ВВЕДЕНИЕ

Деструктивная социальная инженерия (ДСИ) представляет собой широкий класс целенаправленных воздействий, в которых злоумышленник использует доверие [1–5], авторитет [5–9], срочность [10–18], страх [19–26], дефицит информации [27–30] и иные [31–49] психологические факторы, чтобы склонить человека к нужному действию. Её практические формы не ограничиваются фишингом [50–60]; к ним также относятся подмена личности [61–63] и реквизитов [64–70], компрометация деловой переписки [71–79], ложная техническая поддержка [80–90], инвестиционные [91–99] и романтические [100–111] схемы, имитация государственных органов [112–120], мошенничество при трудоустройстве [121–124], с платежами [125–130] и доставкой [131–143]. Такое многообразие делает ДСИ разнородной угрозой, для которой недостаточно единственного универсального описания или одной защитной меры.

Опасность ДСИ состоит в том, что объектом первичного воздействия становится человек (сотрудник, клиент или гражданин), а результатом может быть не только разовая финансовая потеря, но и раскрытие учётных данных, захват аккаунта, компрометация корпоративной переписки, нарушение деловых процессов и последующие повторные атаки. Технические средства защиты остаются необходимыми, но не устраняют риск полностью, если атакующему удаётся убедить жертву самостоятельно подтвердить операцию, передать код или предоставить доступ. Поэтому противодействие должно объединять не только технические, но и организационно-процессуальные и поведенческие меры, привязанные к конкретным сценариям реализациям атак [11–18].

В 2025 году противоправные деяния, совершаемые с использованием информационно-телекоммуникационных технологий,

сохраняют статус одного из ключевых факторов риска для граждан и организаций. По данным Генеральной прокуратуры Российской Федерации, по итогам 2025 года на IT-преступность приходилось 38,2 % всех зарегистрированных преступлений; совокупный массив таких деяний составил около 627 тыс. случаев. Одновременно фиксируется доминирование мошенничества в структуре дистанционной преступности, где за тот же период зарегистрировано 382,3 тыс. мошенничеств, из которых 84 % (322,8 тыс.) составили IT-мошенничества [19].

Содержательно значительная часть указанных эпизодов реализуется именно как деструктивная социальная инженерия, ибо злоумышленник не столько «взламывает» технические средства, сколько управляет действиями человека (жертвы или сотрудника организации), побуждая его самостоятельно раскрыть сведения, предоставить доступ или инициировать перевод денежных средств. Практическая значимость этого компонента подтверждается как правоохранительной, так и регуляторной статистикой. Так, МВД России в официальной сводке отмечает, что за январь–ноябрь 2025 года зарегистрировано меньше преступлений, совершённых с использованием информационно-коммуникационных технологий, однако при этом в массиве дистанционных посягательств сохраняется высокая доля мошеннических схем [20].

Дополнительным эмпирическим аргументом выступают данные Банка России по инцидентам информационной безопасности при переводе денежных средств: в III квартале 2025 года банки отразили 28,5 млн попыток совершения мошеннических операций и предотвратили хищение средств на 3,5 трлн руб. При этом злоумышленникам удалось совершить 460,1 тыс. мошеннических операций, а объём фактических хищений составил 8,2 млрд руб. Важно, что в отчётности Банка России среди основных типов выявляемых компьютерных атак устойчиво выделяется использование методов социальной инженерии (например, в III квартале 2025 года — 13 166 случаев фиксации данного типа атак) [21].

Наконец, правоохранительные органы прямо указывают на «сценарный» характер массовых мошеннических кампаний. Так, в 2025 году среди наиболее распространённых дистанционных схем называются сценарии с переводом денег на «безопасный счёт», фишинговые ссылки и иные формы обмана, реализуемые через звонки и мессенджеры. Совокупность приведённых данных показывает, что социальная инженерия представляет собой

не частный случай киберугроз, а самостоятельный и масштабный класс воздействий, требующий формализованной классификации, сопоставимой оценки и управляемых мер защищённости [22].

Монография посвящена анализу информационных рисков деструктивной социальной инженерии и разработке подхода, обеспечивающего их сценарную классификацию, оценку и управление защищённостью на основе воспроизводимых процедур и сопоставимых статистических показателей. Основной целью данной работы является разработка сценарно-ориентированного подхода к оценке информационных рисков деструктивной социальной инженерии и управление защищённостью на основе сопоставимой аналитики и систематизации мер противодействия.

Для реализации поставленной цели решаются следующие ключевые задачи: разработка сценарной классификации деструктивной социальной инженерии (единый шаблон сценария и правила разграничения типов атак и последствий); формирование сопоставимой модели оценки риска по выбранным категориям на основе статистики с выделением показателей «масштаб — тяжесть»; разработка инструментария управления защищённостью через систему мер по сценариям и матричный контроль покрытия.

Работа выполнена при частичной поддержке РФФИ (проект 18-29-22042), а также в рамках проекта «Безопасный Интернет» (рег. № АААА-А18-118050700061-7).

Авторы выражают благодарность В.Д. Любарскому за содействие в подготовке материала для настоящей монографии.