Департамент образования и науки города Москвы
Государственное бюджетное образовательное учреждение дополнительного профессионального образования города Москвы
«Московский центр «Патриот.Спорт»

«Утверждаю»
Исполняющий обязанности
Заместителя директора
ГБОУ ДПО МЦПС
_____Д. Г. Степыко
«25» марта 2022 г.

Дополнительная общеобразовательная программа
(Дополнительная общеразвивающая программа)

«КИБЕРБЕЗОПАСНОСТЬ. КИБЕРСПОРТ»

Уровень программы: ознакомительный
Направленность: техническая
Возраст обучающихся - от 14 лет
Срок реализации – 36 часов

Разработчики программы:
Сиденко А.Г. – специалист отдела воспитательных практик,
Салаватов Х.А. – педагог-организатор отдела воспитательных практик.

г. Москва
2022 г.

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Модульная дополнительная общеобразовательная программа «**Кибербезопасность. Киберспорт**» относится к ознакомительному уровню, имеет техническую направленность, составлена в соответствии с типовым положением об образовательном учреждении дополнительного образования детей, нормативными документами Министерства просвещения Российской Федерации и Минспорта России.

Настоящая программа составлена в соответствии с требованиями следующих нормативных документов:

– Федеральный Закон РФ от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (далее – ФЗ);

– Федеральный закон РФ от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

– Стратегия развития воспитания в РФ на период до 2025 года (распоряжение Правительства РФ от 29 мая 2015 г. № 996-р);

– Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ;

– Федеральный закон Российской Федерации от 21 июля 2011 г. №2252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»;

– Федеральный закон от 04.12.2007 № 329-ФЗ "О физической культуре и спорте в Российской Федерации" // Собрание законодательства РФ", N 50, ст. 6242;

– Приказ Министерства спорта Российской Федерации от 29.04.2016 г. № 470 «О признании и включении во Всероссийский реестр видов спорта спортивных дисциплин, видов спорта и внесении изменений во Всероссийский реестр видов спорта, а также в приказ Министерства спорта, туризма и молодежной политики Российской Федерации от 17.06.2010 № 606 «О признании и включении видов спорта, спортивных дисциплин во Всероссийский реестр видов спорта»;

– Постановление Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»;

– Постановление Главного государственного санитарного врача РФ от 28.01.2021 № 2 «Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» (рзд.VI. Гигиенические нормативы по устройству, содержанию и режиму работы организаций воспитания и обучения, отдыха и оздоровления детей и молодежи»);

– Паспорт федерального проекта «Успех каждого ребенка» (утвержден на заседании проектного комитета по национальному проекту «Образование» 07 декабря 2018 г., протокол № 3);

– Приказ Министерства просвещения РФ от 09.11.2018 № 196 ;

– «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам» (далее – Порядок);

– Приказ Министерства просвещения РФ от 03.09.2019 № 467;

– «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;

– Приказ Министерства образования и науки РФ от 23.08.2017 № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

– Приказ Министерства образования и науки РФ и Министерства просвещения РФ от 5.08.2020 № 882/391 «Об организации и осуществлении образовательной деятельности по сетевой форме реализации образовательных программ»;

– Концепции развития дополнительного образования детей (утв. Распоряжением Правительства РФ от 04.09.2014 № 1726-р);

– Письма Минобрнауки РФ от 11.12.2006 № 06-1844 «О примерных требованиях к программам дополнительного образования детей»;

– Письма Минобрнауки РФ от 18.11.2015 № 09-3242 «О направлении информации» (Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разно-уровневые программы);

– Приказа Департамента образования города Москвы от 17.12.2014 № 922 «О мерах по развитию дополнительного образования детей в 2014–2015 учебном году»;

– Приказа Департамента образования города Москвы от 07.08.2015 № 1308 «О внесении изменений в приказ Департамента образования города Москвы от 17 декабря 2014 г. № 922»;

– Приказа Департамента образования города Москвы от 08.09.2015 № 2074 «О внесении изменений в приказ Департамента образования города Москвы от 17 декабря 2014 г. № 922».

Программа предназначена для педагогов дополнительного образования и является основным документом для проведения занятий и воспитательной работы

Компьютеризация и цифровизация многих сфер жизни общества стали неотъемлемой частью современности, на основе цифровых технологий появляются новые профессии, новые виды деятельности. Стремительно появляются и входят в нашу жизнь компьютерные и информационные технологии, которые помогают нам в различных видах деятельности, но и

которые требуют от нас новых знаний и умений.

