователей при анализе защищённости персонала информационных систем от социоинженерных атак: дис. … канд. техн. наук. СПб., 2013. 232 с.

2. Абрамов М.В. Методы и алгоритмы анализа защищённости пользователей информационных систем от социоинженерных атак: оценка параметров моделей: дис. … канд. техн. наук. СПб., 2018. 232 с.

3. Старостенко Н.И. Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий: дис. … канд. юрид. наук. Краснодар, 2023. 230 с.

4. Зотина Е.В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование: дис. … канд. юрид. наук. Казань, 2024. 249 с.

5. Aldawood H.A. An Awareness Policy Framework for Cyber Security Social Engineering Threats: diss. The University of Newcastle, Australia. 2020.

6. Social Engineering Defense Mechanisms and InfoSec Policies: A Survey and Qualitative Analysis. URL: https://escholarship.org/uc/item/7h783589 (дата обращения: 20.08.2025).

7. The impact of source characteristics on users' susceptibility to social engineering Victimization in social networks. URL: https://eprints.qut.edu.au/95604/ (дата обращения: 23.08.2025).

8. A user-centric framework for addressing vulnerability to social engineering in social networks: a mixed methods study of a Saudi academic community. URL: https://stax.strath.ac.uk/concern/theses/n009w2322 (дата обращения: 26.08.2025).

9. Bullee, J-W. Enschede: Centre for Telematics and Information Technology (CTIT). URL: https://research.utwente.nl/en/publications/experimental-social-engineering-investigation-and-prevention/ (дата обращения: 26.08.2025).

10. Utilising the concept of human-as-a-security-sensor for detecting semantic social engineering attacks. URL: https://gala.gre.ac.uk/id/eprint/23420/ (дата обращения: 30.08.2025).

11. Mouton F. Social engineering attack detection model: diss. University of Pretoria, South Africa. 2018.

12. Kikerpill K. Crime-as-communication: detecting diagnostically useful information from the content and context of social engineering attacks. 2021.

13. Vargis J. M. Analyzing COVID-19 Era Cyber Threats on the Elderly: Toward Realizing N-Of-1 Countermeasures to Enhance Cyber Situational Awareness of Social Engineering Attacks: diss. Marymount University, 2023. DOI:10.13140/RG.2.2.25092.81289.

14. Social engineering, imperfect human / J. Neumeier [et al.] // Economic Vector. 2022. № 2 (29). P. 11–16. DOI: 10.36807/2411-7269-2022-2-29-11-16.

15. Деструктивная социальная инженерия как угроза экономической безопасности: масштабы явления и меры предотвращения / Л. В. Санина [и др.] // Baikal Research Journal. 2021. Т. 12. № 2. DOI: 10.17150/2411-6262.2021.12(2).14.

16. Журин С.И., Д.Е. Комарков Защита внешнего информационного периметра организации от целевого фишинга // Безопасность информационных технологий. 2018. Т. 25. № 4. С. 95–107.

17. Федосенко М.Ю., Менщиков А.А. Возможности применения методов социальной инженерии в организации телефонного мошенничества // Экономика и качество система связи. 2021. № 4 (22). С. 36–47.

18. Наумова К.Д., Радыгин В.Ю. Исследование основных методов противодействия атакам, основанным на методах социальной инженерии, на предмет их эффективности и применимости к современной ситуации в РФ // Инновационные механизмы управления цифровой и региональной экономикой: сб. материалов V Междунар. студ. науч. конф. Москва, 2023. С. 145–158.

19. Исследование механизмов социальной инженерии и анализ методов противодействия / В.Ю. Евглевский [и др.] // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2021. № 2. С. 57–68.

20. Воробьева И.А., Сазонов А.И. Методы социальной инженерии в контексте кибербезопасности // Colloquium-Journal. 2020. № 8-1 (60). С. 65–70.

