



МЦК КТИТС

Международный центр компетенций –
Казанский техникум информационных
технологий и связи

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ РЕСПУБЛИКИ ТАТАРСТАН
ГАПОУ «МЕЖДУНАРОДНЫЙ ЦЕНТР КОМПЕТЕНЦИЙ-КАЗАНСКИЙ ТЕХНИКУМ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ»

ПРИНЯТО

на заседании Педагогического совета
ГАПОУ «МЦК-КТИТС»

Протокол № 5 от «19» января 2022 г.

УТВЕРЖДАЮ

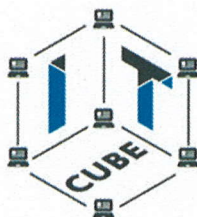
Директор

Ю.Н. Багров

Приказ № 4Д/IT-cube
«19» января 2022 г.



ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ
«КИБЕРГИГИЕНА И РАБОТА С БОЛЬШИМИ ДАННЫМИ»



СЕТЬ ЦЕНТРОВ ЦИФРОВОГО
ОБРАЗОВАНИЯ ДЕТЕЙ «IT-КУБ»

Казань - 2022 год

Организация-разработчик: Государственное автономное профессиональное образовательное учреждение «Международный центр компетенций-Казанский техникум информационных технологий и связи» (далее – ГАПОУ «МЦК-КТИТС») Детский центр ИТ-творчества «IT-cube».

Составитель:

Агаева Р.А. – педагог дополнительного образования Детского центра ИТ-творчества «IT-cube»;

Мансурова Г. А. – методист Детского центра ИТ-творчества «IT-cube».

СОДЕРЖАНИЕ

	стр.
1. ПАСПОРТ ПРОГРАММЫ	4
2. СОДЕРЖАНИЕ ПРОГРАММЫ	7
3. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ	13
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ	14

1. ПАСПОРТ ПРОГРАММЫ

Дополнительная общеобразовательная программа технической направленности (далее – ДОП) «Кибергигиена и работа с большими данными» разработана на основе рекомендаций партнера проекта «Цифровая образовательная среда» АО «КРИБРУМ» и с учетом развития науки, техники, культуры, экономики, современных цифровых технологий и социальной сферы.

Категория обучающихся: от 12 до 17 лет.

Количество часов реализации программы: 48 академических часов.

ДОП «Кибергигиена и работа с большими данными» технической направленности предназначена для формирования научного мировоззрения, развития прикладных, исследовательских способностей обучающихся, с наклонностями в области технического творчества.

Новизна программы. Кибергигиена – это защищённость в информационном пространстве. На занятиях обучающиеся поймут структуру интернет-пространства, научатся разбираться в источниках и типах информации в интернете, освоят поисковые системы и средства поиска информации.

Актуальность. Интернет стал неотъемлемой частью жизни. В виртуальном пространстве возможно абсолютно все: приобретать товар, находить знакомых, необходимую информацию и т.д. Но часто пользователи сталкиваются с мошенничеством, поэтому важно знать правила безопасности в интернете. Именно этому обучают на занятиях по ДОП «Кибергигиена и работа с большими данными».

Педагогическая целесообразность данной программы заключается в пробуждении интереса обучающихся к новому виду деятельности. Занятия по программе создают условия по освоению теоретических основ кибербезопасности. В процессе реализации программы обучающиеся освоят основы кибергигиены.

Цель – формирование у обучающихся основных понятий о современных

цифровых технологиях, глобальной сети Интернет, основах безопасности, а так же способности к разностороннему и комплексному анализу информации, размещенной на различных интернет-ресурсах, в интересах безопасного и рационального использования интернет-пространства.

Задачи:

– сформировать у обучающихся представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;

– ознакомить обучающихся с принципами построения исследования, процедурой и этикой его проведения, количественными и качественными методами обработки полученных данных;

– ознакомить обучающихся с методами и средствами поиска информации в интернет-пространстве;

– сформировать у обучающихся навыки планирования, проведения и обработки результатов исследования информации в интернет-пространстве при помощи поисковых систем, общедоступных средств поиска информации и системы мониторинга и анализа социальных медиа «КРИБРУМ»;

– сформировать у обучающихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;

– в защищенной среде продемонстрировать обучающимся возможные угрозы и риски интернет-пространства;

– сформировать у обучающихся способность определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях;

– сформировать у обучающихся способность к успешной самопрезентации и формированию позитивного имиджа в социальных сетях;

– сформировать у обучающихся способность распознавать опасный и вредный контент и идентифицировать явления манипулирования сознанием в интернет-пространстве, внушения деструктивных идей и вовлечения в

социально опасные группы в социальных сетях;

- обучить обучающихся приемам противодействия негативным воздействиям в интернет-пространстве;

- сформировать у обучающихся культуру позитивного использования интернет-пространства.

