**УДК 60**

***Погосян Рубик Артакович***
***студент***
***Финансовый университет при Правительстве РФ***
***Россия, г. Москва***
***e-mail: rubenpogosyan.03@mail.ru***

# ХАКЕРСТВО. ОБЩАЯ ИНФОРМАЦИЯ

***Аннотация:*** *Сегодня интернет все больше и больше охватывается разными сферами для упрощения каких-либо работ, но также интернет популярен среди обычного населения, и пользуется в быту. С этой тенденцией возникают новые преступления и пользование интернетом становится менее безопасным.*

*Данная работа включает в себя детальный разбор одного из видов информационных мошенничеств – хакерства. В следующих главах будет представлено что такое хакерство, его история, а также виды с некоторыми подробностями и влияние хакерства на социальную жизнь обычных людей.*

**Ключевые слова:** хакерство, угроза общества, кража денег, взлом данных, интернет мошенники.

***Poghosyan Rubik Artakovich***
***student***
***Financial University under the Government of the Russian Federation***
***Russia, Moscow***

# HACKING. GENERAL INFORMATION

***Abstract:*** *Today, the Internet is more and more covered in various areas to simplify any work, but the Internet is also popular among the general population, and is used in everyday life. With this trend, new crimes are emerging and Internet use is becoming less secure.*

*This work includes a detailed analysis of one of the types of information fraud - hacking. In the following chapters, it will be presented what hacking is, its history, as well as the types with some details and the impact of hacking on the social life of ordinary people.*

**Keywords:** hacking, threat to society, theft of money, hacking of data, Internet scammers.

Пока стоит обратить внимание на то, какие задачи и цели ставятся перед автором этой работы, в чем заключается ее актуальность.

Цель: изучить хакерство как явление в коммуникационных технологиях со всех его сторон, выявить его признаки, и понять методы борьбы с ним.

Актуальность: как уже было отмечено выше, интернет сегодня широко используем в разных точках мира, поэтому хакерство является одной из тем, которые должны быть обсуждены. Данная работа предоставит каждому понять все аспекты, касающиеся хакерству, предложит способы как избегать от небезопасной ситуации.

После поверхностного рассмотрения какой материал будет рассмотрен в данной работе, можно преступить к изучению следующих глав.

Приятного прочтения!

Слово «хакерство», с английского переводится как взломщик (to hack – рубить, удар). Но несмотря на это в русском языке данное слово может быть употреблено в двух контекстах: первый – это случай, когда мы говорим о правильных и объемных знаниях об информатике и компьютерных технологиях, второй – когда мы говорим взломе электронных устройств с целью похищения каких-либо конфиденциальных данных.

Хотя в быту мы очень много слышим такие слова, как «хакер», «хакерство», в основных источниках информационной безопасности, в документах, связанные с ними эти слова не употребляются1.

1 В таких документах используют слова «злоумышленник», «нарушитель», но эти слова более широки, чем «хакер».

Но все же, отметив факт того, что субъектом хакерства является хакер, попробуем дать определение. Хакер – это человек, который пытается взломать систему, для каких- то целей, например, украсть личные данные.

**Общая информация:**

Слово «хакерство», с английского переводится как взломщик (to hack – рубить, удар). Но несмотря на это в русском языке данное слово может быть употреблено в двух контекстах: первый – это случай, когда мы говорим о

правильных и объемных знаниях об информатике и компьютерных технологиях, второй – когда мы говорим взломе электронных устройств с целью похищения каких-либо конфиденциальных данных [2].

Хотя в быту мы очень много слышим такие слова, как «хакер», «хакерство», в основных источниках информационной безопасности, в документах, связанные с ними эти слова не употребляются.

1 В таких документах используют слова «злоумышленник», «нарушитель», но эти слова более широки, чем «хакер».

Но все же, отметив факт того, что субъектом хакерства является хакер, попробуем дать определение. Хакер – это человек, который пытается взломать систему, для каких- то целей, например, украсть личные данные.

**«Хакерская этика»**

Существует книга, в которой зафиксированы принципы хакерской этики. Они представлены в книге «Хакеры: герои компьютерной революции», написанной Стивеном Леви в 1984 [3]. Эти принципы описываются ниже.

1**.** Доступ к компьютерам должен быть неограниченным и полным.

2. Вся информация должна быть бесплатной.

3. Не верь властям - борись за децентрализацию.

4. Ты можешь творить на компьютере искусство и красоту.

5. Компьютеры могут изменить твою жизнь к лучшему.

**Классификация:**

Учитывая стандарты определения потенциальных нарушителей информационной безопасности, можно составить классификацию, определяющую уровень мастерства того или иного хакера.

Выделяется следующая классификация:

1. «Ламер» - человек слабо и образно представляющий себе взлом как таковой.

2. «Продвинутый ламер» - он интересуется взломом, системами безопасности и хочет овладеть искусством преодоления систем защит, но фактически его знания малы.

3. «Хакер-новичок» - старается себя совершенствовать, уже может сделать преодолеть примитивные механизмы защиты.

