1.
Было сказано использовать только научную литературу, а также только научно-опубликованные статьи и журналы. Нами был произведен сбор информации с таких источников, как https://www.phdays.com/. была просмотрена конференция KARMA: атака на клиентские устройства с Wi-Fi. Из этой конференции была выбрана тема данной научной работы. Большинство статей было взято с https://www.elibrary.ru/(https://www.elibrary.ru/item.asp?id=36712221 ;https://www.elibrary.ru/item.asp?id=42765753, https://elibrary.ru/download/elibrary_30719199_38478982.pdf) Из выбранных статей мы сделали «выжимку» всей информации по данной теме. А также мы воспользовались статьей из научного журнала опубликованную специалистами из нашего университета (Варлатая, С. К. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником //Молодой ученый. — 2015. — № 1 (81). — С. 36-37. — URL:). К сожалению пришлось воспользоваться видно роликом с платформы «Ютуб» о том как производить CRACK атаки(https://www.youtube.com/watch?v=Oh4WURZoR98). Но вся информация из ролика не была представлена в отчете и была лишь использована для нашего личного интереса и понимания как происходят такие вредоносные действия
2.

2.1

- Протоколы защиты Wi-Fi сетей
- способы защиты Wi-Fi сетей
- Linux
- Утилиты Linux
- Krack
- Сети открытого типа (OPEN)
- MITM (человек посередине),
- WPA и WPA2 - Wi-Fi Protected Access
- WEP - Wired Equivalent Privacy
- WPS - Wi-Fi Protected Setup/Quick Security Setup
- MAC адрес

2.2

Автор провел научное исследование и получил следующие результаты. Выяснил какие протоколы защиты Wi-Fi сетей актуальны на данный момент. Их особенности, уязвимости и преимущества. Ознакомился с Linux-оидными системами и почему они актуальны. Так же ознакомился с утилитами для работы в этих системах. Рассмотрел одну из самых актуальных и сложно-

предотвратимых хакинг-атак Krack. Добился определенных результатов в данной работе и приобрел ценный опыт.

2.3 с развитием беспроводных технологий, наиболее востребованным способом доступа в глобальную сеть интернет и к локальным вычислительным сетям является технология Wi-Fi. Её использование, начинается с появлением ноутбуков, персональных компьютеров, мобильных устройств и заканчивается «умной» бытовой техникой. Данный вид связи значительно упростил доступ к сети пользователям и открыл возможности, недоступные при использовании проводных видов связи, однако не каждый знает, сколько опасности поджидает каждого пользователя при неграмотной настройки использовании Wi-Fi. Каждому из пользователей Wi-Fi технологий необходимо знать о безопасности своих устройств и обеспечить себя минимальной защитой от вредоносных атак. Следовательно, каждый из них при использовании своего гаджета с какой- либо сетью Wi-Fi должен заблаговременно позаботиться о её безопасности и подлинности. Если это домашняя сеть Wi-Fi или корпоративная необходимо осуществлять смену пароля ежемесячно, чтобы обезопасить себя от определенного вида атак, нацеленных на эту уязвимость. Рекомендуется отключение WPS так как это является одной из самой сильной уязвимости WPA2 протокола домашних сетей. За корпоративными сетями необходим куда больший контроль специалистов из-за подключения большего количества техники, нуждающихся в Wi-Fi подключении. Даже при соблюдении всех этих и других мер безопасностей есть большой шанс подвержению атаки с последующей потери данных. Поэтому специалисты в сфере информационной безопасности пытаются разработать новые протоколы защиты сетей Wi-Fi, которые не будут подвергаться таким атакам, как Krack.

2.4

На основе полученной информации из проведенного исследования автор получил огромный опыт в данной сфере. Была изучена часть уязвимостей, преимуществ и особенностей каждой из вредоносных атак, сказанных выше. Был вызван интерес в продолжении изучения сказанной темы. Был произведен большой сбор информации, в которую входили только научные опубликованные статьи, научные согласованные конференции, а так же документация из научно опубликованных журналов