DOI 10.36622/1682-7813.2025.28.2.011
УДК 004.056

РИСКИ РЕАЛИЗАЦИИ КИБЕРАТАК: ОСОБЕННОСТИ ВТОРЖЕНИЙ КЛАССА “СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ”

Г.А. Остапенко, А.А. Остапенко, М.А. Грамыкин, М.В. Кондратьев, Н.С. Харламов

Данная научная статья посвящена исследованию способов и мер по обнаружению и регистрации атак класса “социальная инженерия”, осуществляемых на социо-информационное пространство, как меры противодействия атакам заданного типа. Проанализированы различные сценарии атак, представляющие из себя комбинации различных техник. Особое внимание уделено возможности злоумышленников использовать как технические аспекты, так и социально-психологические в ходе атаки. На основе полученных результатов была построена матрица с объектами воздействия, учитывающая различные шаблоны по социальной инженерии. Благодаря объектам воздействия, полученным в результате анализа используемых злоумышленниками техник и социально-психологических уязвимостей человека, возможно построить матрицу с регламентами, представляющими меры и средства для обнаружения. Результаты исследования представляют ценный вклад в повышение уровня защищенности социо-информационного пространства.

Ключевые слова: социальная инженерия, социально-психологические уязвимости, технические уязвимости, регламенты, безопасность.

Введение

Регламенты обеспечения ИБ занимают среднее положение в трехуровневой иерархической модели документов по защите организации. На втором уровне, находятся организационно-правовые аспекты, определяющие требования и рекомендации по применению процедур по обеспечению ИБ [1]. В большинстве своем регламенты направлены на повышение уровня информационной безопасности в среде. Формирование регламентов невозможно без высокого уровня осведомленности в отношении атак класса “социальная инженерия”, где

– большое количество атак проводится на социальные сети и сети коммуникаций, так как дизайн платформ вызывает у людей чувство доверия и безопасности использования, что снижает их настороженность [2];

– оказалось, что за 2024 год 44% лиц в возрасте от 20-29 лет заявили о случаях мошенничества, тогда как для пенсионеров (65-79 лет) этот показатель был почти в два раза меньшие – 24%. Выяснилось, что молодые люди чаще подвержены мошенническим атакам из-за высокой активности в сети «Интернет». Также исследования говорят о том, что молодёжь склонна к быстрому принятию решений, что снижает уровень способности критического мышления [2].

Тематический сайт со своей продукцией «eftsure» говорит, что из 99% организаций заявивших, что у них есть программа обучения по вопросам безопасности, только 27% респондентов охватили социальную инженерию [3].

В свою очередь портал «EMBROKER» приводит следующие актуальные для исследования атак заданного класса данные: согласно индексу киберпреступности «World Cybercrime Index», Россия является страной, наиболее подверженной риску киберпреступлений, это связано с нехваткой специалистов в области обеспечения информационной безопасности, что очень сильно размывает круги представления о мошеннических кибератаках в стране [4].

Все это говорит о том, что высокий уровень опасности атак класса “социальная инженерия” в том числе спровоцирован отсутствием необходимого уровня изученности их сущности.

С учетом вышеизложенного целью настоящей публикации является повышение уровня защищенности социо-информационного пространства за счет решения следящих задач:

1) формирование базы статистических данных по социальной инженерии;

2) формирование перечня техник, подходящих под шаблоны реализации атак класса “социальная инженерия”;

3) формирование перечня социально-психологических уязвимостей для различных поколений;

4) расчёт вероятности успешной реализации атаки с учётом перечня социальных уязвимостей;

5) программная модель, визуализирующая зависимость вероятности атаки от уровня воздействия на массовое и индивидуальное сознание, а также на осведомленность пользователей сети;

6) формирование перечня объектов воздействия для атак класса “социальная инженерия”;

7) разработка комплекса мер и средств для обнаружения и регистрации атак, сгруппированных по инцидентам безопасности.

Формирование сведений об используемых техниках в контексте атаки класса “социальная инженерия”

В ходе реализации любой компьютерной атаки злоумышленник прибегает к техникам, перечисленным в матрице Mitre&Attack. На текущий момент было выявлено порядка 60 техник, непосредственно связанных с реализацией атак класса “социальная инженерия”. Удобно представить информацию об этих техниках в виде таблицы (табл. 1).

Таблица 1

Множество используемых техник

Используемая техника	Описание
Информационный фишинг (T1598)	Фишинговые сообщения для получения информации.
Сбор идентификационной информации (T1589)	Злоумышленники могут собирать информацию о личности жертвы.
Поиск по открытым доменам (T1593)	Поиск на доступных веб-сайтах и/или доменах информацию о жертвах.
Сбор информации об организациях жертв (T1591)	Злоумышленники могут собирать информацию об организации жертвы.
Сбор информации о хосте жертвы (T1592)	Злоумышленники могут собирать информацию о хостах жертвы.
Создание учетных записей (T1585)	Злоумышленники могут создавать и развивать аккаунты с сервисами.
Компрометация учетных записей (T1586)	Злоумышленники могут скомпрометировать учетные записи.
Компрометация инфраструктуры (T1584)	Злоумышленники могут скомпрометировать стороннюю инфраструктуру.
Фишинг (T1566)	Злоумышленники могут рассылать фишинговые сообщения.
Теневая компрометация (T1189)	Доступ к системе через пользователя, посещающего веб-сайт.
Доверительные отношения (T1199)	Доступ через отношения доверенной третьей стороны злоупотребляет существующим соединением.
Использование пользователем (T1204)	Злоумышленник может полагаться на определенные действия пользователя, чтобы добиться выполнения.
Системные службы (T1569)	Злоумышленники могут злоупотреблять системными службами или демонами.
Интерпретаторы командной строки и сценариев (T1059)	Злоумышленники могут использовать интерпретаторы командной строки и сценариев для выполнения команд.
Запланированная задача (T1053)	Злоумышленники могут использовать функцию планирования задач.
Расширения для браузера (T1176)	Вредоносные расширения могут быть установлены в браузер.
Создание учетных записей (T1136)	Учетные записи могут быть созданы в локальной системе или в домене, или облачном клиенте.
Запланированная задача (T1053)	Злоумышленники могут использовать функцию планирования задач.
Действующие учетные записи (T1078)	Злоумышленники могут получать и использовать учетные данные существующих пользователей для первоначального доступа.
Манипуляции с аккаунтом (T1098)	Злоумышленники могут манипулировать учетными записями.
Эксплуатация уязвимостей для повышения привилегий (T1068)	Злоумышленники могут эксплуатировать уязвимости в ПО с целью повышения уровня своих привилегий.
Обход механизмов контроля привилегий (T1548)	Злоумышленники могут обходить механизмы контроля привилегий для получения дополнительных прав в системе.
Существующие учетные записи (T1078)	Скомпрометированные учетные данные могут использоваться для обхода систем управления доступом.
Выполнение кода по событию (T1546)	Злоумышленники могут закрепиться и (или) повысить уровень своих привилегий.

