МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

02.03.03 Математическое обеспечение и администрирование информационных систем
(код и наименование направления подготовки, специальности)

Мобильные и сетевые технологии
(направленность (профиль)/ специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Разработка программного модуля для определения уязвимостей пользователей к социально-инженерным атакам»

Студент Д.Р. Феткуллова
(И.О. Фамилия) (личная подпись)

Руководитель А.П. Тонких
(ученая степень, звание, И.О. Фамилия)

Консультант М.В. Дайнеко
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Аннотация

Тема бакалаврской работы: «Разработка программного модуля для определения уязвимостей пользователей к социально-инженерным атакам».

Бакалаврская работа посвящена разработке автоматизированных инструментов, способствующих повышению степени информированности лиц, принимающих решения, о наиболее подверженных социоинженерным атакам цепочках пользователей, за счёт предложения средств определения критичных траекторий распространения социально-инженерных атак и их визуализации на социальном графе сотрудников.

В ходе выполнения исследований по бакалаврской работе реализован алгоритм, позволяющий проанализировать уровень защиты пользователей от социально-инженерных атак.

Выпускная квалификационная работа состоит из введения, трёх глав, заключения и списка литературы. Во введении рассматривается актуальность исследуемой области, также представлено обоснование цели и задач, решаемых в выпускной работе бакалавра.

В первой главе производится обзор алгоритмов, необходимых для решения поставленных задач.

Во второй главе приводятся методы квантификации характеристик взаимодействия пользователей.

В третьей главе описаны процесс разработки и структура программных модулей: «Анализатора критичных траекторий» и «Построения графа».

В заключении описаны выводы по представленной работе.

В работе имеются 10 рисунков, 3 таблицы, 10 формул. Список использованной литературы включает 56 источников. Общий объём бакалаврской работы – 47 страниц.

Abstract

The topic of the bachelor's work: "Development of a software module for determining user vulnerabilities to social engineering attacks."

The bachelor's work is devoted to the development of automated tools that help to increase the awareness of decision-makers about the user chains most susceptible to socio-engineering attacks by proposing means for determining critical trajectories of the spread of social-engineering attacks and their visualization on the social graph of employees.

In the course of carrying out research on bachelor's work, an algorithm was implemented that allows to analyze the level of protection of users from social engineering attacks.

The final qualifying work consists of an introduction, three chapters, a conclusion and a list of references. The introduction examines the relevance of the area under study, and also provides a rationale for the goal and tasks solved in the final bachelor's work.

The first chapter provides an overview of the algorithms required to solve the assigned tasks.

The second chapter provides methods for quantifying the characteristics of user interactions.

The third chapter describes the development process and structure of software modules: "Analyzer of critical trajectories" and "Building a graph".

In the conclusion, the conclusions of the presented work are described.

The work contains 10 figures, 3 tables, 10 formulas. The list of used literature includes 56 sources. The total volume of the bachelor's work is 47 pages.

Содержание

Введение

Актуальность темы. Несмотря на рост эффективности и повышение качества средств защиты конфиденциальной информации от программно-технических атак, информационные системы остаются уязвимыми [47, 53]. Часто ключевую роль в инцидентах нарушения безопасности информации играет человек – санкционированный пользователь системы [26, 27, 31, 40, 43].

В настоящее время стали чаще происходить программно-технические атаки злоумышленников на пользователей с применением социоинженерных методов. Эти атаки приводят к крупному ущербу. Выявление источника таких атак расходует большое количество временных ресурсов [28]. В соответствии с [38], атака с использованием инструментария социальной инженерии представляет собой комплекс методов прикладного анализа и прикладной психологии, используемый атакующим для тайного воздействия на пользователей информационных систем с целью нарушениям ими существующих правил и политик безопасности, установленных в корпоративной или публичной сети.

Рассматриваемая тема является актуальной, так как по сведениям представителей крупного бизнеса, использование социоинженерных приёмов составляет 80% атак злоумышленников в Российской Федерации [48]. Эти данные подтверждаются отчётностью разработчиков систем безопасности для профилактики киберпреступлений [40, 44]. Специалисты сферы защиты информации также подтверждают, что эта тема является актуальной [32]. В соответствии с их прогнозами [54], в ближайшие несколько лет ожидается рост активности злоумышленников-социоинженеров.

Помимо сотрудников организаций жертвами социоинженерных атак также становятся и частные лица. Последние годы в России в этой роли оказывались 1,2 миллиона человек ежегодно [45]. В первом полугодии 2018

года у жертв в среднем было похищено 5000 рублей, что составляет 12% среднемесячной зарплаты россиянина [45].

По классификации, представленной в монографии [39], особую группу социоинженерных атак составляют фишинг-атаки, кроме того, отмечается их существенный рост за последнее время. Данный факт также находит подтверждение в отчёте компании Group-IB [53]: при помощи веб-фишинга хакерам удалось украсть около 4,2 миллиона долларов. При этом в среднем за день совершается более 1,2 тысяч социоинженерных атак [53].

В связи с этим актуальным представляется вопрос безопасности пользователей корпоративных и публичных сетей в области кибератак с использованием методов социальной инженерии. Чтобы обеспечить безопасность пользователей корпоративных и публичных сетей в области кибератак с использованием методов социальной инженерии, выполняют анализ защищённости. Поэтому актуальным является вопрос обеспечения высокоуровневой защиты информации в компании путём создания программного обеспечения для определения уровня защиты пользователей корпоративных и публичных сетей от кибератак с использованием методов социальной инженерии.

Часто социоинженерные атаки осуществляются через цепочку пользователей. Такие атаки называются многоходовыми социоинженерными атаками [2]. Атаковать целевого пользователя при этом можно через разные цепочки, и оценки вероятности прохождения по ним будут отличаться.

Если представить сотрудников организации в виде социального графа, то можно говорить о разных траекториях реализации многоходовых социоинженерных атак. При этом оценки вероятности успешного прохождения этих траекторий отличаются, в связи с чем возникает необходимость выявления наиболее вероятной траектории распространения многоходовой кибератаки с использованием социальной инженерии или совокупности таких траекторий.

Кроме того, важно учитывать, что от реализации разных траекторий организация несёт отличающиеся по размеру убытки. Таким образом, существенно выявлять не только наиболее вероятные траектории, но разработать подход к идентификации наиболее критичных траекторий.

Исследования, направленные на изучение характера взаимодействия пользователей, квантификацию характеристик данного взаимодействия и его влияния на распространение социоинженерной атаки, проводились и продолжают проводиться на базе Санкт-Петербургского института информатики и автоматизации РАН (ТиМПИ СПИИРАН). А именно, был разработан набор моделей: «критичные документы – информационная система – персонал – злоумышленник» [5]. А также исследованы вопросы по построению и анализу социальных графов сотрудников компании [2]. Предложены подходы выявления аккаунтов сотрудников организации в соцсетях [30]. Рассмотрены вопросы идентификации связей, получаемых из социальных сетей [50].

Цель выпускной квалификационной работы заключается в разработке автоматизированных инструментов, способствующих повышению степени информированности лиц, принимающих решения, о наиболее подверженных социоинженерным атакам цепочках пользователей, за счёт предложения средств определения наиболее критичных траекторий распространения многоходовых кибератак с использованием методов социальной инженерии и их визуализации на социальном графе сотрудников.

В соответствии с этой целью, были поставлены и решены следующие задачи:

- изучение предметной области и релевантных работ по теме исследования;

- создание алгоритмов определения наиболее вероятных траекторий распространения многоходовых кибератак с использованием методов социальной инженерии;

- создание метрик для оценивания критичности траекторий распространения многоходовых кибератак с использованием методов социальной инженерии;

- изучение силы влияния возможных типов взаимоотношений между пользователями, на вероятность распространения кибератаки с использованием методов социальной инженерии;

- разработка алгоритмов, основанных на предложенных методах, и их реализация в прототипе модуля комплекса программ.

Объектом исследования является социальный граф сотрудников компании, построенный исходя из данных, извлечённых из социальных сетей и частично задаваемых экспертно. Такие данные дают одну из возможностей построения оценок вероятности успеха распространения кибератаки с использованием методов социальной инженерии.

Предметом исследования являются траектории распространения многоходовых кибератак с использованием методов социальной инженерии, моделируемые на социальном графе пользователей.

Все результаты, выносимые на защиту, являются новыми. Впервые предложены методы выявления наиболее вероятных траекторий распространения многоходовых кибератак с использованием методов социальной инженерии, методы определения наиболее критичных траекторий распространения этих атак. Впервые было проведено исследование по изучению величины воздействия возможных типов взаимоотношений пользователей в соцсети на вероятность распространения кибератаки с использованием методов социальной инженерии. Впервые были разработаны алгоритмы по выявлению наиболее вероятных траекторий распространения многоходовых кибератак с использованием методов социальной инженерии и выполнена их реализация.

Предлагаемые методы и алгоритмы, реализованные в программном обеспечении по определению уровня защиты корпоративной сети от кибератаки с использованием методов социальной инженерии,

предоставляют возможность выполнять поиск наиболее вероятных траекторий распространения многоходовых кибератак с использованием методов социальной инженерии. Данная оптимизация способствует дальнейшему развитию исследований по данной тематике, быстрому и эффективному нахождению наиболее уязвимых мест в информационной системе и, как следствие, позволяет лицам, принимающим решения, производить оперативные меры по обеспечению высокоуровневой защищённости организации.

Методология работы заключается в выявлении наиболее вероятных траекторий распространения многоходовых кибератак с использованием методов социальной инженерии, созданию методов, нацеленных на выявление наиболее критичных траекторий, а также апробации полученных теоретических результатов посредством их реализации в программном комплексе.

Методы включают подходы теории вероятностей, математического анализа, теории графов и объектно-ориентированного программирования. Комплекс программ реализован на языке Java в среде программирования Intellij IDEA 2020.

В работе предложены:

- метод выявления наиболее вероятных траекторий распространения многоходовых кибератак с использованием методов социальной инженерии;

- метрика оценки критичности траекторий распространения многоходовых кибератак с использованием методов социальной инженерии;

- изучение силы влияния возможных типов взаимоотношений между пользователями на возможность распространения кибератаки с использованием методов социальной инженерии;

- алгоритмы по выявлению наиболее вероятных траекторий распространения многоходовых кибератак с использованием методов социальной инженерии и их реализация.

Высокая степень достоверности результатов выпускной квалификационной работы обеспечивается глубоким и всесторонним анализом исследований по тематике социоинженерных атак, подтверждается согласованностью полученных результатов.

Работа включает в себя введение, три главы, заключение, список используемой литературы. Общий объём выпускной работы бакалавра – 47 страниц.

В главе 1 описывается актуальность исследуемой области, также представлено обоснование цели и задач, решаемых в выпускной работе бакалавра. Приводится анализ подходов, решающих схожие задачи и описывается теоретическая часть, послужившая фундаментом для решения поставленных задач, также производится обзор алгоритмов, необходимых для решения поставленных задач.

