ГБПОУ «Дзержинский педагогический колледж»

**Лекции по учебной дисциплине**

**ЕН 02. Информатика и ИКТ в профессиональной деятельности**

|  |  |
| --- | --- |
| **Одобрена на заседании предметно - цикловой комиссии** **преподавателей спец. «Дошкольное образование» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****Протокол №\_\_\_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_\_г.****Председатель ПЦК \_\_\_\_\_\_\_\_\_\_\_\_\_ /Н.Ю. Казачкова/****Составитель: Кузнецова Н.В., Блинкова А.С.** | **Методические разработки лекций составлены в соответствии с требованиями федеральных государственных образовательных стандартов среднего профессионального образования по спец. 44.02.01. Дошкольное образование**  |

Методические разработки лекций по учебной дисциплине ЕН.02. Информатика и ИКТ в профессиональной деятельности специальность 44.02.01. Дошкольное образование содержат план лекций в соответствии с рабочей программой учебной дисциплины. Каждая лекция содержит план, полный текст лекции, список литературы, вопросы и задания для проверки и самоконтроля.

**Содержание**

|  |  |  |
| --- | --- | --- |
| **Наименование разделов и** **тем** | **Содержание учебного материала** | **Стр.** |
| **Тема 1. Правила техники безопасности и гигиенические требования при использовании средств ИКТ в образовательном процессе**  | 1.Инструкция по охране труда в кабинете информатики. Гигиенические требования при использовании средств ИКТ в образовательном процессе. Санитарно-эпидемиологические правила и нормативы. |  |
| **Тема 9. Информационные ресурсы сети Интернет в профессиональной деятельности** | 1. Безопасность при работе в сети Интернет
 |  |

**Пояснительная записка**

Методические разработки лекций по дисциплине Информатика и ИКТ в профессиональной деятельности разработаны в соответствии с рабочей программой учебной дисциплины ЕН.02. Информатика и ИКТ в профессиональной деятельности.

Содержание методических разработок лекций по данной дисциплине соответствует требованиям Федерального Государственного Образовательного Стандарта среднего профессионального образования нового поколения.

Цель: подготовить обучающихся по углубленной подготовке к освоению профессиональных модулей ОПОП по специальности «Преподавание в начальных классах» и овладению профессиональными компетенциями (ПК), соответствующими основным видам профессиональной деятельности:

Задачи:

1.Обеспечить глубокую теоретическую подготовку.

2.Приобщать к самостоятельной учебно – исследовательской деятельности.

3.Формировать готовность к постоянному повышению уровня профессиональной и общей культуры.

По учебному плану рекомендуемое количество часов на освоение программы дисциплины следующее: максимальная учебная нагрузка обучающегося **126 часов**, в том числе:

- обязательное аудиторная учебная нагрузка обучающегося **84 часов**:

-лекции – **4 часа**

- практические занятия **80 часов**.

В соответствии с требованиями ФГОС СПО по специальности 44.02.01 Дошкольное образование в ходе изучения дисциплины. ЕН.02 Информатика и ИКТ в профессиональной деятельности выпускник должен обладать следующими общими и профессиональными компетенциями:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, определять методы решения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Оценивать риски и принимать решения в нестандартных ситуациях.

ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.

ОК 6. Работать в коллективе и команде, взаимодействовать с руководством, коллегами и социальными партнерами.

ОК 7. Ставить цели, мотивировать деятельность воспитанников, организовывать и контролировать их работу с принятием на себя ответственности за качество образовательного процесса.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Осуществлять профессиональную деятельность в условиях обновления ее целей, содержания, смены технологий.

ПК 3.2. Проводить занятия с детьми дошкольного возраста

ПК 3.5. Вести документацию, обеспечивающую организацию занятий

ПК 5.1. Разрабатывать методические материалы на основе примерных с учетом особенностей возраста, группы и отдельных воспитанников.

ПК 5.2. Создавать в группе предметно-развивающую среду.

ПК 5.3. Систематизировать и оценивать педагогический опыт и образовательные технологии в области дошкольного образования на основе изучения профессиональной литературы, самоанализа и анализа деятельности других педагогов.

ПК 5.4. Оформлять педагогические разработки в виде отчетов, рефератов, выступлений.

ПК 5.5. Участвовать в исследовательской и проектной деятельности в области дошкольного образования.

Дисциплина Информатика и ИКТ в профессиональной деятельности (ЕН.02) входит в математический и общий естественнонаучный цикл (ЕН.00.)