Продолжение табл. 1

Используемая техника	Описание
Манипуляции с токенами доступа (T1134)	Злоумышленники могут изменить токены доступа для выполнения операций от лица другого пользователя.
Имперсонация (T1656)	Злоумышленники могут выдавать себя за доверенных лиц или организации.
Внедрение шаблона (T1221)	Злоумышленники могут создавать или изменять ссылки в шаблонах пользовательских документов.
Сокрытие артефактов (T1564)	Злоумышленник может скрывать файлы, процессы или другие артефакты своей деятельности.
Удаление индикаторов (T1070)	Злоумышленник может удалять или изменять журналы событий, историю команд или другие следы своей активности.
Кража токена доступа к приложению (T1528)	Кража токенов также может произойти с помощью социальной инженерии.
Кража или подделка сертификатов аутентификации (T1649)	Злоумышленники могут украсть или подделать сертификаты, используемые для аутентификации.
Кража или подделка билетов Kerberos (T1558)	Злоумышленники могут попытаться обойти аутентификацию Kerberos.
Изменение процесса аутентификации (T1556)	Злоумышленники могут изменить механизмы и процессы аутентификации.
Манипуляции с токенами доступа (T1134)	Злоумышленники могут изменить токены доступа для выполнения операций.
Подделка учетных данных для веб-ресурсов (T1606)	Злоумышленники могут подделать учетные данные и использовать их.
Обнаружение информации о браузере (T1217)	Злоумышленники могут перечислить информацию о браузерах, чтобы узнать больше о скомпрометированных средах.
Обнаружение учетной записи (T1087)	Злоумышленники могут попытаться получить список действительных учетных записей, имен пользователей или адресов электронной почты в системе.
Изучение установленного ПО (T1518)	Злоумышленники могут попытаться получить список установленных в системе или облаке программ и их версий.
Изучение сведений о конфигурации сети (T1016)	Злоумышленники могут получить подробную информацию о конфигурации и параметрах сети.
Изучение файлов и каталогов (T1083)	Злоумышленники могут получать списки файлов и каталогов.
Изучение установленного ПО (T1518)	Злоумышленники могут попытаться получить список установленных в системе или облаке программ и их версий.
Изучение сетевых служб (T1046)	Злоумышленники могут попытаться получить список служб.
Изучение местоположения системы (T1614)	Злоумышленники могут собирать информацию с целью определить географическое расположение целевого узла.
Изучение владельца или пользователей системы (T1033)	Злоумышленники могут попытаться определить основного пользователя системы, пользователя, находящегося в текущий момент в системе, а также группы частых или активных пользователей системы.
Изучение групп разрешений (T1069)	Злоумышленники могут попытаться получить информацию о настройках групп и разрешений.
Изучение периферийных устройств (T1120)	Злоумышленники могут попытаться получить информацию о подключенных периферийных устройствах и компонентах системы.
Внутренний целевой фишинг (T1534)	Получив доступ к учетным записям или системам в среде, злоумышленники могут использовать внутренний целевой фишинг.
Использование альтернативных материалов для аутентификации (T1550)	Злоумышленники могут использовать ранее украденные альтернативные материалы для аутентификации
Автоматизированный сбор (T1119)	После создания в системе или сети злоумышленник может использовать автоматизированные методы для сбора внутренних данных.
Сбор электронной почты (T1114)	Злоумышленники могут использовать электронную почту пользователей для получения конфиденциальной информации.
Данные со съемных носителей (T1025)	Злоумышленники могут осуществлять поиск интересующих их файлов на съемных носителях, подключенных к скомпрометированным компьютерам.
Захват входных данных (T1056)	Механизмы захвата ввода могут быть прозрачными для пользователя (например, Credential API Hooking).
Захват экрана (T1113)	Злоумышленник получает данные с экрана устройства.

Окончание табл. 1

Используемая техника	Описание
Захват видеоданных (T1125)	Злоумышленники могут использовать периферийные устройства компьютера.
Программное обеспечение для удаленного доступа (T1219)	Злоумышленник может использовать законное программное обеспечение.
Перенос входящего инструмента (T1105)	Злоумышленники могут передавать инструменты или другие файлы из внешней системы в скомпрометированную среду.
Веб-сервис (T1102)	Злоумышленники могут использовать существующую законную внешнюю веб-службу.
Протоколы (кроме прикладного уровня) (T1095)	Злоумышленники могут использовать протокол модели OSI, не являющийся протоколом прикладного уровня.
Сокрытие инфраструктуры (T1665)	Злоумышленники могут манипулировать сетевым трафиком.
Эксфильтрация через веб-сервис (T1567)	Злоумышленники могут использовать для кражи данных существующую законную внешнюю веб-службу.
Эксфильтрация по каналу C2 (1041)	Злоумышленник может убедить жертву установить вредоносное ПО, которое передает данные через легитимные каналы связи.
Эксфильтрация через стороннюю среду (T1011)	Злоумышленники могут попытаться извлечь данные через сетевую среду.
Эксфильтрация через физическую среду (T1052)	Злоумышленник убеждает жертву скопировать данные на физический носитель.
Передача по расписанию (T1029)	Злоумышленники могут настроить график извлечения данных из системы.
Шифрование данных (T1486)	Злоумышленники могут зашифровывать данные (как на отдельных системах в сети, так и массово).
Уничтожение диска (T1561)	Злоумышленники могут стереть или повредить данные на дисках.
Повреждение программы (T1495)	Злоумышленники могут перезаписать или повредить содержимое флеш-памяти BIOS.
Уничтожение данных (T1485)	Злоумышленники могут уничтожать данные и файлы в определенных системах.
Манипулирование данными (T1565)	Злоумышленники могут вставлять, удалять или манипулировать данными.

