**ИССЛЕДОВАТЕЛЬСКИЙ ПРОЕКТ**

**На тему «Исследование сети «DarkNet»**

Работу выполнил:

студент группы 651

Габдинов Равиль

Руководитель: Ножкин Е.Н.

г. Балаково 2020 г

**СОДЕРЖАНИЕ**

[1 ОСНОВНАЯ ЧАСТЬ 4](#_Toc4662154)

[1.1 История появление сети «DarkNet» 4](#_Toc4662155)

[1.2. Основные понятия и программное обеспечение сети «DarkNet» 5](#_Toc4662156)

[1.3. Программное обеспечение(VPN) 6](#_Toc4662157)

[1.3.1. Уровни реализации 6](#_Toc4662158)

[1.3.2. Структура VPN 7](#_Toc4662159)

[1.3.3. Классификация VPN 7](#_Toc4662160)

[1.4. «Три уровня интернета» 10](#_Toc4662161)

[1.5. Услуги предоставляемые в «DarkNet» 12](#_Toc4662162)

[1.6. Сайты «DarkNet» 13](#_Toc4662163)

[1.7. Влияния «DarkNet» 14](#_Toc4662164)

[2 ОХРАНА ТРУДА И БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ 16](#_Toc4662165)

[ЗАКЛЮЧЕНИЕ 25](#_Toc4662166)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 26](#_Toc4662167)

[РЕСУРСЫ УДАЛЕННОГО ДОСТУПА 27](#_Toc4662168)

**ВВЕДЕНИЕ**

Термином «Тёмная паутина» обозначают совокупность веб-сайтов, видимых публично, при этом имеющих скрытый IP-адрес сервера, на котором они размещаются. Такие сайты могут посещать все веб-пользователи, но выяснить, кто является их автором, очень сложно. В то же время, на подобные сайты невозможно попасть, используя популярные поисковые системы.

Практически все сайты, находящиеся в «DarkNet», скрывают свою принадлежность, используя инструмент шифрования Tor. Инструмент шифрования Tor позволяет пользователям сохранять свою анонимность в Интернете при посещении сайтов, ведении блогов, отправке сообщений и т.п.

Tor позволяет скрыть личность и «подменить» местоположение. В случае, когда в управлении сети Tor находится веб-сайт, эффект наблюдается тот же, что и в ситуации с конечным пользователем. Для того, чтобы посетить сайт в «DarkNet», который использует инструмент шифрования Tor, веб-пользователь должен также использовать Tor.

Большинство людей использует инструмент шифрования Tor, как торговую площадку. Именно в Tor можно купить практически всё, при этом покупатель и продавец остаются анонимны. Для оплаты обычно используют криптовалюту, так как она не имеет никаких данных о владельце.

Цель работы: исследование сети «DarkNet»

Задачи:

1. Ознакомить с историей появление сети «DarkNet»
2. Рассказать основные понятия и программное обеспечение сети «DarkNet»
3. Объяснить что такое «Три уровня интернета»
4. Привести примеры услуг предоставляемые в «DarkNet»
5. Сайты «DarkNet»
6. Влияния «DarkNet»
7. **ОСНОВНАЯ ЧАСТЬ**

## История появление сети «DarkNet»

Термин «DarkNet» появился в 1970-х годах и в целях безопасности использовался для обозначения сетей, изолированных от «ARPANET», которая впоследствии эволюционировала в Интернет. «DarkNet»[[1]](#footnote-1) мог получать данные от «ARPANET», но имели такие адреса, которые не появлялись в списках сетей и не отвечали на запросы извне.

«ARPANET» или «Advanced Research Projects Agency Network» - это сеть, созданная в 1969 году Агенством Министерства Обороны США.

Термин «DarkNet» получил широкое распространение благодаря публикации «The Darknet and the Future of Content Distribution», с англ. — «Темная сеть и будущее распространения информации», работе 2002 года, за авторством Питера Биддла, Пола Инглэнда, Маркуса Пейнаду и Брайана Уиллмана, сотрудников компании Microsoft.[[2]](#footnote-2)

По их мнению, идея «DarkNet» основана на трёх предположениях:

1. Любой объект, предназначенный для широкого распространения, будет доступен определённой части пользователей с разрешением на копирование.
2. Пользователи будут копировать объекты, если это возможно и если они этого захотят.
3. Пользователи соединены каналами с высокой пропускной способностью.

