Государственное бюджетное профессиональное образовательное учреждение

«Дзержинский техникум бизнеса и технологий»

**ПРОЕКТ**

**внеурочного мероприятия**

**УРОК ИНФОРМАЦИОННОЙ** **БЕЗОПАСНОСТИ.**

**ЦИФРОВАЯ ГИГИЕНА**

Разработала: Радевич Любовь Ивановна,

преподаватель информационных технологий и профессиональных модулей

Дзержинск

2023г.**Содержание**

[Введение 3](#_Toc136353629)

[1 Паспорт 4](#_Toc136353630)

[2 План внеклассного мероприятия 4](#_Toc136353631)

[3 Самоанализ внеклассного мероприятия 6](#_Toc136353632)

[Список источников информации 7](#_Toc136353633)

[Приложение А Словарь используемых понятий 8](#_Toc136353634)

[Приложение Б Задания теста 10](#_Toc136353635)

Введение

Министерством просвещения Российской Федерации подготовлен календарь образовательных событий на 2022/2023 учебный год, приуроченных к государственным и национальным праздникам России, памятным датам и событиям российской истории и культуры. Именно этот календарь стал основой для проведения тематических классных часов, организации спецпроектов и поездок, проведения школьных и внеклассных мероприятий.

В течение всего 2022/2023 учебного года во всех образовательных организациях страны проводятся открытые уроки ОБЖ.

Понимая, как важно привить студентам правила грамотного поведения в Интернете, как важно сформировать понимание ценности человеческой жизни в ГБПОУ ДТБТ на учебных занятиях и во внеурочной деятельности на протяжении семи лет проводится комплекс мероприятий, включающий проведение Единого урока по основам информационной безопасности, викторины, конкурсов плакатов и листовок, тестирование на сайте «Сетевичок» и «Лаборатории Касперского», участие в вебинаре «Учителя, родители и дети в цифровом пространстве».

Урок информационной безопасности «Цифровая гигиена» имеет цель – представить обучающимся информацию об угрозах и правилах поведения в цифровой среде. Тема, цель и задачи мероприятия соответствует требованиям ФГОС СПО (в том числе ФГОС СПО по ТОП-50) и программы воспитания.

Проводимое мероприятие направленно на формирование общих и профессиональных компетенций (знать основные угрозы и методы обеспечения информационной безопасности; уметь использовать информационные ресурсы для поиска и хранения информации, уметь применять методы и средства защиты информации), личностных результатов воспитания (ЛР7, ЛР10, ЛР16), Soft Skils аналитической группы.

Проект внеурочного занятия разработан с учётом информационных, технических и коммуникативных аспектов информационной безопасности. Используемое оснащение соответствует требованиям ФГОС СПО, задачам мероприятия и программам воспитания.

Методические материалы разработаны на основе учебных изданий АО «Издательство «Просвещение»». Материалы могут быть использованы преподавателями ИКТ, классными руководителями, педагогами дополнительного образования.

1 Паспорт

|  |  |
| --- | --- |
| **1 Наименование внеклассного мероприятия** | Урок информационной безопасности.  Цифровая гигиена |
| **2 Группы** | 2 курс |
| **3 Форма проведения** | Внеурочное аудиторное мероприятие |
| **4 Цель мероприятия** | Актуализировать информацию о правилах поведения в цифровой среде  Научить анализировать информационный материал с целью обеспечения безопасности жизнедеятельности |
| **5 Задачи мероприятия** |  |
| Образовательные | - знают правила безопасного обращения с компьютером и основные правила по защите от вредной и опасной информации;  - имеют понятия о внешних и внутренних киберугрозах |
| Воспитательные | - проявляют уважение и навыки этичного отношения к собеседникам и принимают меры защиты от кибермошенников |
| Развивающие | - узнают схему работы кибермошенников, основные виды интернет-афер. |
| **6 Оборудование и оснащение мероприятия** | Персональный компьютер, подключенный к сети Интернет,;  Образовательная платформа «Просвещение» |
| **7 Средства обучения** | Видеоролик «Цифровая гигиена»  Тестовый контроль on-line |
| **8 Основные термины и понятия** | Компьютер, смартфон, игровая приставка, наушники, электромагнитное излучение, информационная безопасность, кибербуллинг, троллинг, преследование, использование личной информации, агрессия, буллинг, мошенничество, вымогательство |