Модульная дополнительная общеобразовательная программа **«Кибербезопасность. Киберспорт»,** как следует из названия, знакомит обучающихся с двумя элементами дисциплины, неотъемлемо связанных с компьютерными технологиями – это «Кибербезопасность» и новый вид спорта по адаптированным названием – «Киберспорт».

Безопасность в обществе и информационном пространстве является одним из основных направлений фундаментальных исследований в области информационных технологий. Наряду с позитивными результатами компьютеризации жизнедеятельности общества человек столкнулся с новым видом угроз - киберугрозой.

Киберугрозы существуют везде, где применяются информационные технологии, следовательно, любой человек может как в профессиональной деятельности, так и в обыденной жизни, столкнуться и со спамом, и с вирусами, и со взломом компьютера и с многими другими проблемами, на которые нужно не только оперативно реагировать, но и уметь предотвращать их появление.

В современном мире цифровизации происходит стремительное развитие различных областей деятельности общества, а развитие индустрии компьютерных игр привело к появлению такого вида профессионального спорта, как киберспорт (e-sport).

Киберспорт — это не просто игра, а комплекс действий, который развивает стратегическое мышление, логику, скорость реакции, внимание, память, а также навыки командной работы. Кроме этого, занятия киберспортом расширяют цифровой кругозор и общую компьютерную грамотность, улучшают владение аппаратным ИТ-комплексом, развивают навыки программирования.

Часть профессиональных игр тесно связана с математикой, информатикой, эвристикой, военно-патриотической культурой, ряд игр дает опыт прикладного программирования. Навыки, формируемые на занятиях киберспортом, входят в число профессиональных компетенций многих современных профессий.

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

– обеспечение различных сфер экономики качественными информационными технологиями;

– обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Актуальность программы.

В реалиях цифровизации современного общества компьютерные технологии являются неотъемлемым элементом различных областей деятельности, требующим от работника регулярного обучения, непрерывного овладения новыми знаниями и умениями. Использование информационных технологий позволяет ускорить успешное освоение материала в предпрофильные классах. Для современного врача, ученого, педагога, военного, инженера, специалиста по пиару и многих других профессий, основы которых изучают в рамках проектов предпрофессионального образования, ключевое значение имеет уровень навыков работы с организацией безопасности личного информационного пространства и соблюдения требования кибербезопасности в практической деятельности.

Каждый проект предпрофессионального образования тесно связан с овладением информационными технологиями, и поэтому получение обучающимся знаний по цифровой и компьютерной безопасности является необходимым.

Вместе с тем внедрение новых цифровых технологий напрямую связано с развитием механизмов защиты информации и предотвращению киберпреступлений.

Программа в рамках изучения основ киберспорта позволяет сформировать и укрепить практические навыки (быстрота реакции, моторика и точность работы руками и др.), необходимые для успешного овладения новыми профессиями, например оператора беспилотных летательных аппаратов(БПЛА), ряда медицинских и инженерных направлений.

Программа «Кибербезопасность. Киберспорт» направлена на расширение цифрового кругозора, формирование навыков для основных профессиональных компетенций многих современных профессий, повышение компьютерной грамотности и овладение навыками и приемами кибербезопасности, что является важным компонентом обучения по предпрофессиональным программам Департамента образования и науки г. Москвы.

В настоящее время, выполняя социальный заказ общества, система дополнительного образования должна решать новую задачу: подготовки подрастающего поколения к жизни, будущей профессиональной деятельности в высокоразвитом информационном обществе.

Данная программа способствует формированию умения работать в условиях дефицитов, развивает сообразительность и любознательность у обучающихся. Создание на занятиях ситуаций активного поиска, предоставление возможности сделать собственное «открытие», знакомство с оригинальными путями рассуждений позволят обучающимся реализовать свои возможности, работая в команде приобрести уверенность в своих силах.

Новизной и отличительной особенностью модульной программы является то, что она не только прививает навыки и умение работать с программами, но и способствует формированию информационной, научно-технической и эстетической культуры обучающегося.

С точки зрения педагогической целесообразности киберспортивные соревнования являются мощнейшим инструментом для развития коммуникативных навыков и положительной социализации подрастающего поколения. Таким образом, вместо запрета и отрицания электронных игр, этот курс позволяет направить детские увлечения в позитивное русло. Кроме того, в рамках программы предполагается использование нестандартных материалов при выполнении различных проектов.

Категория обучающихся – обучающиеся образовательных организаций от 14 до 17 лет.

Срок реализации программы. Модульная дополнительная общеобразовательная общеразвивающая программа «**Кибербезопасность. Киберспорт**» рассчитана на 36 часов обучения.