Особенность социальной инженерии заключается в том, что, идя по сценарию, злоумышленник в ходе реализации перечисленных техник может прибегнуть как к использованию социально-психологических, так и технических уязвимостей. Так как при реализации атаки через различные шаблоны, комбинации «техника → используемые CVE» могут отличаться, целесообразно при формировании перечня объектов воздействия (а как следствие – мер по обнаружению и регистрации атаки, связанных с технической составляющей) опираться на контекст используемых техник, представленный в открытом доступе на сайте Mitre&Attack. [5].

Формирование перечня используемых злоумышленниками социально-психологических уязвимостей различных поколений в контексте атаки “социальная инженерия”

В отличие от ситуации с техническими аспектами, где от шаблона к шаблону (CAPEC) в одних и тех же техниках могли наблюдаться различные используемые уязвимости (в силу уникальности каждого шаблона), в случае с социально-психологическими аспектами, для реализации всякой техники может быть использована любая социально-психологическая уязвимость поколения (например, сбор данных может быть реализован за счет слабого уровня цифровизации поколения B или чрезмерного доверия в сети поколения Z, и так далее). Таким, образом целесообразно сформировать полный список социально-психологических уязвимостей и на их основе далее строить перечень объектов воздействия и дальнейшие меры по обнаружению.

Анализируя научную литературу, удалось выделить ряд поколений, а также уровень воздействия социальной инженерии на эти поколения (количество атак в %). Такая статистика изброжена на рис. 1.

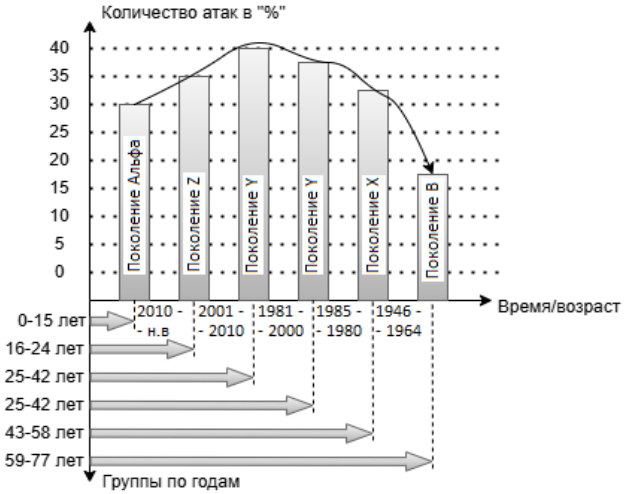

Рис. 1. Влияние социальной инженерии на различные возрастные категории

Как видно из схемы, наибольший интерес для социальных инженеров, действительно, составляют люди возрастом от 25 до 42 лет. Однако для понимания полной картины и примерного прогноза ближайших лет необходимо сформировать перечень социально-психологических уязвимостей по поколениям (табл. 2) [1, 6].

Как видно из табл. 2, наибольшим количеством “социальных” уязвимостей обладают поколения A и Z. Далее следует осветить основную тенденцию относительно текущих особенностей поколений и то, как дальше будет развиваться класс атак “социальная инженерия”.

Таблица 2

Матрица социальных уязвимостей

Возрастная категория / Уязвимость	A (2010+)	Z (2001-2010)	Y (1981-2000)	X (1965-1980)	B (1946-1964)
Трудности освоения цифровых технологий	-	-	-	+	+
Социальная изоляция из-за цифровизации	+	+	-	+	+
Риск депрессии и тревожности из-за изменений	+	+	+	+	+
Снижение занятости из-за роботизации	+	+	+	+	+
Потеря квалификации	-	-	-	+	+
Уязвимость к цифровому мошенничеству	+	-	-	+	+
Дискриминация на рынке труда	-	-	-	+	+
Сложности в живом общении	+	+	+	-	-
Девиантное поведение	+	+	+	-	-
Упрощенное системное мышление	+	+	+	-	-
Дезадаптация к социальной реальности	+	+	+	-	-
Чрезмерное доверие к информации из интернета	+	+	+	-	-
Нарушение межличностных коммуникаций	+	+	+	-	-
Снижение уважения к старшим поколениям	+	+	-	-	-
Проблемы с логическим и аналитическим мышлением	+	+	-	-	-
Зависимость от виртуального мира	+	+	-	-	-
Сложности в социализации со сверстниками	+	+	-	-	-
Риск формирования фейковой реальности	+	+	-	-	-

Вероятность реализации атак класса “социальная инженерия” с учетом количества уязвимостей на каждое поколение

Основными проблемами B и X -поколений стали психологические стрессы при освоении новых технологий в скупе с отставанием за столь стремительно-развивающимися технологиями в целом. Кроме того, рост дискриминации на рынке труда по отношению к данной возрастной категорий провоцирует развитие депрессии и чувства тревожности. Все это в совокупности подводит эти поколения под удар цифрового мошенничества.

Поколение миллениалов в свою очередь, как выяснилось имеет заметные сложности в контексте живого общения в силу другого воспитания, также фиксируются частые случаи девиации и упрощенного системного мышления.