DarkNet - это файлообменная сеть, которая возникает при появлении общедоступных данных, согласно предположению 1, и при распространении этих данных, согласно предположениям 2 и 3.

Исследователи Microsoft утверждают, что существование «DarkNet» было основной помехой для разработки работоспособных DRM технологий.

«DarkNet» может быть использован в определённых случаях, таких как:

1. Неприкосновенность частной жизни и страх политических репрессий
2. Преступления в сфере информационных технологий
3. Распространение файлов, защищённых авторскими правами
	1. **Основные понятия и программное обеспечение сети «DarkNet»**

«DarkNet»– скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. Анонимная «сеть» не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

«DarkNet» отличается от других распределённых одноранговых сетей, так как файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства.[[3]](#footnote-3)

Для получение доступа к «Darknet» необходимо скачать Tor-браузер ([рис.1](https://9net.ru/191-darknet-kak-voyti.html)) с официального сайта. При первом входе необходимо выбрать из двух параметров: просто соединиться или настроить сетевые параметры. Если требуется использовать браузер для того чтобы получить доступ к заблокированному сайту, то необходимо нажать на кнопку «соединиться». Если нужна анонимность, то нужен вариант «настроить». Tor работает так же как и обычные браузеры, но по более сложной схеме, что негативно влияет на скорости загрузки страниц.



Рисунок 1 - Схема работы Tor-браузера.

Соединение состоит из слоёв - цепочки прокси. Информация проходит через 3 случайно выбранных узла сети. На стороне клиента перед отправкой пакета происходит последовательное шифрование для каждого из узлов.

## Программное обеспечение(VPN)

VPN - обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети. Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия, уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии.

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.[[4]](#footnote-4)

### Уровни реализации

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы.

Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети - PPTP, причём используемую зачастую не для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол — IP (такой способ использует реализация PPTP - Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия).

Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» на постсоветском пространстве для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в Сети

### Структура VPN

VPN состоит из двух частей: «внутренняя» сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение.

Возможно также подключение к виртуальной сети отдельного компьютера.

Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов удалённый пользователь наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

### Классификация VPN



Рисунок 2 - Классификация VPN.

Классифицировать решения VPN [рис.2](http://www.gpedia.com/ru/gpedia/%D0%A4%D0%B0%D0%B9%D0%BB%3A%D0%9A%D0%BB%D0%B0%D1%81%D1%81%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_VPN.jpg) можно по нескольким основным параметрам:

1. По степени защищенности используемой среды
* Защищённые

Наиболее распространённый вариант виртуальных частных сетей. С его помощью возможно создать надежную и защищенную сеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

* Доверительные

Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Проблемы безопасности становятся неактуальными. Примерами подобных решений VPN являются: Multi-protocol label switching (MPLS) и L2TP (Layer 2 Tunnelling Protocol) (точнее будет сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec).

1. По способу реализации[[5]](#footnote-5)
* В виде специального программно-аппаратного обеспечения

Реализация сети VPN осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

* В виде программного решения

Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

* Интегрированное решение

Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

1. По назначению
* Intranet VPN

Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.

* Remote Access VPN

Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет-киоска.

* Extranet VPN

Используют для сетей, к которым подключаются «внешние» пользователи. Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

* Internet VPN

Используется для предоставления доступа к интернету провайдерами, обычно если по одному физическому каналу подключаются несколько пользователей. Протокол PPPoE стал стандартом в ADSL-подключениях.

L2TP был широко распространён в середине 2000-х годов в домовых сетях: в те времена внутрисетевой трафик не оплачивался, а внешний стоил дорого. Это давало возможность контролировать расходы: когда VPN-соединение выключено, пользователь ничего не платит. В настоящее время проводной интернет дешёвый или безлимитный, а на стороне пользователя зачастую есть маршрутизатор, на котором включать-выключать интернет не так удобно, как на компьютере. Поэтому L2TP-доступ отходит в прошлое.

* Client/Server VPN

Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика используется его шифрование.

1. По типу протокола

Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство решений VPN поддерживает именно его. Адресация в нём чаще всего выбирается в соответствии со стандартом RFC5735, из диапазона Приватных сетей TCP/IP.