4. «Хакер-любитель» - достаточно опытный и хорошо представляющий технологии взлома и защиты человек.

5. «Хакер» - профессионал.

Также самих хакеров выделяют по специализации: кардер, фрикер, дефейсер, взломщик сайтов и программного обеспечения и т.д. Профессионал должен прекрасно разбираться во всех областях.

Выделяют по отношению к вопросам этики и такую классификацию [3]:

1. Романтики-одиночки. Они, как правило, взламывают базы данных из чистого любопытства. В целом они довольно безопасны и бескорыстны, но и наиболее талантливы.

2. Прагматики или классики. Работают как в одиночку, так и группами. Похищают, как говорится, что придется: базы данных, программы, электронные версии разных изданий.

3. Разведчики. Сегодня в любой уважающей себя фирме имеется хакер, оформленный обычно как программист. Его задача – взламывать сети конкурентов и похищать оттуда самую разную информацию. Этот тип пользуется сейчас наибольшим спросом.

4. Кибергангстеры. Это уже профессиональные компьютерные преступники. Их пока не так много, и работают они в основном на преступные организации и группировки. Действуют почти всегда группами. Тут задачи конкретные: блокировка и развал работы компьютерных сетей разных неугодных фирм, а также кража денег с банковских счетов. Дело это дорогое и небезопасное, зато самое высокооплачиваемое. В частности, не так давно группа российских хакеров взломала сеть солидного европейского банка и, запустив туда вирус, на сутки полностью дезорганизовала его работу [4].

**Глава 2. История**

Хакерство появилось почти сразу же после изобретения первого компьютера. В следующих подглавах будет представлена краткая история хакерства, от ее истоков до сегодняшнего дня.

**Зарождение [1]**

В самом начале хакеры были не взломщиками систем, а обычными шутниками. Все берет свое начало в Массачусетском Технологическом Университете, где выпускники вешали на купол здания какой-то большой предмет. Такие шутки студенты называли «хаками», откуда и пошло слово, которое имеет место в сегодняшней компьютерной лексике.

Таким образом, можно считать, что первоисточником хакерства является Массачусетский Технологический Университет, находящийся в США, студенты которого в скором будущем переведут свои забавные шутки на виртуальный уровень.

**Телефонные фрикеры – 1970 год**

Читатели задаются вопросом, кто такие фрикеры? Фрикер – это телефонный хакер, который взламывает сети с целью обеспечить бесплатный региональный или даже международный звонок.

Первым фрикером стал Джон Дрейпер. Вот его история: Джон заметил, что частота самого обычного игрушечного свистка составляет 2600 Гц, удивительно то, что такой же характеристикой обладал коммутирующая система AT&T. Дрейпер создал устройство, способное совершить бесплатные звонки по всему миру (использовав при этом свисток и телефонный аппарат). Вскоре в разных журналах стали печататься статьи об изобретении такого механизма. И число фрикеров стало увеличиваться. Фрикерами также были будущие основатели Apple, Стив Джобс и Стив Возняк.

**Глава 2: История**

Хакерство появилось почти сразу же после изобретения первого компьютера. В следующих подглавах будет представлена краткая история хакерства, от ее истоков до сегодняшнего дня.

**Зарождение**

В самом начале хакеры были не взломщиками систем, а обычными шутниками. Все берет свое начало в Массачусетском Технологическом Университете, где выпускники вешали на купол здания какой-то большой предмет. Такие шутки студенты называли «хаками», откуда и пошло слово, которое имеет место в сегодняшней компьютерной лексике.

Таким образом, можно считать, что первоисточником хакерства является Массачусетский Технологический Университет, находящийся в США, студенты которого в скором будущем переведут свои забавные шутки на виртуальный уровень.

**Телефонные фрикеры – 1970 год**

Читатели задаются вопросом, кто такие фрикеры? Фрикер – это телефонный хакер, который взламывает сети с целью обеспечить бесплатный региональный или даже международный звонок.

Первым фрикером стал Джон Дрейпер. Вот его история: Джон заметил, что частота самого обычного игрушечного свистка составляет 2600 Гц, удивительно то, что такой же характеристикой обладал коммутирующая система AT&T. Дрейпер создал устройство, способное совершить бесплатные звонки по всему миру (использовав при этом свисток и телефонный аппарат). Вскоре в разных журналах стали печататься статьи об изобретении такого механизма. И число фрикеров стало увеличиваться. Фрикерами также были будущие основатели Apple, Стив Джобс и Стив Возняк.

**Хакерские объединения:**

Со смещением фрикеров в область компьютерной техники, начали появляться электронные доски (например, sherwood forest), которые были предшественниками электронных почт, и новостных архивов. Это подрожало появлению групп хакеров, которые стали обмениваться друг с другом ценной информацией, личными данными, т.е. паролями, номерами карт и т.д. Такими группами были «Legion of Doom» в США и «Chaos Computer Club» в Германии.

