Федоров Кирилл Петрович
студент
ФГБОУ ВО «Чувашский государственный
университет им. И.Н. Ульянова»
г. Чебоксары, Чувашская Республика

МЕРЫ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ И ВОЗМОЖНОСТИ КОРПОРАТИВНОГО СЕКТОРА ПО ПРОТИВОДЕЙСТВИЮ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В МОШЕННИЧЕСКИХ ЦЕЛЯХ

***Аннотация**: одним из ключевых элементов предотвращения мошенничества является надежный внутренний контроль. Однако наибольшую угрозу для информационной безопасности организации представляют манипуляции ее сотрудников, которые часто становятся жертвами тактики и техники ловких мошенников, известных как социальные инженеры. Цель статьи – сформировать закономерности выявленных атак инструментами социальной инженерии и оценить, что может сделать бизнес для предотвращения будущих инцидентов и борьбы с мошенническими схемами. Представлен краткий обзор наиболее распространенных методов социальной инженерии. Рассматриваются существующие законодательные инициативы, программы повышения осведомленности среди населения и сотрудников компаний, а также лучшие практики, применяемые организациями для защиты от атак.*

***Ключевые слова**: социальная инженерия, информационная безопасность, государственное регулирование, мошенничество.*

Одним из ключевых компонентов предотвращения мошенничества является сильный внутренний контроль. Он неизменно оценивается как главный фактор предотвращения мошенничества, и многие организации взяли на себя обязательство расходовать ресурсы на укрепление своего внутреннего контроля. Однако наибольшую угрозу информационной безопасности организации представляет собой манипулирование сотрудниками, которые слишком часто стано-

вятся жертвами уловок и приемов, используемых ловкими мошенниками, известными как социальные инженеры [3].

Так что же такое социальная инженерия? В контексте информационной безопасности этот термин обозначает набор приемов психологического манипулирования. Цель мошенников, использующих социальную инженерию, – заставить собеседника предоставить конфиденциальную информацию, предоставить доступ к защищенным ресурсам или перевести деньги на счет злоумышленника. Другими словами, социальная инженерия – это когда мошенники пытаются заставить человека совершить любое действие, которое идет вразрез с его интересами.

Не так-то просто заставить человека сделать то, чего он не хочет. Для этого мошеннику необходимо собрать хотя бы минимальную информацию о человеке, такую как его имя, возраст и сведения о банке, в котором у него открыт счет, например, является ли он участником схемы «безопасного счета».

Иногда сами граждане также помогают мошеннику узнать о них больше. Вспомните, что в социальных сетях часто встречаются опросы, в которых вас спрашивают о марке первого купленного вами автомобиля или о том, родились ли вы в 1990 году. Ответы могут помочь мошенникам узнать пароль от вашего аккаунта или угадать ваш банковский PIN-код.

Такую подготовку специалисты называют «нулевой этап атаки». Благодаря полученной информации аферистам легче войти в доверие. Они могут написать от лица директора, назвать имена и должности коллег, а потом попросить ответить на звонок «из ФСБ» или «из Центрального банка» [2].

В результате даже технически подкованные люди, знающие, как работает афера, передают мошенникам деньги. Например, доктор физико-математических наук, подполковник ФСБ, банкир и программист перевели миллионы рублей благодаря тщательной подготовке мошенников и последующей социальной инженерии.

Большинство хакеров перешли от написания вирусов к написанию звонков и спама по электронной почте. В результате количество тактик социальной инженерии резко возросло, и разные группы мошенников придумали свои тактики.

Фишинг. Это могут быть логины и пароли, данные банковских карт и паспортов, коды авторизации, интимные фотографии, важные письма – любая информация, которая может помочь им украсть деньги.

Вишинг, или голосовой фишинг. Квинтэссенция социальной инженерии – те самые звонки из банка, полиции, ФСБ и других ведомств.

Смишинг. Это фишинг через смс.

Бейтинг, или «дорожное яблоко». Например, хакер оставляет в офисе флешку с надписью «пароль от биткоин-кошелька» или диск с надписью «управленческая ведомость». Сотрудник вставляет этот носитель в свой компьютер и заражает его вирусом, что позволяет хакеру получить доступ к сети компании.

Спуфинг. В контексте сетевой безопасности это относится к атакам, при которых злоумышленник каким-то образом маскирует себя или свои действия под то, чему пользователь доверяет. Например, злоумышленник может обнаружить социальную сеть жертвы, подделать профили друзей и родственников, написать от имени жертвы и попросить взаймы.

Это далеко не все методы социального инжиниринга. На самом деле их гораздо больше, это основные и самые распространенные из них. С целью контроля и регулирования мошеннических действий государство принимает следующие меры.

1. Законодательные меры: государство разрабатывает и принимает законы, направленные на борьбу с мошенничеством и социальной инженерией. Эти законы могут предусматривать уголовную ответственность за совершение подобных преступлений. Так, к примеру, необходимо напоминать сотрудникам, что в случае разглашения коммерческой тайны каждого из них ждет увольнение по соответствующим статьям Трудового и Гражданского кодекса РФ.

