РАЗРАБОТКА АВТОМАТИЧЕСКОЙ СИСТЕМЫ ДЛЯ ОБУЧЕНИЯ ПРОТИВОДЕЙСТВИЮ ПРЕТЕКСТИНГУ

Е.А. Костюхина, П.С. Ладыгин
Алтайский государственный университет, г. Барнаул
email: pavel-ladygin@yandex.ru

Аннотация. В работе предложена методика противодействия такому методу социальной инженерии, как претестинг. Предлагаемая методика направлена на повышение осведомленности персонала о средствах, методах и приемам действий злоумышленников по проникновению в информационную систему организации. Описано содержание методики и способа ее апробации. Для апробации использованы чат-боты в социальной сети, разработанные с помощью версии платформы Senler в специально созданном сообществе. Продемонстрирован вариант использования методики, приведены результаты тестирования, описаны ее преимущества и недостатки.

Ключевые слова: защита информации, чат-боты, претекстинг, машинное обучение.

Атаки с использованием методов социальной инженерии являются одними из самых опасных видов атак, нацеленных на конфиденциальную информацию и получение доступа к личным данным. Существует множество методов социальной инженерии, и к одним из них является претекстинг – действие, отработанное по заранее составленному сценарию [1] путем доверительного общения с жертвой посредством переписки в мессенджерах, социальных сетях, с помощью электронной почты или непосредственного разговора по сотовой связи. Противодействие претекстингу [2] чаще всего заключается в изучении теории, которая не может показать в полной мере, как злоумышленники используют данный метод для сбора необходимой информации. Специалисты по защите данных в различных организациях используют рассылку памяток по сотрудникам [3], что является способом повышения осведомленности, однако при текущей тенденции на киберучения [4] и необходимости замены «бумажной» безопасности на практическую [5] не способно в полной мере обеспечить снижение вероятности эксплуатации данной уязвимости в организации.

Содержание предлагаемой методики заключается в следующем: разрабатываются чат-боты, одним из которых будет являться «злоумышленник», остальные – люди, выполняющие роль обычных собеседников. Задача пользователя, который будет практически обучаться противодействию претекстингу – выявить в ходе общения, какой из чат-ботов является настоящим злоумышленником. В каждом диалоге с чат-ботом будет присутствовать претекстинг, чтобы было сложнее определить настоящего злоумышленника.

Схема работы чат-ботов, которые являются симуляцией общения со злоумышленниками, изображена на рисунке 1.

Чат-боты (симуляторы общения со злоумышленником) имеют заранее подготовленные сообщения, которые содержат:

1. Вопросы о личных данных и конфиденциальной информации.
2. Просьбы установить или скачать что-то.
3. Просьбы перейти на какой-либо сайт.
4. Предлоги, под которыми можно заполучить информацию или денежные средства.
5. Просьбы одолжить деньги.

