Муниципальное образование города Краснодар

муниципальное бюджетное учреждение муниципального образования город Краснодар средняя общеобразовательная школа №76 имени 4-го Гвардейского Кубанского Казачьего Кавалерийского корпуса

Программирование: создание скриптов.

Хакерство и его виды.

Седина Милана Юрьевна

ученица 10 «Б» класса

Абдуллина Ирина Юрьевна

Харченко Сергей Владимирович

Краснодар, 2022

Содержание:

Введение

Гава 1. Программы для создания скриптов.

Глава 2. Хакерство как социальное явление

Заключение.

Список используемых источников.

**Введение**

Лень — двигатель прогресса. Благодаря ей были созданы многие вещи, которыми мы пользуемся в повседневной жизни, в том числе и компьютер. Человек ленился делать вычисления вручную и автоматизировал этот процесс.

Автоматизация — штука хорошая, но есть и обратная сторона медали. Вспомним ХХ век: тотальная индустриализация. Огромные заводы с тысячами рабочих мест, небольшие города вокруг этих заводов. Сейчас людей на рабочих местах сменяют роботы. Так, в этом году была открыта полностью автоматизированная линия производства кроссовок Adidas в Германии.

У роботов неоспоримые преимущества: они не отдыхают, не ошибаются, не болеют, не совершают самоубийств из-за проблем в личной жизни, а главное — им не нужно платить зарплату. Люди боятся потерять рабочее место и лишиться средств к существованию.

**Проблемы программирования:**

Многие считают, что профессия программиста неактуальна. Ведь скоро искусственный интеллект начнет создавать сам себя, а роботы научатся чинить роботов.

Но искусственный интеллект такого уровня — дело будущего, а полностью автоматизированные рабочие места — дело настоящего. Терминалы самообслуживания, автоответчики в кол-центрах — все это примеры автоматизации, ставшие реальностью. В то же время никто не задумывается, что один терминал самообслуживания смог сократить количество сотрудников банка. Выдать наличку и принять оплату вполне может и «робот». А чем больше таких терминалов, тем больше работы у программистов.

**Задачи:**

1. Изучить программы для создания скриптов
2. Рейтинг языков программирования 2021 г.
3. Особенности хакерской культуры
4. Как преследуют и судят хакеров в России

**План выполнения работы:**

1. Используя различные источники знаний составить краткую информацию о скриптах
2. Познакомиться с некоторыми программами для создания скриптов
3. Узнать положительные и отрицательные стороны хакеров

**Что такое скрипт?**

В современном программировании в Сети скрипты (сценарии) – это отдельные последовательности действий, созданные для автоматического выполнения задачи. Если готового сценария нет, пользователь выполняет эти действия вручную с соответствующими затратами времени и возможностями появления ошибок. Для написания скриптов используются специальные языки программирования, которые так и называются – скриптовые. Соответственно, скриптовый язык программирования – это набор лексический, семантических и синтаксических правил для создания и редактирования скриптов. Корректно также синонимичное название «язык сценариев».

С английского языка слово «скрипт» переводится как сценарий, из чего уже можно сделать определенные выводы. Это набор команд, то есть строк кода, которые вкупе выполняют конкретную задачу. Для ее выполнения и создаются скрипты. Они могут быть как очень маленькими по объему и отвечать за запуск каких-то простых служб операционной системы, так и объемными, сравнивая переменные и выводя результат на сайте. Скрипт хранится в текстовом файле, поэтому при желании его содержимое можно легко просмотреть и даже изменить. Этот текстовый файл запускает цепочку выполнения задачи, которая и запрограммирована в скрипте. Если все строки написаны правильно и целевые объекты удается найти, задача выполняется успешно и скрипт срабатывает.

Скрипты сейчас активно интегрируются на сайтах, в качестве примера можно привести популярный скриптовый язык – JavaScript. Однако изначально они работали в операционных системах и выполнялись при помощи внутреннего синтаксиса командной оболочки.

**Глава 1.**

**Программы для создания скриптов:**

* IDLE
* PyCharm
* Intellij IDEA
* Eclipse
* Netbeance
* RubyMine
* Notepad++
* SublimeText

**IDLE:**

IDLE (Integrated Development and Learning Environment) — это интегрированная среда для разработки (и обучения), которая поставляется вместе с Python. Сама IDLE написана на Python с использованием библиотеки Tkinter, поэтому является кроссплатформенным приложением (может работать на Windows, MacOS, Linux).

IDLE это по сути текстовый редактор с подсветкой синтаксиса, автозаполнением, умным отступом и другими функциями для удобства написания кода на Python.

**PyCharm:**

PyCharm — продвинутая альтернатива предыдущему решению, созданная известной компанией под названием JetBrains. Разработчики постарались реализовать в своей программе те опции, которые пригодятся профессиональным разработчикам и окажут значимое влияние на комфортность взаимодействия с софтом. Самая главная из них, предназначенная для повышения удобства, — встроенный умный редактор. Как только вы начинаете набирать команду, редактор отображает возможные варианты автозаполнения, а вам остается лишь подтвердить его, нажав по клавише Enter. Это же позволяет исключить большинство опечаток или случайных ошибок еще до запуска компилирования, сэкономив тем самым время, которое могло быть затрачено на исправление в дальнейшем.

**IntelliJ IDEA:**

IntelliJ IDEA — интегрированная среда разработки Java приложений от компании JetBrains.

Ее позиционируют как самую умную и удобную среду разработки для Java с поддержкой всех последних технологий и фреймворков.

