УДК 004.056:004.738.5

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В КИБЕРАТАКАХ: АНАЛИЗ УЯЗВИМОСТИ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Кузнецов М. И. (ВКА), **Плаксеев Д.А.** (ВКА), **Тельбух В.В.** (ВКА)
Научный руководитель – кандидат технических наук, преподаватель Тельбух В. В.
(Военно-космическая академия имени А.Ф.Можайского)

Введение. Согласно данным исследований, более 80% успешных кибератак связаны с использованием социальной инженерии. Это подчёркивает важность анализа уязвимостей человеческого фактора в современных системах безопасности. Социальная инженерия представляет собой метод манипуляции людьми с целью получения конфиденциальной информации или доступа к защищённым системам. В условиях роста числа киберугроз и усложнения методов атак актуальным становится вопрос разработки эффективных мер противодействия [1]. Целью данной работы является анализ уязвимостей человеческого фактора в контексте социальной инженерии и разработка рекомендаций для повышения уровня защиты информационных систем.

Основная часть. Социальная инженерия — это использование психологических приёмов для эксплуатации человеческих слабостей. Среди методов социальной инженерии можно выделить фишинг, вишинг, претекстинг, бэйтинг и другие, однако все они опираются на человеческий фактор, который остаётся главной уязвимостью в системах безопасности [2].

Основные причины успеха атак:

- недостаток осведомлённости о методах социальной инженерии;
- перегрузка информацией и стрессовые ситуации;
- эмоциональные реакции (например, страх, желание помочь);
- когнитивные искажения (например, эффект авторитета, эффект срочности) [2].

Примерами наиболее громких атак последних лет могут послужить взлом электронной почты директора ЦРУ Джона Бреннана в октябре 2015 года, ограбление криптовалютной компании Sky Mavis на полмиллиарда долларов в 2022 и атака на Twitter в 2020 году, когда злоумышленники использовали смесь социальной инженерии и фишинга, чтобы получить доступ к системе от сотрудников Twitter и рассылать мошеннические сообщения с аккаунтов, принадлежащих бизнесменам, знаменитостям, политикам и компаниям [3]. Для защиты от подобных атак и минимизации рисков рекомендуется принять следующие меры.

Обучение сотрудников:

- регулярные тренинги по кибербезопасности;
- симуляция атак (например, отправка тестовых фишинговых писем).

Технические меры:

- использование многофакторной аутентификации;
- настройка фильтров для блокировки подозрительных писем;
- регулярное обновление программного обеспечения;
- правильный подбор и периодическая смена пароля.

Автоматизированные системы анализа:

- разработка алгоритмов машинного обучения для анализа поведения пользователей;
- выявление аномалий в действиях сотрудников (например, необычные запросы доступа) [4].

Вывод. В результате исследования были выявлены основные уязвимости человеческого фактора в контексте социальной инженерии. Подчёркивается важность комплексного подхода, включающего обучение сотрудников, внедрение технических мер и использование технологий искусственного интеллекта. Дальнейшие исследования могут быть направлены на разработку

более совершенных алгоритмов анализа поведения пользователей и создание систем раннего предупреждения о потенциальных атаках.

Список использованных источников:

1. Психологические аспекты информационной безопасности организации в контексте социоинженерных атак [Электронный ресурс] // КиберЛенинка. – URL: https://cyberleninka.ru/article/n/psihologicheskie-aspekty-informatsionnoy-bezopasnosti-organizatsii-v-kontekste-sotsioinzhenernyh-atak/viewer (дата обращения: 25.01.2025
2. Грей, Дж. Социальная инженерия и этичный хакинг на практике / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2023. – 226 с.: ил.
3. Социальная инженерия: как злоумышленники манипулируют людьми [Электронный ресурс] // Kaspersky. – URL: https://www.kaspersky.ru/blog/social-engineering-cases/35808/ (дата обращения: 25.01.2025).
4. Социальная инженерия: методы и защита [Электронный ресурс] // Habr. – URL: https://habr.com/ru/companies/first/articles/670766/ (дата обращения: 25.01.2025).