2. Образование и информирование: государство проводит образовательные кампании, чтобы повысить осведомлённость граждан о рисках социальной инженерии и способах защиты от неё. Это может включать в себя распространение информационных материалов, проведение семинаров и тренингов.

3. Сотрудничество с правоохранительными органами: государство сотрудничает с правоохранительными органами для выявления и пресечения случаев мошенничества, включая социальную инженерию. Это включает в себя обмен информацией, совместные операции и сотрудничество в расследовании преступлений.

4. Регулирование деятельности финансовых учреждений: государство регулирует деятельность финансовых учреждений, таких как банки и платёжные системы, чтобы обеспечить защиту клиентов от мошенничества. Это может включать в себя требования к безопасности систем и процедур, а также контроль за соблюдением этих требований.

5. Технические меры: государство поддерживает разработку и внедрение технических решений, которые помогают предотвратить социальную инженерию и другие виды мошенничества [1]. Например, это может быть разработка и использование технологий аутентификации, шифрования данных и других мер безопасности.

6. Мониторинг и анализ: государство отслеживает тенденции и методы социальной инженерии, чтобы своевременно реагировать на новые угрозы и разрабатывать соответствующие меры защиты.

На практике многие компании уже внедрили эффективные меры противодействия социальной инженерии. Например, крупные финансовые учреждения активно используют технологии машинного обучения для анализа поведения клиентов и выявления подозрительных действий. Также некоторые организации проводят регулярные «имитационные атаки», чтобы проверить готовность своих сотрудников к реальным угрозам.

Корпоративный сектор может предпринять ряд мер для противодействия социальной инженерии в мошеннических целях. Вот некоторые из них:

Обучение сотрудников: проведение тренингов и семинаров по распознаванию и противодействию социальной инженерии, а также по соблюдению правил информационной безопасности.

Использование систем обнаружения и предотвращения мошенничества (FDS): внедрение технологий, которые анализируют поведение пользователей и выявляют подозрительную активность, связанную с социальной инженерией.

Ограничение доступа к конфиденциальной информации: внедрение политик безопасности, ограничивающих доступ сотрудников к определённым данным, особенно если они не связаны с их должностными обязанностями.

Мониторинг и анализ инцидентов: сбор и анализ данных о попытках мошенничества, включая социальную инженерию, для выявления тенденций и уязвимостей.

Внедрение многофакторной аутентификации: использование дополнительных методов проверки личности пользователя, таких как SMS-коды или биометрические данные, для защиты от несанкционированного доступа.

Регулярное обновление программного обеспечения и систем безопасности: установка последних версий антивирусного ПО, брандмауэров и других защитных инструментов для предотвращения кибератак, связанных с социальной инженерией.

Создание корпоративной культуры безопасности: поощрение сотрудников к ответственному отношению к защите информации и соблюдению правил безопасности.

Сотрудничество с правоохранительными органами: обмен информацией о случаях мошенничества и участие в расследовании инцидентов, связанных с социальной инженерией.

Проведение аудита безопасности: регулярный анализ систем и процессов на предмет уязвимостей, связанных с социальной инженерией, и разработка рекомендаций по их устранению.

Эффективность этих мер зависит от конкретных условий и политики компании. Некоторые организации могут уделять больше внимания обучению сотрудников и внедрению FDS, в то время как другие могут сосредоточиться на обновлении программного обеспечения и создании корпоративной культуры

безопасности. Важно регулярно оценивать риски и принимать меры, соответствующие специфике бизнеса и уровню угроз.

Противодействие социальной инженерии требует комплексного подхода, включающего как меры государственного регулирования, так и активные действия со стороны корпоративного сектора. Эффективное сотрудничество между государственными органами и бизнесом может значительно повысить уровень безопасности и снизить количество мошеннических схем. Важно продолжать развивать законодательство, внедрять современные технологии и повышать осведомленность граждан о рисках социальной инженерии.

Список литературы

1. Аркадьева О.Г. Формирование модели государственного регулирования развития технологий искусственного интеллекта в финансовом секторе / О.Г. Аркадьева, Н.В. Березина // Oeconomia et Jus. – 2023. – №4. – С. 12–21. – DOI 10.47026/2499–9636–2023–4-12–21. EDN RXEYSM

2. Малахов А. Как работает социальная инженерия, и как этим пользуются мошенники / А. Малахов // Т – Ж: Журнал про ваши деньги [Электронный ресурс]. – Режим доступа: https://journal.tinkoff.ru/social-engineering/ (дата обращения: 11.10.2024).

3. Броуди Р.Дж. Пролетая незаметно: социальная инженерия / Р.Дж. Броуди, У.Б. Бриззи, Л. Кано // Международный журнал бухгалтерского учета и управления информацией. – 2012. – Т. 20. Вып. 4. – С. 335–347.