IntelliJ IDEA входит в тройку самых популярных IDE для Java вместе с Eclipse IDE и NetBeans IDE. Сравнение трех сред разработки есть в данном материале о выборе среды для разработки.

IntelliJ IDEA хорошо знакома сообществу Javarush. Уже с третьего уровня студенты выполняют задания в IntelliJ IDEA, которая легко интегрируется с курсом. Ученики курса получают практические задания прямо в среде разработки. В ней же студент может отправить выполненное задание на проверку и сразу получить обратную связь.

Хоть IntelliJ IDEA известна как среда разработки для Java, в ней из коробки поддерживаются несколько языков программирования. Кроме того, IntelliJ IDEA интегрирована с рядом современных фреймворков. В данную среду разработки встроены все популярные системы контроля версий и системы сборки приложения. В IDEA реализована поддержка многих серверов приложений. Начиная с шестой версии, IntelliJ IDEA предоставляет интегрированный инструментарий для разработки графического пользовательского интерфейса.

У этой среды разработки есть мощные аналитические возможности. Благодаря им эта IDE на лету подсказывает разработчику лучшие варианты кода в текущем контексте. IDEA располагает набором инструментов для рефакторинга существующего кода и быстрого написания шаблонных конструкций.

**Производительность**

Программы, написанные на Java, имеют репутацию более медленных и занимающих больше оперативной памяти, чем написанные на языке Си. Тем не менее, скорость выполнения программ, написанных на языке Java, была существенно улучшена с выпуском в 1997—1998 годах так называемого JIT-компилятора в версии 1.1 в дополнение к другим особенностям языка для поддержки лучшего анализа кода (такие как внутренние классы, класс StringBuffer, упрощенные логические вычисления и т. д.). Кроме того была произведена оптимизация виртуальной машины Java — с 2000 года для этого используется виртуальная машина HotSpot. В настоящее время[уточнить], код Java 2.0 приблизительно лишь в 2 раза медленнее кода, написанного на языке Cи.

Некоторые платформы предлагают аппаратную поддержку выполнения для Java. К примеру, микроконтроллеры выполняющие код Java на аппаратном обеспечении вместо программной JVM, а также основанные на ARM процессоры, которые поддерживают выполнение байткода Java через опцию Jazelle.

**Рейтинг языков программирования 2021 г.**

Что изменилось? Прежде всего привлекает внимание рост TypeScipt: похоже, он со временем станет основным языком в экосистеме JavaScript. В этом году он впервые обошел С ++ по популярности.

Еще из интересного: впервые за несколько лет мы увидели снижение доли Python: возможно, использование Data Science дошло до точки насыщения.

Впервые с 2012 года выросла доля C#. Использование Java продолжает уменьшаться, хотя и не так активно, как раньше. В общем видно уменьшение доли JVM: доля Kotlin стабильна (хотя он и уступил место Ruby), использование Scala возобновилось после значительного снижения в 2019-м и сегодня, если сравнивать с 2018-м, даже немного возросло. Еще стоит отметить незначительный рост Dart (график 1).

Ниже приведена диаграмма с динамикой по актуальным языкам программирования по годам. Статистически значимыми являются изменения для C ++, TypeScript, Ruby, 1C, Scala, Pascal/Delphi, T-SQL. Напомним, что изменения статистически значимы, если с вероятностью 95% мы не можем получить результаты с изменениями и без, если будем равномерно выбирать две группы респондентов с одной популяции ( диаграмма 1).

Видно, что примерно половина разработчиков - это бэкенд 52%, далее сегменты фронтенд 19% и мобильной разработки 8%, обработка массивов данных (туда относятся и Big Data и машинное обучение) - 6%. Desktop-программирование еще существует и занимает 4% от объема, системное программирование - 3% (сейчас небольшая доля) и Full-Stack разработка - примерно 1%.

Несмотря на языки программирования, также имеет смысл рассмотреть структуру распределения опыта в динамике (диаграмма 2).

Вывод.

Изобретение языков программирования высшего уровня, а также их постоянное совершенствование и развитие, позволило человеку не только общаться с машиной и понимать ее, но использовать ЭВМ для сложнейших расчетов в области самолетостроения, ракетостроения, медицины и даже экономики.

На сегодняшний день, любое среднее и крупное предприятие, имеет в своем штате группу программистов, обладающими знаниями программирования различными языками, которые редактируют, изменяют, и модифицируют программы используемыми сотрудниками предприятия. Это говорит о том, что на рынке труда пользуются спросом обладающими знаниями и опытом работы с различными языками программирования.

Несмотря на то, что современный уровень развития языков программирования находятся на высоком уровне, тенденция их развития, а также развития информационных технологий в целом, складывается таким образом, что можно предположить, что в ближайшем будущем, человеческие познания в этой сфере, помогут произвести на свет языки, умеющие принимать, обрабатывать и передавать информации в виде мысли, слова, звука или жеста.

**Глава 2.**

**Хакерство как социальное явление**

Информатизация и компьютеризация в современном обществе приобретают все больший размах. Компьютеры входят во все новые и новые области человеческой практики, трансформируя при этом не только отдельные действия, но и человеческую деятельность в целом, оказывая влияние на все психические процессы.

Применение информационных технологий при конкретных действиях или видах деятельности может оказывать влияние даже на всю личность в целом.

Явление хакерства часто объясняется как один из способов ухода или погружения в мир иллюзорной реальности, творимой и видоизменяемой самим хакером сообразно своему вкусу и в некоторой степени – групповым представлениям. Часто хакеров описывают с негативной стороны, подчеркивая их запретные действия.