В главе 2 представлены основные результаты выпускной квалификационной работы, а именно описывается метод для нахождения наиболее вероятных траекторий и метрика для оценки критичности траекторий распространения многоходовых кибератак с использованием методов социальной инженерии, приводятся методы квантификации характеристик взаимодействия пользователей.

В главе 3 описаны процесс разработки и структура программных модулей: «Анализатора критичных траекторий» и «Построения графа».

1 Анализ подходов и методов определения уязвимостей пользователей к социально-инженерным атакам

В данной главе описывается актуальность исследуемой области, также представлено обоснование цели и задач, решаемых в выпускной квалификационной работе бакалавра. Приводится анализ подходов, решающих схожие задачи, и описывается теоретическая часть, послужившая фундаментом для решения поставленных задач, приводится обзор существующих алгоритмов по поиску кратчайшего пути в графе.

1.1 Актуальность задач защиты от кибератак с использованием методов социальной инженерии

Анализ уровня защиты пользователей корпоративных и публичных сетей от кибератак с использованием методов социальной инженерии является одной из актуальных проблем, что подтверждается количеством инцидентов и интенсификацией роста убытков от них [26, 27, 32, 41, 43, 47]. Одним из подтверждений актуальности исследуемой тематики может служить информация, предоставляемая крупными российскими компаниями, свидетельствующая о применении методов социальной инженерии в 80% случаев от числа всех инцидентов нарушения безопасности [48]. Данная информация также отражена и в отчётах компаний, специализирующихся на разработке систем защиты от кибератак [40, 44]. Актуальность данного направления находит подтверждение и у экспертов в области информационной безопасности [32]. Согласно их прогнозам [54] в ближайшие несколько лет ожидается рост активности злоумышленников-социоинженеров.

Злоумышленник – социальный инженер, целью которого является получение доступа к конкретному документу/ряду документов при помощи

методов социальной инженерии, зачастую эксплуатируя доверчивость, лень, любезность и энтузиазм пользователей и сотрудников организаций. [33]

Документ – материальный объект с зафиксированной на нём информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования [48].

Безопасность информации – состояние защищённости информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами [49].

Помимо сотрудников организаций жертвами социоинженерных атак также становятся и частные лица. Последние годы в России в этой роли оказывались 1,2 млн человек ежегодно [45]. В первом полугодии 2018 года у жертв в среднем было похищено 5000 рублей, что составляет 12% среднемесячной зарплаты россиянина [45]. По классификации, представленной в монографии [39], особую группу социоинженерных атак составляют фишинг-атаки, кроме того, отмечается их существенный рост за последнее время. Данный факт также находит подтверждение в отчёте компании Group-IB [53]: при помощи веб-фишинга хакерам удалось украсть около $4,2 млн. При этом в среднем за день совершается более 1,2 тысяч социоинженерных атак [53].

В связи с этим актуальным представляется вопрос безопасности пользователей корпоративных и публичных сетей в области кибератак с использованием методов социальной инженерии. Чтобы обеспечить безопасность пользователей корпоративных и публичных сетей в области кибератак с использованием методов социальной инженерии, выполняют анализ защищённости. Поэтому актуальным является вопрос обеспечения высокоуровневой защиты информации в компании путём создания

программного обеспечения для определения уровня защиты пользователей корпоративных и публичных сетей от кибератак с использованием методов социальной инженерии.

1.2 Многоходовые кибератаки с использованием методов социальной инженерии

Многоходовая социоинженерная атака – социоинженерная атака, которая включает в себя взлом более чем одного сотрудника таким образом, что взломанные сотрудники непосредственно участвуют во взломе последующих жертв. [2]

Чтобы разработать программное обеспечение для определения уровня защиты пользователей корпоративных и публичных сетей от кибератак с использованием методов социальной инженерии, требуется оценить уровень защиты от одноходовых и многоходовых кибератак с использованием методов социальной инженерии. Многоходовая кибератака с использованием методов социальной инженерии отличается от одноходовой тем, что для её осуществления необходима цепь пользователей, а не происходит опосредованно. Многоходовые социоинженерные атаки, как правило, могут распространяться по нескольким траекториям. Оценки вероятности успешного распространения многоходовой атаки злоумышленника на пользователя по разным траекториям обычно имеют отличающиеся значения. В связи с этим необходимо выявить траектории, успешное прохождение по которым произойдёт с большей вероятностью. Для этого предлагается производить анализ на социальном графе взаимодействия сотрудников.

Социальный граф пользователей – граф, узлы которого представлены социальными объектами, такими как пользовательские профили с различными атрибутами (например: имя, день рождения, родной город и

т.д.), сообщества, медиа-контент и т.д., а рёбра – социальными связями между ними [24].

Оценка уровня защиты при многоходовых кибератаках с использованием социальной инженерии и определение возможности распространения кибератаки от одного пользователя к другому рассматриваются в [2, 39, 52]. В [2] представлены неориентированные социальные графы, поэтому не учитывается, что оценка возможности распространения кибератаки от одного пользователя к другому в прямом и обратном направлении может отличаться. В [2] не описано выявление наиболее критичных траекторий развития кибератаки. Обычно имеется ряд вероятных траекторий распространения кибератаки от пользователя к пользователю и вероятности успешного развития кибератаки по каждой траектории будут отличаться. В связи с этим, актуальной является задача определения наиболее возможных траекторий развития кибератаки.

Данная работа является продолжением указанного выше общего исследования и опирается на полученные ранее результаты [2, 30, 38, 39, 51, 52]. А именно анализ траекторий осуществляется в уже построенном и размеченном графе [39], отражающем социальные связи между пользователями системы и вероятности успеха перехода злоумышленника от пользователя к пользователю. Предполагается, что данное решение будет способствовать повышению оперативности выявления наиболее незащищённых звеньев информационной системы, вследствие чего могут быть приняты своевременные меры по их защите.

1.3 Постановка задачи

Приводимые выше сведения обосновывают актуальность проблематики социоинженерных атак. Вместе с тем одним из малоизученных мест по данной тематике видится исследование сложных социоинженерных атак, осуществляемых через цепочку пользователей. Такие атаки называются

многоходовыми социоинженерными атаками [2]. Атаковать целевого пользователя при этом можно через разные цепочки, и оценки вероятности прохождения по ним будут отличаться. Если представить сотрудников организации в виде социального графа, то можно говорить о разных траекториях реализации многоходовых социоинженерных атак. При этом оценки вероятности успешного прохождения этих траекторий отличаются, в связи с чем возникает необходимость выявления наиболее вероятной траектории развития многоходовой кибератаки с использованием методов социальной инженерии или совокупности таких траекторий.

Кроме того, важно учитывать, что от реализации разных траекторий организация несёт отличающиеся по размеру убытки. Таким образом, существенно выявлять не только наиболее вероятные траектории, но разработать подход к идентификации наиболее критичных траекторий. В связи с этим была выдвинута следующая цель, достигаемая в выпускной квалификационной работе бакалавра.

Цель выпускной квалификационной работы заключается в разработке автоматизированных инструментов, способствующих повышению степени информированности лиц, принимающих решения, о наиболее подверженных социоинженерным атакам цепочках пользователей за счёт предложения средств определения наиболее критичных траекторий развития многоходовых кибератак с использованием методов социальной инженерии и их визуализации на социальном графе сотрудников.

В соответствии с целью были поставлены и решены следующие задачи:

- разработка методов выявления наиболее вероятных траекторий развития многоходовых кибератак с использованием методов социальной инженерии;

- разработка метрик оценивания критичности траекторий развития многоходовых кибератаки с использованием методов социальной инженерии;

- изучение силы влияния возможных типов взаимоотношений между пользователями на возможность развития кибератаки с использованием методов социальной инженерии;

- разработка алгоритмов, основанных на предложенных методах, и их реализация в прототипе модуля комплекса программ.

1.4 Обзор литературы

В основу легли работы [2, 5], рассматривающие оценку уровня защиты пользователей корпоративных и публичных сетей от одноходовых и многоходовых кибератак с использованием методов социальной инженерии. Исследования по повышению уровня защищённости пользователя были представлены в [18]. В данной работе авторы рассматривают несколько уровней оценки уязвимости пользователей к кибератакам с использованием методов социальной инженерии, базирующейся на трёх основных элементах: способ связи, состояние системы и сценарий атаки. Также проведены эксперименты по анализу эффективности разработанной системы. Подход, описанный в [36], основывается на преобразовании требований безопасности в элементы обучающей игры, в результате использования разработанной игровой программы пользователи информационной системы могут распознать основные сценарии социоинженерных атак.

Часть рассмотренных исследований была направлена на изучение поведения пользователей в социальных сетях. Результатом исследования [4, 14, 19, 25] являются эмпирические оценки восприимчивости пользователей к социоинженерным атакам. Сделанные на основе упомянутых исследований выводы могут быть полезны для оптимизации процесса анализа контента, извлекаемого из социальных сетей. Схожую направленность имеет исследование [23], в нём приводятся факторы, влияющие на соблюдение сотрудниками политики безопасности. В [3] рассматриваются факторы,

которые воздействуют на уязвимости пользователей и причины подверженности социоинженерным атакам.

Социальная сеть – платформа, онлайн-сервис и веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений в Интернете [34].

Уязвимость пользователя – некоторая характеристика пользователя которая делает возможным успешное завершение социоинженерного атакующего действия злоумышленника [38].

Профиль уязвимостей пользователя – совокупность пар «уязвимость пользователя» – «степень выраженности уязвимости» [38].

Исследование, основывающиеся на анализе текста и направленное на выявление фишинговых писем, представлено в [6]. В исследовании [7] изучается вопрос защиты от прогнозирования скрытых конфиденциальных данных пользователей социальных сетей, также исследуется зависимость между открытой и скрытой информацией в социальном профиле пользователя, результатом исследования является разработка способа защиты. Схожая проблема поднимается в источнике [16]. Подход, предлагаемый авторами данной статьи, базируется на автоматизированном сборе информации из открытых источников, её анализе и выявлении критических с точки зрения безопасности мест. Результатом [21] стала разработка web-сервиса, основанного на интеллектуальном анализе данных и позволяющего распознавать угрозы безопасности в социальной сети Twitter. Авторы [8, 20, 37] производят анализ неявного социального графа (графа, формируемого на основе данных о «друзьях» в социальной сети) с целью обнаружения аномального поведения, а также подозрительных и ложных учётных записей. В [1] поднимается проблема нарушения конфиденциальности данных социальных сетей и предлагается ряд методов для её решения. Исследование [11] предоставляет комплексный обзор ключевых исследований в области конфиденциальности информации за последние 40 лет.