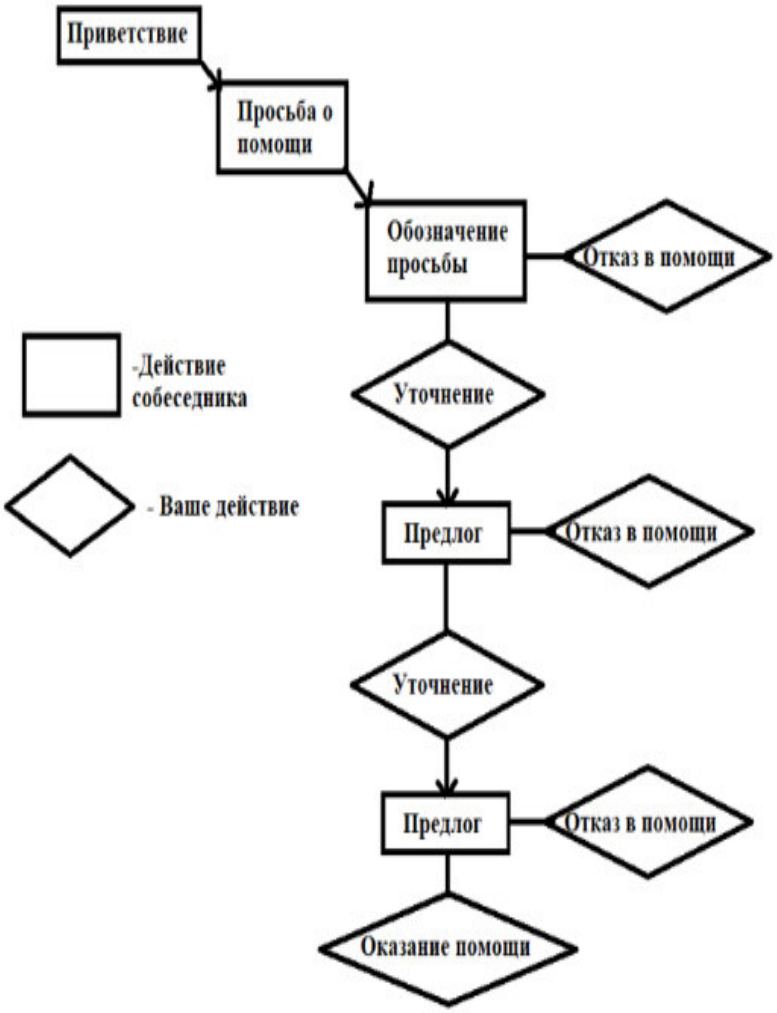

Рисунок 1. Структура чат-ботов.

Для разработки чат-ботов и методики противодействия была использована бесплатная версия сервиса Senler [6]. Для работы с чат-ботами создано сообщество «Информационная безопасность», в которое можно перейти по ссылке https://vk.com/infoclub26.

При непосредственном обучении противодействию претекстингу нужно перейти к диалогу с сообществом. Для начала беседы с одним из чат-ботов нужно нажать определенную цифру от 1 до 5, которые соответствуют определенным диалогам со «злоумышленниками» и диалогам с «обычными пользователями». Цифра 6 приведет к диалог с чат-ботом, содержащим информацию о том, какой из чат-ботов выступал в какой роли. На рисунке 2 показан процесс создания чат-ботов в Senler. Данный чат-бот является симуляцией общения со злоумышленником. Синим цветом помечены нейтральные ответы, красным – потенциально опасные, зеленым – неопасные ответы. На рисунке 3 показан результат тестирования чат-бота в социальной сети ВКонтакте.

В рассмотренном примере в качестве претекстинга используется просьба поучаствовать в голосовании. В век современных технологий такие случаи не редки, поэтому обычно люди соглашаются помочь. Кроме того, предлогом является и то, что ссылки можно пересылать только по почте. На самом деле, этот диалог можно связать с еще одним методом социальной инженерии – фишингом, так как ссылка, отправленная по почте, является вредоносной и не имеет никакого отношения к конкурсу. Методом противодействия является проверка ссылки на вредоносность, что является одним из последних действий в диалоге.