Поколения Z и Альфа часто склонны к принятию мгновенных решений, снижению уважения к старшим, проблемам с логическим и аналитическим мышлением, зависимости от виртуального мира. Часто люди этой возрастной категории пребывают в так называемой «фейковой» реальности.

Несмотря на то, что на текущий момент наиболее подвержены атакам социальной инженерии Z-поколение и миллениалы, в будущем тенденция изменится. Чтобы это понять необходимо рассчитать вероятность реализации атаки для каждого поколения, исходя из общего числа уязвимостей в целом по формуле (1).

$$P_v = 1 - \left(1 - \frac{1}{n}\right)^m, \qquad (1)$$

где P_v – это вероятность реализации атаки в текущем поколении с учетом уязвимостей социального характера,

m – это количество уязвимостей для текущей возрастной категории,

n – количество уязвимостей всего.

$\frac{1}{n}$ – это вероятность того, что одна конкретная уязвимость приведет к успешной атаке, если предположить, что все уязвимости равновероятны. $1 - \frac{1}{n}$ – это вероятность того, что одна конкретная уязвимость не приведет к успешной атаке. $(1 - \frac{1}{n})^m$ – это вероятность того, что ни одна из m уязвимостей текущего поколения не приведет к успешной атаке. $1 - (1 - \frac{1}{n})^m$ – это вероятность того, что хотя бы одна уязвимость из m уязвимостей текущего поколения приведет к успешной атаке (то есть искомая вероятность).

Таким образом, получатся значения вероятности, что злоумышленник реализует атаку на текущее поколение с учетом того количества уязвимостей, которые ему присущи (табл. 2). Значения удобно представить в виде диаграммы. (рис. 2) [7,8,9].

Как видно из рис. 2, вероятность атак на более молодое поколение, как и количество уязвимостей устойчиво растет, причем график роста представляет из себя экспоненциальную функцию.

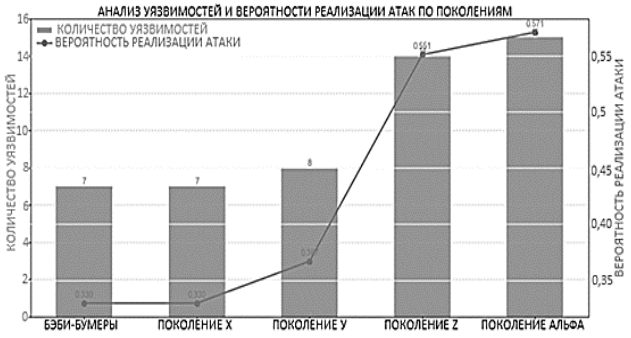

Рис. 2. Вероятность и количество уязвимостей для каждого поколения при условии равнозначных критичностей

Таким образом, из описанного выше можно выделить три объекта воздействия на социальном уровне: уровень осведомленности пользователей, влияние на массовое сознание, влияние на сознание индивида. с использованием библиотеки Matplotib было написано мини приложение, отражающее зависимость вероятности от уровня осведомленности пользователя, уровня влияния на массовое сознание и на сознание индивида. Так как текущие глобальные объекты воздействия были получены путем анализа равновероятных “человеческих уязвимостей”, то и модификаторы для этих объектов брались одинаковыми. Приложение (рис. 3) опирается на форму кривой, которая прослеживается на рис. 2.

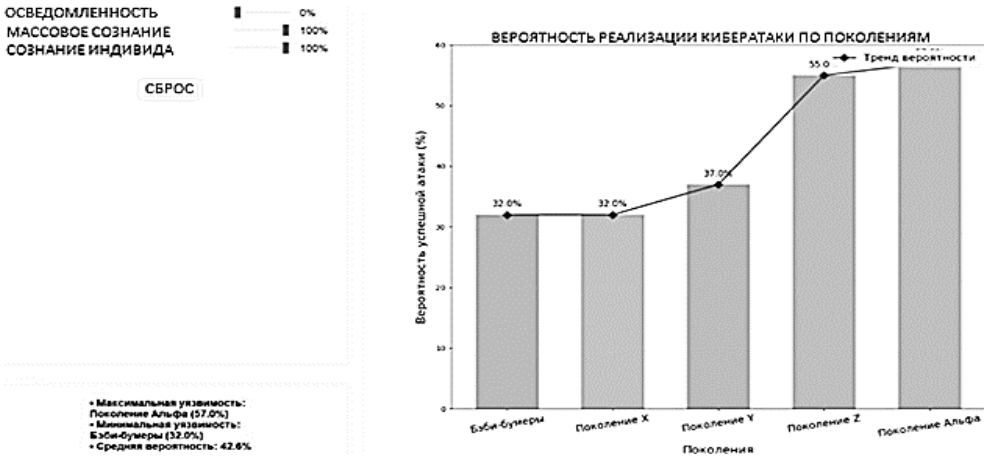

Рис. 3. Результат работы приложения

Важно, что все вышеописанные процедуры актуальны в случае, если не проводить анализ критичности каждой отдельной уязвимости. Однако в реальности зачастую требуются расчеты для конкретного сценария с точным значением вероятностей и критичностей для каждой уязвимости. Для каждой уязвимости представляется возможным определить ее критичность по следующей шкале:

0 - 0,975 – встречается у 1-го поколения из 5-ти;

1,95 – встречается у 2-х поколений из 5-ти;

3,9 – встречается у 3-х поколений из 5-ти;

6,9 – встречается у 4-х поколений из 5-ти;

9,9 – встречается у 5-ти поколений из 5-ти.

Шкала оценки является несколько модифицированной версией шкалы CVSS калькулятора [10]. Имея в обороте критичность для каждой уязвимости возможен расчет вероятности по формуле (2) индивидуально для каждой социальной уязвимости:

$$P_i = \frac{Sf}{\sum S_f}, \qquad (2)$$

где P_i – вероятность эксплуатации *i*-й социальной уязвимости;

Sf – оценка критичности уязвимости, полученная из количества возможных реализаций во всех пяти поколениях.