1.5 Алгоритмы поиска кратчайшего пути на социальном графе сотрудников компании

В ходе проведения исследований было выявлено, что для решения поставленных задач необходимо уметь осуществлять поиск наиболее короткого пути на социальном графе сотрудников. Пусть n – количество сотрудников, m – количество дуг в графе. Для осуществления поиска наиболее короткого пути рассмотрены алгоритм Беллмана-Форда, алгоритм Дейкстры и его модификации, алгоритм Левита, алгоритм WFI, поиск A*, топологическая сортировка [12, 22, 29].

Применение алгоритмов Левита и WFI нецелесообразно, так как они обладают высокой вычислительной сложностью в контексте социального графа сотрудников. Для применения топологической сортировки требуется ациклический граф. Социальный граф пользователей обычно не является ациклическим, поэтому топологическая сортировка использована быть не может. Поиск A* решает задачу поиска наиболее короткого расстояния только между двумя вершинами социального графа, а не между всеми, что является удобством этого алгоритма. Однако применение поиска A* нецелесообразно, так как, во-первых, сложность поиска A* состоит в подборе правильной эвристической функции, а во-вторых, поиск A* требует большого объёма памяти для выполнения. Алгоритм Дейкстры подходит для выполнения поиска наиболее короткого пути и имеет вычислительную сложность O(n2). В то же время оптимальная сложность для алгоритмов, которые основаны на алгоритме Дейкстры, равна O(nlogn+m). Такую вычислительную сложность алгоритм, которые основаны на алгоритме Дейкстры, достигает в случае хранения данных в фибоначчиевых кучах. Но на практике величины констант, которые скрыты в асимптотических оценках трудоёмкости модификации алгоритма Дейкстры с представлением данных в виде фибоначчиевых куч, обычно оказываются большими. Тем не менее, если представлять данные в виде сортирующего дерева, вычислительная

сложность будет равна O(nlogn+mlogn). При этом такой алгоритм будет работать быстрее, чем оригинальный алгоритмом Дейкстры, только если социальный граф пользователей является разрежённым, то есть m≪n2. Социальный граф пользователей не всегда будет являться разрежённым.

Если количество дуг меньше количества сотрудников (m<n), то для решения задачи поиска кратчайшего пути применяется алгоритм Беллмана-Форда. Его вычислительная сложность в данном случае меньше, чем у алгоритма Дейкстры, и составляет O(mn).

1.6 Оценка вероятности перехода кибератаки с использованием методов социальной инженерии между двумя сотрудниками

Будем анализировать вероятные траектории кибератаки на направленном графе пользователей. Граф пользователей представляет собой граф, в котором вершины обозначают пользователей, а дуги – отношения между пользователями. Опишем в формализованном виде. Пусть дан граф (1):

$$G = (U, E), \tag{1}$$

где $U = \{User_i\}_{i=1}^{n}$ – множество сотрудников компании;

$E = \{(u_i, u_j, p_{i,j})\}_{1 \le i,j \le n, i \ne j}$ – множество упорядоченных троек с предопределённой оценкой возможности распространения кибератаки от сотрудника к сотруднику $p_{i,j}$.

Здесь не предполагается, что $p_{i,j} = p_{j,i}$, то есть вероятность распространения кибератаки в прямом и обратном направлении может принимать разные значения. В соответствии с [38] оценка вероятности развития кибератаки с использованием методов социальной инженерии от сотрудника к сотруднику вычисляется по формуле (2):

$$p_{i,j} = 1 - \prod_t \left(1 - p_t^{i,j}\right)^{n_t}, \quad (2)$$

где $p_t^{i,j}$ – оценка вероятности успешной кибератаки с использованием методов социальной инженерии на сотрудника по дуге t;

n_t – количество кибератак.

Оценка вероятности $p_{i,j}$ должна быть больше нуля. Дуги, для которых оценка вероятности $p_{i,j}$ равна нулю, не включаются в граф. Поиск максимально возможной траектории распространения многоходовой кибератаки с использованием методов социальной инженерии от пользователя $User_i$ к пользователю $User_j$ осуществляется решением задачи поиска пути от одной вершины к другой, для которого произведение вероятностных оценок переходов от одного сотрудника компании к другому имеет наибольшее значение: $p_{ml} = \max_{trajectories}\left(p_m \prod_{i,j} p_{ij}\right)$, $p_{ml} = arg\max_{trajectories}\left(p_m \prod_{i,j} p_{ij}\right)$.

Длина пути – вероятностная оценка успешной многоходовой кибератаки с использованием методов социальной инженерии, равная произведению вероятностных оценок развития кибератаки от сотрудника к сотруднику и прямой кибератаки на первого сотрудника компании.

Выводы по главе

В данной главе была показана актуальность исследуемой области, описаны многоходовые социоинженерные атаки. Представлено обоснование цели и задач, решаемых в выпускной работе бакалавра.

Приведён анализ подходов, решающих схожие задачи и описывается теоретическая часть, послужившая фундаментом для решения поставленных задач. Также приведён обзор существующих алгоритмов по поиску кратчайшего пути в графе.

2 Траектории реализации многоходовых социоинженерных атак

В данной главе описываются метрики для нахождения наиболее вероятных траекторий развития многоходовых кибератак с использованием методов социальной инженерии, а также представлены методы квантификации характеристик взаимодействия пользователей.

2.1 Квантификация интенсивности взаимодействия пользователей

В ходе процесса исследования возникла задача квантификации одной из характеристик интенсивности взаимодействия пользователей, являющихся узлами в социальном графе сотрудников. А именно, требовалось сопоставить рёбрам социального графа их веса. Произвести это предлагается при помощи численной оценки взаимосвязей пользователей, которые классифицированы пользователем в соцсети vk.com как братья, сёстры, прочие родственники, лучшие друзья и так далее. Чтобы произвести численную оценку взаимосвязей пользователей, воспользуемся имеющимися в соцсети vk.com классами друзей: «в гражданском браке», «влюблён в» или «влюблена в», «всё сложно», «встречаюсь с», «друзья по вузу», «друзья по школе», «жених» или «невеста», «коллеги», «лучшие друзья», «муж» или «жена», «родственники», «дедушка» или «бабушка», «родитель», «брат» или «сестра», «сын» или «дочь», «внук» или «внучка». Данные категории были разбиты на три группы.

1. Список друзей, который видят остальные пользователи: «друзья по вузу», «друзья по школе», «коллеги», «лучшие друзья», «родственники».

2. Основная информация в аккаунте: «в гражданском браке», «влюблён в» или «влюблена в», «всё сложно», «встречаюсь с», «жених» или «невеста», «муж» или «жена».

3. Родственные отношения: «бабушка» или «дедушка», «брат» или «сестра», «внук» или «внучка», «родитель», «сын» или «дочь».

Для удобства внесения ответов и обработки результатов был разработан web-документ, содержащий анкету по категории «друзья».

Отвечающему на вопросы анкетирования необходимо указать целочисленное значение вероятности в процентах в диапазоне от 0 до 100 того, что он выполнит какое-либо действие, которое попросит пользователь социальной сети из категории «друзья», который принадлежит тому или иному классу. Наибольшее значение вероятности будет обозначать, что пользователь обязательно выполнит просьбу. Наименьшее значение вероятности будет обозначать, что пользователь не выполнит просьбу в любом случае. Вопрос анкеты формулируется так: «Представьте следующую ситуацию: Вам пришло приглашение вступить в группу ВКонтакте. Оцените, пожалуйста, с какой вероятностью Вы бы откликнулись на эту просьбу, если бы Вам пришло приглашение от человека, который отмечен у Вас во ВКонтакте как:» (рисунок 1).

Анкетирование прошли 145 пользователей, из них 88 женского пола и 57 мужского. Среднее арифметическое значение возраста респондентов – 22 года, среднее медианное значение возраста респондентов – 20 лет. Анкетирование в основном проходили обучающиеся по гуманитарным, техническим, гуманитарным и управленческим направлениям в университетах Российской Федерации.

Проведённое анкетирование выявило, что некоторые респонденты не видели разницу между классами пользователей, т.е. эти респонденты указывали одни и те же значения вероятностей для различных классов «друзей», а некоторые указывали одни и те же значения вероятностей для всех классов «друзей». Значительное количество пользователей указали одни и те же значения вероятностей для всех «друзей» в категории «родственники», то есть эти пользователи выполнят просьбы бабушки, брата, дедушки, родителей, сестры с одной и той же вероятностью. Поэтому было принято решение найти количество пользователей, которые проранжировали «друзей» одним и тем же образом.