21. Полянская Е.П. Использование информационно-телекоммуникационных технологий в методах социальной инженерии // Криминологический журнал. 2023. № 1. С. 204–209. DOI: 10.24412/2687-0185-2023-1-204-209.

22. Максименко Р.О., Звягинцева П.А. Типовой алгоритм воздействия в социальной инженерии // Интерэкспо Гео-Сибирь. 2019. Т. 6. № 2. С. 33–38. DOI: 10.33764/2618-981X-2019-6-2-33-38.

23. Rao U. H., Nayak U. Social engineering // The InfoSec Handbook: An Introduction to Information Security. Berkeley, CA: Apress, 2014. P. 307–323. DOI: 10.1007/978-1-4302-6383-8_15.

24. Advanced social engineering attacks / K. Krombholz [et al.] // Journal of Information Security and applications. 2015. T. 22. P. 113–122. DOI: 10.1016/j.jisa.2014.09.005.

25. Generic taxonomy of social engineering attack and defence mechanism for handheld computer study / C.F.M. Foozy [et al.] // Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor. 2011.

26. A comprehensive survey on social engineering-based attacks on social networks / A. Naz [et al.] // International Journal of Advanced and Applied Sciences. 2024. T. 11. №. 4. C. 139–154. DOI: 10.21833/ijaas.2024.04.016.

27. Salahdine F., Kaabouch N. Social engineering attacks: A survey // Future internet. 2019. T. 11. №. 4. C. 89. DOI: 10.3390/fi11040089.

28. SEAtech: Deception Techniques in Social Engineering Attacks: An Analysis of Emerging Trends and Countermeasures / D. Chapagain [et al.] // arXiv preprint arXiv:2408.02092. 2024. DOI: 10.48550/arXiv.2408.02092.

29. Alnusif M. Emerging Threats in Cybersecurity: A Comprehensive Analysis of DDoS and Social Engineering Attacks // International Journal of Engineering and Computer Science. 2025. Vol. 13, Iss. 07. P. 27473–27487. DOI: 10.18535/ijecs.v14i07.5185.

30. Huseynov F., Ozdenizci Kose B. Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks // Information Development. 2024. T. 40. №. 2. C. 298–318. DOI: 10.1177/02666669221116336.

31. Комашинский Д.В., Котенко И.В., Чечулин А.А. Категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности. 2011. Т. 7. № 2. С. 102–106.

32. Дайнеко А.С., Кюнер А.П., Чечулин А.А. Социальная инженерия. Характеристики атакующего и схема атаки // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Сер. 1: Естественные и технические науки. 2024. № 3. С. 68–74. DOI: 10.46418/2079-8199_2024_3_11.

References

1. Azarov A.A. Veroyatnostno-relyacionnye modeli i algoritmy obrabotki profilya uyazvimostej pol'zovatelej pri analize zashchishchyonnosti personala informacionnyh sistem ot socioinzhenernyh atak: dis. … kand. tekhn. nauk. SPb., 2013. 232 s.

2. Abramov M.V. Metody i algoritmy analiza zashchishchyonnosti pol'zovatelej informacionnyh sistem ot socioinzhenernyh atak: ocenka parametrov modelej: dis. … kand. tekhn. nauk. SPb., 2018. 232 s.

3. Starostenko N.I. Pervonachal'nyj etap rassledovaniya hishchenij, sovershennyh s primeneniem metodov social'noj inzhenerii i informacionno-telekommunikacionnyh tekhnologij: dis. … kand. yurid. nauk. Krasnodar, 2023. 230 s.

4. Zotina E.V. Moshennichestvo s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij i priemov social'noj inzhenerii: kriminologicheskoe issledovanie: dis. … kand. yurid. nauk. Kazan', 2024. 249 s.

5. Aldawood H.A. An Awareness Policy Framework for Cyber Security Social Engineering Threats: diss. The University of Newcastle, Australia. 2020.