Планируемые результаты:

Для формирования поставленной цели планируется достижение следующих результатов:

Знания:

- структуры интернет-пространства, типов источников информации и разновидностей контента;

- методологий исследования информации в интернет-пространстве;

- признаков рискованного и опасного поведения и различных угроз в интернет-пространстве (фишинг, мошенничество, вовлечение в опасные виды деятельности) и умение идентифицировать их в социальных сетях;

- понимание и принятие правил безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий.

Умения:

- работать с поисковыми системами, общедоступными средствами поиска информации в интернет-пространстве и системой «КРИБРУМ»;

- анализировать информацию в интернет-пространстве при помощи количественных и качественных методов, формировать целостное представление об объекте, ситуации или социальной группе на основе разных источников с применением системы «КРИБРУМ» и без;

- определять индивидуальные особенности людей на основе аккаунтов в социальных сетях;

- работать в команде, развитие коммуникативных навыков;

- представлять результаты своей работы окружающим, аргументировать свою позицию;

- свободно ориентироваться в интернет-пространстве, использовать различные типы источников для решения собственных задач;
- рационально и безопасно использовать социальные сети;
- грамотно представлять в интернет-пространстве свои личные и персональные данные, формировать и поддерживать собственный позитивный имидж в социальных сетях;
- распознавать признаки рискованного и опасного поведения в своем окружении в социальных сетях;
- избегать «ловушек», связанных с коммуникационными, контентными, потребительскими и некоторыми технологическими рисками интернет-пространства.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Наименование модуля	Всего, ак.час.	Лекци и	Практ. Занят.	Итог. аттест.
Модуль 1. Основы анализа информации в интернет-пространстве (на примере обзора интернет-источников)	4	2	2	-
Модуль 2. Анализ мнений интернет-пользователей (на примере мнений о фильме)	6	3	3	-
Модуль 3. Порядок действий ликвидации последствий сбоя системы, кибератак. Возможные пути решения проблемы	8	4	4	-
Модуль 4. Анализ социальных групп на основе данных интернет-пространства (на примере фанатских сообществ)	8	4	4	-
Модуль 5. Безопасное и рациональное использование	10	5	5	-

личных и персональных данных в социальных сетях (на примере собственного аккаунта)				
Модуль 6. Распознавание опасного и вредного контента в интернет-пространстве (на примере подозрительных объявлений)	10	5	5	-
Защита проектов	2	-	-	2
Итого	48	23	23	2

2.2 Учебно-тематический план

№ п/п	Наименование разделов, тематика занятий	Количество часов		
		Всего	Теоретических	Практических
Модуль 1. Основы анализа информации в интернет-пространстве (на примере обзора интернет-источников)		4	2	2
1	Информационная структура интернета, поисковые системы. Ознакомление с инструментом представления результатов работы в рамках курса, принципами подготовки эффективной презентации	2	1	1
2	Постановка задачи групповой работы – эффективный поиск в интернете. Принципы эффективного поиска информации в интернете. Принципы оценки качества источников информации.	2	1	1
Модуль 2. Анализ мнений интернет-пользователей (на примере мнений о фильме)		6	3	3
3	Элементы контента социальных сетей. Постановка задачи исследования мнений интернет-пользователей. Программа исследования и методы исследования.	2	1	1
4	Анализ упоминаний фильма, сообщений и авторов с помощью системы «КРИБРУМ».	2	1	1
5	Представление результатов работы.	2	1	1
Модуль 3. Порядок действий ликвидации		6	3	3