В последнее время интерес к проблеме хакеров возрос, особенно в средствах массовой информации. Следует отметить, что такая популярность этой темы привлекает многих подростков, которые начинают изучать информационные технологии ради того, чтобы когда-нибудь называться хакерами.

**Особенности хакерской культуры**

Интернет становится все более распространенным средством коммуникации в обществе постмодерна, а хакеры – неотъемлемой частью информационного общества. "Хакеры обладают качествами, важными для общества и помогающими гражданам понять различие между грязными деяниями крэкеров и обычно более мирной и явно более полезной работой хакеров1". По роду своей деятельности именно хакеры задают вектор и специфику информационного развития в обществе, создают, трансформируют, предопределяют будущее современного общества. Поэтому важно рассматривать хакеров как особую социальную группу, исходя из имеющихся этических принципов и ценностей, мотивации их деятельности, общественной полезности результатов их работы.

В настоящее время существуют достаточно противоречивые представления о том, кто такие хакеры, причем данные противоречивые мнения характерны не только для широкой общественности, но и для социологического сообщества. Многие отечественные и российские социологи (Скородумова О., Букин М., Вершинин М., Осипов Е., Терин В.) толкуют этот феномен в его одностороннем и зачастую лишь негативном смысле, рассматривают хакеров лишь как преступников и хулиганов, орудующих в Интернете. Например, О.Б. Скородумова выделяет следующие группы хакеров: "шутники" — осуществляют взлом компьютерной системы для достижения известности, не склонны причинять серьезного вреда системе и выражают себя внесением различных юмористических заставок, вирусов с различными визуально-звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок и т.п.); "фрикеры" - осуществляют взлом телекоммуникационных сетей, подключаются к чужому оборудованию по передаче голоса посредством телефонных, компьютерных, сотовых и спутниковых сетей в личных целях и для обогащения; "сетевые хакеры" — осуществляют взлом интрасети в познавательных целях для получения информации о топологии сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, методах защиты; "взломщики- профессионалы" — осуществляют взлом компьютерной системы с целью кражи или подмены хранящейся там информации; "вандалы" — осуществляют взлом компьютерной системы для ее разрушения: порчи и удаления данных, создания вирусов или "троянских коней3". Как видим, данным автором, как и многими другими, термин "хакер" отождествляется лишь с различными формами киберпреступности. В конструировании такой позиции по отношению к хакерам ведущую роль сыграли СМИ, обозначающие компьютерных преступников (крякеров, стрипкидди, фрикеров, пиратов) только одним понятием "хакер". Однако такая позиция не соответствует реальной специфике сформировавшегося сообщества хакеров, которые на самом деле осуждают взлом, и чья деятельность направлена, прежде всего, на развитие свободного программного обеспечения.

Ближе всего к определению характеристик хакерской культуры подошли европейские социологи Мануэль Кастельс и Пекка Химанен. Они определяют хакеров как высококвалифицированных компьютерных специалистов, принадлежащих к техномеритократической культуре, характеризуемой верой во врожденную полезность научно-технического развития как ключевой составляющей прогресса человечества. Кастельс и Химанен среди отличительных черт сообщества хакеров выделяют принадлежность к хакерской этике, высокий уровень определенных знаний и сотрудничество в развитии открыто-исходных проектов. Культура хакеров, по мнению Кастельса, играет главную роль в построении сети Интернет, т.к. она является питательной средой для выдающихся технических инноваций благодаря принципам сотрудничества и свободной коммуникации. Цель деятельности хакеров лежит в достижении максимальной продуктивности и технического совершенства – технических инноваций. Важными характеристиками хакерской культуры, выделяемые Химаненом, являются ценности радости творчества, свободы и независимости личности, свободы и полной открытости информации, творческого потенциала и развития, сотрудничества в сообществе, авторитета среди коллег. Для хакеров деньги не являются целью, главное для них – привнести ценный вклад в техническое развитие, поэтому хакеры сотрудничают по открыто-исходной модели, на основе которой и формируется особая социальная группа хакеров.

**Положительные и отрицательные стороны хакеров**

Хороших хакеров также называют белыми шляпами или хакерами безопасности, а плохих хакеров называют крекерами или черными шляпами. Хороший и плохой хакер работают почти одинаково и даже используют идентичные навыки для выполнения взлома, так что же делает одного лучше другого?

Хотя большинство подвигов, о которых мы услышим в новостях, исходят от людей, у которых есть злые намерения, гораздо больше невероятно талантливых и преданных своему делу людей используют свои хакерские навыки для блага. Важно понимать разницу.

Белые и черные хакеры — это всего лишь пара классификаций хакера. Есть также серые шляпы хакеров и сценарий детишки, например.

Что такое хакер?

Когда большинство людей слышат о хакере, они думают о том, как их изображают в хакерских фильмах: человек в толстовке с капюшоном скрыт где-то скрытно с десятью компьютерными мониторами, которые помогают ему или ей взломать удаленный компьютер.

Хотя это вполне может иметь место в реальном мире, важно знать, что есть еще одна сторона взлома, которая считается этичной и полностью законной.

И хороший, и обратный хакер, скорее всего, очень хорошо разбираются в компьютерном программировании, работе в сети и / или других связанных функциях и используют эти навыки для проникновения в компьютерную систему.

Однако термин «хакер» может относиться к двум типам людей в зависимости от обстоятельств:

Хороший хакер: использует свои знания с разрешения для проверки уязвимостей и других уязвимостей, а затем предлагает подробности о том, как улучшить систему, чтобы злоумышленники не воспользовались ею.

Плохой хакер: атакует систему без предварительного разрешения, что они могут сделать, чтобы украсть, изменить или уничтожить информацию, или вызвать проблемы, такие как задержки или полное отсутствие доступа.