1. По уровню сетевого протокола

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

##  «Три уровня интернета»

Clearnet или Surface Web- это часть Всемирной паутины, находящаяся в открытом лёгком доступе для широкой публики и индексируемая поисковыми системами. Страницы из этой сети свободно можно найти при поисковом запросе. Она является полной противоположностью Глубинной сети (DeepWeb)[[6]](#footnote-6). Веб-страница Surface Web состоит только из 10 процентов информации, которая находится в Интернете. Surface Web создается с помощью набора статических страниц. Это веб-страницы, которые находятся на сервере, доступные для доступа любой поисковой системой.

Согласно источнику internetlivestats.com, по состоянию на 28 февраля 2019 года индекс веб-сайта Google содержит около 1,757,266,207 Страниц.

Глубокая сеть или Deep Web — множество веб-страниц Всемирной паутины, не индексируемых поисковыми системами. Наиболее значительной частью глубокой паутины является Глубинный веб состоящий из веб-страниц, динамически генерируемых по запросам к онлайн-базам данных.[[7]](#footnote-7)

Не следует смешивать понятие «DeepWeb» с понятием «DarkNet», под которым имеются в виду сетевые сегменты, хотя и подключённые к общей сети Интернет, но требующие для доступа определённые программные средства.

«Темная сеть» или «DarkNet» – скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. Анонимная «сеть» не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

«DarkNet» отличается от других распределённых одноранговых сетей, так как файлообмен происходит анонимно, поскольку IP-адреса недоступны публично, и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства.

Именно поэтому «DarkNet» часто воспринимается как инструмент для осуществления коммуникации в незаконной деятельности. В более общем смысле термин «DarkNet» может быть использован для описания некоммерческих «узлов» интернета или относиться ко всем «подпольным» интернет-коммуникациям и технологиям, которые в большинстве своём связаны с незаконной деятельностью или инакомыслием.

Из трёх известных уровней интернета, «DarkNet», он же «теневая сеть» условно располагается на самом нижнем (третьем) уровне после видимой и глубокой сетей. Хотя он и расположен на самом нижнем уровне, его можно считать также частью или «дном» глубокой сети.



Рисунок 3 - DarkNet на примере айсберга и глубины океана.

По другой теории «DarkNet» [рис.3](http://www.prisedeconscience.org/campagne-de-dons-linternet-cache-darkweb-lassassinat-president-trump/) и глубокий интернет вовсе не пересекаются между собой. Они являются двумя из четырёх ответвлений глобального интернета. Данная схема рассматривается не как слои всемирной паутины, а как четыре ветки, подключенные к интернету.

## Услуги предоставляемые в «DarkNet»[[8]](#footnote-8)

«DarkNet» можно использовать во всех страх мира кроме Северной Кореи, где для доступа к компьютеру с интернетом нужно специально разрешение. Даже у Китая не получилось запретить его. «Золотой щит» автоматически блокирует все новые адреса входных узлов Tor, но люди, которым надо, обходят эту преграду c помощью VPN и прокси-серверов.

1. Площадки для торговли наркотиками
2. Сайты с объявлениями о трудоустройстве
3. Магазины товаров для совершения преступлений
4. «Хакерские» торговые площадки и форумы

В «DarkNet» есть раздел Digital Goods, в котором можно купить трояны, средства для взлома Wi-Fi, средства для взлома программ, инструменты для DDOS-атак и множество других разновидностей «средств для незаконного доступа к цифровой информации».

Также в «DarkNet» есть множество хакерских форумов. Там люди делятся между собой опытом, ищут исполнителей и сообщников для различных кибер-преступлений.

 «Черные» биржи криптовалюты

Описанные выше сайты и организации совершают финансовые расчеты в биткоинах. И естественно, не платят с этого никаких налогов. С помощью криптовалют обналичиваются деньги, полученные незаконным путем.

В Tor есть биржи для вывода биткоинов на обычные электронные кошельки или банковские карты. Также там полно объявлений людей, которые выводят деньги с криптовалютных кошельков на офшорный счета или переводят на счет «фирмы-однодневки». [[9]](#footnote-9)

Там же можно заказать банковские карты, оформленные на подставных лиц или «виртуалов». И нанять дропов, которые будут ходить к банкомату, светить свое лицо перед камерами, снимать с карт наличность и доставлять вам.

## Сайты «DarkNet»

Сайты в сети Tor располагаются в доменной зоне **«.onion»** Ссылки на Тор сайты можно найти на странице godnotaba.xyz.

Годнотаба— это открытый мониторинг сайтов в сети TOR. На данном ресурсе можно посмотреть функционирующие сайты, а так же прочитать отзывы о любом из них.