последствий сбоев системы, кибератак. Возможные пути решения проблемы				
6	Понятие сбоя системы и синего экрана. Способы восстановления системы. Постановка задачи исследования. Изучение сообщений о синем экране.	2	1	1
7	Рассмотрение наиболее крупных взломов системы и кибератак. Проблема хакерства. Исследование юридических аспектов проблемы хакерства с помощью поисковых систем.	2	1	1
8	Проблема краж персональных данных с помощью вредоносного ПО. Исследование сообщений в системе «КРИБРУМ».	2	1	1
Модуль 4. Анализ социальных групп на основе данных интернет-пространства (на примере фанатских сообществ)		10	5	5
9	Понятие социальная группа, сообщество, субкультура, фэндом. Постановка задачи исследования. Изучение сообщений о сообществе в социальных сетях с помощью системы «КРИБРУМ».	2	1	1
10	Изучение правил функционирования сетевых сообществ. Правила сетевого общения.	2	1	1
11	Анализ с помощью системы «КРИБРУМ» активности участников группы сообщества, связей, поведенческих особенностей, предпочтений и интересов сообщества (в том числе с использованием контент-анализа).	2	1	1
12	Дополнительный анализ сообщества на усмотрение учащихся в системе «КРИБРУМ», подготовка к представлению результатов проделанной работы.	2	1	1
13	Представление результатов проделанной работы.	2	1	1
Модуль 5: безопасное использование личных и персональных данных в интернет-пространстве (на примере собственного аккаунта в социальной сети).		10	5	5
14	Защищенность данных в сети. Проблемы утечки данных. Действия при взломе	2	1	1

	аккаунтов. Безопасные пароли. Подготовка к групповой работе по разработке рекомендаций по рациональному и безопасному использованию личных и персональных данных в социальных сетях			
15	Политика социальных сетей в области конфиденциальности пользовательских данных. Структура аккаунта пользователя социальной сети.	2	1	1
16	Риски нерационального и небезопасного использования личных и персональных данных в социальных сетях. Проблемы использования в сообщениях геотегов, столкновения с неразумным и агрессивным поведением в сети. Анализ сообщений с использованием системы «КРИБРУМ».	2	1	1
17	Проблемы рискованного поведения, нежелательных и сомнительных знакомств, манипулирования и вовлечения в опасное поведение в социальных сетях. Исследование аккаунтов в социальных сетях с использованием контент-анализа, анализ личных профилей в социальных сетях.	2	1	1
18	Представление результатов работы.	2	1	1
Модуль 6: распознавание опасного и вредного контента в интернет-пространстве (на примере подозрительных объявлений в социальных сетях).		10	4	6
19	Проблема контентных рисков и меры противодействия им. Механизмы защиты социальных сетей от негативного контента. Постановка задачи исследования по подготовке интеллектуальной карты реагирования при столкновении с подозрительным контентом в сети.	2	1	1
20	Благотворительность с помощью интернет. Исследование с помощью «КРИБРУМ» подозрительных объявлений о пожертвованиях в благотворительные фонды и частных сборах на лечение. Риски потребительского поведения. Правила социальных сетей по размещению рекламы.	2	1	1

	Анализ объявлений о продаже в социальных сетях.			
21	Торговля в интернете. Анализ с использованием системы «КРИБРУМ» подозрительных объявлений о дарении, об акциях, розыгрышах призов и конкурсах репостов в социальных сетях.	2	1	1
22	Проблема оказания поддельных услуг и распространения подозрительных объявлений об удаленной работе в социальных сетях, анализ подозрительных сообщений с использованием системы «КРИБРУМ», составление интеллектуальной карты действий при столкновении с подозрительным контентом.	2	1	1
23	Представление результатов работы.	2	1	1
24	Итоговое занятие и защита проектных работ	2		2
Итого:		48	22	26

Форма организации занятий: групповая.

Форма проведения занятий: комбинированная.

На каждом занятии проводится повторение и закрепление умений и знаний, полученных на предыдущем занятии, проверка домашнего задания.

2.3 Календарный учебный график (порядок освоения модулей)

Период обучения (неделя)*	Наименования модуля
1 неделя	Модуль 1. Основы анализа информации в интернет-пространстве (на примере обзора интернет-источников)
2 неделя	Модуль 1. Основы анализа информации в интернет-пространстве (на примере обзора интернет-источников)
3 неделя	Модуль 2. Анализ мнений интернет-пользователей (на примере мнений о фильме)
4 неделя	Модуль 2. Анализ мнений интернет-пользователей (на примере мнений о фильме)
5 неделя	Модуль 2. Анализ мнений интернет-пользователей (на примере мнений о фильме)