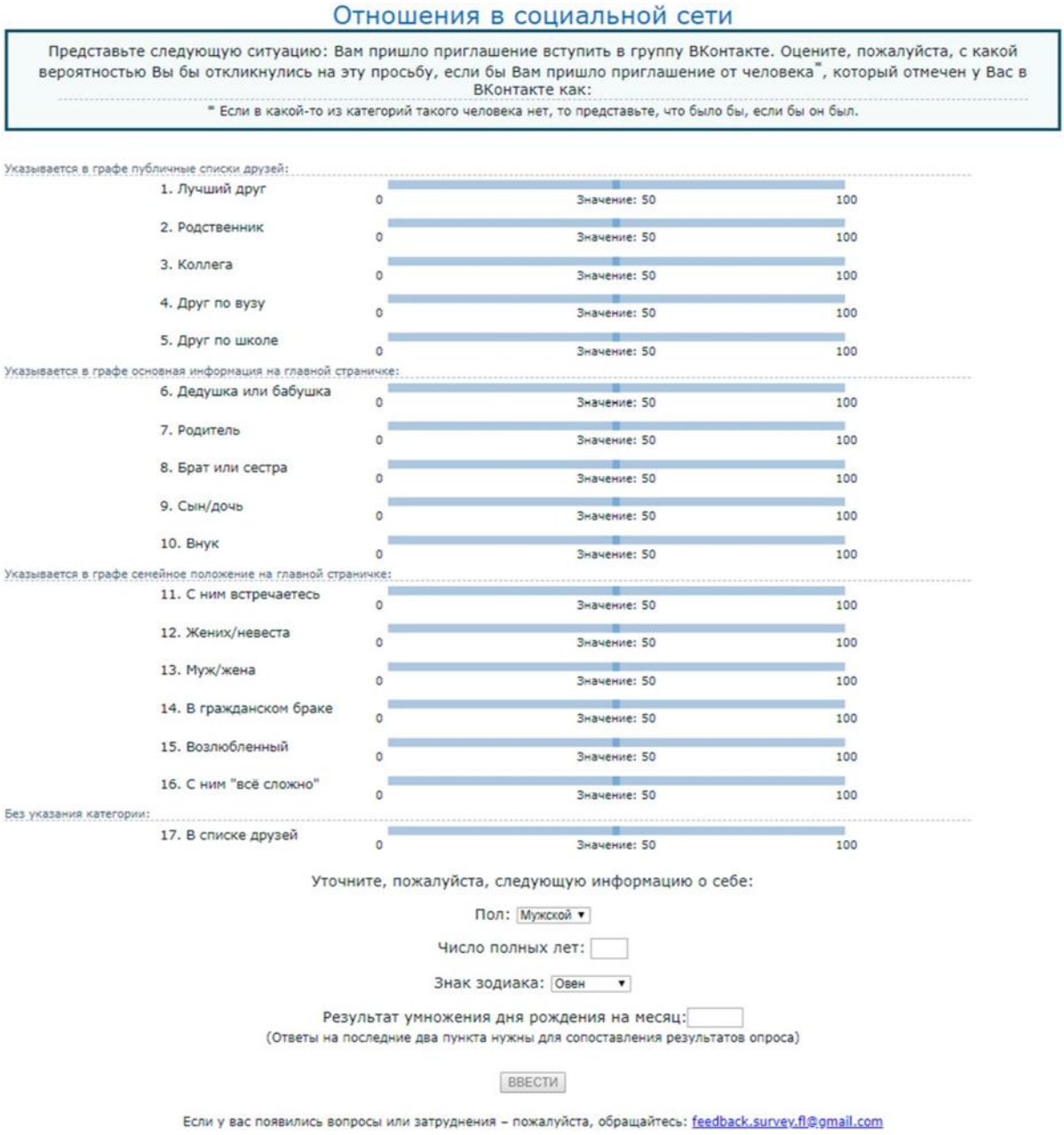

Рисунок 1 – Скриншот web-страницы с опросом

Для автоматизации данного процесса была разработана программа на языке C# с использованием библиотеки Microsoft Excel Object Library. В качестве входных данных программы служит документ Microsoft Excel с результатами опроса. На выходе подаётся также документ Microsoft Excel с добавленными страницами, по одной на каждую подгруппу. Каждая из таких страниц содержит сгенерированный порядок ответов, расшифровку данного порядка и число раз, которое такой порядок встретился в упорядоченных

ответах респондентов по каждой подгруппе. Пример результата работы программы по одной из групп представлен в таблице 1.

Таблица 1 – Пример части обработанных результатов опроса

Порядок	Частот-ность	Расшифровка порядка					
[123456]	24	Прочие родственники	Бабушка или дедушка	Мать или отец	Брат или сестра	Ребёнок	Внук или внучка
[23456]1	7	Бабушка или дедушка	Мать или отец	Брат или сестра	Дочь или сын	Внук или внучка	Прочие родственники
1[23456]	5	Прочие родственники	Бабушка или дедушка	Мать или отец	Брат или сестра	Дочь или сын	Внук или внучка
[1234][56]	3	Прочие родственники	Бабушка или дедушка	Мать или отец	Брат или сестра	Дочь или сын	Внук или внучка
[2356]41	2	Бабушка или дедушка	Мать или отец	Дочь или сын	Внук или внучка	Брат или сестра	Прочие родственники
[61234]5	2	Внук или внучка	Прочие родственники	Бабушка или дедушка	Мать или отец	Брат или сестра	Дочь или сын
1[2364]5	2	Прочие родственники	Бабушка или дедушка	Мать или отец	Внук или внучка	Брат или сестра	Дочь или сын
[12356]4	2	Прочие родственники	Бабушка или дедушка	Мать или отец	Дочь или сын	Внук или внучка	Брат или сестра
1[6234]5	2	Прочие родственники	Внук или внучка	Бабушка или дедушка	Мать или отец	Брат или сестра	Дочь или сын
[41256]3	2	Брат или сестра	Прочие родственники	Бабушка или дедушка	Дочь или сын	Внук или внучка	Мать или отец
231654	1	Бабушка или дедушка	Мать или отец	Прочие родственники	Внук или внучка	Дочь или сын	Брат или сестра

Анализ показал, что более трети пользователей не различают отношения с «друзьями» с точки зрения вероятности отреагировать на ту или иную просьбу. Таких пользователей оказалось 50. Среди этих пользователей для 37 респондентов оказались равнозначными отношения «друзья по вузу»,

«друзья по школе», «коллеги». Для 21 респондента из 50 равнозначны все имеющиеся отношения (рисунок 2). С точки зрения вероятности отреагировать на ту или иную просьбу 51 пользователь указали, что они одинаково отреагируют на просьбу бабушки, брата, дедушки, родителей или сестры. 24 пользователя из 51 указали одни и те же значения для всех родственников (рисунок 3). Никак не различают «друзей» по параметру «семейное положение» 78 респондентов, что составляет более 50% анкетируемых. 39 пользователей из 78 никак не различают отношения по этому параметру (рисунок 4).

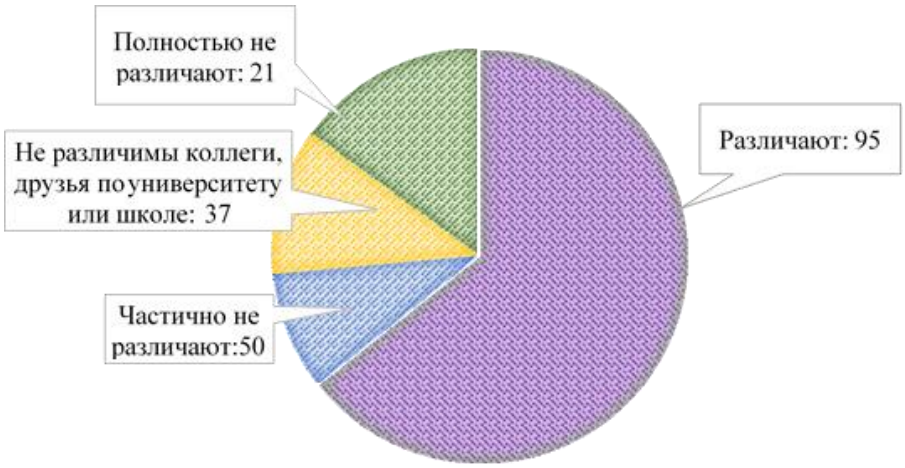

Рисунок 2 – Соотношение результатов опроса в категории «Друзья»

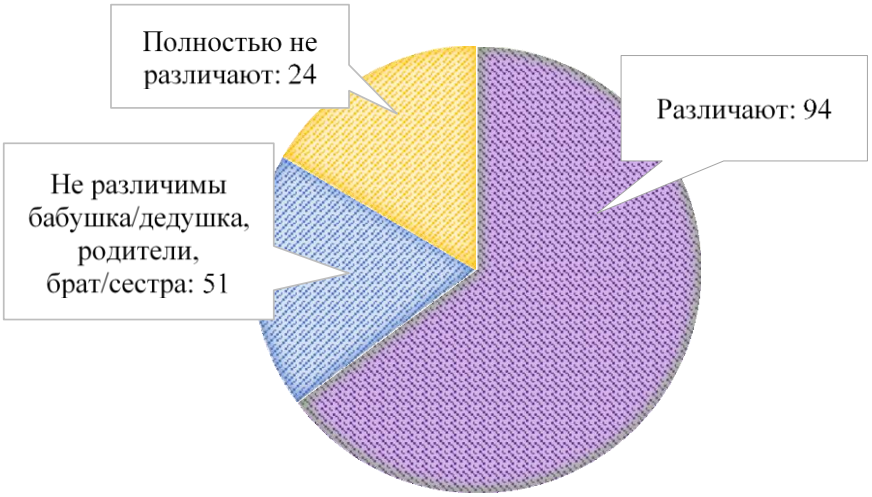

Рисунок 3 – Соотношение результатов опроса в категории «Родственники»

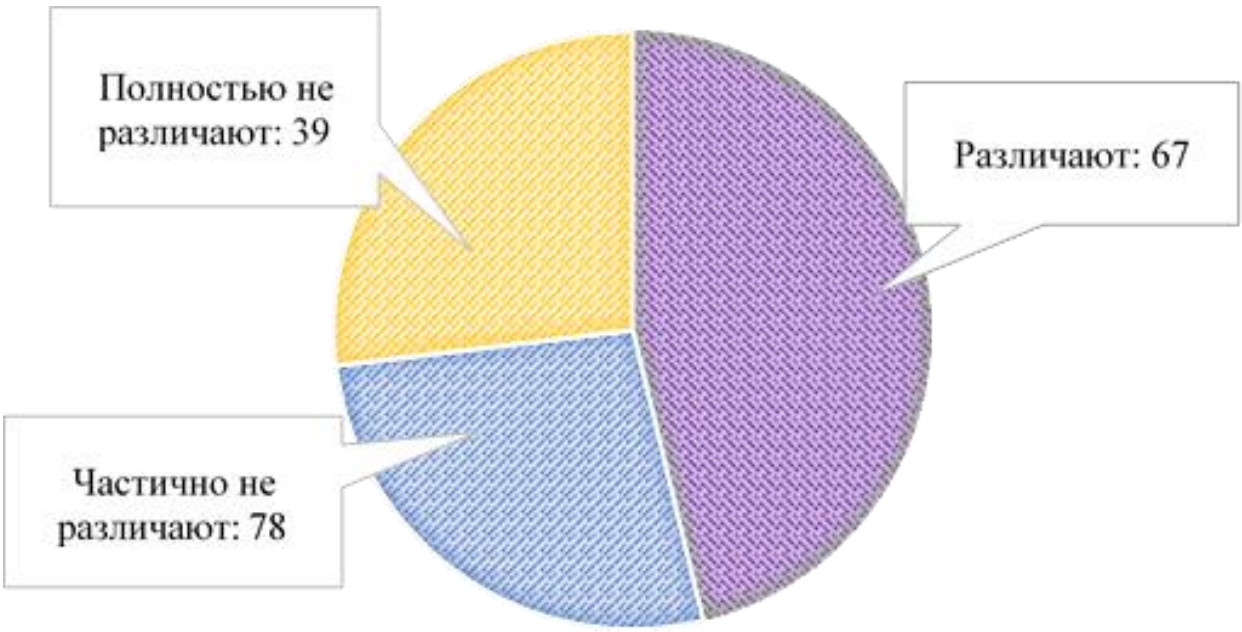

Рисунок 4 – Соотношение результатов опроса по параметру «Семейное положение»

Анализ проведённого анкетирования показал, что вероятность выполнить просьбу одного из «друзей» пользователя отличается для разных классов «друзей», однако для «друзей» одного типа такая вероятность практически не различается.

Вывод, показывающий, что вероятности в рамках одного класса отношений отличаются незначительно, важен, однако при этом необходимо детально рассмотреть ранжирование отношений у некоторых пользователей. В то же время из-за отсутствия репрезентативности выборки нельзя утверждать, что выявлены все допустимые комбинации, так как порядки классов «друзей» по степени готовности выполнить просьбу могут быть самыми разными. Можно также проанализировать полученные результаты по возрасту пользователя. Запланировано ещё одно такое же анкетирование для анализа того, насколько пользователи повторят свои ответы. Чтобы обработать полученные ответы можно применить методологию Хованова [46, 55]. Методология Хованова предоставляет возможность рассмотреть взаимоотношение указанных пользователем порядков. Метод Хованова

предполагает, что определение конкретного значения вероятности выбирается случайным образом, в то время как инструментарий, который разработан Хованов, позволяет пользователям указать порядок отношений. Возможно, что полученные таким образом результаты будут обладать большей устойчивостью по сравнению с числовыми.