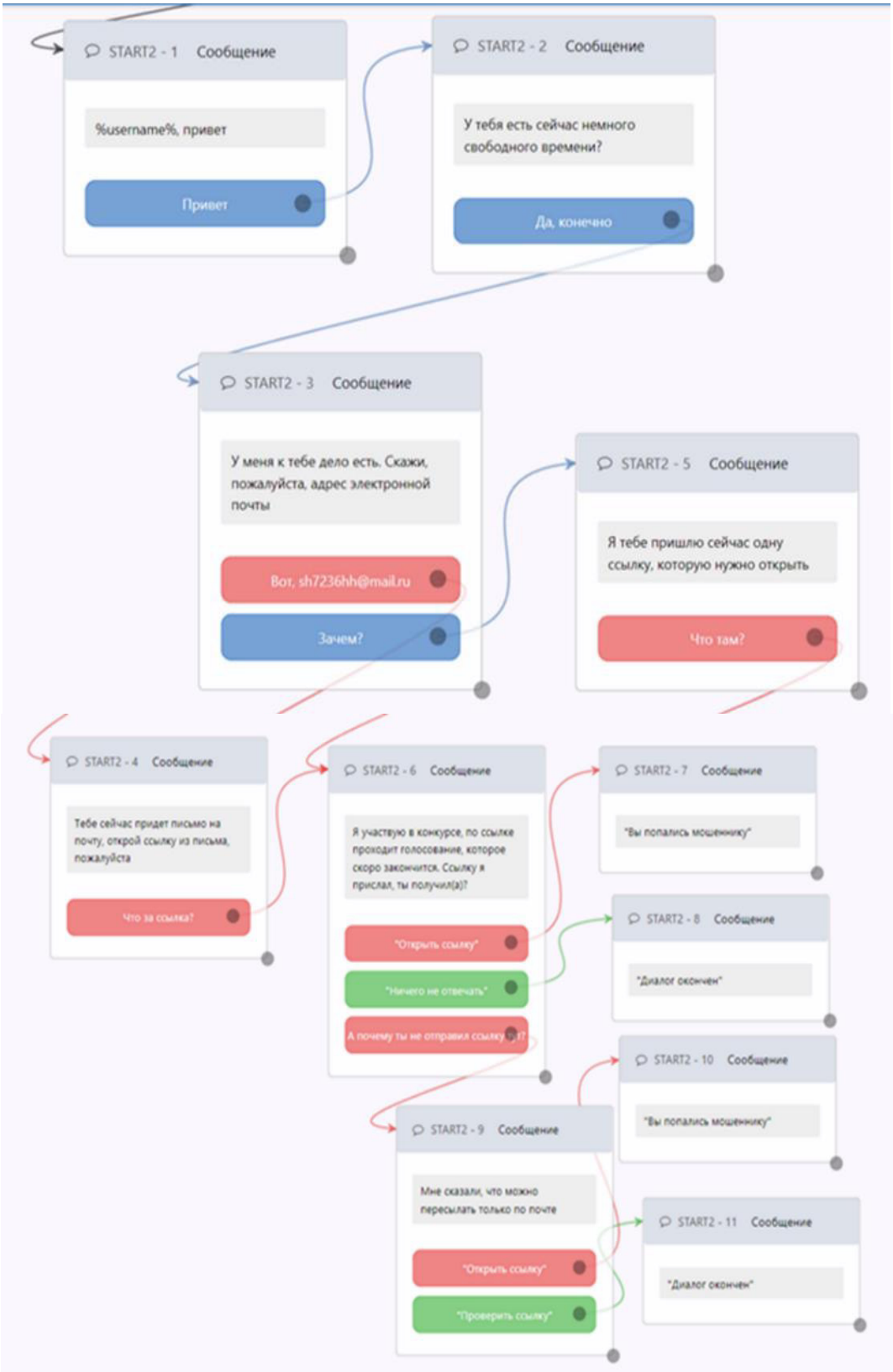

Рисунок 2. Разработка чат-бота в Senler.

Для разработанных диалогов были написаны рекомендации, которые призваны помочь понять, в каком чат-боте ведется переписка с мошенником:

1. Необходимо анализировать каждое действие, чтобы понять, насколько данная ситуация возможна в реальности;
2. Попытаться выяснить как можно больше деталей, а не стараться быстрее окончить диалог. Чем он подробнее, тем легче понять, что это за собеседник;

3. Постараться выбрать такие варианты, которые в итоге приведут к какому-либо действию, оказывающему противодействие претекстингу;
4. Один из диалогов имеет подсказку, которая говорит о том, что это просто собеседник;
5. Помнить о том, что все эти ситуации могут случиться в реальной жизни;
6. Постараться ответить на вопрос о том, какая ситуация является наиболее странной.

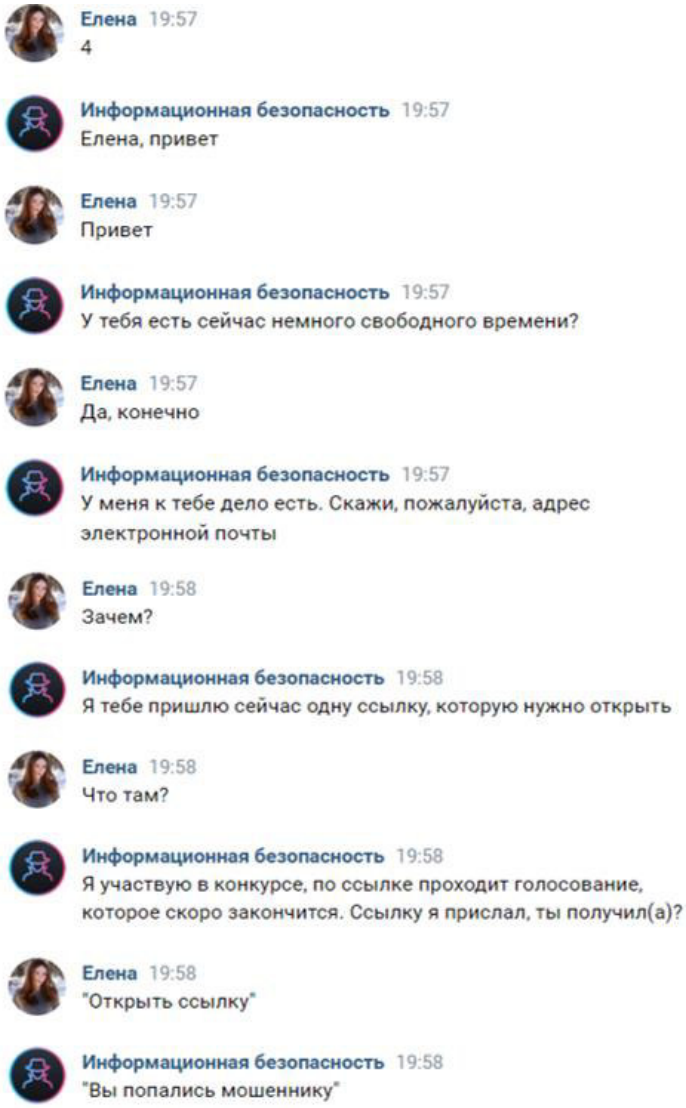

Рисунок 3. Результат работы чат-бота.