Хакеры в белой шляпе, или этические хакеры, работают внутри компании. Бизнес нанимает хакера, чтобы повысить безопасность своей системы, проникая в нее, как это сделал бы плохой хакер.

Компания полностью осведомлена о присутствии хакера и дает им полное разрешение использовать свои хакерские способности, чтобы найти недостатки. Хакер сообщает об этих проблемах компании и, возможно, даже сможет их исправить или, по крайней мере, предоставит отчет о том, где есть уязвимости, которые необходимо устранить.

В этом случае хакерство хорошо, потому что хакер не вошел в систему без разрешения. Он или она ничего не крал, не портил веб-сайт компании, не раскрывал личную информацию сотрудников и т. Д. Все это было сделано на законных основаниях и с полного разрешения компании с явной целью.

Этический взлом как работа

Хотя хакеров в белых шапках не обязательно признают так, как следовало бы, все больше и больше компаний ищут людей, которые могут опередить людей, решивших сломать свои системы.

Нанимая белых хакеров, у компаний есть шанс на победу. Несмотря на то, что эти гуру программирования когда-то считались отверженными в глазах общественности, многие хакеры теперь занимают критически важные и чрезвычайно высокооплачиваемые должности в корпорациях, правительствах и других организациях. На самом деле, в некоторых случаях хакер может даже попасть в тюрьму за плохой взлом, а затем быть нанятым позже, чтобы сделать это на законных основаниях!

Конечно, не все нарушения безопасности могут быть предотвращены, но если компании нанимают людей, которые смогут обнаружить их, прежде чем они станут критическими, то половина битвы уже выиграна.

Большинство хакеров в белых шапках работают в агентствах компьютерной безопасности, таких как DXC Technology (ранее CSC). Как указано на их сайте, у них есть тысячи «специалистов по безопасности с глубокими специализациями, которые включают тестирование на проникновение, управление уязвимостями, аналитику SOC, криминалистические расследования и анализ угроз».

Почему там плохие хакеры?

Если хакер может зарабатывать на жизнь хакингом на законных основаниях, почему любой плохой хакер остается хакером в черной шляпе, а не просто «переключается» на хорошего хакера?

Хакеры в черной шляпе никуда не денутся, потому что большинство хакеров мотивировано ненавистью или совершается в попытке сделать заявление или раскрыть секретную информацию. Другими словами, хакер, который делает это неэтично, чувствует необходимость сделать это, чтобы высказать свое мнение или разоблачить человека, компанию, правительство и т. д.

Рассмотрим пример, когда сотрудника увольняют из компании. Он может взломать сайт компании и осквернить его непристойными фотографиями и словами в качестве мести за потерю работы. Этот тип взлома явно не так, потому что компания не просила об этом.

Другой хакер может просочиться в электронные письма от политического деятеля, но может сделать это не как часть личного возмездия, а скорее как общественную службу. Хакер может подумать, что она может использовать свои навыки, чтобы разоблачить кого-то и сообщить общественности детали, которые обычно скрыты.

Другие хакеры могут просто любить острые ощущения от проникновения систем и разрушения сетей. Возможно, это просто слишком весело, чтобы избежать, или интеллектуальная стимуляция не похожа ни на что другое. Это очень умные люди, у которых нет моральных сомнений в поиске и разрушении компьютерной инфраструктуры.

Некоторые люди используют Интернет для демонстрации по политическим или социальным причинам, используя действия, называемые хактивизмом .

Черная шляпа

Аноним: слабо связанная группа хакеров со всего мира с местами встреч на различных форумах и форумах социальных сетей. Они наиболее известны своими усилиями по поощрению гражданского неповиновения и / или беспорядков путем клеветы и порчи различных веб-сайтов, атак на отказ в обслуживании и публикации личной информации в Интернете.

Джонатан Джеймс: печально известен тем, что взломал Агентство по уменьшению угроз обороны и похитил программный код.

Адриан Ламо: известен тем, что проник в сети нескольких организаций высокого уровня, в том числе Yahoo , New York Times и Microsoft, для использования уязвимостей в безопасности.

Кевин Митник: осужден за многочисленные преступления в компьютерной сфере после уклонения властей от чрезвычайно широко разрекламированной погони в течение двух с половиной лет. После службы в федеральной тюрьме за свои действия Митник основал фирму по кибербезопасности, чтобы помочь предприятиям и организациям обеспечивать безопасность своих сетей.

Белая шляпа

Тим Бернерс-Ли: Самый известный за изобретение Всемирной паутины , HTML и системы URL .

Винтон Серф: известный как «отец интернета», Серф сыграл важную роль в создании интернета, который мы используем сегодня.

Дэн Камински: Многоуважаемый эксперт по вопросам безопасности самым известным за его роль в раскрытии защиты от копирования Sony BMG руткит скандал.

Кен Томпсон: создал операционную систему Unix и язык программирования C.

Дональд Кнут: Один из самых влиятельных людей в области компьютерного программирования и теоретической информатики.

Ларри Уолл: создатель PERL, языка программирования высокого уровня, который можно использовать для самых разных задач.

**Как преследуют и судят хакеров в России**

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

Основным законом, регулирующим свободу доступа к информации, является N 149 ФЗ "Об информации, информационных технологиях и защите информации". Этот закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; использовать информацию, в том числе распространять ее, по своему усмотрению; защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо его воли.

Порядок доступа к персональным данным граждан устанавливается федеральным законом "О персональных данных".