В дальнейших исследованиях полученные результаты предоставят возможность определять характеристики моделей формирования оценок развития многоходовых кибератак с использованием методов социальной инженерии.

2.2 Выявление наиболее возможной траектории развития кибератаки между двумя пользователями

Рассмотрим граф $G = (U, E')$, в котором $U = \{User_i\}_{i=1}^{n}$ – множество сотрудников компании, $E = \left\{\left(u_i, u_j, \frac{1}{p_{i,j}}\right)\right\}_{1 \le i,j \le n, i \ne j}$ – множество упорядоченных троек, в которых двум сотрудникам u_i, u_j соответствует оценка возможности распространения кибератаки от сотрудника к сотруднику $\frac{1}{p_{i,j}}$. В соответствии с [38] вероятность успешного распространения многоходовой кибератаки с использованием методов социальной инженерии от сотрудника m к сотруднику l вычисляется по формуле $p_{ml} = p_m \prod_{i=m}^{l-1} p_{i,i+1}$. При этом если $p_{i,j} \ge p_{l,k}$, то $\frac{1}{p_{i,j}} \le \frac{1}{p_{l,k}}$, длина пути может быть рассчитана по формуле $\frac{1}{p_{ml}} = \frac{1}{p_m} \prod_{i=m}^{l-1} \frac{1}{p_{i,i+1}}$, в которой p_{ml} представляет собой вероятностную оценку успешного распространения кибератаки от сотрудника m к сотруднику l, p_m – вероятностная оценка успешной одноходовой кибератаки с использованием методов социальной инженерии на сотрудника, $p_{i,i+1}$ – вероятностная оценка развития кибератаки на сотрудника посредством другого сотрудника. Перейдём от задачи

нахождения пути с наибольшей длиной к задаче нахождения пути с наименьшей длиной.

Для использования методов поиска наикратчайшего пути, требуется выполнить некоторые преобразования. В соответствии с главным алгебраическим тождеством, связанным с логарифмами, $\frac{1}{p_{i,j}} = e^{log\frac{1}{p_{i,j}}}$, длина пути вычисляется по формуле $\frac{1}{p_{ml}} = \frac{1}{p_m}\prod_{i=m}^{l-1}\frac{1}{p_{i,i+1}} = e^{log\frac{1}{p_m}}\prod_{i=m}^{l-1}e^{log\frac{1}{p_{i,i+1}}} = exp\left\{log\frac{1}{p_m} + \sum_{i=m}^{l-1} log\frac{1}{p_{i,i+1}}\right\}$. В связи с тем, что вероятность успешной одноходовой кибератаки с использованием методов социальной инженерии на сотрудника m – p_m – одна и та же для любых траекторий, которые начинаются с сотрудника m, то перейдём к задаче нахождения пути, для которого значение $-\sum_{i=m}^{l-1} log\ p_{i,i+1}$ является наименьшим по сравнению со всеми потенциальными траекториями, которые начинаются от сотрудника m, а заканчиваются сотрудником l, то есть значение $\sum_{i=m}^{l-1} log\ p_{i,i+1}$ является наибольшим. Задача сводится к нахождению минимального пути в орграфе, который не содержит дуги с весом, имеющим значения меньше нуля.

2.3 Обобщение задачи

В связи с тем, что выявление наиболее вероятных траекторий без оценки ущерба от их реализации не даёт необходимой информации для принятия мер по повышению уровня безопасности, в ходе дальнейших исследований возникла проблема нахождения наиболее критичных траекторий атак не с точки зрения вероятности поражения пользователя или документа, а с точки зрения ожидаемого ущерба. Такая характеристика может быть построена на основе анализа возможностей и прав доступа пользователя к документам различной критичности. Отметим, что критичные документы в информационной системе могут иметь разные уровни критичности и, соответственно, их компрометация будет приводить к

различающимся по размеру ущербу. Часто критичные документы подразделяют на типы согласно степени критичности. Таким образом на первом уровне находятся документы с высоким уровнем критичности, а на последнем – с минимальным. Обозначим подходы к распределению прав доступа в информационных системах к критичным документам разных уровней.

Первый подход состоит в следующем. Документы делят на классы в соответствии со степенью их критичности. Каждому сотруднику компании доступны документы только одной степени (рисунок 5). Модели сотрудника компании и документов разной степени критичности можно представить таблицей, аналогичной таблице 2.

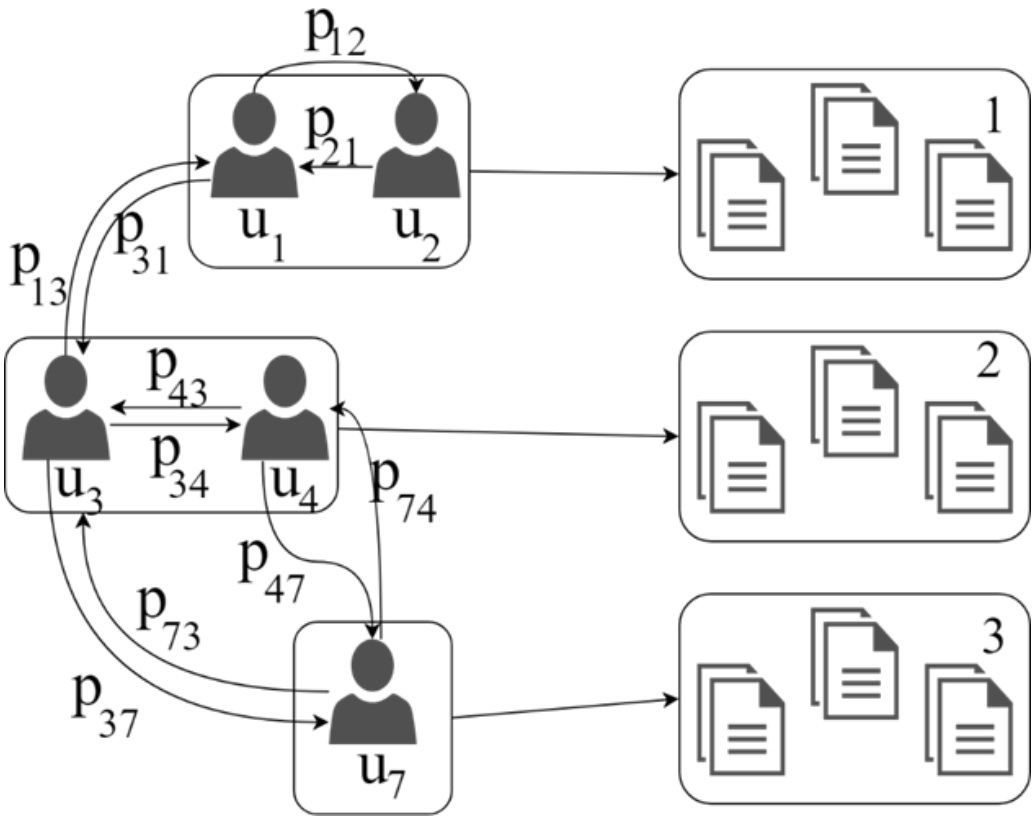

Рисунок 5 – Распределение прав доступа сотрудников компании, при котором каждому сотруднику доступны документы только одной степени критичности

Таблица 2 – Модели документов разной степени критичности и сотрудников компании

№	Наименование	Представление	Комментарий
1	Документ какой-либо степени критичности	documents(id,cl)	Документы имеют идентификатор и степень критичности.
2	Сотрудник компании	users(id,cl)	Сотрудник компании имеет идентификатор, посредством которого сотрудник связывается с остальными характеристиками, и уровень прав доступа к документам.

Но чаще сотрудникам компании доступны не только документы соответствующей степени критичности, но также документы с более низкой степенью критичности (рисунок 6). Если документы распределены по классам в соответствии с их степенью критичности, то сотрудникам компании доступны документы, соответствующие их правам доступа, и документы более низких уровней. Наиболее распространённой является модель, при которой сотрудникам компании доступны не все критичные документы соответствующей степени, а лишь некоторые (рисунок 7). В этом случае критичные документы распределены по степеням, а сотрудникам доступно заданное число документов соответствующей степени.

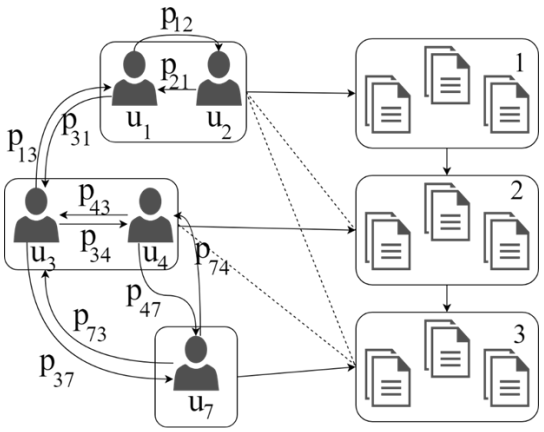

Рисунок 6 – Распределение прав доступа пользователей: каждый пользователь имеет доступ к документам определённого уровня критичности и ко всем документам нижнего уровня

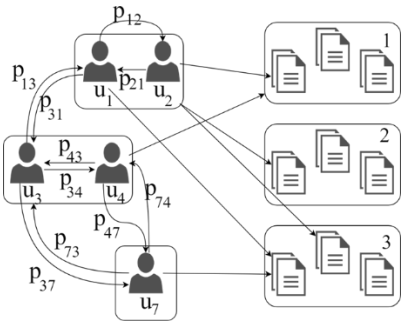

Рисунок 7 – Распределение прав доступа пользователей: каждый пользователь имеет доступ к определённым документам разных уровней критичности

В работе рассматривается проблема определения самой критичной траектории развития кибератаки с использованием методов социальной инженерии в информационной системе, в которой права доступа распределены так, что документы разделены на классы в соответствии с их степенью критичности, и всем сотрудникам компании доступны критичные документам только одной степени критичности.

2.4 Подход к идентификации наиболее критичной траектории

В [39] отмечено, что вероятность распространения кибератаки от сотрудника m к сотруднику l – это (3).

$$p_{ml} = \max_{trajectories}\left(p_m \prod_{i,j} p_{ij}\right), \quad (3)$$

где $trajectories = \left\{\left(User_m, E_{i_1}, \dots, E_{i_k}, User_l\right)\right\}_{i_1,\dots,i_k}$ – множество всех потенциальных траекторий развития многоходовой кибератаки с использованием методов социальной инженерии между соответствующими сотрудниками; p_m – вероятностная оценка успешной одноходовой кибератаки с использованием методов социальной инженерии на сотрудника m; p_{ij} – вероятностная оценка развития кибератаки на сотрудника j посредством сотрудника i.