6 неделя	Модуль 3. Порядок действий ликвидации последствий сбоя системы, кибератак. Возможные пути решения проблемы
7 неделя	Модуль 3. Порядок действий ликвидации последствий сбоя системы, кибератак. Возможные пути решения проблемы
8 неделя	Модуль 3. Порядок действий ликвидации последствий сбоя системы, кибератак. Возможные пути решения проблемы
9 неделя	Модуль 3. Порядок действий ликвидации последствий сбоя системы, кибератак. Возможные пути решения проблемы
10 неделя	Модуль 4. Анализ социальных групп на основе данных интернет-пространства (на примере фанатских сообществ)
11 неделя	Модуль 4. Анализ социальных групп на основе данных интернет-пространства (на примере фанатских сообществ)
12 неделя	Модуль 4. Анализ социальных групп на основе данных интернет-пространства (на примере фанатских сообществ)
13 неделя	Модуль 4. Анализ социальных групп на основе данных интернет-пространства (на примере фанатских сообществ)
14 неделя	Модуль 5. Безопасное и рациональное использование личных и персональных данных в социальных сетях (на примере собственного аккаунта)
15 неделя	Модуль 5. Безопасное и рациональное использование личных и персональных данных в социальных сетях (на примере собственного аккаунта)
16 неделя	Модуль 5. Безопасное и рациональное использование личных и персональных данных в социальных сетях (на примере собственного аккаунта)
17 неделя	Модуль 5. Безопасное и рациональное использование личных и персональных данных в социальных сетях (на примере собственного аккаунта)
18 неделя	Модуль 5. Безопасное и рациональное использование личных и персональных данных в социальных сетях (на примере собственного аккаунта)
19 неделя	Модуль 6. Распознавание опасного и вредного контента в интернет-пространстве (на примере подозрительных объявлений)
20 неделя	Модуль 6. Распознавание опасного и вредного контента в интернет-пространстве (на примере подозрительных объявлений)
21 неделя	Модуль 6. Распознавание опасного и вредного контента в интернет-пространстве (на примере подозрительных объявлений)
22 неделя	Модуль 6. Распознавание опасного и вредного контента в интернет-пространстве (на примере подозрительных объявлений)

23 неделя	Модуль 6. Распознавание опасного и вредного контента в интернет-пространстве (на примере подозрительных объявлений)
24 неделя	Защита проектов
*Точный порядок реализации модулей (дисциплин) обучения определяется в расписании занятий.	

3. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

3.1 Критерии оценки

Оценка освоения программы осуществляется во время проведения текущего, промежуточного и итогового контроля в соответствии с критериями оценивания контрольных знаний.

Итоговым контролем является защита проектов и участие в конкурсах.

Оценка результатов освоения образовательной программы выполняется по совокупности работ, выполненных каждым обучающимся, включая результаты участия в различных мероприятиях, фестивалях, конкурсах

Оценка	Критерий
Высокий уровень	Получен полный и развёрнутый ответ на вопрос, приведены иллюстрирующие ответ примеры, получены ответы на дополнительные вопросы преподавателя
Средний уровень	Получен полный и развёрнутый ответ на вопрос, приведены иллюстрирующие ответ примеры, но не получены ответы на дополнительные вопросы преподавателя
Низкий уровень	Получен неполный ответ на вопрос, не приведены иллюстрирующие ответ примеры, получены неполные ответы на дополнительные вопросы преподавателя

3.2 Тематики проектных работ

№	Тема проектной работы
1	Проблемы безопасности в современном мире и их зависимость от цифровых технологий.
2	Инструментарий современного специалиста по большим данным.
3	Методологии информационного моделирования.
4	Анализ безопасности Телеграмм.

5	Поиск в открытом доступе наборов данных для обучения нейронных сетей.
6	Методы получения доступа к конфиденциальной информации
7	Использование Excel для обработки больших данных.
8	Синий экран смерти
9	Перспективы развития цифровых технологий и критерии их безопасности.
10	Спам ссылки.

Данный перечень тем является далеко не полным. На основе данных тем можно проводить занятия на основе детализации выбранной темы. Также данные темы могут помочь обучающимся при выборе направления учебно-исследовательских проектов. Все темы являются на текущий момент актуальными для современного общества и не потеряют своей актуальности в ближайшей перспективе.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1 Материально-технические условия реализации программы

Для реализации программы необходимо следующее оборудование:

Наименование оборудования	Назначение/краткое описание функционала оборудования	Количество, шт.
Основное оборудование		
Системный блок	Lenovo M720t MT, комплект (клавиатура, мышь)	15
Монитор 24"	BENQ GW2480-T	15
Источники бесперебойного питания	PowerMan Back PRO 800 Plus	15
Наушники полноразмерные	Sennheiser HD 206	15
WEB-камера	Logitech HD Webcam B525	1
Многофункциональное устройство, тип 1	Canon i-SENSYS MF421 dw (принтер, копир, сканер) A4	1