В результате освоения учебной дисциплины Численные методы в программировании обучающийся **должен:**

**уметь:**

* соблюдать правила техники безопасности и гигиенические рекомендации при использовании средств ИКТ в профессиональной деятельности;
* создавать, редактировать, оформлять, сохранять, передавать информационные объекты различного типа с помощью современных информационных технологий для обеспечения образовательного процесса:
* создавать, загружать, редактировать и сохранять графические изображения в графическом редакторе Paint; выполнять основные действия над объектами; моделировать в графическом редакторе;
* создавать, редактировать, оформлять, сохранять мультимедийные презентации; создавать презентацию, совмещающую изображение, звук, анимацию и текст; создавать интерактивную презентацию;
* набирать и редактировать текст в текстовом процессоре MS Word; форматировать символы, абзацы, страницы, разделы документа; вставлять и редактировать символы, формулы; создавать нумерованные и маркированные списки; вставлять, создавать, редактировать графические объекты; создавать и форматировать таблицы; работать с колонками, буквицей, нумеровать страницы документа;
* вводить и редактировать данные в ячейке электронной таблицы; выполнять основные операции манипулирования с фрагментами электронной таблицы: копирование, удаление, вставка, сортировка; форматировать данные и ячейки; использовать в формулах абсолютные и относительные ссылки; строить, редактировать и форматировать диаграммы;
* создавать и редактировать таблицы, формы, запросы, отчеты в среде MS Access;
* создавать и редактировать буклеты, плакаты, календари, визитные карточки и приглашения в среде MS Publisher
* использовать сервисы и информационные ресурсы сети Интернет в профессиональной деятельности: работать с одной из программ – «браузеров»; осуществлять поиск информации в компьютерных сетях; работать с информационными ресурсами и сервисами сети Интернет;
* осуществлять отбор обучающих программ в соответствии с возрастом и уровнем психического развития воспитанников;

**знать:**

* правила техники безопасности и гигиенические требования при использовании средств ИКТ в образовательном процессе;
* основные технологии создания, редактирования, оформления, сохранения, передачи и поиска информационных объектов различного типа (текстовых, графических, числовых и т.п.) с помощью современных программных средств:
* назначение, область применения, основные возможности, интерфейс MS Paint; основные форматы графических файлов; отличие растрового графического редактора от векторного; примеры растровых и векторных графических редакторов;
* назначение, область применения, основные возможности, интерфейс MS PowerPoint; сущность понятия «мультимедиа технологии»;
* назначение, область применения, основные возможности и достоинства, интерфейс MS Word; основные форматы текстовых файлов; основные элементы текстового документа; правила набора текста в текстовом процессоре MS Word; виды списков, виды форматирования, типы графических объектов в текстовом процессоре MS Word;
* назначение, область применения, основные возможности, интерфейс MS Excel; примеры основных функций (математических, логических), используемых при записи формул в электронную таблицу; основные информационные единицы электронной таблицы: ячейки, строки, столбцы, диапазоны и способы их идентификации; отличие абсолютных ссылок от относительных, используемых в электронных таблицах; типы данных, заносимых в электронную таблицу;
* назначение, область применения, основные возможности, интерфейс MS Access; типы баз данных и основные элементы баз данных;
* назначение, область применения, основные возможности, интерфейс MS Publisher
* возможности использования ресурсов сети Интернет для совершенствования профессиональной деятельности, профессионального и личностного развития: роль и состояние компьютерных коммуникаций в современном мире; правила работы в сети, правила общения с помощью сети; правила защиты информации от несанкционированного использования;
* программное обеспечение персонального компьютера (ПК), применяемое в профессиональной деятельности.

**Разработка лекций**

**Тема 1. Правила техники безопасности и гигиенические требования при использовании средств ИКТ в образовательном процессе**

**Инструкция по охране труда в кабинете информатики. Гигиенические требования при использовании средств ИКТ в образовательном процессе. Санитарно-эпидемиологические правила и нормативы.**

План:

1.Требования СанПиН

2. Влияние средств ИКТ на детей младшего школьного возраста

3.Снятие напряжения от воздействия средств ИКТ

4. Построение урока

Санитарно-гигиенические требования к использованию ИКТ в начальной школе.