Как было отмечено выше, выявление наиболее вероятных траекторий без оценки ущерба от их реализации не даёт нам необходимой информации, которая позволила бы принимать превентивные таргетированные меры, способствующие усилению защиты информации в компании. В связи с этим, необходимо перейти от выявления наиболее вероятных траекторий к определению самых значимых траекторий. Самой критичной траекторией будем называть наиболее вероятную траекторию реализации социоинженерной атаки, которая принесёт максимальный ущерб организации. Для оценки критичности траекторий предлагается ввести соответствующую метрику, заданную формулой (4).

$$ct_{ml} = p_{ml} \cdot loss(l, cl), \quad (4)$$

где ct_{ml} – оценка критичности траектории между сотрудниками m и l;

p_{ml} – наибольшая вероятностная оценка распространения кибератаки с использованием методов социальной инженерии между этими сотрудниками;

$loss(l, cl)$ – возможный ущерб компании в случае компрометации критичных документов степени cl, к которым имеет доступ сотрудник l.

Требуется определить траекторию ct: $ct = \max_{User_{m,l} \in U}(ct_{ml})$.

Простейшим вариантом нахождения такой траектории является расчёт и ранжирование всевозможных вариантов значений ct_{ml} для разных m и l. Однако указанный подход является ресурсозатратным. Для снижения ресурсозатратности можно двигаться в сторону сужения области перебора значений оценок вероятностей. Подобным фильтром может выступать задание нижнего порога для оценок вероятностей прохождения траекторий. А также задание порогового уровня критичности документа, убытка при его компрометации, при которых итоговое значение критичности траектории будет минимальным. Для большей наглядности предложенного подхода рассмотрим пример. Пусть дан социальный граф, состоящий из трёх сотрудников компании, с указанными вероятностными оценками развития кибератаки с использованием методов социальной инженерии от сотрудника к сотруднику. Представим, что в информационной системе содержатся три

критичных документа трёх разных уровней критичности. К каждому из таких документов имеет доступ один пользователь. Определим значения для $loss(l, cl)$: $loss(1,1) = 1$, $loss(2,2) = 2$, $loss(3,3) = 3$. Это означает, что критичный документ 1 обладает степенью 1, критичный документ 1 обладает степенью 2, критичный документ 3 обладает степенью 3. Первая степень является минимальной. Третья степень является максимальной. В соответствии с формулой (4) вычислим оценки критичности траекторий между сотрудниками:

$$c_{12} = 0.9 \cdot 0.8 \cdot 2 = 1.44, \quad (5)$$

$$c_{13} = 0.9 \cdot (0.8 \cdot 0.6) \cdot 3 = 1.296, \quad (6)$$

$$c_{21} = 0.67 \cdot 0.9 \cdot 1 = 0.603, \quad (7)$$

$$c_{23} = 0.9 \cdot 0.6 \cdot 3 = 1.62, \quad (8)$$

$$c_{31} = 0.23 \cdot (0.8 \cdot 0.9) \cdot 1 = 0.1656, \quad (9)$$

$$c_{32} = 0.23 \cdot 0.8 \cdot 2 = 0.368. \quad (10)$$

Таким образом, $ct = 1.62$, что соответствует кибератаке на документ третьей степени критичности через третьего сотрудника, который подвергся атаке через второго сотрудника. Для примера были рассмотрены наиболее простые значения функции $loss(l, cl)$, был использован наиболее простой пример компании с тремя пользователями, критичным документами и степенями критичности. Возможно, дальнейшие исследования покажут необходимость изменения принципов задания и распределения уровней критичности документов, данные величины могут быть заданы экспертами и выражены более сложным образом.

Выводы по главе

Были введены метод нахождения наиболее вероятных и метрики оценки критичности траекторий развития многоходовых кибератак с использованием методов социальной инженерии, а также представлены методы квантификации характеристик взаимодействия пользователей.

3 Программная реализация

В данной главе описывается структура программных модулей: «Анализатора критичных траекторий» и «Построения графа».

3.1 Структура программного модуля

Разработанный программный модуль является частью программного комплекса [38, 39], представленного на рисунке 8. Программный комплекс реализует комплексный анализ информационной системы компании на предмет выявления наиболее уязвимых мест к воздействию злоумышленников-социоинженеров. Работа комплекса включает в себя сбор информации из соцсетей, анализ данных о психологических особенностях сотрудников компании, обработку полученной информации, построение на её основе социального графа и его дальнейшего анализа.

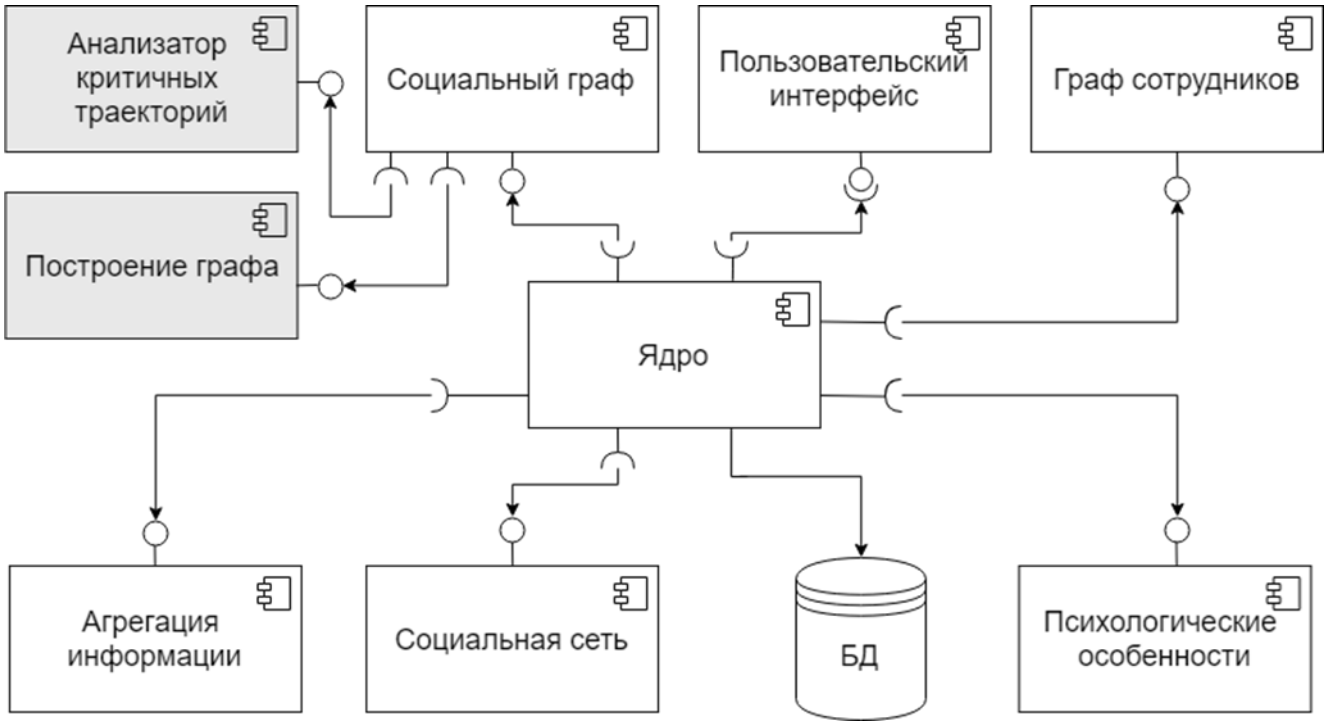

Рисунок 8 – Диаграмма программного комплекса

Разработка программных модулей велась на языке программирования Java в программной среде Intellij Idea 2020. В качестве исходной структуры для исследования была взята структура Social Graph [39], включающая в себя следующие два объекта users и connections. Для связи с разработанными раннее модулями и для предоставления удобного доступа в дальнейшем к разрабатываемым модулям была использована технология Apache Maven.

Разработанный программный модуль «Анализатор критичных траекторий» предназначен для реализации модели поиска наиболее вероятных и критичных траекторий развития кибератак с использованием методов социальной инженерии в социальном графе сотрудников компании. Модуль «Построение графа» осуществляет визуальное построение социального графа сотрудников компании, включая отображение наиболее критичных траекторий распространения, информацию о которых он получает из вышеописанного модуля. Более подробное описание данных модулей приводится в следующих двух параграфах.

3.2 Выявление наиболее вероятной траектории развития многоходовой кибератаки с использованием методов социальной инженерии

Согласно подходу, предложенному в 2.2, поиск наиболее вероятной траектории развития многоходовой кибератаки с использованием методов социальной инженерии сводится к нахождению кратчайшего пути на социальном графе сотрудников компании. С учётом указанных в параграфе 1.5 особенностей оптимальными алгоритмами решения задачи нахождения наиболее возможной траектории развития являются алгоритмы Беллмана-Форда и Дейкстры. Эти алгоритмы предоставляют возможность организовать работу в случае ожидаемых вариантов социальных графов пользователей в компании. Чтобы ускорить выполнение алгоритма, не снижая его точности, введём следующие допущения. Для снижения вычислительной сложности

алгоритма зададим следующий порог. Если вероятностная оценка успеха развития кибератаки с использованием методов социальной инженерии от исходного сотрудника до сотрудника, который рассматривается в настоящий момент, оказывается ниже установленного порогового значения, то этот алгоритм более не рассматривается.

Такой подход использовался в реализации компьютерной программы для определения уровня защиты сотрудников компании от кибератак с использованием методов социальной инженерии. Описание программного модуля для определения уязвимостей пользователей к социально-инженерным атакам и его схема предложены в [39]. Этот программный модуль реализован на основе алгоритма, показанного на рисунке 9.

Описанный подход был реализован в качестве модуля программного комплекса для автоматизированного анализа защищённости пользователей информационных систем от социоинженерных атак, схема и описание которого представлены в [39]. Блок-схема алгоритма, заложенного в реализации данного модуля, представлена на рисунке 9.