Форма и режим занятий: форма занятий – групповая (занятия проводятся в разновозрастных группах, численный состав группы 10-20 человек).

В данной образовательной программе занятия проводятся 2 раза в неделю по 2 часа (время занятия включает 45 мин. учебного времени и обязательный 15 минутный перерыв).

Особенности организации образовательного процесса. Учебный материал рассчитан на последовательное и постепенное освоение теоретических знаний и приобретение практических умений и навыков.

Структура занятий:

Занятия строятся в следующей последовательности:

- изучение теоретического материала;
- практические задания (форма организации зависит от сложности материала);
- обсуждение результатов.

Цель программы: формирование основ безопасного поведения в киберпространстве, овладение навыками, умениями и знаниями по киберспорту.

Задачи:

Обучающие:

- познакомить обучающихся с потенциальными опасностями интернета и способами противодействия им;
- сформировать умения работать с информацией (осуществлять передачу, хранение, преобразование и поиск);
- познакомить обучающихся с основными терминами и понятиями в области киберспорта и научить использовать специальную терминологию;
- сформировать представление об основных особенностях киберспорта.

Развивающие:

- развить мыслительные операции: анализ, синтез, обобщение, сравнение, конкретизация;
- развить у обучающихся критическое мышление;

- развить внимание и память;
- развитие интеллектуальных способностей учащихся;
- развитие мелкой моторики, реакции и стратегического мышления;
- развитие навыков командного взаимодействия и лидерства.

Воспитательные:

– воспитывать взаимоуважение друг к другу, формировать эстетический вкус, бережное отношение к оборудованию и технике, дисциплинированность;

– формировать умение работать в команде и договариваться.

Дополнительная общеобразовательная программа «**Кибербезопасность. Киберспорт**» основана на взаимосвязи процессов обучения, воспитания и развития обучающихся. Основными принципами работы по программе являются:

- *принцип научности*, который заключается в сообщении знаний об устройстве персонального компьютера, программах, соответствующих современному состоянию науки;
- *принцип доступности* выражается в соответствии образовательного материала возрастным особенностям детей и подростков;
- *принцип сознательности* предусматривает заинтересованное, а не механическое усвоение воспитанниками знаний, умений и навыков;
- *принцип наглядности* выражается в демонстрации киберугроз различной сложности;
- *принцип вариативности*. Некоторые программные темы могут быть реализованы в различных видах технической деятельности, что способствует вариативному подходу к осмыслению этой или иной творческой задачи, исследовательской работы.

Содержание занятий дифференцировано с учетом возрастных и индивидуальных особенностей детей и подростков. В программе предусмотрены условия для индивидуального творчества, а также для раннего личностного и профессионального самоопределения детей, их самореализации и саморазвития.

Метапредметные результаты:

– умение самостоятельно определять цели деятельности и составлять планы деятельности;

– самостоятельно осуществлять, контролировать и корректировать деятельность;

– использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности;

– выбирать успешные стратегии в различных ситуациях;

– умение продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты;

– готовность и способность к самостоятельной информационно-

познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;

– умение использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Планируемые результаты и способы определения их результативности.

По итогам реализации программы обучающиеся должны

знать:

– отличия достоверных сведений от недостоверных, вредной информации от безопасной;

– нормы информационной этики и права;

– признаки злоупотребления неопытностью и доверчивостью, признаки вовлечения в противоправную и иную антиобщественную деятельность;

– ассортимент современных игровых аксессуаров, их технические характеристики и особенности, способы и приёмы их детальной настройки;

– программы для голосового общения, принципы работы, настройки и особенности использования;

– основные дисциплины и особенности компьютерных игр;

– основные принципы командных соревновательных киберспортивных дисциплин различных направлений;

уметь:

– искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях;

– соблюдать требования кибербезопасности в практической деятельности и организовывать безопасность личного информационного пространства;

– критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;

– избегать навязывания информации, способной причинить вред здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

– применять основные правила создания текстовых документов;

– составлять запросы для поиска информации в Интернете;

– настраивать аппаратуру компьютера под игры, калибровку игровых аксессуаров;

– создавать аккаунт, устанавливать и настраивать программы для голосового общения.

По результатам обучения по программе «Кибербезопасность. Киберспорт» учащиеся предпрофессиональных классов (всех профилей) овладеют следующими навыками и умениями.