Пример ресурсов:

1. not Evil - поисковик по сети Tor
2. TORCH - еще один поисковик
3. Флибуста - книжная библиотека
4. Hidden Answers - сервис анонимных вопросов и ответов
5. rutrackerripnext.onion - Зеркало rutracker.org
6. rutorc6mqdinc4cz.onion - Зеркало rutor.info
	1. **Влияния «DarkNet»**

«DarkNet**»** позиционируется как механизм защиты прав в Интернете, средство борьбы с интернет-цензурой. Браузер, совершенно бесплатно предлагающий надёжнейший механизм анонимности в сети. Его для передачи информации используют журналисты, известные люди, борцы с коррупцией, правительственные сотрудники, а также прочие пользователи, опасающееся слежки и изъятия информации. А жители тоталитарных государств могут иметь связь с внешним миром, в частности, с демократическими странами.[[10]](#footnote-10)

Известно, что Tor запрещён в некоторых странах, в том числе и в России. И причина этому – игнорирование создателями браузера интернет-цензуры. В РФ за нарушение этого запрета предполагается блокировка публичных серверов Tor. Санкций для обычных пользователей пока что не предусмотрено.

Система Tor построена по принципу передачи зашифрованной информации через несколько прокси-серверов. IP-адрес последнего прокси могут вычислить спецслужбы. И так уже было в ряде стран, в том числе в России. Примером служит тот факт, что в апреле 2017 года был арестован россиянин Юрий Богатов за якобы публикацию в Интернете призывов к терроризму и организацию массовых беспорядков. Защитником были представлены неопровержимые доказательства того, что сам Богатов никаких публикаций не делал, но его домашний компьютер был настроен в качестве выходной ноды сети Tor.

Для обычных пользователей, не являющихся владельцами конечных узлов Tor, опасность кроется в самой «луковой» сети.

# **2 ОХРАНА ТРУДА И БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ**

Пользователь автоматизированного рабочего места несет ответственность за сохранность и правильную эксплуатацию компьютерного оборудования.

Установка и изменение конфигурации операционной системы и состава программного обеспечения производятся специалистами отдела технического обслуживания информационных систем.

В случае неисправности компьютерного оборудования об этом необходимо сообщить в отдел технического обслуживания информационных систем.

1. Эксплуатация ЭВМ

Перед включением ЭВМ (ПК) необходимо ознакомиться с аппаратным журналом и убедиться, что все устройства ЭВМ были исправны при работе ранее. Для подключения к сети электропитания необходимо использовать только исправные силовые кабели, поставляемые с компьютерным оборудованием. Включение ЭВМ (ПК) производить согласно инструкции по включению и выключению на данную ЭВМ.

Запрещается включать устройства, к работе которых сотрудник не имеет доступа. Запрещается снимать крышки и щиты, закрывающие доступ к токоведущим частям. Запрещается включать и отключать разъемы кабелей электропитания и блоков вентиляторов под напряжением. Прикасаться к задней панели компьютерного оборудования; переключать разъемы кабелей периферийного оборудования; производить самостоятельный ремонт компьютерного оборудования; удалять с корпуса наклейки с заводскими и лицензионными номерами.

При необходимости временного прекращения работы корректно закрыть все активные программы.

Для корректного выключения компьютера необходимо закрыть все работающие программы, выбрать в меню «Пуск» команду «Завершение работы» и в появившемся меню выбрать пункт «Завершение работы» и нажать кнопку «ОК». Дождаться отключения питания системного блока, выключить монитор и принтер.

1. Противопожарные мероприятия

При техническом обслуживании и эксплуатации ЭВМ (ПК) необходимо строго соблюдать правила противопожарной безопасности. Запрещается хранить в машинном зале смазочные материалы. Включенные паяльники необходимо класть на специальные подставки. Рабочие места, проходы и выход не должны загромождаться посторонними предметами. По окончании работы все электроприборы должны быть выключены. Курение, пользование электронагревательными приборами, открытым огнем в данных классах запрещается. При возникновении пожара отключить оборудование (электроустановку), принять меры к ликвидации пожара, сообщить дежурному персоналу. При ликвидации пожара применять средства тушения, гасящее вещество которых не проводит электрический ток (огнетушители углекислотные, порошковые). Лица, работающие в классах, должны быть обучены приемам освобождения пострадавшего от электрического тока, приемам искусственного дыхания, правилам оказания первой помощи и способам тушения пожара в производственном помещении. Лица, допустившие нарушения, несут дисциплинарную, административную, уголовную ответственность.