Этот закон призван обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Действия хакеров на территории РФ в зависимости от цели и мотивов могут предполагать уголовную, административную и гражданско правовую ответственность.

Административная ответственность за хакерскую деятельность может возникнуть в случае нарушения Статьи 13 Кодекса РФ об административных правонарушениях РФ (Административные правонарушения в области связи и информации). Данная статья предполагает ответственность за разглашение информации с ограниченным доступом, а также нарушение установленного порядка хранения, использования или распространения информации персональных данных.

В зависимости от тяжести правонарушения размер штрафа может составить от трехсот до двадцати тысяч рублей.

Различные случаи редактирования и декомпилирования программ могут подпадать под действие статей 273 и 146 УК РФ.

Согласно статье 273 УК РФ создание, использование и распространение вредоносных компьютерных программ, которые предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, является уголовно наказуемым. Предполагаемое наказание лишение свободы на срок до четырех лет (если действия хакеров повлекли тяжкие последствия до семи лет) с выплатой штрафа в размере до двухсот тысяч рублей.

В случае, если данные правонарушения были совершены группой лиц по предварительному сговору либо с использованием служебного положения, нарушитель может также лишиться права занимать определенные должности на срок до трех лет.

Нарушение хакерами авторских и смежных прав предполагает штраф в размере до двухсот тысяч рублей, которые могут быть заменены исправительными работами либо лишением свободы на срок до двух лет.

Хакерская деятельность в компьютерной сети может подпадать под действие статей 272 и 274 УК РФ. Неправомерный доступ к компьютерной информации в случае, если действия лица повлекли уничтожение, блокирование, модификацию либо копирование компьютерной информации, предполагает наказание в виде штрафа в размере до двухсот тысяч рублей либо ограничение свободы или принудительные работы на срок до двух лет.

В случае, если доказана корыстная заинтересованность нарушителя или нанесенный его действиями ущерб превышает один миллион рублей, штраф может вырасти до трехсот тысяч рублей, а срок ограничения свободы до четырех лет. Возможно также лишение свободы на срок до полугода.

Для группы лиц, наказание предполагает штраф в размере до пятисот тысяч рублей с лишением нарушителей права занимать определенные должности на срок до трех лет, а также лишение свободы на срок до пяти лет, а при возникновении тяжких последствий до семи лет.

В случае если в действиях нарушителя усматривается нарушение правил эксплуатации обработки или передачи охраняемой компьютерной информации либо информационно телекоммуникационных сетей, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации (статья 274 УК РФ), ему грозит лишение свободы на срок до двух лет. Эта мера может быть заменена выплатой штрафа в размере до пятисот тысяч рублей.

В случае если компьютер являлся средством совершения преступления, предусматриваемого иными статьями действующего законодательства, возможна ответственность хакеров и по другим статьям УК РФ.

Вывод:

Хакеры, как явление официально считается вне закона, но фактически это одна из движущих сил нашего общества по пути научно-технического прогресса.

Сегодня сообщество хакеров оформилось в особую социальную группу, деятельность которой направлена на урегулирование глобальных социальных и информатизационных процессов.

Благодаря тесному сотрудничеству хакеров между собой и информационной открытости и бескорыстности в процессе творческой деятельности происходит усовершенствование программного обеспечения и широкое внедрение их достижений в повседневную практику пользователей. Выполнение столь серьезных задач хакерами предполагает формирование у них специфических норм и правил взаимодействия, построение особой системы ценностей, создание внутригрупповой иерархии и выстраивание внешних социальных отношений.

Таким образом, хакеры, как члены организованного сообщества, чья деятельность направлена на созидание и развитие проектов, способствующих развитию информационного общества (как с технической, так и с социальной стороны), совершенно не соотносятся с теми характеристиками, которыми их наделяют средства массовой информации.

**Заключение проекта:**

К 2020 году программирование настолько глубоко вошло в быт, что люди перестали замечать, как изменилась жизнь. Сотни тысяч привычных вещей не существовали бы без программирования или были бы гораздо менее удобными в использовании. Привычные бытовые приборы: микроволновая печь, стиральная машина — работают благодаря заложенным в них программам.

Всего 50 лет назад невозможно было представить, как легко будет найти любую необходимую информацию, насколько экономнее станет использоваться время, затрачиваемое на решение некоторых задач.

Поначалу для каждого крохотного действия приходилось создавать программу с нуля. Сейчас же программ написано такое множество, что в их разнообразии трудно ориентироваться. Например, чтобы смонтировать клип, придётся потратить часы на изучение существующих видеоредакторов и выбор подходящего.

Наше время диктует новые условия буквально в каждой области деятельности. Если компания хочет облегчить жизнь себе и своим клиентам, обойти конкурентов, то будет внедрять компьютерные технологии. Музыкальная индустрия и кино, мультипликация и игры, мобильная связь, банковское дело, дизайн и журналистика — все области тесно переплетены с программированием и используют специальные программы на разных этапах работы.

**Список используемых источников:**

Абрамов, С.А. Математические построения и программирование / С.А. Абрамов. - М.: Наука, 2016. - 192 c.

Крамм Программирование в Access для "чайников" / Крамм, Роб. - М.: Диалектика, 2016. - 304 c.

Э. Фримен, Э. Робсон – Изучаем программирование на JavaScript

Интернет-ресурсы.

<https://ria.ru/20130808/955191308.html> - РИА Новости.

<https://rg.ru/2006/07/29/informacia-dok.html> - Закон об информации, информационных технологиях и защите информации.