Важно произвести нормировку полученных по шкале значений по формуле 3.

$$S_{norm} = \frac{S - S_{min}}{S_{max} - S_{min}}, \qquad (3)$$

где S_{norm} – нормализованная оценка калькулятора;

S – актуальная оценка;

S_{max} – максимальная оценка;

S_{min}– минимальная оценка.

В итоге получим матрицу (табл. 3), в которой будут отражены вероятности и критичности каждой уязвимости для всех рассматриваемых поколений.

Далее возможно рассчитать среднюю вероятность реализации атак класса «социальная инженерия», взяв среднее значение по каждому поколению (столбцу). Для удобства возможно представить полученные выше результаты в виде диаграммы (рис. 4).

Из рис. 4 отчетливо видно, что график по-прежнему имеет похожую форму (рис. 2 и 3), а значения разнятся в пределах погрешности, это еще раз подтверждает правильность вышеизложенного и доказывает корректность разработанного приложения.

Таблица 3

Вероятности эксплуатации социальных уязвимостей [6]

Возрастная категория / Уязвимость	A (2010+)	Z (2001-2010)	Y (1981-2000)	X (1965-1980)	B (1946-1964)	Sf
Трудности освоения цифровых технологий	0	0	0	0,028017	0,028017	0,195
Социальная изоляция из-за цифровизации	0,099137	0,099137	0	0,099137	0,099137	0,69
Риск депрессии и тревожности из-за изменений	0,142241	0,142241	0,142241	0,142241	0,142241	0,99
Снижение занятости из-за роботизации	0,142241	0,142241	0,142241	0,142241	0,142241	0,99
Потеря квалификации	0	0	0	0,040816	0,040816	0,195
Уязвимость к цифровому мошенничеству	0,056034	0	0	0,056034	0,056034	0,39
Дискриминация на рынке труда	0	0	0	0,040816	0,040816	0,195
Сложности в живом общении	0,056034	0,056034	0,056034	0	0	0,39
Девиантное поведение	0,056034	0,056034	0,056034	0	0	0,39
Упрощенное системное мышление	0,056034	0,056034	0,056034	0	0	0,39

Продолжение табл. 3

Возрастная категория / Уязвимость	A (2010+)	Z (2001-2010)	Y (1981-2000)	X (1965-1980)	B (1946-1964)	Sf
Дезадаптация к социальной реальности	0,056034	0,056034	0,056034	0	0	0,39
Чрезмерное доверие к информации из интернета	0,056034	0,056034	0,056034	0	0	0,39
Нарушение межличностных коммуникаций	0,056034	0,056034	0,056034	0	0	0,39
Снижение уважения к старшим поколениям	0,028017	0,028017	0	0	0	0,195
Проблемы с логическим и аналитическим мышлением	0,028017	0,028017	0	0	0	0,195
Зависимость от виртуального мира	0,028017	0,028017	0	0	0	0,195
Сложности в социализации со сверстниками	0,028017	0,028017	0	0	0	0,195
Риск формирования фейковой реальности	0,028017	0,028017	0	0	0	0,195

Рис. 4. Средние вероятности реализации атак по поколениям с учетом критичности отдельно взятых социальных уязвимостей

Результатами раздела стали:

– во-первых, рассчитанные вероятности реализации атаки (с учётом социальных уязвимостей, а конкретно их количества) при равных значениях критичности (равнозначные) и индивидуальных значениях критичности (неравнозначные);

– во-вторых, разработанное мини-приложение, иллюстрирующее изменения в вероятности, при снижении/увеличении уровня воздействия на сознание индивида, массовое сознание и уровень осведомленности.

Также необходимо отметить, что перспектива развития атак класса “социальная инженерия”, говорит о том, что в ближайшем будущем альфа-поколение не только заменит Z-поколение и миллениалов, но и количество атак разительно увеличится, судя по экспоненциальному характеру роста кривой вероятностей.

Формирование объектов воздействия и перечня мер и средств по обнаружению и регистрации для атак класса “ социальная инженерия”

Теперь, когда есть понимание технической и социально-психологической сторон, можно составить таблицу с объектами воздействия социальной инженерии для успешного формирования регламентов обнаружения и регистрации. Объекты воздействия приведены в табл. 4.

Таблица 4

Объекты воздействия атак класса “социальная инженерия”

Направление	Объект воздействия/класс шаблона	Обманное метадезинформирование	Десимуляционное дезинформирование	Симуляционное дезинформирование	Кажущееся псевдо-информирование	Обобщенное псевдоинформирование	Избыточное целенаправленное псевдоинформирование
Социально-психологическое	Сознание индивида	-	-	CAPEC-173 CAPEC-194	CAPEC-194	CAPEC-410	CAPEC-98 CAPEC-163 CAPEC-164 CAPEC-656
	Массовое сознание	-	CAPEC-89 CAPEC-630 CAPEC-631	CAPEC-194	CAPEC-194	CAPEC-630 CAPEC-631	CAPEC-98 CAPEC-163 CAPEC-164 CAPEC-656
	Уровень осведомленности (обученности) персонала	-	CAPEC-630 CAPEC-631	CAPEC-194 CAPEC-173	CAPEC-194	CAPEC-410 CAPEC-630 CAPEC-631	CAPEC-98 CAPEC-163 CAPEC-164 CAPEC-656
Техническое	Программно-аппаратные средства	CAPEC-698	-	CAPEC-504 CAPEC-654	-	-	-
	Программные средства	CAPEC-698	CAPEC-630 CAPEC-631	CAPEC-173	-	CAPEC-631 CAPEC-630	-
	Привилегированные и непривилегированные пользователи систем	-	-	CAPEC-504 CAPEC-151 CAPEC-654	-	-	-
	Средства защиты информации	CAPEC-698	-	CAPEC-504 CAPEC-194	CAPEC-194	-	-
	Морально-психологическая обстановка в обществе	-	CAPEC-89	CAPEC-173	-	CAPEC-410	CAPEC-98 CAPEC-163 CAPEC-164 CAPEC-656
	Информация	-	-	CAPEC-504 CAPEC-194	CAPEC-194	CAPEC-410	-
	Машинные носители	CAPEC-698	-	-	-	-	-
	Авторизованные и неавторизованные пользователи системы	-	CAPEC-630 CAPEC-631	CAPEC-151 CAPEC-504 CAPEC-654	-	CAPEC-630 CAPEC-631	-
Технические	Операционная система (ПАК)	CAPEC-698	CAPEC-89	CAPEC-173 CAPEC-654 CAPEC-504	-	-	-
	Механизмы аутентификации	-	CAPEC-89	CAPEC-194 CAPEC-654 CAPEC-151	CAPEC-194	-	-
	Телекоммуникационное оборудование	-	CAPEC-89 CAPEC-630 CAPEC-631	-	-	CAPEC-630 CAPEC-631	CAPEC-98 CAPEC-164
	Обеспечивающие системы	CAPEC-698	-	CAPEC-194 CAPEC-173	CAPEC-194	CAPEC-410	-
	Средства защиты	CAPEC-698	-	CAPEC-173 CAPEC-504 CAPEC-194	CAPEC-194	-	-
	Коммуникационное оборудование (сетевое)	-	CAPEC-89	CAPEC-194 CAPEC-173	CAPEC-194	-	-