Согласно нормам и требованиям СанПиН рекомендуемая непрерывная длительность работы, связанной с фиксацией взора непосредственно на экране, на уроке не должна превышать для обучающихся в I классе – 10 минут, во 2-4 классах - 15 минут, прослушивание аудиозаписи – 20 минут. Возможно использовать компьютер фрагментами по 2-3 минуты, распределяя время взаимодействия детей с компьютерными программами в режиме фронтальной деятельности на протяжении всего урока. Оптимальное количество занятий с использованием ПК в течение учебного дня для обучающихся 1-4 классов составляет 1 урок Внеучебные занятия с использованием ПК рекомендуется проводить не чаще 2 раз в неделю общей продолжительностью для обучающихся в 1-4 классах - не более 60 мин.

Занятия в кружках с использованием ПК следует организовывать не раньше, чем через 1 час после окончания учебных занятий в школе. Это время следует отводить для отдыха и приема пищи.

Для учащихся начальной школы занятия в кружках с использованием компьютерной техники должны проводиться не чаще двух раз в неделю. Продолжительность одного занятия - не более 60 минут. После 10-15 минут непрерывных занятий за ПК необходимо сделать перерыв для проведения физкультминутки и гимнастики для глаз.

Несомненно, что утомление во многом зависит от характера компьютерных занятий. Наиболее утомительны для детей компьютерные игры, рассчитанные, главным образом, на быстроту реакции. Поэтому не следует отводить для проведения такого рода игр время всего занятия. Продолжительное сидение за компьютером может привести к перенапряжению нервной системы, нарушению сна, ухудшению самочувствия, утомлению глаз. Поэтому для учащихся этого возраста допускается проведение компьютерных игр только в конце занятия длительностью не более 10 минут.

Для уменьшения зрительного напряжения важно следить за тем, чтобы изображение на экране компьютера было четким и контрастным. Необходимо также исключить возможность засветки экрана, поскольку это снижает контрастность и яркость изображения. При работе с текстовой информацией предпочтение следует отдавать позитивному контрасту: темные знаки на светлом фоне. Расстояние от глаз до экрана компьютера должно быть не менее 50 см. Одновременно за компьютером должен заниматься один ребенок, так как для сидящего сбоку условия рассматривания изображения на экране резко ухудшаются.

Оптимальные параметры микроклимата в дисплейных классах следующие: температура - 19-21° С, относительная влажность - 55-62 %.

Перед началом и после каждого академического часа учебных занятий компьютерные классы должны быть проветрены, что обеспечит улучшение качественного состава воздуха. Приобщение детей к компьютеру следует начинать с обучения правилам безопасного пользования, которые должны соблюдаться не только в школе, но и дома.

Существует влияние частоты использования аудиовизуальных средств на эффективность процесса обучения. Оно обусловлено тем, что средства ИКТ влияют на оценочно-мотивационную сферу личности. Если средства ИКТ используются редко, то каждое их применение превращается в чрезвычайное событие, вновь создаёт у обучающихся повышенное эмоциональное возбуждение, мешающее восприятию и усвоению учебного материала. Наоборот, слишком частое использование в течение многих уроков подряд приводит к потере учащимися интереса к ним.

Оптимальная частота и длительность применения средств ИКТ определяется возрастом учащихся, характером учебного предмета и необходимостью их использования в познавательной деятельности учащихся.

Эффективность применения ИКТ зависит также от этапа урока. Использование их в начале урока (на 5 минут) сокращает подготовительный период с 3 до 0,5 минуты, а усталость и потеря внимания наступают на 5-10 минут позже обычного. Использование ИКТ в интервалах между 30-й и 35-й минутой позволяет поддерживать устойчивое внимание учащихся практически в течение всего урока. Это обусловлено тем, что в течение каждого урока у учащихся периодически изменяются характеристики зрительного и слухового восприятия (их острота, пороги, чувствительность), внимание, утомляемость. При монотонном использовании одного средства обучения нового материала у учащихся уже к 30-й минуте возникает запредельное торможение, почти полностью исключающее восприятие информации. В то же время правильное чередование средств и методов обучения может исключить это явление. Периоды напряжённого умственного труда и волевых усилий необходимо чередовать с эмоциональной разрядкой, релаксацией зрительного и слухового восприятия.

Для профилактики зрительного и общего утомления на уроках необходимо соблюдать следующие рекомендации.

• Оптимальная продолжительность непрерывных занятий с компьютером для учащихся 2-4 классов должна быть не более 15 минут.

• С целью профилактики зрительного утомления детей после работы на персональных компьютерах рекомендуется проводить комплекс упражнений для глаз, которые выполняются сидя или стоя, отвернувшись от экрана, при ритмичном дыхании, с максимальной амплитудой движений глаз. Для большей привлекательности их можно проводить в игровой форме.