Для оценки эффективности данной модели была специально обучена группа из 30 лиц, добровольно принявших участие в испытаниях. Исходя из результатов обучения и отзывов, была составлена таблица, в которой, кроме результатов, представлены также преимущества и недостатки обучения и экспертные оценки эффективности. Таким образом, была получена средняя оценка эффективности и сделаны выводы по эффективности автоматической системы, используемой в качестве метода обучения.

Анализ таблицы 1 позволяет сделать вывод о том, что использование предложенной методики организации тренингов для персонала с помощью разработанных программных средств позволит повысить осведомленность персонала о средствах и методах действий злоумышленников по проникновению в информационную систему организации. Практическое внедрение разработанной методики обеспечит повышение защищенности информационной сети организации от атак в форме претестинга.

Таблица 1. Результаты обучения.

Испы-туемый	Попался мошеннику	Отгадал, кто мошенник	Преимущества	Недостатки	Экспертная оценка
1	Нет	Да	Затронуты основные варианты проведения атак, возможность научиться понимать и находить отличия между злоумышленником и обычным собеседником	Нет	5
2	Нет	Нет	В конце диалогов есть методы противодействия претекстингу, что помогает не попасться мошеннику и учит, как нужно действовать в подобных ситуациях	Неподходящая платформа для обучения	3
3	Нет	Да	Простота обучения, обусловленная использованием автоматической системы	Нехватка поясняющих сообщений об исходе выбранных действий	4
4	Нет	Нет	Возможность больше узнать о способах мошенничества и «злоумышленни-чества»	Некорректная работа автомати-ческой системы	4
5	Нет	Да	Простота обучения, обусловленная использованием автоматической системы	Необходи-мость в более подробном изучении теоретических сведений	4
Средняя оценка:					4

Библиографический список.

1. Encyclopedia by Kaspersky // [Электронный ресурс] / Режим доступа: https://encyclopedia.kaspersky.ru/glossary/pretexting/.

2. Старостенко Н.И., Старостенко О.А Криминалистическая характеристика способов мошенничества, совершенного с использованием методов социальной инженерии // Научный журнал «Проблемы правовой и технической защиты информации» [Электронный ресурс] / 2020. – Заглавие с экрана. - Режим доступа: http://elibrary.asu.ru.

3. Интервью социального инженера: как "взломать" человека // Securitylab [Электронный ресурс] / 2020. – Заглавие с экрана. - Режим доступа: https://www.securitylab.ru/blog/company/axxtel/349562.php (дата обращения: 20.11.2022).

4. Киберучения в национальном масштабе: как работают киберполигоны в России // РБК: [Электронный ресурс] / 2022. Заглавие с экрана. — Режим доступа: https://www.rbc.ru/technology_and_media/01/11/2022/635bfe3f9a794799a7e0b42e (дата обращения: 20.11.2022).

5. Постановление Правительства РФ "О проведении эксперимента по повышению уровня защищенности государственных информационных систем

федеральных органов исполнительной власти и подведомственных им учреждений" от 13.05.2022 № 860 // Официальный интернет-портал правовой информации.
6. Senler // [Электронный ресурс] / Режим доступа: https://senler.ru.

DEVELOPMENT OF AN AUTOMATIC SYSTEM FOR TRAINING IN COUNTERING PRETEXTING

E.A. Kostyukhina, P.S. Ladygin
Altai state university, Barnaul
email: pavel-ladygin@yandex.ru

Annotation. The paper proposes a method of countering such a method of social engineering as pretesting. The proposed methodology is aimed at increasing staff awareness of the means, methods and techniques of intruders' actions to penetrate the organization's information system. The content of the methodology and the method of its approbation are described. For testing, chatbots in a social network developed using a version of the Senler platform in a specially created community were used. A variant of using the technique is demonstrated, the results of testing are presented, its advantages and disadvantages are described.

Keywords: chatbots, pretexting, training.