Как видно из табл. 4, по сформированному перечню объектов воздействия (сформирован из контекста описания техник и социальных уязвимостей) распределены шаблоны, которые упоминаемые ранее. Текущие шаблоны выбраны не случайно: каждый шаблон имеет в себе до 14 этапов реализации, и именно для отобранных шаблонов на каждом этапе используются техники характерные для социальной инженерии [11].

Очевидно, что реализация атаки не может осуществляться без инцидентов. Как уже упоминалось ранее – вся атака осуществляется посредством последовательного применения техник. Для формирования мер по обнаружению и регистрации будет удобно разбить имеющиеся техники по генерируемым ими инцидентам. Таким образом, получается матрица, где для каждого инцидента подробно изложены регламенты противодействия, представляющие из себя меры по обнаружению и регистрации атак заданного класса (табл. 5).

Таблица 5

Меры и средства для обнаружения и регистрации атак класса “социальная инженерия”

Инцидент	Техники	Меры для обнаружения (по поколениям)	Меры для обнаружения (технические)
Фишинг и сбор информации	T1598 T1589 T1593 T1591 T1592 T1114 T1534 T1566	1) Проведение тренингов по цифровой грамотности для молодых поколений (A-поколение). 2) Создание общественных программ по информированию о фишинговых атаках через СМИ и социальные сети (Z-поколение). 3) Организация "горячих линий" для консультаций по подозрительным сообщениям (Y, X, B - поколения). 4) Развитие волонтерских сетей для помощи уязвимым группам населения (X, B - поколения).	1) Детальный анализ писем (DMARC, SPF, DKIM). 2) Мониторинг запросов к данным с сопутствующим аудитом. 3) Выявление аномалий в поведении пользователей (SIEM-системы). 4) Ручной или автоматизированный анализ логов на предмет сканирования. 5) Проведение тестовых фишинговых кампаний.
Компрометация учетных записей	T1585 T1136 T1586 T1078 T1098 T1087 T1550	1) Обучение молодых пользователей основам создания и защиты паролей (A - поколение). 2) Проведение мастер-классов по безопасному использованию учетных записей (Z - поколение). 3) Создание общественных советов по кибербезопасности на местном уровне (Y, X, B - поколения). 4) Внедрение программ инструктирования для старших поколений (B - поколение).	1) Анализ журнала входов и фиксация странного поведения пользователя. 2) Ручной или автоматизированный сбор данных о запросах к Active Directory внутри домена. 3) Мониторинг политики домена и списка учетных записей.
Кража учетных данных и токенов	T1528 T1649 T1558 T1056 T1606	1) Объяснение молодому поколению рисков и механизмов кражи данных учетных записей (A-поколение). 2) Организация общественных дискуссий о важности защиты УД и токенов (Z - поколение). 3) Создание локальных групп взаимопомощи для выявления мошенничества (Y, X, B - поколения). 4) Популяризация программ по повышению осведомленности и наставничества в обеспечения кибербезопасности (X, B - поколения).	1) Анализ контекста использования токенов (наиболее эффективно OAuth). 2) Мониторинг использования билетов. 3) Анализ логов аутентификации.
Внедрение вредоносного кода	T1189 T1204 T1569 T1059 T1053 T1176 T1546 T1105	1) Обучение детей и подростков распознаванию подозрительных ссылок и вложений (A - поколение). 2) Популяризация среди школьников и студентов обучения по основам кибергигиены (Z-по). 3) Создание общественных центров по борьбе с вредоносным ПО (Y, X, B - поколения). 4) Развитие программ поддержки для пожилых пользователей (X, B - поколения).	1) Внедрение и использование систем выявления вредоносных процессов (EDR/XDR). 2) Анализ поведения приложений с сопутствующим аудитом. 3) Мониторинг и контроль планировщика задачи (Windows/Linux - системы).