2 План внеклассного мероприятия

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Этап** | **Деятельность**  **преподавателя** | **Деятельность**  **обучающихся** | **Методы и средства**  **обучения** | **Ожидаемый**  **результат** |
| 1. Предварительная подготовка | Объявление на сайте DTBT Moodle | Изучение методических материалов [[1]](#footnote-1) | Дистанционая форма обучения | Активность студентов |
| Организационный момент  3 мин | Оценивает готовность студентов к мероприятию | Анализируют предлагаемое программное обеспечение  Организуют рабочее место. | Интерактивная форма обучения | Организация внимания всех студентов, готов- ность группы к просмотру |
| Мотивационная установка  7 мин | Мотивирует, задает, наво-дящие вопросы для постановки цели и задач. | Высказывают свои предполо-жения и догад-ки, делают вы-воды. Ставят цель, формули-руют задачи. | Эвристическая беседа. | Студенты замотивированы |
| Просмотр видео ролика  15 мин | Демонстрирует видео «Цифровая гигиена»[[2]](#footnote-2) | Смотрят видео | Наглядно-демонстрационный | Активизация мыслительной деятельности. Аналитическая, критическая составляющая |
| Проверка усвоения информации  Тестирование  12 мин | Организует тестирование студентов Подготавливает бланк тестирования[[3]](#footnote-3). | Заполняют форму теста | Интерактивная форма обучения | Удовлетворенность полученными знаниями, разрешение возникших проблем |
| Рефлексия  8 мин | Предлагает студентам высказаться о просмотренном материале  Поддерживает адекватную оценку студентов | Высказываются о видеомате-риале, слушают, осмысливают.  Сохраняют на телефон памятку (Рисунок 1) | Интерактивная форма обучения | Положительная оценка деятельности и эффективности самостоятельной работы студентов |



Рисунок 1

3 Самоанализ внеклассного мероприятия

Мероприятие было подготовлено целенаправленно для студентов, изучающих информационные технологии в профессиональной деятельности.  Мероприятия проведено форме беседы, просмотра видеофильма, интерактивного тестирования и рефлексии в виде обмена мнениями.  Оно входит в систему методической работы и является одной из форм работы по защите обучающихся и их личных данных.

Мероприятие носит систематический характер. Подготовка  к занятию осуществлялась  в течение 1 семестра, подготавливались необходимые материалы для работы, оборудование.

В процессе подготовки предусматривалась необходимость формирования общих компетенций (ОК2-ОК6) и SoftSkils аналитической группы (умение работать с информацией, компьютерная грамотность).

В ходе подготовки и проведения мероприятия были соблюдены гигиенические требования: занятие организовано и проводилось в оборудованном кабинете.

Деятельность преподавателя и деятельность обучающихся организована слаженно. Начиналось мероприятие с приветствия преподавателя и постановки цели, с акцентом на необходимость формирования информационной культуры. Студенты нацелены на решение ситуационных задач и сотрудничество с преподавателем.

Мероприятие способствовало организации содержательного досуга обучающихся, созданию доброжелательной атмосферы, положительного эмоционального настроения, познавательной активности, результативности усвоения информации.



Рисунок 2

По ходу мероприятия обучающиеся проявили активность. Общение носило неформальный характер.

Длительность занятия  и информационная нагрузка соответствовала особенностям студентов и профилю обучения и специальности, спланирована обратная связь.

Внеаудиторная самостоятельная работа выполнялась обучающимися с использованием общего программного обеспечения.

В заключение мероприятия подведен итог, по результатам тестирования двадцати студентам выданы сертификаты. Пример сертификата приведен на рисунке 2.

Содержание внеурочного мероприятия полностью соответствует современным требованиям ФГОС. Взаимодействие между преподавателем и студентами можно охарактеризовать как демократическое.

Считаю, что поставленная цель достигнута.

Преподаватель ИКТ и ПМ Радевич Л.И.

Список источников информации

1. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 c. — ISBN 978-5-94836-612-8. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/108023
2. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт : монография / Л. Л. Ефимова, С. А. Кочерга. — Москва : ЮНИТИ-ДАНА, 2017. — 239 c. — ISBN 978-5-238-02405-9. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/81631
3. Методические рекомендации педагогу по организации и проведению Всероссийского урока безопасности. Режим доступа: https://safetylesson.prosv.ru/\_data/personal/379/metod-posobie-information-security23.pdf
4. Словарь терминов по информационной безопасности. Режим доступа: https://ib-bank.ru/glossary/

Приложение А   
Словарь используемых понятий

**Социальная инженерия** — приёмы, направленные на получение несанкционированного доступа к конфиденциальной информации и основанные на знании особенностей психологии людей.

Спам — массовая рассылка не запрошенных пользователем электронных писем и сообщений в мессенджерах. Как правило, спам-сообщения носят рекламный или агитационный характер. Спам может нанести вред компьютеру и причинить неудобства его пользователю, так как на очистку почтового ящика уходит значительное количество времени, а открытие некоторых сообщений может повлечь за собой установку вредоносного ПО.