6. Social Engineering Defense Mechanisms and InfoSec Policies: A Survey and Qualitative Analysis. URL: https://escholarship.org/uc/item/7h783589 (data obrashcheniya: 20.08.2025).

7. The impact of source characteristics on users\' susceptibility to social engineering Victimization in social networks. URL: https://eprints.qut.edu.au/95604/ (data obrashcheniya: 23.08.2025).

8. A user-centric framework for addressing vulnerability to social engineering in social networks: a mixed methods study of a Saudi academic community. URL: https://stax.strath.ac.uk/concern/theses/n009w2322 (data obrashcheniya: 26.08.2025).

9. Bullee, J-W. Enschede: Centre for Telematics and Information Technology (CTIT). URL: https://research.utwente.nl/en/publications/experimental-social-engineering-investigation-and-prevention/ (data obrashcheniya: 26.08.2025).

10. Utilising the concept of human-as-a-security-sensor for detecting semantic social engineering attacks. URL: https://gala.gre.ac.uk/id/eprint/23420/ (data obrashcheniya: 30.08.2025).

11. Mouton F. Social engineering attack detection model: diss. University of Pretoria, South Africa. 2018.

12. Kikerpill K. Crime-as-communication: detecting diagnostically useful information from the content and context of social engineering attacks. 2021.

13. Vargis J. M. Analyzing COVID-19 Era Cyber Threats on the Elderly: Toward Realizing N-Of-1 Countermeasures to Enhance Cyber Situational Awareness of Social Engineering Attacks: diss. Marymount University, 2023. DOI:10.13140/RG.2.2.25092.81289.

14. Social engineering, imperfect human / J. Neumeier [et al.] // Economic Vector. 2022. № 2 (29). P. 11–16. DOI: 10.36807/2411-7269-2022-2-29-11-16.

15. Destruktivnaya social'naya inzheneriya kak ugroza ekonomicheskoj bezopasnosti: masshtaby yavleniya i mery predotvrashcheniya / L. V. Sanina [i dr.] // Baikal Research Journal. 2021. T. 12. № 2. DOI: 10.17150/2411-6262.2021.12(2).14.

16. Zhurin S.I., D.E. Komarkov Zashchita vneshnego informacionnogo perimetra organizacii ot celevogo fishinga // Bezopasnost' informacionnyh tekhnologij. 2018. T. 25. № 4. S. 95–107.

17. Fedosenko M.Yu., Menshchikov A.A. Vozmozhnosti primeneniya metodov social'noj inzhenerii v organizacii telefonnogo moshennichestva // Ekonomika i kachestvo sistema svyazi. 2021. № 4 (22). S. 36–47.

18. Naumova K.D., Radygin V.Yu. Issledovanie osnovnyh metodov protivodejstviya atakam, osnovannym na metodah social'noj inzhenerii, na predmet ih effektivnosti i primenimosti k sovremennoj situacii v RF // Innovacionnye mekhanizmy upravleniya cifrovoj i regional'noj ekonomikoj: sb. materialov V Mezhdunar. stud. nauch. konf. Moskva, 2023. S. 145–158.

19. Issledovanie mekhanizmov social'noj inzhenerii i analiz metodov protivodejstviya / V.Yu. Evglevskij [i dr.] // Elektronnyj setevoj politematicheskij zhurnal «Nauchnye trudy KubGTU». 2021. № 2. S. 57–68.

20. Vorob'eva I.A., Sazonov A.I. Metody social'noj inzhenerii v kontekste kiberbezopasnosti // Colloquium-Journal. 2020. № 8-1 (60). S. 65–70.

21. Polyanskaya E.P. Ispol'zovanie informacionno-telekommunikacionnyh tekhnologij v metodah social'noj inzhenerii // Kriminologicheskij zhurnal. 2023. № 1. S. 204–209. DOI: 10.24412/2687-0185-2023-1-204-209.