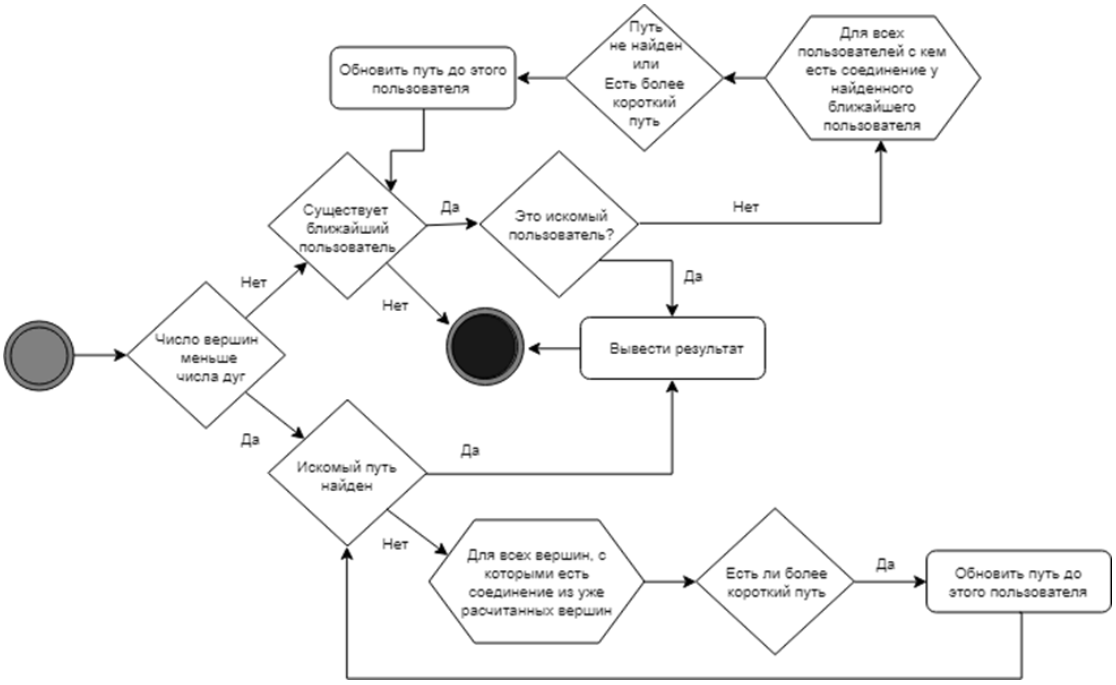

Рисунок 9 – Алгоритм нахождения наиболее возможной траектории развития кибератаки с использованием методов социальной инженерии

Исходными значениями являются идентификаторы двоих сотрудников, между которыми требуется определить самую критичную траекторию развития кибератаки с использованием методов социальной инженерии. Входным параметром также является социальный граф, который формируется одним из модулей программного комплекса для автоматизированного анализа защищённости пользователей информационных систем от социоинженерных атак исходя из информации, которая добывается из данных, опубликованных сотрудниками в соцсети vk.com. Выходным параметром служит самая критичная траектория развития кибератаки с использованием методов социальной инженерии с наибольшей вероятностной оценкой успешного распространения от одного сотрудника ко другому.

Практическая значимость предложенного алгоритма состоит в дополнении функционала имеющейся программы и её дальнейшем применении при проверке безопасности сотрудников компаний при многоходовых социоинженерных атаках.

3.3 Визуализация социального графа сотрудников

Согласно проанализированным данным (таблица 3) для наглядного представления социального графа сотрудников компании была выбрана библиотека GraphStream. Помимо достоинств, указанных в таблице 3, ещё одним из преимуществ её использования является задание стилей графа, имитирующее работу CSS.

На вход модуля по визуализации графа GraphBuilder подаётся социальный граф пользователей, принадлежащий классу SocialGraph. Подробная структура данного класса представлена в [38]. Сам граф может быть задан в программе, загружен из документа Microsoft Excel или получен из других программных модулей. Затем создаётся ориентированный мультиграф, узлы которого соответствуют структуре users, а рёбра –

структуре connections. После чего узлам и рёбрам ставятся в соответствие классы css node и edge с прописанными свойствами элементов. В связи с тем, что социальные графы пользователей обычно имеют большое число вершин и рёбер, была добавлена функция масштабирования графа, причём метки узлов и рёбер появляются только при определённом масштабе приближения. Также было реализовано представление результатов работы модуля по нахождению наиболее вероятного пути: происходит выделение, входящих в него узлов и рёбер более тёмным цветом.

Таблица 3 – Сравнение библиотек для представления социальных графов

Название	Свободный доступ	Наглядность представления	Возможность изображения			Интерак-тивность	Итог
			Больших графов	Орграфов	Взвешенных графов		
JUNG	+	?	?	+	+	–	–
Neo4j	+	+	+	+	+	?	–
Graphviz	+	?	?	+	+	–	–
yFiles	–	+	+	+	+	?	–
Prefuse	+	?	?	+	+	+	–
JGraphT	+	–	–	+	+	–	–
GraphStream	+	+	+	+	+	+	+
JavaFX	+	–	–	+	+	+	–

Таким образом, в ходе работы было реализовано построение социального графа сотрудников на основе данных, выделение узла и рёбер по клику кнопки мыши, масштабирование графа, построение графа с выделением в нём наиболее вероятного пути. Кроме того, было осуществлено ориентированное представление социального графа. На рисунке 10 представлен пример работы программы, входными данными которой являлся документ Microsoft Excel с данными о сотрудниках компании со штатом 250 человек.

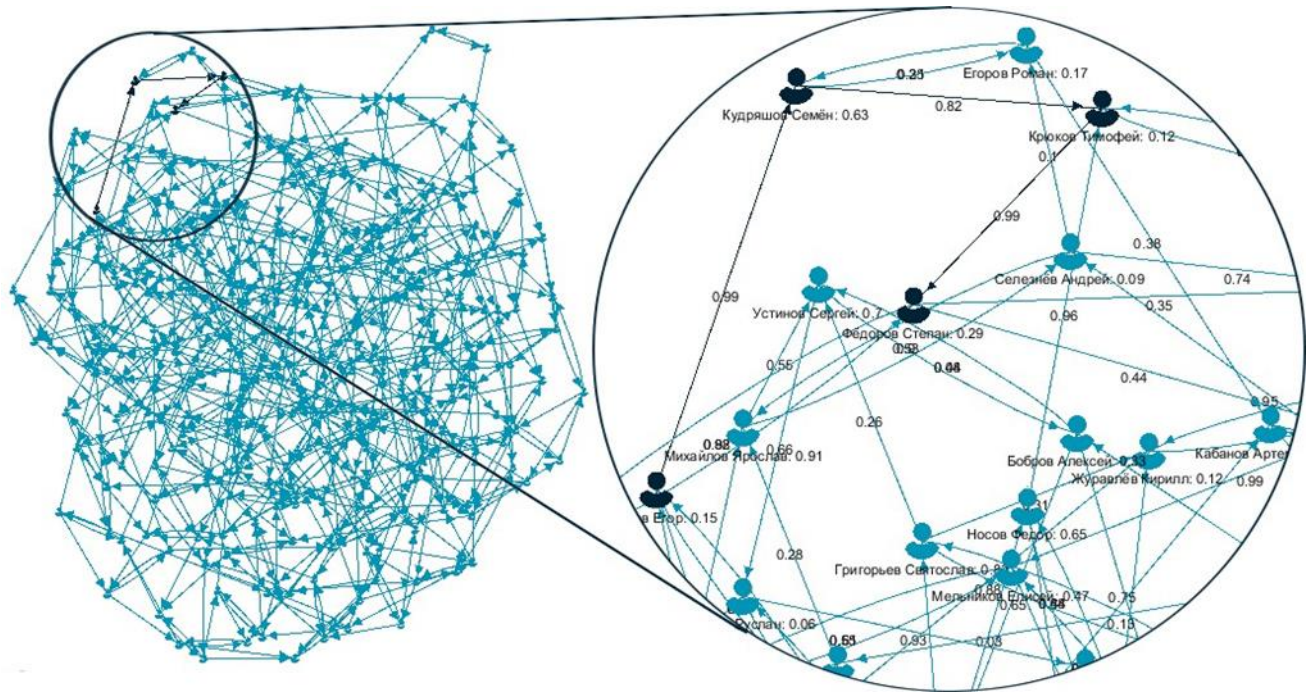

Рисунок 10 – Визуализация тестового графа сотрудников компании со штатом 250 человек

В данном разделе была приведена структура следующих программных модулей: «Анализатора критичных траекторий» и «Построения графа».

Заключение

Выпускная квалификационная работа бакалавра была посвящена разработке автоматизированных инструментов определения самых критичных траекторий развития многоходовых кибератак с использованием методов социальной инженерии и визуализации этих кибератак с помощью социальном графа пользователей. Для реализации этой цели решены нижеперечисленные задачи:

- выбран метод определения наиболее возможных траекторий развития многоходовой кибератаки с использованием методов социальной инженерии;
- предложена метрика для оценки самых критичных траекторий развития многоходовой кибератаки с использованием методов социальной инженерии;
- разработан и реализован алгоритм нахождения наиболее вероятных траекторий развития многоходовых кибератак с использованием методов социальной инженерии;
- предложены методы по изучению силы влияния возможных типов взаимоотношений между пользователями на возможность развития кибератаки с использованием методов социальной инженерии.

Обобщая вышеизложенное, все поставленные задачи были выполнены. Цель работы была успешно достигнута. Практическая значимость работы состоит в увеличении функционала имеющейся программы определения уровня защиты сотрудников компании от кибератак с использованием методов социальной инженерии. Расширенный комплекс может быть рекомендован для использования в компаниях с целью проведения предупреждающей диагностики информационных сетей от социоинженерных атак. Перспективы дальнейшего исследования заключаются в рассмотрении моделей, которые более детально описывают контекст и учитывают распределение вероятностей поражения доли документов, доступных пользователю.

Список используемой литературы

1. Abawajy, J.H. Privacy preserving social network data publication / J.H. Abawajy, M.I.H. Ninggal, T. Herawan // IEEE communications surveys & tutorials. 2016. 18(3). Pp. 1974-1997.

2. Abramov, M.V. Analysis of users' protection from socio-engineering attacks: social graph creation based on information from social network websites / M.V. Abramov, A.L. Tulupyev, A.A Sulejmanov // Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2018. Vol. 18. № 2. Pp. 313-321.

3. Albladi, S.M. User characteristics that influence judgment of social engineering attacks in social networks / S.M. Albladi, G.R.S. Weir // Human-centric Computing and Information Sciences. 2018. 8(1). P. 5.

4. Algarni, A. An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook / A. Algarni, Y. Xu, T. Chan // European Journal of Information Systems. 2017. Vol. 26, № 6. Pp. 661-687.

5. Azarov, A.A. Sotsioinzhenernye ataki: problemy analiza [Social engineering attacks: the problem of analysis] / A.A. Azarov, T.V. Tulupyeva, A.V. Suvorova, A.L. Tulupyev, M.V. Abramov, R.M. Usupov // St Petersburg: Nauka Publ., 2016. 349 p.

6. Bhakta, R. Semantic analysis of dialogs to detect social engineering attacks / R. Bhakta, I.G Harris // Semantic Computing (ICSC), 2015 IEEE International Conference on. – IEEE, 2015. Pp. 424-427.

7. Cai, Z. Collective data-sanitization for preventing sensitive information inference attacks in social networks / Z. Cai, Z. He, X. Guan, Y. Li // IEEE Transactions on Dependable and Secure Computing. 2018. № 15(4). Pp. 577-590.