Рис.1. CryEngine 3

Рис. 2. Kodu

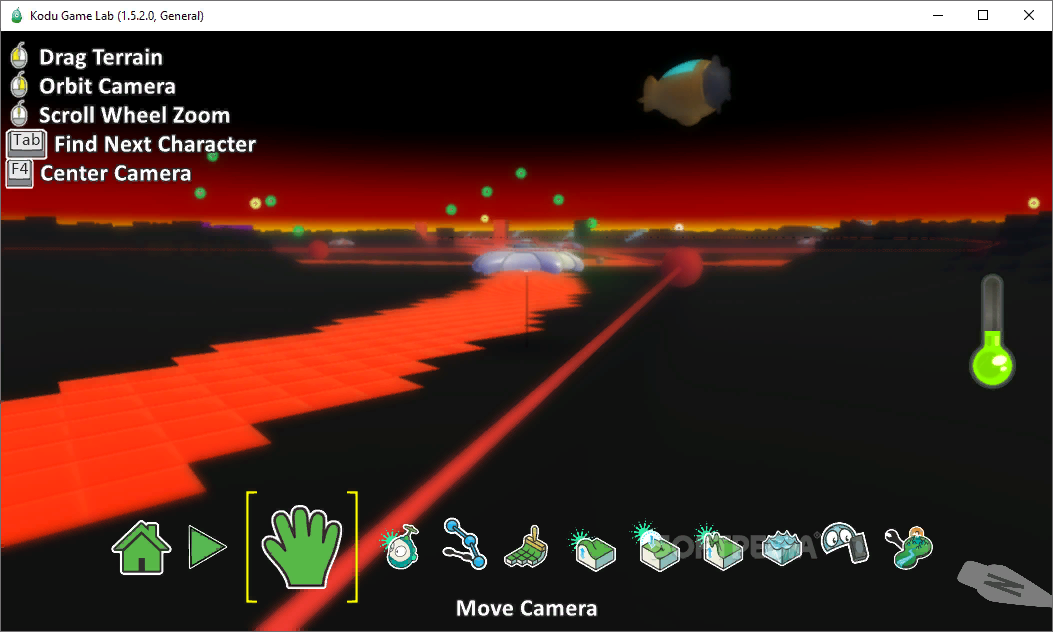


Рис. 2. 3D Rad



Рис. 3. Unity3d

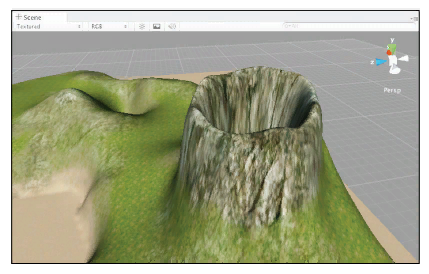


Рис. 4. Game Maker

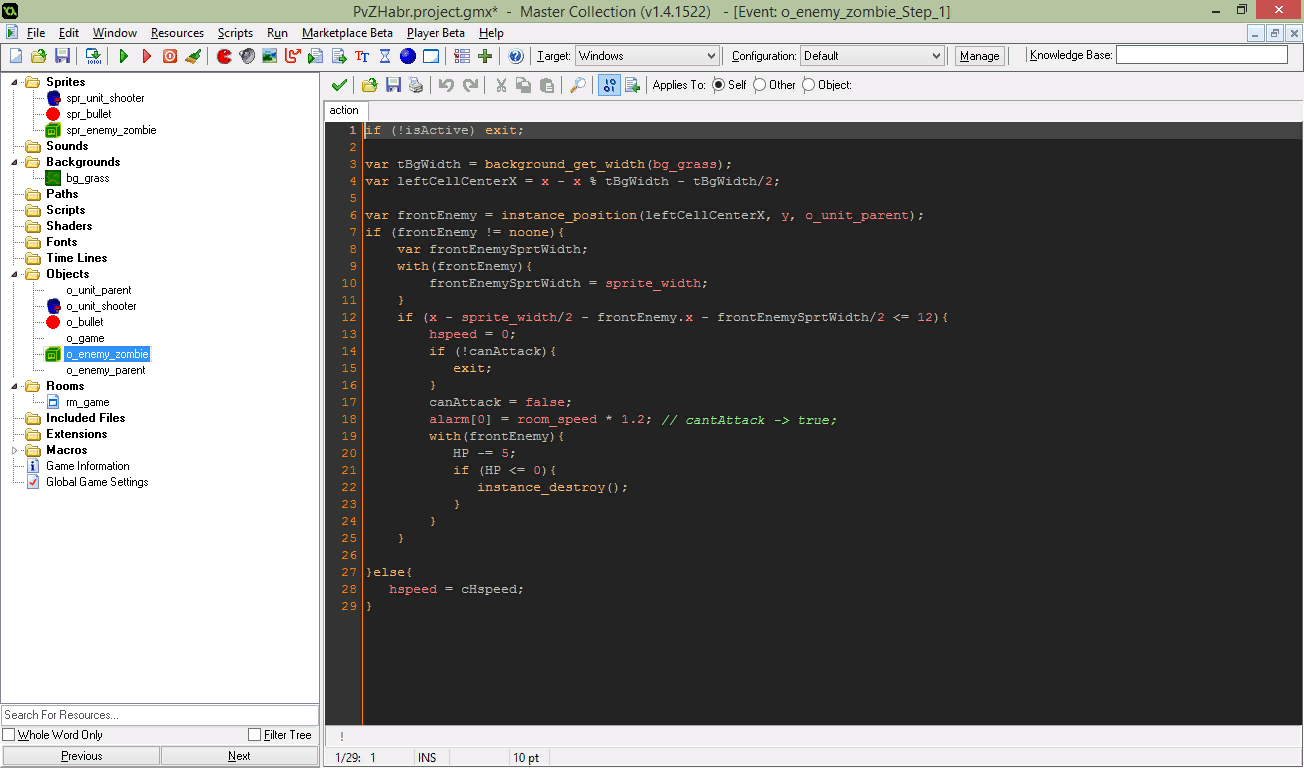


Рис.5. Visual Studio.

