ОЦЕНКА ЭФФЕКТИВНОСТИ ТЕХНИК ЗАЩИТЫ ОТ АТАК, ОСНОВАННЫХ НА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, В КОРПОРАТИВНЫХ СИСТЕМАХ

Арушанян А.В. (Университет ИТМО)
Научный руководитель – заместитель ректора по безопасности Кузьмич П. А.
(Университет ИТМО)

Введение. Изучение эффективности методов защиты от атак, основанных на социальной инженерии, в корпоративных системах играет важную роль в обеспечении безопасности информации. В связи с увеличением числа таких атак возникает необходимость анализа современных методов и оценки их эффективности для обеспечения информационной безопасности. В данном исследовании рассматриваются современные методы социальной инженерии, применяемые в корпоративных системах, а также существующие техники защиты и их эффективность в предотвращении атак, основанных на социальной инженерии. Результаты исследования могут помочь предприятиям и организациям укрепить свои системы безопасности и повысить уровень защищенности от социально-инженерных атак.

Основная часть.

1. Обзор современных техник социальной инженерии в корпоративных системах. В данном разделе описываются основные методы и техники социальной инженерии, используемые злоумышленниками для атак на корпоративные системы, а также приводятся наиболее известные случаи социально-инженерных атак.
2. Анализ существующих методов защиты от социально-инженерных атак. В этом разделе рассматриваются различные техники и инструменты, используемые для защиты корпоративных систем от атак, основанных на социальной инженерии.
3. Оценка эффективности существующих методов защиты от социально-инженерных атак. В данном разделе на основе анализа результатов реальных социально-инженерных атак и экспериментов проводится оценка эффективности различных методов защиты.
4. Разработка новых подходов к защите от социально-инженерных атак. В этом разделе предлагаются новые подходы к защите корпоративных систем от социально-инженерных атак, основанные на анализе результатов оценки эффективности существующих методов защиты.

Выводы. Анализ эффективности методов защиты от атак на корпоративные системы, основанных на социальной инженерии, подчеркивает важность превентивных мер для обеспечения безопасности информации. В частности, обучение персонала, использование многофакторной аутентификации и установка программного обеспечения для обнаружения аномалий в сетевом трафике являются важными инструментами защиты. Однако, чтобы обеспечить максимальную защищенность, необходимо использовать комплекс методов и инструментов, которые должны постоянно обновляться и улучшаться в соответствии с изменяющимися угрозами. Реализация этих мер позволит предприятиям и организациям защитить свои системы от кибератак, основанных на социальной инженерии, и обеспечить безопасность конфиденциальной информации.

Арушанян А. В. (автор)
Куимов М. К. (автор)

Кузьмич П. А. (научный руководитель)