8. Cao, J. Discovering hidden suspicious accounts in online social networks / J. Cao, Q. Fu, Q. Li, D. Guo // Information Sciences. 2017. № 394. Pp. 123-140.

9. Chiew, K.L. A survey of phishing attacks: their types, vectors and technical approaches / K.L. Chiew, K.S.C. Yong, C.L. Tan // Expert Systems with Applications. 2018.

10. Chin, T. Phishlimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking / T. Chin, K. Xiong, C. Hu // IEEE Access. 2018. Vol. 6. Pp. 42516-42531.

11. Choi, H.S. Analyzing research trends in personal information privacy using topic modeling / H.S. Choi, W.S. Lee, S.Y. Sohn // Computers & Security 67. 2017. Pp. 244–253.

12. Cormen, T.H. Introduction to Algorithms / T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein // Second Edition MIT Press and McGraw-Hill. 2001. Pp. 580-642.

13. Curtis, S.R. Phishing attempts among the dark triad: Patterns of attack and vulnerability / S.R. Curtis, P. Rajivan, D.N. Jones, C. Gonzalez // Computers in Human Behavior. 2018.

14. Dang-Pham, D. Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace / D. Dang-Pham, S. Pittayachawan, V. Bruno // Computers in Human Behavior 67. 2017. Pp. 196-206.

15. Dou, Z. Systematization of Knowledge (SoK): A Systematic Review of Software-Based Web Phishing Detection / Z. Dou, I. Khalil, A. Khreishah, A. Al-Fuqaha, M. Guizani // IEEE Communications Surveys & Tutorials. 2017. Vol. 19. №. 4. Pp. 2797-2819.

16. Edwards, M. Panning for gold: automatically analysing online social engineering attack surfaces / M. Edwards, R. Larson, B. Green, A. Rashid, A. Baron // Computers & Security 69. 2017. Pp. 18-34.

17. Gupta, B.B. Fighting against phishing attacks: state of the art and future challenges / B.B. Gupta, A. Tewari, A.K. Jain, D.P. Agrawal // Neural Computing and Applications. 2017. Vol. 28, № 12. Pp. 3629-3654.

18. Jaafor, O. Multi-layered graph-based model for social engineering vulnerability assessment / O. Jaafor, B. Birregah // Advances in Social Networks Analysis and Mining (ASONAM), IEEE. Springer, Paris. 2015. Pp. 1480-1488.

19. Junger, M. Priming and warnings are not effective to prevent social engineering attacks / M. Junger, L. Montoya, F.J. Overink // Computers in human behavior. 2017. Vol. 66. Pp. 75-87.

20. Kaur, R. A comparative analysis of structural graph metrics to identify anomalies in online social networks / R. Kaur, S. Singh // Computers & Electrical Engineering 57. 2017. Pp. 294-310.

21. Lee, K.C. Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation / K.C. Lee, C.H. Hsieh, L.J. Wei, C.H. Mao, J.H. Dai, Y.T. Kuang // Soft Computing. 2017. №21(11). Pp. 2883-2896.

22. Levitin, A. Introduction to the design & analysis of algorithms / A. Levitin // USA: Addison-Wesley. 2012. Pp. 304-337.

23. Li, H. Self-control, organizational context, and rational choice in Internet abuses at work / H. Li, X.R. Luo, J, Zhang, R. Sarathy // Information & Management. 2018. № 55(3). Pp. 358-367.

24. Melville, P. Content-Boosted Collaborative Filtering for Improved Recommendations / P. Melville, R. Mooney, R. Nagarajan // University of Texas, USA: AAAI-02, Austin, TX, USA, 2002. Pp. 187-192.

25. Öğütçü, G. Analysis of personal information security behavior and awareness / G. Öğütçü, Ö.M. Testik, O. Chouseinoglou // Computers & Security 56. 2016. Pp. 83-93.

26. One Coffee? Your Total Is Some Personal Data [Электронный ресурс] URL: https://nymag.com/intelligencer/2018/08/shiru-cafs-offer-students-free-coffee-for-harvested-data.html (дата обращения: 01.06.2021).

27. Phishing campaign targets developers of Chrome extensions [Электронный ресурс] URL: https://www.zdnet.com/article/phishing-campaign-targets-developers-of-chrome-extensions/ (дата обращения: 01.06.2021).

28. Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks [Электронный ресурс] URL: https://www.proofpoint.com/us/resources/threat-reports/quarterly-threat-analysis (дата обращения: 01.06.2021).

29. Russell, S. Artificial Intelligence: A Modern Approach / S. Russell, P. Norvig // Artificial Intelligence 175. 2011. Pp. 935-937.

30. Shindarev, N. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities / N. Shindarev, G. Bagretsov, M. Abramov, T. Tulupyeva, A. Suvorova // Advances in Intelligent Systems and Computing. Proceedings of the Second International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’17). 2017. Vol. 1. Pp. 441-447.

31. The White Company Series: Operation Shaheen Report [Электронный ресурс] URL: https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf (дата обращения: 01.06.2021).

32. Warwick, A. Social engineering is top hacking method, survey shows / A. Warwick [Электронный ресурс] URL: https://www.computerweekly.com/news/4500272941/Social-engineering-is-top-hacking-method-survey-shows (дата обращения: 01.06.2021).

33. Wikipedia: Социальная инженерия [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/Социальная_инженерия (дата обращения: 01.06.2021).

34. Wikipedia: Социальная сеть [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/Социальная_сеть (дата обращения: 01.06.2021).

35. Yang, Z. VoteTrust: Leveraging friend invitation graph to defend against social network sybils / Z. Yang, J. Xue, X. Yang, X. Wang, Y. Dai, // IEEE Transactions on Dependable and Secure Computing. 2016. № 13(4). Pp. 488-501.

36. Yasin, A. Design and preliminary evaluation of a Cyber Security Requirements Education Game (SREG) / A. Yasin, L. Liu, T. Li, J. Wang, D. Zowghi // Information and Software Technology. 2018. № 95. Pp. 179-200.

37. Zhang, M. Satisfying link perturbation and k-out anonymous in social network privacy protection / M. Zhang, S. Qin, F. Guo // Communication Technology (ICCT), 2017 IEEE 17th International Conference on. – IEEE. IEEE Xplore, Chengdu. 2017. Pp. 1387-1391.

38. Абрамов, М.В. Методы и алгоритмы анализа защищенности пользователей информационных систем от социоинженерных атак: оценка параметров моделей: автореферат диссертации кандидата технических наук / М.В. Абрамов // Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт- Петербург, 2018. С. 148-154.

39. Абрамов, М.В. Социоинженерные атаки: социальные сети и оценки защищенности пользователей / М.В. Абрамов, Т.В. Тулупьева, А.Л. Тулупьев // СПб. ГУАП, 2018. 266 с.

40. Актуальные киберугрозы. I квартал 2018 года [Электронный ресурс] URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-Q1-rus.pdf (дата обращения: 01.06.2021).

41. Атаки на информацию с помощью методов социальной инженерии [Электронный ресурс] URL: http://www.jetinfo.ru/stati/chelovek-cheloveku (дата обращения: 01.06.2021).

42. Бычек, В. Социальная инженерия в интеллектуальной битве «добра» и «зла» / В. Бычек // Защита информации. Инсайд. 2006. № 6. С. 20-27.

43. Деньги с карт россиян киберворы стали снимать новым способом [Электронный ресурс] URL: http://www.amur.info/news/2018/09/05/143017 (дата обращения: 01.06.2021).

44. Каталков, Д. Как социальная инженерия открывает хакеру двери в вашу организацию / Д. Каталков // Positive Research 2018. Сборник исследований по практической безопасности. 2018. С. 26-30.

45. Киберпреступность в домашних тапочках [Электронный ресурс] URL: http://www.enforce.spb.ru/chronicle/publications-of-the-media/7130-aleksej-knorre-vedomosti-extra-jus-kiberprestupnost-v-domashnikh-tapochkakh (дата обращения: 01.06.2021).

46. Колесников, Г.И. Применение метода квантификации нечисловых оценок вероятности для выбора оптимального портфеля ценных бумаг / Г.И. Колесников, Н.В. Хованов, М.С. Юдаева // Вестник Санкт-Петербургского университета. Серия 5. Экономика. 2007. №. 3. С. 58-67.

47. На Avito замечена новая опасная схема развода россиян [Электронный ресурс] URL: https://bloha.ru/news/na-avito-zamechena-novaya-opasnaya-skhema-raz/ (дата обращения: 01.06.2021).

48. Российская Федерация. Законы. Закон Российской Федерации «Об информации, информатизации и защите информации». Федер. закон: в ред. от 10.01.2003 №15-ФЗ. М. Ось-89, 2005. 32 с.

49. Сбербанк: Основной угрозой для клиентов является социальная инженерия [Электронный ресурс] URL: https://www.anti-malware.ru/news/2017-12-07-1447/25019 (дата обращения: 01.06.2021).

50. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Решение Коллегии Гостехкомиссии России №7/02.03.01 г. [Электронный ресурс] URL: https://cadastral-engineer.ru/wp-content/uploads/2015/01/str-k-.pdf (дата обращения: 01.06.2021).

51. Сулейманов, А.А. Автоматизация построения социального графа сотрудников компании на основе публикуемого ими контента в социальных

сетях / А.А. Сулейманов, М.В. Абрамов // Школа-семинар по искусственному интеллекту: сборник научных трудов. Тверь: ТвГТУ. 2018. С. 32-40.

52. Сулейманов, А.А. Оценка вероятности поражения критичного документа при многоходовых социоинженерных атаках / А.А. Сулейманов, М.В. Абрамов, А.Л. Тулупьев // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2018). Санкт-Петербург. Том 1-2. Т. 1. 2018. С. 130-133.

53. ФНС России предупреждает о создании мошеннического сайта-клона [Электронный ресурс] URL: https://www.nalog.ru/rn77/news/activities_fts/7245895/ (дата обращения: 01.06.2021).

54. Хакеры украли у россиян миллионы рублей через лжесайты [Электронный ресурс] URL: https://news.ru/den-gi/hakery-pohitili-u-rossiyan-svyshe-250-mln-rublej-cherez-lzhesajty/?bulk_email_rid=259&contactId=c71d6b02-74c9-4a59-8227-44fe0265622e&bulkEmailRecipientId=94c550cc-95c4-4a5b-be33-4ed062e77878/ (дата обращения: 01.06.2021).

55. Хованов, Н.В. Модели учета неопределённости при построении сводных показателей эффективности деятельности сложных производственных систем / Н.В. Хованов, Ю.В. Федотов // Научные доклады. 2006. № 28R-2006. 37 с.

56. ЦБ ожидает роста активности мошенников, использующих социальную инженерию. [Электронный ресурс] URL: https://ria.ru/economy/20171213/1510861611.html (дата обращения: 01.06.2021).