1. Поиск информации (на основе принципов построения запросов) в базах данных, компьютерных сетях.
2. Организация безопасности личного информационного пространства.
3. Критическое отношение к сообщениям и иной информации, распространяемой электронными средствами массовой коммуникации.
4. Противодействие навязыванию информации, в том числе способной причинить вред здоровью, нравственному и психическому развитию.
5. Общение в цифровой среде в соответствии с нормами информационной этики.
6. Идентификация достоверных сведений и безопасной информации в Интернете.
7. Проектное управление, в том числе умение составлять планы, контролировать и корректировать деятельность проектной группы.
8. Умение выбирать и реализовывать успешные стратегии в различных ситуациях;
9. Умение продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников, эффективно разрешать конфликты;
10. Умение настраивать аппаратуру компьютера для решения различных персонализированных задач, осуществлять калибровку цифровых аксессуаров, в том числе игровых;
11. Умение создавать аккаунты, устанавливать и настраивать программы, необходимые для голосового общения.
12. Умение защищать персонализированную информацию, кодировать и идентифицировать данные.

II. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Название тем	Количество часов			Формы контроля
		Всего	Теория	Практика	
Модуль Кибербезопасность					
1.	Тема 1. Вводное занятие. Техника безопасности на занятиях. История развития вычислительной техники. История интернета. Обзор возможных угроз, которые можно встретить в сети.	2	1	1	Вводный
2	Тема 2. Хакерские атаки. Виды атак. Расследование кибератак.	1	1	-	Текущий
3.	Тема 3. Кодирование и шифры.	2	1	1	Текущий
4.	Тема 4. Файловая система. Интерфейс командной строки.	3	1	2	Текущий
5.	Тема 5. IP-адресация. Доменная система имен.	2	1	1	Текущий
6.	Тема 6. Что такое вредоносный код и какие у него.	2	1	1	Текущий
7.	Тема 7. Онлайн-мошенничество. Виды угроз, который можно встретить в сети.	2	1	1	Текущий
8.	Тема 8. Безопасность в социальных сетях. Настройки приватности.	2	1	1	Текущий
9.	Тема 9. Методы социальной инженерии. Поиск информации в сети.	2	1	1	Текущий
10.	Подведение итогов. Тест по пройденному модулю.	2	1	1	Итоговый
	Итого по модулю	**20**	**10**	**10**	
Модуль Киберспорт					
1	Тема 1. Вводное занятие. Техника безопасности на занятиях. История развития киберспорта.	1	1	-	Вводный

2	Тема 2. Выбор и настройка периферийных игровых устройств. Программы для текстового и голосового	2	1	1	Текущий
3	Тема 3. Программы для онлайн трансляций игр.	1	1	-	Текущий
4	Тема 4. Тактики и стратегия ведения игр	2	1	1	Текущий
5	Тема 5. Распределение ролей в команде (на примере 1-2 игр)	1	1	-	Текущий
6	Тема 6. Просмотр и обсуждение профессиональных матчей	1	1	-	Текущий
7	Тема 7. Практика командных игр (специализация) - выбор конкретной дисциплины	4	1	3	Текущий
8	Тема 8. Требования к физической подготовленности в киберспорте	2	1	1	Текущий
9.	Итоговое занятие по знаниям пройденного модуля.	2	1,5	0,5	Итоговый
	Итого по модулю	**16**	**9,5**	**6,5**	
	Итого по программе	**36**	**19,5**	**16,5**	

III. СОДЕРЖАНИЕ УЧЕБНО-ТЕМАТИЧЕСКОГО ПЛАНА

Модуль Кибербезопасность

Тема 1. Вводное занятие. Техника безопасности. История развития вычислительной техники. История интернета. Обзор возможных угроз, которые можно встретить в сети.

Теория и практика

Как развивалась компьютерная техника и как устроены компьютер и интернет в настоящее время. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение).

Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях. Интернет как оружие массового поражения. Социальные последствия безответственного поведения в интернете.

Тема 2. Хакерские атаки. Виды хакерских атак.

Теория

Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Кибершпионаж.

Тема 3. Кодирование и шифры

Теория и практика

Введение в тему криптографии. Разбор древних криптографических задач. Виды шифров и их сферы применения в настоящее время. Практика шифрования (Шифр Цезаря и т.п.)

Тема 4. Файловая система. Интерфейс командной строки

Теория и практика

Устройство файловой системы: виды, применение. Для чего используется командная строка. Типы команд. Обзор базовых команд и практика их применения.

Тема 5. IP-адресация. Доменная система имен.

Теория и практика

Как устроена IP адресация. Система DNS и принципы его работы. Уровни взаимодействия сетей. Сетевая топология. Решение задач на определение количества компьютеров в сети.

Тема 6. Что такое вредоносный код и какие у него возможности?