1. Меры предосторожности

К самостоятельной работе на ПК допускаются лица не моложе 18-ти лет, прошедшие медицинское освидетельствование, специальное обучение, инструктаж по охране труда на рабочем месте, изучившие “Руководство по эксплуатации” и усвоившие безопасные методы и приемы выполнения работы.

ПК должен подключаться к однофазной сети с нормальным напряжением 220 (120) В, частотой 50 (60) Гц и заземленной нейтрально. Заземляющие контакты розеток должны быть надежно соединены с контуром защитного заземления помещения. В помещении должен быть установлен автомат аварийного или рубильник общего отключения питания.

Запрещается самостоятельно производить ремонт ПК (его блоков), если это не входит в круг ваших обязанностей.

При эксплуатации ПК должны выполняться следующие требования, правила:

* не подключать и не отключать разъемы и кабели электрического питания при поданном напряжении сети;
* не оставлять ПК включенным без наблюдения;
* не оставлять ПК включенным во время грозы;
* по окончании работы отключить ПК от сети;
* устройства должны быть расположены на расстоянии 1 м от нагревательных приборов; рабочие места должны располагаться между собой на расстоянии не менее 1,5 метров;
* устройства не должны подвергаться воздействию прямых солнечных лучей;
* непрерывная продолжительность работы при вводе данных на ПК не должна превышать 4 часов при 8-часовом рабочем дне, через каждый час работы необходимо делать перерыв 5-10 минут, через 2 часа на 15 минут;
* в помещении, где расположена компьютерная техника, должен быть оборудован уголок пожаротушения.

Санитарно-гигиенические требования при работе с компьютером

В соответствии с СанПиН: 2.2.2.542-96 «Гигиенические требования к ВДТ и ПЭВМ. Организация работы»

Все вредности, возникающие при работе ВДТ и ПЭВМ можно разделить на три группы:

Параметры рабочего места и рабочей зоны.

Визуальные факторы (яркость, контрастность, мерцание изображения, блики).

Излучения (рентгеновское, электромагнитное излучение ВЧ и СВЧ диапазона, гамма-излучение, электростатические поля).

Внедрение ЭВМ имеет как положительные, так и отрицательные моменты. С одной стороны, это обеспечение более высокой эффективности производства за счет совершенствования технологического процесса и повышение производительности труда, а с другой - увеличение нагрузки на работающих в связи с интенсификацией производственной деятельности и специфическими условиями труда.

Условия труда работающих с ЭВМ характеризуются возможностью воздействия на них следующих производственных факторов: шума, тепловыделений, вредных веществ, статического электричества, ионизирующих и неионизирующих излучений, недостаточной освещенности, параметров технологического оборудования и рабочего места. Основными источниками шума в помещениях, оборудованных вычислительной техникой, являются принтеры, плоттеры, множительная техника и оборудование для кондиционирования воздуха, вентиляторы систем охлаждения, трансформаторы. Для снижения шума и вибрации в помещениях вычислительных центров оборудование, аппараты необходимо устанавливать на специальные фундаменты и амортизирующие прокладки, предусмотренные нормативными документами.

Уровень шума на рабочих местах не должен превышать 50 дБА. Нормируемые уровни шума обеспечиваются путем использования малошумного оборудования, применением звукопоглощающих материалов (специальные перфорированные плиты, панели, минераловатные плиты). Кроме того, необходимо использовать подвесные акустические потолки.

В помещениях с избытком тепла необходимо предусматривать регулирование подачи теплоносителя для соблюдения нормативных параметров микроклимата. Микроклиматические условия на рабочих местах в помещениях с вычислительной техникой должны соответствовать требованиям. Воздух, поступающий в рабочие помещения операторов ЭВМ, должен быть очищен от загрязнений, в том числе от пыли и микроорганизмов. Патогенной микрофлоры быть не должно.

При профессиональном отборе работников ЭВМ основное внимание обращается на состояние органов зрения: состояния мышечного равновесия глаз, положительный запас аккомодации, цветовую чувствительность, остроту зрения, рефракционную способность глаз, контрастную чувствительность и поле зрения.