Примерный комплекс упражнений для глаз.

1. Закрыть глаза, сильно напрягая глазные мышцы, на счет 1-4, затем раскрыть глаза, расслабить мышцы глаз, посмотреть вдаль на счет 1-6. Повторить 4-5 раз.

2. Посмотреть на переносицу и задержать взор на счет 1 -4. До усталости глаза не доводить. Затем открыть глаза, посмотреть вдаль на счет 1-6. Повторить 4-5 раз.

3. Не поворачивая головы, посмотреть направо и зафиксировать взгляд на счет 1-4, затем посмотреть вдаль прямо на счет 1-6. Аналогичным образом проводятся упражнения, но с фиксацией взгляда влево, вверх и вниз. Повторить 3-4 раза.

4. Перевести взгляд быстро по диагонали: вправо вверх - налево вниз, потом прямо вдаль на счет 1-6; затем налево вверх - направо вниз и посмотреть вдаль на счет 1-6. Повторить 4-5 раз.

Проведение гимнастики для глаз не исключает проведение физкультминутки. Регулярное проведение упражнений для глаз и физкультминуток эффективно снижает зрительное и статическое напряжение. Занятия с ПК независимо от возраста детей должны проводиться в присутствии воспитателя или педагога.

При разработке урока с использованием компьютерных технологий уделяется особое внимание заботе о здоровье учащихся. ИКТ должно выполнять определенную образовательную функцию: помочь ребёнку разобраться в потоке информации, воспринять её, запомнить, а ни в коем случае не подорвать здоровье. Компьютеризация должна касаться лишь той части учебного процесса, где это необходимо.

**Литература**

1. Информатика [Электронный ресурс] : учебное пособие для студентов первого курса очной и заочной форм обучения / . — Электрон. текстовые данные. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2015. — 158 c. — 978-5-8265-1490-0. — Режим доступа: <http://www.iprbookshop.ru/64094.html>
2. Алексеев А.П. Сборник лабораторных работ по дисциплине «Информатика». Часть 1 [Электронный ресурс] : методические указания к проведению лабораторных занятий по дисциплине «Информатика», для студентов первого курса специальностей 10.03.01 и 10.05.02. / А.П. Алексеев. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015. — 305 c. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/71878.html>

**Вопросы и задания для проверки и самоконтроля**

1.Сколько по времени можно работать за компьютером ребенку 2 класса?

2. Требования к кабинету информатики.

3. Какое воздействие оказывают средства ИКТ на детей?

4. Какие упражнения помогают снять напряжение после работы с ИКТ?

**Тема 9. Информационные ресурсы сети Интернет в профессиональной деятельности**

**Безопасность при работе в сети Интернет**

План

1. Опасности в сети Интернет

2. Способы защиты

С каждым годом молодежи в интернете становиться больше, и как правило это одна из категорий самых активных пользователей Рунета.

Социальные сети — это один из самых востребованных ресурсов Интернета. Благодаря им  сделан огромный шаг вперёд в деле [информатизации](https://infourok.ru/go.html?href=https%3A%2F%2Fwww.kv.by%2Fpost%2F1050286-obzor-zakonodatelstva-respubliki-belarus-v-sfere-informatizacii-za-dekabr-2016-goda) общества. Это настоящий подарок для любителей интерактивного общения. Казалось бы, чем можно навредить человеку, сидя за монитором? Между тем, помимо огромного количества возможностей, интернет несет и проблемы.

**1 ролик «Интернет безопасность»**

**Компьютерные вирусы**
Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю. В большинстве случаев распространяются вирусы через интернет.
**Методы защиты от вредоносных программ:**
• Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
• Постоянно устанавливай обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
• Ограничь физический доступ к компьютеру для посторонних лиц;
• Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
• Работай на своем компьютере под правами пользователя, а не администратора.
• Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
• Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.
**Сети WI-FI**
Да, бесплатный интернет-доступ в общественных местах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.
**Советы по безопасности работе в общедоступных сетях Wi-fi:**• Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
• Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
• При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
• Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
• Ипользуй только защищенное соединение через HTTPS, а не НТТР, т.е. при наборе веб-адреса вводи именно «https://»;
• В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.
**Социальные сети**
Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.
**Основные советы по безопасности в социальных сетях:**
• Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
• Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
• Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
• Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
• Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
• При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
• Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

**Видео «Шокирующая правда о социальных сетях»**

Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Основные советы по безопасной работе с электронными деньгами:

• Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

• Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

• Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль.

• Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

• Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

• Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13»;

• Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

• Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

• Если есть возможность написать самому свой личный вопрос, используй эту возможность;

• Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

• Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

• После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

• Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

• Управляй своей киберрепутацией;

• Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

• Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

• Соблюдай свой виртуальную честь смолоду;

• Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

• Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

• Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

• Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

• Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

• Необходимо обновлять операционную систему твоего смартфона;

• Используй антивирусные программы для мобильных телефонов;

• Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

• После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

• Периодически проверяй какие платные услуги активированы на твоем номере;

• Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

• Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивиfшь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей.

Основные советы по борьбе с фишингом:

• Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

• Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

• Используй сложные и разные пароли.

• Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

• Установи надежный пароль (PIN) на мобильный телефон;

• Отключи сохранение пароля в браузере;

**Цифровая репутация**

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети. Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

 **Основные советы по защите цифровой репутации:**

* Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
* В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»
* Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

**Подставная работа**

*Интернет* уже настолько стал частью нашей жизни, что никого уже не удивишь различными способами *Интернет* заработка. Тем более, что заработок в Интернете во многом может превосходить заработок в реальной жизни и на реальных работах. Есть множество сайтов, которые якобы предлагают различную легкую работу пользователю за неплохие деньги. И вроде вначале не возникает никаких вопросов, насколько может быть законна такая работа, ведь с первого взгляда все довольно честно. Также не возникает у новоиспеченных работников вопросов о том, как обстоят дела с безопасностью на таких сайтах, и не может ли быть сама работа опасной для персональных данных пользователя. Одним из примеров такой работы может быть работа, которая заключается в том, что *пользователь* регистрируется на различных сервисах под своими данными и потом передает эти аккаунты работодателю. Казалось бы, на первый взгляд, нет ничего необычного, работа несложная, *пользователь* делает регистрации, а работодатель платит за это деньги. Но только на первый взгляд такая работа выглядит честной и порядочной, на самом деле работодатель может использовать такие аккаунты для того, чтобы распространять вредоносные программы. Ваш аккаунт может быть использован в любых целях, которые нужны злоумышленнику, вплоть до рекламы каких-либо порнографических вещей, что уже само *по* себе является аморальным.

Также некоторые злоумышленники предлагают работу *по* распознаванию букв с картинки (капча- *распознавание* символов с картинки). При этом они говорят о том, что ничего нелегального в этом нет, а само *распознавание* производится в целях какого-либо научного исследования. *Пользователь* при этом может не знать о том, что такой труд может быть использован для того, чтобы обходить защиту многих сайтов от автоматической регистрации. То есть на стороне злоумышленника создаются различные аккаунты на сайте, основной преградой которых остается как раз капча, которую уже самостоятельно заносят пользователи. Естественно, такие аккаунты могут быть использованы как угодно и в любых целях.

Стоит отметить и то, что не все подобные предложения о работе могут являться предложениями от злоумышленников. Некоторые из таких предложений могут быть предложениями серьезных компаний, которые действительно заинтересованы в различных научных исследованиях в области распознавания символов. Так же и предложения, которые связаны с регистрацией на различных сайтах, вполне могут быть предложениями, которые происходят от вполне честных людей с честными намерениями. Для того, чтобы понять добросовестность человека, который предлагает работу, необходимо проверить его в различных источниках на наличие положительных или отрицательных отзывов на этого человека. Если доминирует большое количество отрицательных отзывов о человеке, то будет лучше поискать другую работу в сети *Интернет*. Также, если у новоиспеченного работодателя нет каких-либо документов, подтверждающих его причастность к крупной компании или научной лаборатории, но этот работодатель говорит, что он на самом деле причастен, то такому работодателю лучше не доверять.

**Литература**

1. Информатика [Электронный ресурс] : учебное пособие для студентов первого курса очной и заочной форм обучения / . — Электрон. текстовые данные. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2015. — 158 c. — 978-5-8265-1490-0. — Режим доступа: <http://www.iprbookshop.ru/64094.html>
2. Алексеев А.П. Сборник лабораторных работ по дисциплине «Информатика». Часть 1 [Электронный ресурс] : методические указания к проведению лабораторных занятий по дисциплине «Информатика», для студентов первого курса специальностей 10.03.01 и 10.05.02. / А.П. Алексеев. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015. — 305 c. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/71878.html>

**Вопросы и задания для проверки и самоконтроля**

1. Перечислите опасности сети Интернет
2. Какие меры безопасности вы знаете?