Теория и практика

Что такое зловредное программное обеспечение. Его виды и принципы работы. Способы распространения. Целевая атака и расследование кибератак. Крупные кибератаки, с которыми сталкивались пользователи интернета в последнее время.

Тема 7. Онлайн-мошенничество. Виды угроз, который можно встретить в сети.

Теория и практика

Виды интернет - мошенничества (письма, реклама, охота за личными данными и т.п.). Фишинг (фарминг). Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры.

Онлайн - казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею. Технологии манипулирования в Интернете. Техника безопасности при интернет-общении.

Техника безопасности при регистрации на веб-сайтах. Техника безопасности на сайтах знакомств. Компьютерное пиратство. Плагиат. Кибернаемники и кибердетективы. Оценка ущерба от киберпреступлений.

Тема 8. Безопасность в социальных сетях. Настройки приватности.

Теория и практика

Угрозы, с которыми можно столкнуться в социальных сетях. Спам и фишинг. Виды спама. Подделка профилей пользователей. Похищение логина и пароля. Как использовать настройки приватности для того, чтобы обезопасить свои данные в социальной сети. Какую информацию не стоит оставлять в открытом доступе.

Тема 9. Методы социальной инженерии. Поиск информации в сети.

Теория и практика

Какими уловками пользуются злоумышленники для того, чтобы похитить информацию у пользователей. Практическая работа по поиску информации в сети. Поиск информации о личности. Поиск информации о различных фактах. Какую информацию пользователи оставляют в сети? Команды для поисковых запросов.

Тема 10. Подведение итогов.

Тест по пройденному модулю.

Модуль Киберспорт

Тема 1. Введение в киберспорт.

Теория

История киберспорта. Виды компьютерных игр. Дисциплины, по которым проходят турниры.

Основные классы компьютерных игр, возможность их использования для развития способностей, применение игр в качестве обучающих программ.

Конфигурация компьютера, установка новых элементов. Совместимость комплектующих компьютера, согласование параметров одних устройств с другими, требования к энергоснабжению.

Практика

Работа за компьютером с интернет-источниками, организация своего игрового места, просмотр учебных фильмов.

Тема 2. Выбор и настройка периферийных игровых устройств. Программы для текстового и голосового общения во время игры. Настройка приватности в программах для общения.

Теория

Ассортимент современных игровых аксессуаров. Их технические характеристики и особенности. Способы и приёмы их настройки. VR-устройства. Рекомендации по использованию.

Установка настроек аппаратуры, установка графических и звуковых настроек.

Компьютерные программы, предназначенные для голосового общения в сети Интернет.

Принципы работы, настройка и особенности использования на примере программы Discord.

Настройка программы TeamSpeak, выбор сервера и подключение к нему.

Практика

Работа за компьютером с интернет-источниками, создание аккаунта, установка и настройка программ для голосового общения, настройка и калибровка аксессуаров на своем игровом месте.

Тема 3. Программы для онлайн трансляций игр.

Теория

Знакомство с сервисами для игры через Интернет. Предоставляемые возможности игровой платформы. Установка, настройка и использование Steam.

Практика

Работа за компьютером с интернет-источниками, создание аккаунта, установка и настройка программ.

Тема 4. Тактики и стратегия ведения игр

Теория

Командные стратегии и тактические приёмы при игре в команде, особенности реализации своей роли в команде при различных игровых моментах.

Практика

Работа за компьютером, командная игровая практика.

Тема 5. Распределение ролей в команде (на примере 1-2 игр)

Теория

Особенности игры на каждой роли в команде по киберспортивной дисциплине, различные тактические приёмы, используемые при игре на каждой роли в команде по киберспортивной дисциплине.

Практика

Работа за компьютером, командная игровая практика.

Тема 6. Просмотр и обсуждение профессиональных матчей

Теория

Командные стратегии и тактические приёмы, применяемые профессиональными игроками на чемпионатах. Особенности их реализации в различных игровых моментах.

Изменения стратегии команды в зависимости от стратегии противника.

Тема 7. Практика командных игр (специализация) - выбор конкретной дисциплины

Теория

Основные направления современных командных соревновательных киберспортивных дисциплин. Примеры различных дисциплин этих направлений. Правила киберспортивной дисциплины. Дополнительное программное обеспечение, используемое в киберспортивной дисциплине.

Различные роли в команде по киберспортивной дисциплине, особенности игры на каждой роли в команде по киберспортивной дисциплине.

Практика

Работа за компьютером, игровая практика, тактическая подготовка.