1. Организация рабочего места

Приступая к работе на компьютере желательно:

1. Осмотреть рабочее место (расположение блоков и их состояние).
2. Подобрать по высоте стул.
3. Монитор должен располагаться на уровне глаз и перпендикулярно углу зрения.
4. Экран монитора и защитный экран (с обеих сторон) должны быть чистыми.
5. Освещение должно соответствовать нормам СанПиН.
6. Не рекомендуется располагать монитор около яркого источника света, т.к. приходится повышать яркость и контрастность, что влечет за собой: увеличение нагрузки на глаза, излучения, выгорает люминофор экрана, сокращается срок службы монитора.
7. На мониторе не должно быть бликов, сильного контраста с внешним освещением.
8. Мышь располагается так, чтобы было удобно работать с ней. Провод должен лежать свободно. При работе с мышью по периметру коврика должно оставаться пространство не менее 2-5 сантиметров.
9. Клавиатуру следует располагать прямо перед пользователем, работающим на компьютере. По периметру оставляется свободное место 2-5 сантиметров.
10. Десять шагов по обеспечению безопасности и комфорта домашнего компьютера.
11. Системный блок. Устанавливать системный блок следует устойчиво на ровной поверхности таким образом, чтобы углы системного блока не выступали за края стола. Лучше установить его на полу (специальной подставке) под столом.
12. Стол. Лучше всего использовать специальный компьютерный стол со столешницей достаточной глубины, местом под системный блок и выдвижной доской для клавиатуры и мышки. Это позволит использовать стол и для других целей.
13. Питание. Чтобы надежно обезопасить компьютер от неожиданностей и неприятностей, имеет смысл потратить средства на источник бесперебойного питания или, как минимум, установить заземленную розетку с фильтрами.
14. Чистота. Содержите вентиляционные отверстия системного блока и монитора открытыми, не захламляйте стол бумагами, журналами и книгами. Ухудшение условий охлаждения может существенно сократить срок жизни монитора и компьютера. Если на столе скапливается много документов, имеет смысл установить монитор на специальном кронштейне (подставке), чтобы приподнять его.
15. Мышь. Даже в работе с мышкой следует обзавестись хорошими привычками. Есть правила, которые стоит неукоснительно выполнять:
16. Запястье должно быть прямым. Никогда не опирайтесь на запястье, лежащее на столе. Не изгибайте суставы запястья: оно должно лежать в естественном положении.
17. Не сжимайте мышку с силой. Это вызывает ненужное напряжение мышц, нарушает кровообращение и затрудняет движения. Если мышь не слушается, почистите ее.
18. Не работайте с мышкой полностью вытянутой рукой. Подбирая рабочий стол, выбирайте такой, чтобы за мышкой не приходилось тянуться слишком далеко. Для движения мышкой должно быть достаточно свободного места.
19. Различные дополнительные приспособления, такие как коврики для мыший, подушки и подпорки для отдыха запястий рук, помогают только в том случае, если правильно используются.
20. Некоторые предпочитают обычной мыши трэкбол. Этот манипулятор имеет свои достоинства и недостатки: для него требуется меньше пространства на столе и меньше приходиться двигать рукой, зато гораздо больше приходиться работать пальцами. Используйте то устройство, применение которого вам лично кажется более естественным.
21. Клавиатура. Оптимальная высота стола или выдвижной полки для клавиатуры 68 – 73 см. над полом. Высоту стула и стола следует подобрать так, чтобы минимально напрягать мышцы плечей, рук и запястий. Запястья могут касаться стола перед клавиатурой. Но ни в коем случае нельзя переносить на них хотя бы часть веса тела. Клавиатура регулируется по высоте наклона. Подберите для себя наиболее удобный угол наклона. Некоторые клавиатуры, например, Microsoft Natural Keyboard, имеют большие возможности для регулировки. Такие клавиатуры имеют расщепление в середине буквенной части и особую форму, предназначенную для более естественного положения запястий над клавишами. Однако такой клавиатурой имеет смысл обзаводиться только в том случае, если вы много пишите и владеете слепым десятипальцевым методом печати. В остальных случаях от такой клавиатуры нет никакого эргономического выигрыша. В компьютерных салонах можно найти специальные подпорки и подушки для установки перед клавиатурой, предназначенные для отдыха запястий и предупреждения туннельного синдрома – острых болей из-за перегрузки и повреждения сухожилий запястий. Проку от этих приспособлений не так уж и много, если вы не привыкнете правильно их использовать. А вот регулярные короткие перерывы в работе на клавиатуре могут реально помочь. Так что лучше обзаведитесь такой привычкой, чем захламлять стол ненужными приспособлениями.
22. Кабели. У компьютера довольно много кабелей и проводов. Их лучше всего собрать сзади стола. Но стол необходимо отодвинуть от стены, чтобы в этом пространстве кабели не запутались между собой.
23. Освещение. Чтобы уменьшить отражение и блики на экране, размещайте домашний компьютер перпендикулярно окну. Обеспечьте достаточное местное освещение, направленное на документ, чтобы можно было выключать общее освещение в помещении и снижать яркость бликов.
24. Компьютер всегда должен находиться в чистоте. Чистить компьютер необходимо как снаружи, так и внутри. Перед тем как приступить к такой процедуре, обязательно нужно отключить компьютер от электросети.