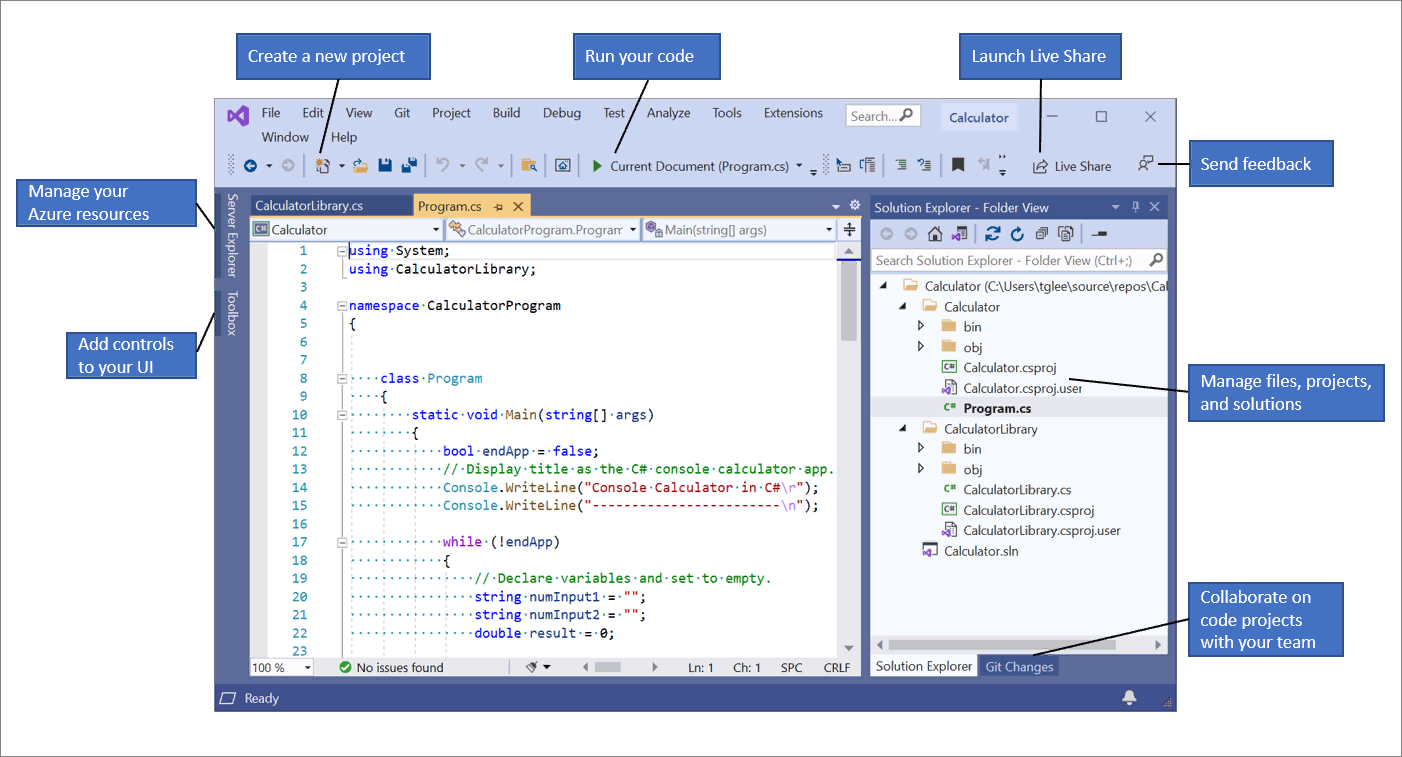


Рис.6. Android Studio

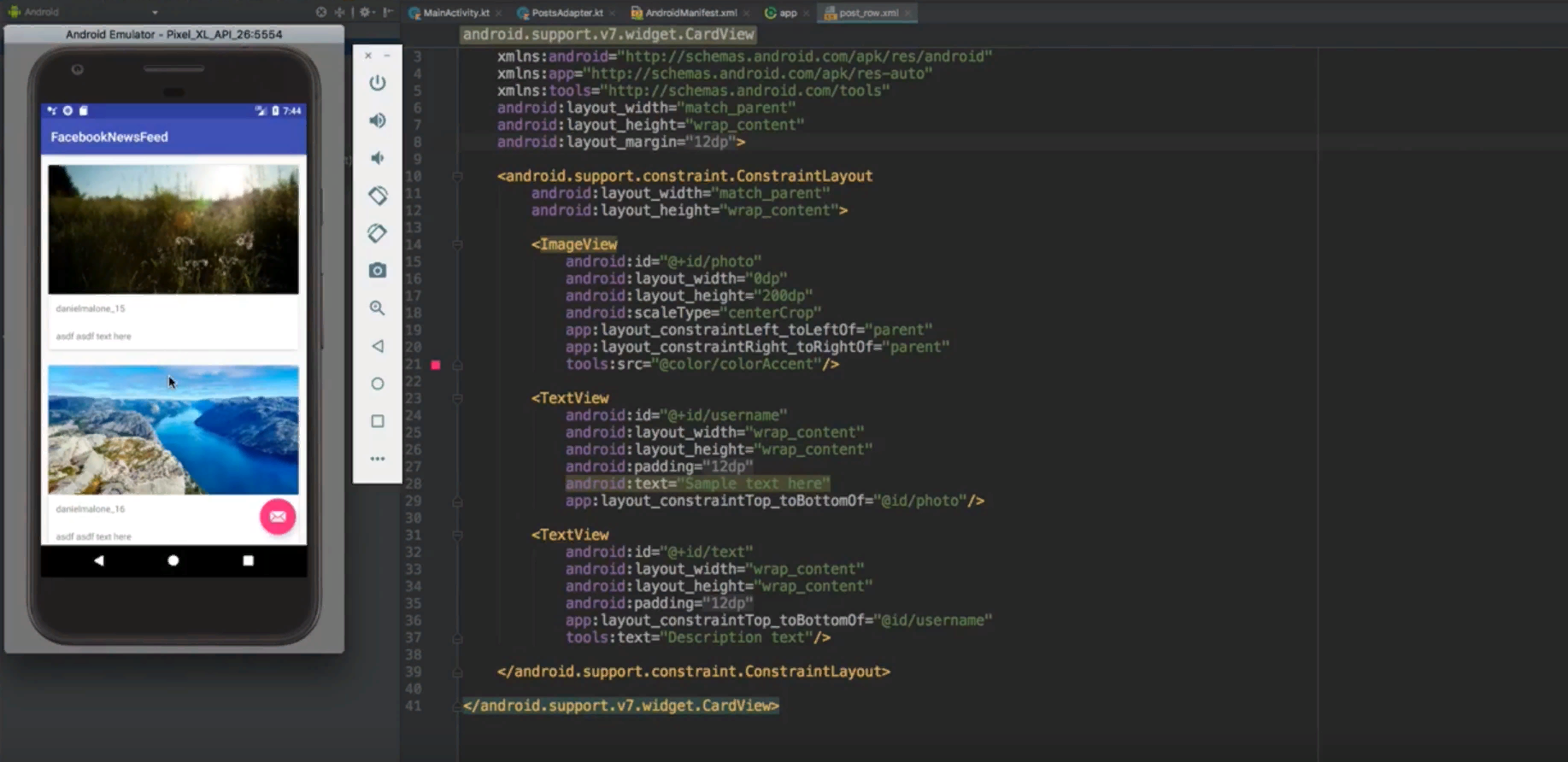


Рис.7. Мануэль Кастельс и Пекка Химанен