Тема 8. Требования к физической подготовленности в киберспорте

Теория и практика

Роль физической формы в игровом процессе. Комплекс физических упражнений для развития общей и статической выносливости. Комплекс специальных физических упражнений для развития быстроты реакции, точности движения, двигательной памяти, мышечной чувствительности. Система нагрузки и отдыха в киберспорте.

Тема 9. Итоговое занятие

Теория

Тестовые вопросы

Практика

Контрольные игры

IV МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Формы контроля и оценочные материалы

4.1 Формы и подведения итогов реализации дополнительной общеразвивающей программы

Контроль и оценка знаний предполагает степень достижения обучающихся в решении поставленных задач. Цель оценки заключается в формировании у ребенка уважительного отношения к себе и поддержания уверенности его в своих силах, возможностях и способностях при освоении учебного материала.

- Основными формами контроля реализации программы являются:
- индивидуальная;
- фронтальная;
- групповая;
- наблюдения педагога.

Тестовая форма контроля с заданиями множественного выбора позволяет за небольшой период времени проверить усвоение пройденного материала. Использование электронных учебных пособий также значительно облегчает оценить индивидуальную подготовку обучающегося.

4.2 Виды контроля реализации дополнительной общеразвивающей программы:

- текущий (проводится на всех этапах изучения тем);

– тематический (проводится с целью проверки усвоения программного материала по разделам учебно-тематического плана программы, а оценка фиксирует результат. Контроль за уровнем усвоения материала носит систематический характер и осуществляется в конце каждой изученной темы при помощи письменных тестов и устного опроса, носящего фронтальный, групповой и индивидуальный характер);

– итоговый.

Дает возможность педагогу оценить уровень знаний, умений и практических навыков каждого обучающегося по данной программе.

4.3 Используемые оценочные средства:

– тестовые;

– оценочные листы;

– дневник достижений;

– тренажерные.

Для отслеживания динамики освоения данной дополнительной общеобразовательной программы и анализа результатов образовательной деятельности в течение всего учебного процесса осуществляется мониторинг, который включает первичную диагностику, текущий контроль и итоговую аттестацию.

Вводный контроль (первичная диагностика) проводится в начале учебного процесса для определения уровня подготовки обучающихся.

Форма проведения – собеседование.

Текущий контроль осуществляется в процессе проведения каждого учебного занятия и направлен на закрепление теоретического материала по изучаемой теме и на формирование практических умений.

Форма проведения – педагогическое наблюдение, самооценка обучающихся.

Итоговое занятие проводятся в конце обучения в форме теста и контрольных игр.

Примерные вопросы по контролю и оценки знаний (приложение 1и 2).

Материально-техническое обеспечение реализации дополнительной общеобразовательной программы «Кибербезопасность. Киберспорт» включает следующий перечень необходимого оборудования:

Для кибербезопасности

1. Ноутбуки диагональ 14 – 17 дюймов – 10 шт.
2. Столы ученические – 10 шт.
3. Стулья – 10 шт.
4. Интерактивная доска – 1 шт. или
5. Мультимедийный проектор – 1 шт.
6. Акустическая система с радиомикрофоном – 1 шт.
7. Лазерная указка – 1 шт.
8. Доступ к сети Интернет.

Для киберспорта

1. Игровая клавиатура – 10 шт.
2. Игровая мышь – 10 шт.
3. Игровая гарнитура – 10 шт.
4. Коврик для игровой мыши - 10 шт.
5. Монитор для киберспорта от 60 до 140 ГЦ – 10 шт.
6. Игровой компьютер – 10 шт.
7. Кресло игровое– 10 шт.
8. Стол для оборудования по киберспорту – 10 шт.
9. Консоль (геймпад) для геймеров – 10 шт.
10. Игровые приставки PS-4, PS-5 – 10 шт.
11. Программное обеспечение, киберспортивные дисциплины– (Google Chrome/Opera/Firefox Steam, Riot Client, Origin,TeamSpeak, Discord, игры: Dota-2, World of Tanks и другие киберспортивные дисциплины).

V. ЛИТЕРАТУРА

Основная литература:

1. Бирюков А.А. Информационная безопасность защита и нападение 2-е издание: Издательство: ДМК-Пресс., 2017, 434 с.

2. Бирюков А.А. Информационная безопасность защита и нападение. Издательство: ДМК-Пресс., 2012, 474 с.

3. Колесниченко Д.Н. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240 с.

4. Мазаник С.В. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.

5. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии: Издательство: М.: НОУ "Интуит", 2016, 571 с.

6. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. Учрежд. высш. проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2013, 336 с.

7. Проскурин В.Г. Защита в операционных системах: Издательство: Горячая линия – Телеком, 2014, 192 с.

8. Савченко Е.А. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с.

9. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.

10. Корепова В.В. Киберспорт как основа создания спортивных кластеров // Кластеры. Исследования и разработки. - 2017. - Т 3. - № 3 (8).

11. Панкина В.В., Хадиева Р.Т. Киберспорт как явление XXI века // Физическая культура. Спорт. Туризм. Двигательная рекреация. - 2016. -

12. Рассел, Д. Киберспорт / Джесс Рассел, Рональд Кон = Jess Russell, Ronald Cohn.: VSD, 2012. - 118 с.

Интернет –ресурсы

1. Федерация компьютерного спорта России https://resf.ru.
2. История развития киберспорта в России и мире http://киберспорт.рф .
3. Steam - https://store.steampowered.com/about/Steam?l=russian
4. Discord - https://discord.com/download
5. Origin - https://www.origin.com/rus/ru-ru/store/download
6. Riot Client - https://www.riotgames.com/en
7. TeamSpeak - https://www.teamspeak.com/en/downloads/
8. World of Tanks - https://worldoftanks.ru/
9. Dota2 - https://www.dota2.com/home?l=russian

Приложение 1

Тестовые вопросы по модулю – кибербезопасность.

Вводный уровень контроля.

Примерные вопросы.

1. Как развивалась компьютерная техника и как устроены компьютер и интернет в настоящее время.
2. Угрозы для мобильных устройств.
3. Защита персональных данных, почему она нужна.
4. Категории персональных данных.
5. Биометрические персональные данные.
6. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение).
7. Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях.
8. Интернет как оружие массового поражения. Социальные последствия безответственного поведения в интернете.

Текущий контроль.

1. Хакерские атаки. Виды атак. Расследование кибератак.

Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Кибершпионаж.

2. Кодирование и шифры.

Введение в тему криптографии.

Разбор древних криптографических задач.

Виды шифров и их сферы применения в настоящее время.

Практика шифрования (Шифр Цезаря и т.п.).

3. Файловая система. Интерфейс командной строки.

Устройство файловой системы: виды, применение.

Для чего используется командная строка. Типы команд.

Обзор базовых команд и практика их применения.

4. IP-адресация. Доменная система имен.

Как устроена IP адресация.

Система DNS и принципы его работы.

Уровни взаимодействия сетей.

Сетевая топология.

Решение задач на определение количества компьютеров в сети.

5. Что такое вредоносный код и какие у него возможности?

Что такое зловредное программное обеспечение.

Его виды и принципы работы.

Способы распространения.

Целевая атака и расследование кибератак.

Крупные кибератаки, с которыми сталкивались пользователи интернета в последнее время.

6. Онлайн-мошенничество. Виды угроз, который можно встретить в сети.

Виды интернет - мошенничества.

Фишинг (фарминг). Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы.

7. Безопасность в социальных сетях. Настройки приватности.

Угрозы, с которыми можно столкнуться в социальных сетях.

Спам и фишинг. Виды спама.

Подделка профилей пользователей.

Похищение логина и пароля.

Как использовать настройки приватности для того, чтобы обезопасить свои данные в социальной сети. Какую информацию не стоит оставлять в открытом доступе.

8. Методы социальной инженерии. Поиск информации в сети.

Какими уловками пользуются злоумышленники для того, чтобы похитить информацию у пользователей.

Поиск информации о личности. Поиск информации о различных фактах. Какую информацию пользователи оставляют в сети? Команды для поисковых запросов.

Итоговый контроль.

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных

- Разработка и установка во всех компьютерных правовых сетях журналов учета действий

+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство

+ Перехват данных, хищение данных, изменение архитектуры системы

- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая

- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети

- инсайдерства в организации

- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных

- Информационные системы, психологическое состояние пользователей

- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации

- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности

- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний

+ органы права, государства, бизнеса

- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков

- Внедрение аутентификации, проверки контактных данных пользователей

тест

10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)

- Рисков безопасности сети, системы

- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)

- Усиления основного звена сети, системы

- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)

- Перехода в безопасное состояние работы сети, системы

- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

- Одноуровневой защиты сети, системы

- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой

+ Логические закладки («мины»)

- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить

- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения

- Секретность информации определена скоростью передачи данных

+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь

+ Электронно-цифровая подпись

- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО

+ Ошибки эксплуатации и неумышленного изменения режима работы системы

- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования

- Моральный износ сети, инсайдерство

+ Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет

+ Вирусы в сети, логические мины (закладки), информационный перехват

- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе

- Изменением формы информации

- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность

- Доступность

- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие

- Детерминированное (всегда определенное) событие

- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной

- Правовой

+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

+ Программные, технические, организационные, технологические

- Серверные, клиентские, спутниковые, наземные

- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети

- Администратор сети

- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности

- Инструкций, алгоритмов поведения пользователя в сети

- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер

- Аудит, анализ безопасности

+ Аудит, анализ уязвимостей, риск-ситуаций

Приложение 2

Тестовые вопросы по модулю КИБЕРСПОРТ.