Сервер	INTEL 16B/2U/Xeon Gold5118*2/32GB	1
Демонстрационное оборудование		
Интерактивная панель	Prestigio MultiBoard 70	1
Напольная мобильная стойка	Prestigio PMBST01	1
Крепление для интерактивной панели	Prestigio PMBWMK	1
Флипчарт магнитно-маркерный на треноге		по требованию
Вспомогательное оборудование и аксессуары		
Коврик для мыши	Коврик для мыши размером 335x240x3 мм	15

4.2 Информационное обеспечение обучения

Основная литература:

1. Богачева Т.Ю., Соболева А.Н., Соколова А.А. Риски интернет пространства для здоровья подростков и пути их минимизации // Наука для образования: Коллективная монография. М.: АНО «ЦНПРО», 2015.
2. Кравченко А.И. Методология и методы социологических исследований. Учебник. М.: Юрайт, 2015.
3. Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн рисков: итоги пятилетней работы линии помощи «Дети онлайн» // Консультативная психология и психотерапия. 2015. № 3. С. 50-66.
4. Герцог Г.А. Основы научного исследования: методология, методика, практика: учебное пособие. Челябинск: Изд-во Челяб. гос. пед. ун та, 2013.
5. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей: российский и зарубежный опыт: Монография. М.: ЮНИТИ-ДАНА, 2013.
6. Слугина Н. Активные пользователи социальных сетей Интернета. СПб.: Питер, 2013.
7. Солдатова Г., Зотова Е., Лебешева М., Вляпников В. Интернет:

возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Ч. 1. Лекции. М.: Google, 2013.

8. Солдатова Г., Рассказова М., Лебешева М., Зотова Е., Рогендорф П. Дети России онлайн. Результаты международного проекта EU Kids Online II в России. М.: Фонд Развития Интернет, 2013.

9. Солдатова Г.У., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013.

Электронные ресурсы:

1. Аликберов А. Несколько слов о том, как работают роботы поисковых машин» [Электронный ресурс]. URL: http://www.citforum.ru/internet/search/art_1.shtml.

2. Блог ContentMonster.ru. Руководство по SEO для начинающих [Электронный ресурс]. URL: <http://blog.contentmonster.ru/2014/06/seo-guide/>.

3. Вельчева И.А. Как составить семантическое ядро, не обращаясь к специалисту, руководство для владельцев интернет-магазинов [Электронный ресурс]. URL: <https://netpeak.net/ru/blog/kak-sostavit-semanticheskoe-yadro-ne-obrashchayas-k-spetsialistu-rukovodstvo-dlya-vladelcev-internet-magazinov/>

4. Виды и форматы контента [Электронный ресурс]. URL: <https://andreyspektor.com/socialnye-seti/vidy-i-formaty-kontenta-vkontakte.html>

5. Виды контента. Систематизируй это [Электронный ресурс] URL: <https://smmplanner.com/blog/2016/09/15/vidy-kontenta-sistematiziruj-eto/>

6. Виды социальных сетей: классификация и представители [Электронный ресурс]. URL: <http://darksiteofmarketing.com/stati/vidy-socialnyh-setei-klassifikacija-i-predstaviteli.html>

7. Глоссарий.ru: служба темат. толковых слов [Электронный ресурс]. URL.: <http://www.glossary.ru/>

8. Давыдов А.А. Развитие Интернет-технологий вызов современной российской социологии. М.: ИСАН, 2008. [Электронный ресурс]. URL: http://www.isras.ru/index.php?page_id=957

9. Зернов Д.В., Иудин А.А. Применение новых информационных технологий при анализе документов в социальной и гуманитарной сфере. Электронное учебно-методическое пособие [Электронный ресурс]. Нижний Новгород: Нижегородский университет, 2012. URL: http://www.unn.ru/books/met_files/Zernov_Iudin.pdf
10. Как писать ключевые слова. SEO [Электронный ресурс]. URL: <http://shpargalkablog.ru/2010/07/keywords.html>
11. Основные виды контента для Вашего сайта [Электронный ресурс]. URL: <https://seo-akademiya.com/baza-znanij/kontent/vidyi-kontenta-na-sajte/>
12. Поиск информации в интернет [Электронный ресурс]. URL: http://xn---7sbbfb7a7aej.xnp1ai/informatika_10/informatika_materialy_zanytii_10_35.html