Впервые общество знакомится с хакерами из фильма «военные игры», где главный герой, пытаясь взломать систему видеоигр, проникает в военный

компьютер, имитирующий ядерную войну. Именно тогда появляется первое представление о хакерах-кибергероях.

К одной из сенсаций в компьютерных технологиях относится факт того, что несколько подростков сумели взломать 60 компьютеров в течение одной недели. Вслед за этим публикаторы начинают издавать различные книги и журналы, описывающие действия самых различных хакерств.

**Червь Морриса**

Особого внимания заслуживает так называемая «червь» Морриса. Компьютерная угроза, создателем которого был Роберт Моррис, начала действовать в 1988 году. В ходе своих действий, червь смог поразить 6000 систем, затронув при этом важные документы федеральных и университетских систем. Запустив в сеть arpanet (автоматическая рассылка копий систем по электронным каналам), Моррис хотел посмотреть какое воздействие окажет эта программа на системы под управлением ОС unix. В итоге он был приговорен к 3 годам заключения, а также штрафу – 10 тыс. долларов.

**Глобальная сеть интернет:**

Использование интернета во всем мире началось с появления нового браузера Netscape Navigator, который многократно упростил доступ к получению информации. Было понятно, что хакеры перейдут в новую область, что и случилось.

Кевин Митник, серийный взломщик, был арестован агентами американских спецслужб, после чего был обвинен в хищении 20 тыс. кредитных карт в 1995 году. Он отсидел 4 года, но приобрел известность в кругах хакеров.

Дело касается и российских хакеров, которые украли из банка 10млн. долларов и перевели деньги на счета в другие страны. Группу возглавлял Владимир Левин.

**Глава 3. Уголовная ответственность [5]**

**Законодательная база:**

В России в сфере компьютерной информации была введена уголовная ответственность в 1997 году, которая регулируется Уголовным кодексом

Российской Федерации. Статьи 272, 273, 274 в 28-ой главе предусматривают ответственность за преступления в сфере компьютерной информации.

Получение информации коммерческого характера, перехват финансовых транзакций, добывание конфиденциальных сведений о людях при отсутствии прав на подобную деятельность – называется несанкционированным доступом к компьютерной информации и является признаком состава преступления, предусмотренного статьей 272. Ответственность по данной статье: штраф от 200 до 500 минимальных размеров оплат труда или лишение свободы на срок до двух лет (до 5 лет при сговоре).

Статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ» направлена против создателей всевозможных вирусов, троянских коней и логических бомб3.

Статья 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» также носит важный характер. (Уголовный Кодекс Российской Федерации, 1997).

**Прецедент**

Одним из нарушителей был житель Красноярска. Дело состоялось в 2003 году. Все началось с того, что гражданин 2 года тому назад получил данные о логине и пароле, которые принадлежали красноярскому железнодорожному страховому обществ. В этом же периоде в августе мужчина с помощью пароля и логина, и подключенному роутеру и телефона проводил действия в сети.

Вина была доказана. Однако, уроженец северного района добился смягчения обстоятельств и был признан нарушителем лишь статьи 165 УК РФ «Причинение имущественного ущерба обманным путем». Он был приговорен к исправительным работам и удержанию 5% от заработной платы.

**Методы борьбы**

В данной главе представлен список самых распространенных и минимальных мер, предпринимаемых для защиты лиц от хакерства. Для удобства ниже это будет представлено в виде списка:

• Обратить внимание на настройки роутера и сервера

• Использовать сильное шифрование

• Использовать защищенные протоколы передачи данных

• Устанавливать плагины для браузеров

• Избегать доступа через публичных wi-fi

• Использование Антивируса

• Умение пользоваться при нужде VPN, менеджерами паролей, отслеживать трафик

**Заключение**

В конце своей работы, автор хочет поблагодарить всем читателям за предоставленное внимание и большой интерес к очень важной проблеме современного мира. В заключение, автор научной работы хочет подвести итоги.

Итак, в работе были рассмотрены ключевые понятия, связанные с хакерством, был проведен анализ его истории и развития, были рассмотрены некоторые подробности на международном сфере, также был разбор хакерства в России. Кроме того, в качестве самого главного были указаны методы борьбы с хакерством.

Автор надеется, что данная работа была полезной и информативной для читателей.

**Список литературы:**

1. Блоги экспертов и ИТ-компаний. [Электронный ресурс] // Режим доступа: URL: https://club.cnews.ru/ (дата обращения: 30.10.2020 г.).

2. История Хакерства // Computer world. 2001. № 29. [Электронный ресурс] // Режим доступа: URL: https://www.osp.ru/cw/2001/28-29/42777 (дата обращения: 30.10.2020 г.)

3. Леви С. Хакеры: герои компьютерной революции. Penguin USA, 2001. 330 с.

4. Смыслова О. Психологические последствия применения информационных технологий. [Электронный ресурс] // Режим доступа: URL: https://www.studsell.com/view/137610/ (дата обращения: 30.10.2020 г.).

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 31.07.2020) // Справочно-правовая система «Консультант-Плюс».