График 1.

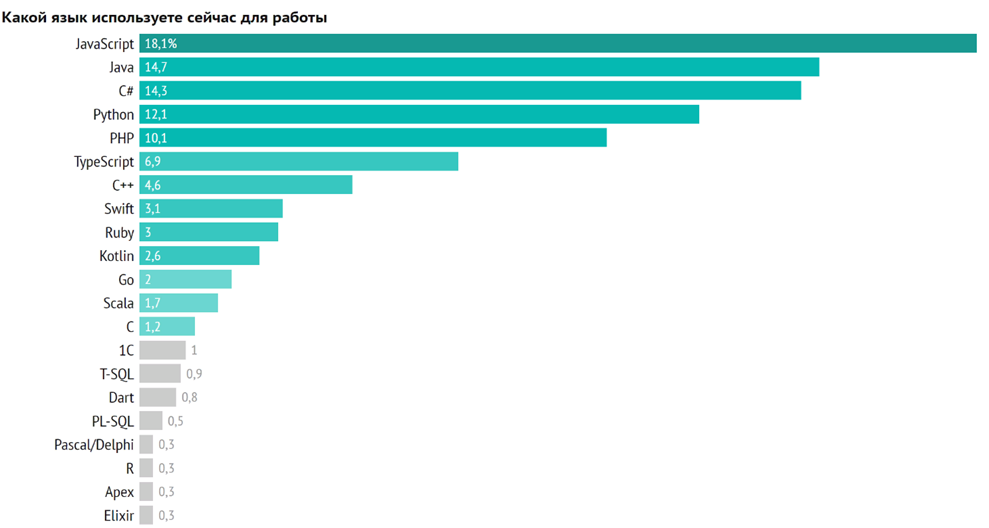


Диаграмма 1.

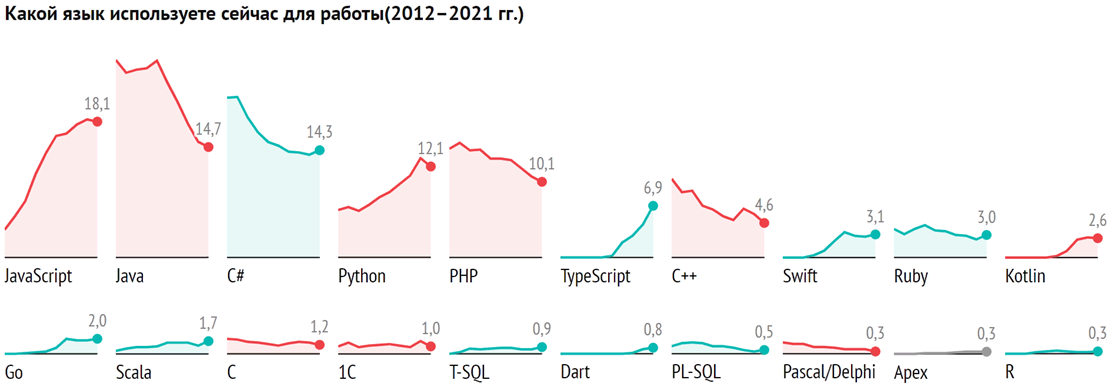


Диаграмма 2.