22. Maksimenko R.O., Zvyaginceva P.A. Tipovoj algoritm vozdejstviya v social'noj inzhenerii // Interekspo Geo-Sibir'. 2019. T. 6. № 2. S. 33–38. DOI: 10.33764/2618-981X-2019-6-2-33-38.

23. Rao U. H., Nayak U. Social engineering // The InfoSec Handbook: An Introduction to Information Security. Berkeley, CA: Apress, 2014. P. 307–323. DOI: 10.1007/978-1-4302-6383-8_15.

24. Advanced social engineering attacks / K. Krombholz [et al.] // Journal of Information Security and applications. 2015. T. 22. P. 113–122. DOI: 10.1016/j.jisa.2014.09.005.

25. Generic taxonomy of social engineering attack and defence mechanism for handheld computer study / C.F.M. Foozy [et al.] // Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor. 2011.

26. A comprehensive survey on social engineering-based attacks on social networks / A. Naz [et al.] // International Journal of Advanced and Applied Sciences. 2024. T. 11. №. 4. S. 139–154. DOI: 10.21833/ijaas.2024.04.016.

27. Salahdine F., Kaabouch N. Social engineering attacks: A survey // Future internet. 2019. T. 11. №. 4. S. 89. DOI: 10.3390/fi11040089.

28. SEAtech: Deception Techniques in Social Engineering Attacks: An Analysis of Emerging Trends and Countermeasures / D. Chapagain [et al.] // arXiv preprint arXiv:2408.02092. 2024. DOI: 10.48550/arXiv.2408.02092.

29. Alnusif M. Emerging Threats in Cybersecurity: A Comprehensive Analysis of DDoS and Social Engineering Attacks // International Journal of Engineering and Computer Science. 2025. Vol. 13, Iss. 07. P. 27473–27487. DOI: 10.18535/ijecs.v14i07.5185.

30. Huseynov F., Ozdenizci Kose B. Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks // Information Development. 2024. T. 40. №. 2. S. 298–318. DOI: 10.1177/02666669221116336.

31. Komashinskij D.V., Kotenko I.V., Chechulin A.A. Kategorirovanie veb-sajtov dlya blokirovaniya veb-stranic s nepriemlemym soderzhimym // Sistemy vysokoj dostupnosti. 2011. T. 7. № 2. S. 102–106.

32. Dajneko A.S., Kyuner A.P., Chechulin A.A. Social'naya inzheneriya. Harakteristiki atakuyushchego i skhema ataki // Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizajna. Ser. 1: Estestvennye i tekhnicheskie nauki. 2024. № 3. S. 68–74. DOI: 10.46418/2079-8199_2024_3_11.

Информация о статье:
Статья поступила в редакцию: 20.09.2025; одобрена после рецензирования: 31.10.2025;
принята к публикации: 05.11.2025

Information about the article:
The article was submitted to the editorial office: 20.09.2025; approved after review: 31.10.2025;
accepted for publication: 05.11.2025

Информация об авторах:
Кюнер Андрей Павлович, аспирант Санкт-Петербургского федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, 14 линия В.О., д. 39), e-mail: kunerandrey@mail.ru, SPIN-код: 7665-5138
Чечулин Андрей Алексеевич, ведущий научный сотрудник Санкт-Петербургского федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, 14 линия В.О., д. 39), кандидат технических наук, доцент, e-mail: andreych@bk.ru, https://orcid.org/0000-0001-7056-6972

Information about authors:
Kyuner Andrey P., postgraduate student of St. Petersburg Federal Research Center of the Russian Academy of Sciences (199178, Saint-Petersburg, 14 line V.O., 39), e-mail: kunerandrey@mail.ru, SPIN: 7665-5138
Chechulin Andrey A., leading researcher of St. Petersburg Federal Research Center of the Russian Academy of Sciences (199178, Saint-Petersburg, 14 line V.O., 39), candidate of technical sciences, associate professor, e-mail: andreych@bk.ru, https://orcid.org/0000-0001-7056-6972