Продолжение табл. 5

Инцидент	Техники	Меры для обнаружения (по поколениям)	Меры для обнаружения (технические)
Эскалация привилегий	T1068 T1548 T1556 T1656	1) Формирование у молодого поколения понимания механизмов разграничения доступа (A, Z - поколения). 2) Проведение тренингов по социальной инженерии в рамках обучения (A, Z - поколения). 3) Создание групповых (корпоративных) каналов обмена информацией об инцидентах с привилегиями (Z, Y, X -поколения). 4) Развитие программ по защите прав уязвимых групп на рабочих местах (X, B - поколения).	1) Обнаружение попыток эксплуатации уязвимостей (IDS/IPS/COB UserGate). 2) Мониторинг доменной политики (списка прав пользователей). 3) Анализ логов (UserGate Log Analyzer или Digital Q.ELK).
Сбор и эксфильтрация данных	T1119 T1025 T1113 T1125 T1567 T1041 T1011 T1052 T1029 T1217	1) Формирование у детей и подростков отчетливого понимания о среде передачи данных или о канале утечки информации (A - поколение). 2) Организация учебных треннингов в группах в рамках обучения по предотвращению утечек данных (A, Z - поколения). 3) Создание добровольческих формирований по мониторингу утечек (Z, Y, X - поколения). 4) Создание волонтерских движений по защите пожилых людей от вторжений класса “социальная инженерия” (B - поколение).	1) Внедрение и использование DLP систем для обнаружения утечек. 2) Интеграция NMS систем для обнаружения странных объемов передаваемого трафика и общего анализа сетевого трафика (в РФ популярны AggreGate Network Manager, Супертел-NMS v3, NMS «ФРАКТАЛ», SI-NEC NMS).
Сокрытие активности	T1564 T1070 T1221 T1665 T1102 T1095	1) Формирование у молодого поколения понимания термина “журналирование событий” (A, Z - поколения). 2) Популяризация семинаров по выявлению скрытых киберугроз (Z - поколение). 3) Создание общественных наблюдательных советов (Y, X, B - поколения). 4) Внедрение механизмов, повышающих уровень прозрачности социальных взаимодействий (X, B - поколения).	1) Бэкапинг логов и журналов и последующий их анализ на предмет удаления событий. 2) Анализ системы на предмет наличия скрытых руткитов (EDR/XDR). 3) Ручной или автоматизированный мониторинг изменений в системе и системных компонентах
Разрушение данных и систем	T1486 T1561 T1495 T1485 T1565	1) Обучение молодого поколения основам резервного копирования (A - поколение). 2) Проведение общественных акций и учебных треннингов по защите важных инфраструктур среди школьников и студентов (A, Z - поколения). 3) Создание сообществ взаимопомощи при кибератаках (Y, X - поколения). 4) Внедрение социальных норм цифровой устойчивости (Y, X, B - поколения).	1) Интеграция инструментов Anti-Ransomware, используемых для обнаружения попыток нанесения вреда информации. 2) Интеграция DCAP-систем для автоматизированного аудита данных в файловой системе, поиска нарушений прав доступа и отслеживания изменений в критичных документах. 3) Специализированное обучение персонала. 4) В случае уничтожения/повреждения/блокировки данных сотрудники должны незамедлительно сообщать об инцидентах

Окончание табл. 5

Инцидент	Техники	Меры для обнаружения (по поколениям)	Меры для обнаружения (технические)
Злоупотребление доверительными отношениями	T1199 T1584 T1219	1) Повсеместное внедрение курсов информационно-психологической подготовки для детей и подростков для распознавания простейших психологических манипуляций и злоупотребления доверием (A, Z - поколения). 2) Проведение треннингов по безопасному сотрудничеству (Z, X, Y - поколения). 3) Развитие программ защиты старших поколений от психологической манипуляции и обманов (X, B - поколения). 4) Разработка и внедрение социальных стандартов доверия в цифровой среде для всех поколений (все поколения).	1) Анализ и контроль сеансов удаленного доступа, осуществляемых через такие протоколы как VPN/RDP. 2) Специализированное обучение персонала. 3) Требование от сотрудников сообщать о подозрительных контактах с коллегами.
Разведка внутренней среды	T1518 T1016 T1083 T1046 T1614 T1033 T1069 T1120	1) Внедрение в программу обучения школьников и студентов основ информационной безопасности вне зависимости от профиля обучения или специальности (A, Z - поколения). 2) Популяризация треннингов по противодействию корпоративной разведке, реализуемых в формате игры, квеста, квиза, корпоратива, и других неформальных активностей (Z, Y - поколения). 3) Разработка и внедрение общественных программ по защите от шпионажа (X, B - поколения). 4) Развитие национальных инициатив для повышения уровня социо-информационного пространства (X, B - поколения). 5) Популяризация культуры бдительности и этики в обществе, для обнаружения и дальнейшего предотвращения разведывательных действий злоумышленников (Z, Y, X, B - поколения).	1) Интеграция систем для обнаружения сканирования сети NIDS/IPS. 2) Ручной или автоматизированный мониторинг запросов к системным компонентам и данным. 3) Анализ попыток авторизации и выявление брутфорса по логам и журналам входа. 4) Специализированное обучение персонала. 5) Требование от сотрудников незамедлительно сообщать о подозрительных моментах во время работы.

Таким образом, был сформирован перечень объектов воздействия с распределенными по ним шаблонами реализации атаки, после чего были определены инциденты по общему перечню техник. Стоит отметить, что наиболее рационально в составлении перечня мер по обнаружению отталкиваться именно от техник, так как это позволит охватить все шаблоны атаки (так как техники для реализации шаблонов выбирались именно из перечня табл. 1), избегая повторяющихся техник в различных шаблонах.

Также, имея список объектов воздействия злоумышленников (куда целится преступник), были определены меры для того, чтобы обнаружить атаку до того, как последствия станут тяжелыми.

Заключение

Учитывая все сказанное выше, можно отметить, что была дополнительно освещена основная особенность вторжений класса “социальная инженерия”, заключающаяся в невозможности проведения технической атаки без деструктивного социального взаимодействия с жертвой.

Результатами работы стали: собранная статистика по социальной инженерии; матрица с техниками, подходящими под шаблоны реализации атак класса “социальная инженерия”; сформированный перечень социально-психологических уязвимостей для различных поколений; произведенный расчёт вероятности успешной атаки с учётом количества социальных уязвимостей; программная модель,

визуализирующая зависимость вероятности атаки от уровня осведомлённости, массового и индивидуального воздействия; сформированная матрица объектов воздействия; комплекс мер и средств для обнаружения и регистрации атак, сгруппированных по инцидентам безопасности.