Фишинг (в переводе с английского дословно означает «выуживание») — рассылка писем от имени известных фирм или крупных организаций с целью получения доступа к конфиденциальным данным (логин, пароль) пользователя Сети.

**К**ибербуллинг - форма запугивания, насилия и травли детей с помощью телефонов и Интернета. Кибербуллинг опасен не меньше, чем издевательства в привычном понимании, ведь жертва кибербуллинга находится в большом психологическом напряжении, и не каждый ребёнок сможет его вынести самостоятельно.

Кибербуллинг включает в себя:

* анонимные угрозы — пересылка писем без подписи отправителя, содержащих угрозы, оскорбления, часто с использованием ненормативной лексики;
* преследование — рассылка неприятных писем своей жертве продолжительное время, которая в дальнейшем может вылиться в шантаж какими-либо фактами её жизни;
* использование личной информации — взлом электронной почты или страниц в социальных сетях для получения личной информации для шантажа или издевательств;
* флейминг — обмен эмоциональными репликами между агрессором (иногда их может быть несколько) и жертвой с целью получения удовольствия от нанесения оскорблений;

хипплейпинг — видеозаписи с издевательствами, которые «заливают» на ресурсы, где их сможет увидеть большое количество пользователей. Такие ролики, естественно, «заливаются» без согласия потенциальной жертвы.

«Нигерийская афера». Обычно пользователю приходит электронное письмо от незнакомца, которому срочно нужно перевести большую сумму денег из одной страны в другую (например, из Нигерии, отсюда и название). Жертве обещают немалое вознаграждение за помощь в переводе денег. Однако сначала просят перевести определённую сумму, чтобы оплатить банковские расходы, а как только перевод денег состоялся, мошенник исчезает.

«Лотерея». Пользователь получает письмо по электронной почте, в котором сообщается, что он выиграл в лотерею и что для получения выигрыша ему необходимо прислать свои данные. Жертву просят перечислить определенную сумму денег, чтобы покрыть банковские и другие расходы. После перечисления денег мошенник исчезает.

«Подружка». На электронную почту пользователя приходит письмо с просьбой о знакомстве. Часто во вложении имеется фотография красивой девушки. В письме говорится, что она мечтает побывать в вашей стране и встретиться с вами, так как влюбилась с первого взгляда. Она хочет приехать незамедлительно, но в последний момент возникают какие-то проблемы, и ей необходимы деньги. Неудивительно, что после перевода названной суммы исчезают не только деньги, но и девушка.

«Приглашение на работу». Жертва получает письмо с приглашением на работу от иностранной компании, которая ищет финансовых агентов в её стране. Работа предельно проста, её можно выполнять, не выходя из дома, и при этом зарабатывать намного больше, чем сейчас. Если жертва соглашается с данным предложением, её просят прислать банковские реквизиты. Деньги перечисляют на счёт жертвы, а потом просят снять деньги со счёта и переслать их через систему перевода. Так жертва становится «переходным звеном» в цепочке мошенников, а когда дело попадает в полицию, жертва превращается в соучастника. В отличие от афер другого типа, в этом случае жертва даже не подозревает о том, что совершает преступление.

«Личные страницы». Мошенники похищают данные для входа на личные страницы, затем меняют логин, чтобы у хозяина страницы больше не было возможности пользоваться своим аккаунтом. Далее преступники отправляютсэтой страницы всем контактам сообщения, указывая, что владелец страницы сейчас в отпуске за границей, что его ограбили как раз перед возвращением домой.

«Компенсация». В электронном письме сообщается, что был создан специальный фонд для выплаты различных компенсаций и что адрес жертвы был в списке пострадавших.

«Ошибка». Этот тип мошенничества очень популярен. Мошенники выходят на контакт с жертвой, которая недавно размещала рекламу о продаже, например, дома, соглашаются купить дом и быстро высылают чек на определённую сумму, которая всегда «случайно» оказывается неверной (как ни странно, всегда больше, чем сумма, о которой договаривались). Жертву просят вернуть разницу. Позже оказывается, что чек недействителен, дом так и не продан, а переведённые жертвой деньги потеряны.