Поверхностная очистка:

1. Монитор следует протирать только специально предназначенными для него салфетками, которые легко можно найти в любом компьютерном магазине. Но запомните, что никогда не стоит протирать его мокрыми тряпками или средством для очищения стекол. Это пагубно для него.
2. Клавиатуру следует протирать чуть влажной тряпкой ежедневно! Это самая часто используемая часть всего ПК, и микробов на ней столько, что трудно себе представить. Можно чистить обычной кисточкой, она поможет удалить ту пыль, до которой Вы не добрались тряпкой, но лучше всего клавиатуру перевернуть, и пропылесосить снизу.

Чистка системного блока:

Для этой операции Вас понадобятся пылесос и кисточка.

1. Открываем крышку корпуса, которая находится с левой стороны, если смотреть спереди. Для этого нам понадобится фигурная отвертка. Затем пылесосом устраняем пыль с вентиляционной решетки и с блока питания.
2. Кулер и радиатор. Пальцем придерживайте кулер (чтобы не было вращения) и аккуратно пропылесосьте все его детали. Но не прикасайтесь к деталям внутренностям компьютера, пылесосьте на небольшом от них расстоянии, чтобы случайно не зацепить элементы, которые припаянные к материнской плате.
Такую уборку необходимо проделывать пару раз в месяц. Но как минимум раз в год нужно отнести компьютер в сервисный центр и сделать «генеральную уборку», то есть разобрать полностью весь ПК, и прочистить все его мельчайшие детали. Это лучше всего доверить профессионалам.

**ЗАКЛЮЧЕНИЕ**

Активисты и революционеры давно используют DarkNet для самоорганизации, не опасаясь открыть свою позицию правительству, против которого они выступают. Разумеется, это означает, что по тем же причинам DarkNet используется террористами, экстремистами и прочими нежелательными организациями и группировками. Любой человек может получить доступ к скрытому сегменту Интернета очень легко. Существует множество сомнительных материалов, а также большое количество преступников. С другой стороны, та же анонимность, что делает DarkNet удобной платформой для незаконной деятельности, также делает его оплотом более благородного дела: свободы слова.

DarkNet также популярен среди журналистов и политических блоггеров, особенно тех, кто живет в странах, где жесткая цензура и тюремное заключение в качестве наказания за ее нарушение являются обычным явлением. Интернет-анонимность позволяет этим людям, а также осведомителям и информаторам общаться с источниками и свободно публиковать информацию, не опасаясь наказания. Такая же анонимность может использоваться читателями новостей для доступа к информации на поверхностной сети, которая обычно блокируется национальными брандмауэрами. Идея о том, что информация должна быть бесплатной и доступной для всех, как представляется, очень дорога пользователям темной стороны Интернета, также как и идея о том, что правительства и крупный бизнес угрожают этому.

В ходе исследования курсовой работы были рассмотрены следующие цели:

1. История появление
2. Основные понятия и программное обеспечение
3. Понятие «Три уровня интернета»
4. Услуг предоставляемые в «DarkNet»
5. Сайты
6. Влияния «DarkNet»