Новизна заключается в том, что был впервые сформирован перечень социальных уязвимостей для разных возрастных групп (от "бэби-бумеров" до "поколения Альфа") и произведено прогнозирование динамики роста вероятности атак, исходя из определенного на основании научной литературы, количества уязвимостей по поколениям. Также впервые были разработаны регламенты обнаружения и регистрации, учитывающие не только технические системы, но и на человеческий фактор.

Практическая ценность работы видится в том, что определены объекты воздействия с закрепленными шаблонами и меры обнаружения готовые для внедрения в системы безопасности SIEM, DLP, EDR; модель на Python (на основании соответствующих формул и алгоритмов), которая может быть интегрирована в системы оценки рисков.

Теоретическая ценность работы заключается в том, что предложен новый подход к исследованию атак, сочетающий технические и социальные параметры, а также в обнаружении природы роста вероятностей и количества уязвимостей (для рассматриваемых поколений), имеющей форму схожую с экспоненциальной.

В целом настоящая работа открывает направление для:

– углубленного изучения критичности социальной инженерии в современном мире;

– разработки инструментов прогнозирования атак на основании данных о социуме (в том числе AI);

– повышения уровня защищенности социо-информационного пространства от вторжений класса “социальная инженерия”.

Список литературы

1. Остапенко Г.А. Организационно-правовая защита от сетевых атак: методики формирования частных политик, регламентов, и инструкций обеспечения безопасности организации (Часть I) / Г.А. Остапенко, Д.В. Щербакова, Т.Ю. Мирошниченко, А.А. Остапенко, А.С. Кривошеин // Информация и безопасность. 2023. Т. 26. Вып. 3. С. 329-340.

2. Статистика воздействия социальной инженерии на возрастные группы. URL: https://www.investopedia.com/ (дата обращения 17.05.2025 г.).

3. Статистика по вопросам обучения в области информационной безопасности. URL: https://eftsure.com/en-au/ (дата обращения 17.05.2025 г.).

4. Статистика воздействия социальной инженерии по странам. URL: https://www.embroker.com/ (дата обращения 18.05.2025 г.).

5. Статистика воздействия социальной инженерии на возрастные группы. URL: https://attack.mitre.org/ (дата обращения 19.05.2025 г.).

6. Воронин В.Н. Социально-психологические риски разных поколений в процессе цифровизации общества / В.Н. Воронин, Д.В., М.В. Ионцева, Л.Ю. Шураева // Современные тенденции в психологии 2022. Вып. 4. С. 169-175.

7. Остапенко А.А. Методики и алгоритмы риск-анализа успешности реализации массированных кибератак / А.А. Остапенко // Информация и безопасность. 2024. Т. 27. Вып. 3. С. 401-420.

8. Хромых С.А. Сетевые атаки на уровне приложений: риск-ландшафт и частная политика информационной безопасности предприятия / С.А. Хромых, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко // Информация и безопасность. 2023. Т. 26. Вып. 2. С. 261-276.

9. Остапенко А.А. Актуальные задачи и некоторые их решения в части риск калькуляции успешности реализации единичных кибератак / А.А. Остапенко // Информация и безопасность. 2024. Т. 27. № 4. С. 543-552.

10. Шаблоны атак класса “социальная инженерия”. URL: https://capec.org/ (дата обращения 19.05.25).

11. Шкала оценки уязвимостей по CVSS. URL: https://bdu.fstec.ru/calc (дата обращения 19.05.25).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Vronezh State Technical University

Поступила в редакцию 17.05.2025

Сведения об авторах

Остапенко Григорий Александрович – д-р техн. наук, профессор, проректор по цифровизации, Финансовый университет при Правительстве Российской Федерации, e-mail: ostg@mail.ru
Остапенко Александр Алексеевич – аспирант, Воронежский государственный технический университет e-mail: alexanderostapenkoias@gmail.com
Грамыкин Максим Алексеевич – студент, Воронежский государственный технический университет e-mail: alexanderostapenkoias@gmail.com
Кондратьев Максим Витальевич – студент, Воронежский государственный технический университет e-mail: alexanderostapenkoias@gmail.com
Харламов Никита Сергеевич – студент, Воронежский государственный технический университет e-mail: alexanderostapenkoias@gmail.com

FEATURES AND REGULATIONS FOR DETECTING THE INVASION CLASS “SOCIAL ENGINEERING”

G.A. Ostapenko, A.A. Ostapenko, M.A. Gramikin, M.V. Kondratyev, N.S. Kharlamov

This scientific article is devoted to the study of methods and measures for detection and registration of attacks such as network attacks of the “social engineering” type, carried out on the socio-information space, as a measure to counteract attacks of a given type. During the study, various attack scenarios were analyzed, which are combinations of various techniques. Particular attention is paid to the ability of attackers to use both technical aspects and socio-psychological ones during the attack. Based on the obtained results, a matrix with objects of influence was built, taking into account various patterns of social engineering. Thanks to the objects of influence obtained as a result of the analysis of the techniques used by attackers and socio-psychological vulnerabilities of a person, it is possible to build a matrix with regulations representing measures and means for detection. The results of the study represent a valuable contribution to increasing the level of security of the socio-information space.

Keywords: social engineering, socio-psychological vulnerabilities, technical vulnerabilities, regulations, security.

Submitted 17.05.2025

Information about the authors

Grigory A. Ostapenko – Dr. Sc (Technical), professor, vice-rector for digitalization, Financial University under the Government of the Russian Federation, e-mail: ostg@mail.ru
Alexander A. Ostapenko – graduate student, Voronezh State Technical University e-mail: alexanderostapenkoias@gmail.com
Maksim A. Gramykin – student, Voronezh State Technical University e-mail: alexanderostapenkoias@gmail.com
Maksim V. Kondratyev – student, Voronezh State Technical University e-mail: alexanderostapenkoias@gmail.com
Nikita S. Kharlamov – student, Voronezh State Technical University e-mail: alex-anderostapenkoias@gmail.com