Приложение Б   
Задания теста

***1 Информация, размешенная в Интернете:***

а) легко удаляется

б)доступна ограниченному кругу людей

в) доступна всем

г) всегда достоверна

***2 Какие цифровые следы фиксирует смартфон?***

а) геоданные

в) поисковые запросы

б) текстовые и голосовые переписки

г) все ответы верны

***3 Что такое кибербуллинг?***

а) форма насилия

б) краха логинов и паролей

в) способ общения

г) вид компьютерного вируса

***4 К кибербуллингу относится:***

а) анонимные угрозы

б) шантаж

в) преследования

г) все ответы верны

***5 С какими опасностями в Интернете можно встретиться чаще всего?***

а) заражение компьютера вирусом в) противоправный контент

б) сомнительные сообщения от незнакомцев г) все ответы верны

***6 Что относится к информационным рискам в Интернете?***

а) фальшивые новости (фейк)

б) опасный контент

в) цифровая зависимость

г) все ответы верны

***7 Какие персональные данные можно сообщать незнакомым людям в Сети?***

а) фамилию, имя, отчество, возраст

б) домашний адрес, номер телефона, адрес электронной почты

в) все данные, которые попросят

г) незнакомым людям в Сети нельзя сообщать никакие персональные данные

***8 Если незнакомец прислал сообщение с просьбой о деньгах, то:***

а) он попал в беду, и нужно ему помочь деньгами

б) нужно выяснить, кто он, и. если он попал в боду, помочь ему деньгами

в) нужно пообщаться с ним через видеозвонок, выяснить все обстоятельства и, если он попал в беду, помочь ему деньгами

г) это обман, и нужно игнорировать сообщение

***9 Если внезапно пришло сообщение от незнакомца о том. что Ваш друг попал в беду и срочно нужно перевести деньги, чтобы ему помочь, то:***

а) нужно срочно перевести деньги, чтобы помочь другу

6) нужно выяснить,что именно случилось с другом, и перевести деньги

в) нужно связаться с другом, а если не получается, связаться с его близкими и выяснить, действительно ли друг попал в беду

г) игнорировать сообщение

***10 Если Вам внезапно приходит сообщение от знакомого человека с просьбой о*** ***деньгах, то:***

а) нужно позвонить ему и уточнить, действительно ли он писал сообщение с просьбой о деньгах

б) нужно перевести деньги

в) нужно вступить в переписку и перевести деньги

г) нужно игнорировать сообщение

***11 Если Вам внезапно пришло приглашение на удалённую работу с большой зарплатой, то:***

а) надо соглашаться и делать то. что просят

б) надо выяснить, в чём суть работы, и, если просят купить стартовый набор (например, рассаду,детали и пр), купить его и начать работать

в) надо выяснить, в чём суть работы, и, если просят перевести деньги со счёта на счёт, перевести их (это же работа)

г) это обман, и нужно игнорировать сообщение

***12 Какова цель настойчивых незнакомцев?***

а) отдать выигрыш в лотерею

б) завладеть личными данными

в) помочь другу в беде

г) дать Вам работу

***13 Какими личными данными хотят завладеть кибермошенники?***

а) паспортными данными

б) домашними адресами и данными банковских карт

в) логинами и паролями

г) все ответы верны

***14 Как можно защититься в Интернете?***

а) создать свою отдельную учётную запись без привязки к банковским картам родителей

б) не реагировать на агрессивные сообщения и самому не провоцировать агрессию

в) использовать настройки конфиденциальности в социальных сетях

г) все ответы верны

***15 Можно ли рассказывать в Интернете, когда и куда Вы идёте, что будете там делать?***

а) рассказывать о своих планах можно, чтобы позлить подписчиков

б) рассказывать о своих планах не нужно, чтобы не стать жертвой преступления

в) рассказывать о своих планах не нужно, чтобы не вызывать зависть подписчиков

г) это личное дело каждого

***16 К основным правилам кибербезопасности можно отнести:***

а) постоянное использование и обновление антивирусных программ

б) избегание сомнительных «улучшений» для самых распространённых приложений

в) скачивание программ и приложений только из надёжных источников

г) все ответы верны

***17 Какие опасности в Интернете для техники и программ наиболее распространённые?***

а) вирусы

б) спам

в) цифровая зависимость

г) мошенники

***18 Что делать, если взломали Ваш аккаунт?***

а) заблокировать доступ к банковским картам

б) обратиться к службе поддержки социальной сети, поменять пароли

в) через другие каналы связи связаться с друзьями и сообщить о взломе

г) все ответы верны

***19 Что делать, если в новостной ленте Вашего аккаунта появились странные публикации?***

а) проверить, какая группа/профиль выкладывает подобные материалы.

б) сообщить администрации ресурса и отписаться

в) попытаться успокоиться и напомнить себе, что находишься в безопасности

г) все ответы верны

***20 Что делать, если Вам угрожают в Интернете?***

а) не отвечать и удалить сообщение

б) не отвечать и показать сообщение родителям

в) отвечать злыми и обидными сообщениями, защищаться

г) нет верного ответа

1. Словарь используемых понятий представлен в приложении А [↑](#footnote-ref-1)
2. Видео «Цифровая гигиена»

   https://vk.com/video\_ext.php?oid=-10474189&id=456240050&hash=2dabbfdbeca49ae2 [↑](#footnote-ref-2)
3. Задания теста представлен в Приложении Б [↑](#footnote-ref-3)