Из этого следует сделать вывод, что DarkNet представляет собой сеть, где возможно все купить и продать, так же поделится своей информацией с другими пользователями DarkNet. Эта сеть позиционирует себя как где все имеют одинаковые права и возможности, где нет никаких запретов. Существует множество форумов по совершенно разным тематиками от хакинга до приготовление различных препаратов.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Айзексон У. Инноваторы. Как несколько гениев, хакеров и гиков совершили цифровую революцию. – ЭКСМО, 2017. 475с.
2. Бабин С. Лаборатория хакера – БВХ-ПЕТЕРБУРГ, 2018. 240с.
3. Бартлетт Д. Подпольный интернет. Кто скрывается в цифровом подполье – ЭКСМО, 2016. -352c.
4. Билтон Н. Киберпреступник №1. История создания подпольной сетевой империи – ЭКСМО 2017. 448с.
5. Волков А. Фейк – БВХ-ПЕТЕРБУРГ, 2018. 121с.
6. Митник К. Искусство обмана - ЭКСМО, 2014. 360с.
7. Огородник О. Хроники будущего.Delete – ЭКСМО, 2018. 364c.
8. Ормсби Э. Темная паутина: Наркотики, смерть и разрушенные жизни… - Alien & Unwin, 2018. 320с.
9. Райтман М. Искусство легального, анонимного и безопасного доступа к ресурсам Интернета – БХВ-ПЕТЕРБУРГ, 2017. 624с.
10. Райтман М. Как найти и скачать в Интернете любые файлы – ЭКСМО, 2016. 378с.
11. Савинов С. Даркнет.Игра реальности – РЕАЛРПГ, 2017. 150с.
12. Садовски Н. Погребенное общество – Penguin Random House Audio, 2018. 459с.
13. Саймон У. Призрак в Сети. Мемуары величайшего хакера – ЭКСМО, 2014. 416с.
14. Саймон Х. Цифровая приватность, Терроризм и Ограничение свободы. – Routledge, 2018. 196с.
15. Сверкунов В. Игры в апокалипсис – ЭКСМО, 2018.
16. Тилье Ф. Пандемия –АЗБУКА,2016. -448с.
17. Филипс К. Зарабатывать на хайпе. Чему нас могут научить пираты, хакеры, дилеры и все, о ком не говорят в приличном обществе – ЭКСМО, 2018. 248с.
18. Фленов М. Linux глазами хакера – БВХ-ПЕТЕРБУРГ, 2018. 432c.
19. Фленов М. Web-сервер глазами хакера – БХВ-ПЕТЕРБУРГ, 2018. 234с.
20. Фленов М. Компьютер глазами хакера – БВХ-ПЕТЕРБУРГ, 2017. 336с.

РЕСУРСЫ УДАЛЕННОГО ДОСТУПА

1. Google Картинки, https://images.google.ru/?gws\_rd=ssl;
2. Википедия, https://ru.wikipedia.org/;
3. HTML самоучитель, https://developer.mozilla.org/ru/;
4. Опасность DarkNet’a, <https://www.iphones.ru/iNotes/680356>
5. Как войти в DarkNet, https://9net.ru/191-darknet-kak-voyti.html
6. Сайт по продажам книг, https://www.ozon.ru/
7. Что такое даркнет (Darknet) и как в него попасть, https://prostocoin.com/blog/darknet
8. Путешествие по даркнету, https://xakep.ru/2018/12/29/darknet-russia/
9. Что читать в даркнете, http://www.furfur.me
10. Какие сайты стоит посетить в даркнете?, https://thequestion.ru/questions/289851/kakie-saity-stoit-posetit-v-darknete
1. Митник К. Искусство обмана - ЭКСМО, 2014. 360с. [↑](#footnote-ref-1)
2. Сверкунов В. Игры в апокалипсис – ЭКСМО, 2018. [↑](#footnote-ref-2)
3. Райтман М. Как найти и скачать в Интернете любые файлы – ЭКСМО, 2016. 378с. [↑](#footnote-ref-3)
4. Бартлетт Д. Подпольный интернет. Кто скрывается в цифровом подполье – ЭКСМО, 2016. -352c. [↑](#footnote-ref-4)
5. Волков А. Фейк – БВХ-ПЕТЕРБУРГ, 2018. 121с. [↑](#footnote-ref-5)
6. Тилье Ф. Пандемия –АЗБУКА,2016. -448с. [↑](#footnote-ref-6)
7. Филипс К. Зарабатывать на хайпе. Чему нас могут научить пираты, хакеры, дилеры и все, о ком не говорят в приличном обществе – ЭКСМО, 2018. 248с. [↑](#footnote-ref-7)
8. Саймон Х. Цифровая приватность, Терроризм и Ограничение свободы. – Routledge, 2018. 196с. [↑](#footnote-ref-8)
9. Айзексон У. Инноваторы. Как несколько гениев, хакеров и гиков совершили цифровую революцию. – ЭКСМО, 2017. 475с. [↑](#footnote-ref-9)
10. Билтон Н. Киберпреступник №1. История создания подпольной сетевой империи – ЭКСМО 2017. 448с. [↑](#footnote-ref-10)