Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2019 г.

Автоматизированная система обнаружения фишинговых сайтов в сети Интернет

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2019.127.ПЗ ВКР

Руководитель проекта,
Начальник отдела ИБ специального управления ЮУрГУ
_____ И.С. Антясов
_____ 2019 г.

Автор проекта,
студент группы КЭ-454
_____ В.С. Хоробрых
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Хоробрых В.С. Автоматизированная система обнаружения фишинговых сайтов в сети Интернет – Челябинск: ЮУрГУ, КЭ-454, 97 с., 20 ил., 3 табл., 16 ил., библиогр. список – 24 наим., 3 прил.

Выпускная квалификационная работа выполнена с целью создания автоматизированная система обнаружения фишинговых сайтов в сети Интернет.

В выпускной квалификационной работе отражены все возможные способы использования фишинговых сайтов, а также методы борьбы с ними.

В процессе выполнения квалификационной работы были проведены исследования, с какой целью и как создаются фишинговые сайты, исходя из этого, было определено, как искать такие сайты, разработан алгоритм работы системы, а также отличительные черты для определения фишинговых сайтов.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ 7
ВВЕДЕНИЕ 8
1 АНАЛИТИЧЕСКАЯ ЧАСТЬ 10
1.1 Анализ информации, которая может использоваться злоумышленниками для создания сайта 10
1.2 Характерные черты фишингового сайта 11
1.3 Методы борьбы с фишинговыми сайтами 14
1.4 Разработка автоматизированной системы 21
1.5 Выводы по разделу 23
2 ПРАКТИЧЕСКАЯ ЧАСТЬ 24
2.1 Проектирование системы 24
2.1.1 Определение основных функций системы 24
2.1.2 Определение среды разработки и языка программирования 27
2.1.3 Разработка структуры базы данных 31
2.1.4 Разработка алгоритмов работы системы 33
2.2 Критерии для внесения сайта в черный список 41
2.3 Руководство пользователя 42
2.3.1 Инструкция оператора 43
2.3.2 Инструкция администратора черного списка 46
2.3.3 Инструкция администратора 47
2.4 Технические требования 48
2.5 Выводы по разделу 49
ЗАКЛЮЧЕНИЕ 51
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 52
ПРИЛОЖЕНИЕ А 54
ПРИЛОЖЕНИЕ Б 62
ПРИЛОЖЕНИЕ В 96

СОКРАЩЕНИЯ

IT – information technology (пер. информационные технологии).
АС – автоматизированная система
АРМ – автоматизированное рабочее место.
БД – база данных.
ВКР – выпускная квалификационная работа.
ГОСТ – государственный стандарт России.
ЗИ – защита информации.
ИБ – информационная безопасность.
ОС – операционная система.
ПО – программное обеспечение.
СУБД – система управления базами данных.

ВВЕДЕНИЕ

Одним из эффективных и прибыльных способов мошенничества в интернете является фишинг. Слово «фишинг» произошло от английского «fishing», что можно перевести как рыбная ловля. Только в интернете мошенники ловят не рыбу, а, в основном, личные данные пользователей.

Злоумышленники часто подделывают банковские сайты, сайты социальных сетей и сайты известных порталов. Чаще всего охота идет за логинами и паролями (от почты, от сайтов, социальных сетей, сервисов), а также за номерами банковских счетов или кредитных карт. Векторы использования фишинговых ресурсов весьма разнообразны.

Одной из основных информационных угроз, согласно доктрины информационной безопасности, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. №646, являются возрастающие масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, рост числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий [1]. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее. И действительно, фишинг с каждым днем развивается и появляются новые способы обмана.

Система преждевременного выявления фишинговых сайтов поможет повысить информационную безопасность, исключив возможность:

- утечки данных через фишинговые сайты;
- использования бренда организации для получения прибыли;
- распространения вредоносного программного обеспеченья.

Цель ВКР - создание автоматизированной системы обнаружения фишинговых сайтов. Система повысит скорости поиска, сделает анализ сайтов для определения их категории фишинговых более удобным и поможет исключить проверку сайтов не соответствующих запросу. Система также поможет правоохранительным органам своевременно найти и заблокировать ресурс, содержащий противоправную

информацию. Автоматизированная система разрабатывается под нужды Отдела «К» ГУ МВД России по Челябинской области.

Предмет ВКР – создание автоматизированной системы для поиска фишинговых сайтов.

Для реализации поставленной цели необходимо решить следующие задачи:

- определить какую информацию злоумышленники используют для создания сайта;
- определить характерные черты фишингового сайта;
- рассмотреть существующие методы борьбы с фишинговыми сайтами;
- определить, как регулируются сайты на законодательном уровне;
- разработать модульную автоматизированную систему обнаружения фишинговых сайтов с реализованным разграничением прав доступа, возможностью ручного корректирования "черного списка" и формирования отчетов.