Вводный уровень

История киберспорта.

Виды компьютерных игр.

Дисциплины, по которым проходят турниры.

Основные классы компьютерных игр, возможность их использования для развития способностей, применение игр в качестве обучающих программ.

Конфигурация компьютера, установка новых элементов.

Совместимость комплектующих компьютера, согласование параметров одних устройств с другими, требования к энергоснабжению.

Текущий уровень

1.Выбор и настройка периферийных игровых устройств. Программы для текстового и голосового общения во время игры. Настройка приватности в программах для общения.

Ассортимент современных игровых аксессуаров. Их технические характеристики и особенности. Способы и приёмы их настройки. VR-устройства. Рекомендации по использованию.

Установка настроек аппаратуры, установка графических и звуковых настроек.

Компьютерные программы, предназначенные для голосового общения в сети Интернет.

Принципы работы, настройка и особенности использования на примере программы Discord.

Настройка программы TeamSpeak, выбор сервера и подключение к нему.

2. Программы для онлайн трансляций игр.

Знакомство с сервисами для игры через Интернет.

Предоставляемые возможности игровой платформы.

Установка, настройка и использование Steam.

3.Тактики и стратегия ведения игр.

Командные стратегии и тактические приёмы при игре в команде.

Особенности реализации своей роли в команде при различных игровых моментах.

4. Распределение ролей в команде (на примере 1-2 игр)

Особенности игры на каждой роли в команде по киберспортивной дисциплине.

Различные тактические приёмы, используемые при игре на каждой роли в команде по киберспортивной дисциплине.

5. Просмотр и обсуждение профессиональных матчей.

Командные стратегии и тактические приёмы, применяемые профессиональными игроками на чемпионатах.

Особенности их реализации в различных игровых моментах.

Изменения стратегии команды в зависимости от стратегии противника.

6. Практика командных игр (специализация) - выбор конкретной дисциплины.

Основные направления современных командных соревновательных киберспортивных дисциплин.

Примеры различных дисциплин этих направлений.

Правила киберспортивной дисциплины.

Дополнительное программное обеспечение, используемое в киберспортивной дисциплине.

Различные роли в команде по киберспортивной дисциплине, особенности игры на каждой роли в команде по киберспортивной дисциплине.

7. Требования к физической подготовленности в киберспорте.

Роль физической формы в игровом процессе.

Комплекс физических упражнений для развития общей и статической выносливости.

Комплекс специальных физических упражнений для развития быстроты реакции, точности движения, двигательной памяти, мышечной чувствительности.

Итоговый контроль

Правильный вариант ответа **выделен**

1. В каком году киберспорт был официально признан спортом в Российской Федерации?

a) **2001**
b) 2010
c) 2020

2. В каком году проводился первый турнир The International по дисциплине Dota 2?

a) 2010
b) **2011**
c) 2012

3. В каком году основана Федерация компьютерного спорта России?

a) **2000**
b) 2005
c) 2010

4. Какая российская киберспортивная организация победила на турнире The International 10 в 2021 году?
a) Virtus.PRO
b) **Team Spirit**
c) Team Empire

5. Какие существуют уровни танков в дисциплине World of Tanks
a) 1-5
b) **1-10**
c) 1-15

6. С каких устройств разрешены соревнования по мобильным играм
a) Планшеты
b) **Смартфоны**
c) Эмуляторы

7. Как называется соревновательный режим в Dota2
a) **Captains Mode**
b) Captains Draft
c) Tournament Mode

8. Как расшифровывается DOTA
a) Defense of the authority
b) **Defense of the ancients**
c) Defense of the arcade

9. Как называется спортивная дисциплина компьютерного спорта, в которой противоборствующие стороны участников соревнований на арене в реальном времени позиционируют и маневрируют объектами управления, для защиты районов карты и / или уничтожения активов своих соперников.
a) Соревновательная головоломка
b) **Стратегия в реальном времени**
c) Спортивный Симулятор
d) Технический симулятор
e) Боевая арена

10. С какого возраста допускаются обучающиеся к соревнованиям по Киберспорту?
a) с 12 лет;
b) **с 14 лет;**
c) с 16 лет;
d) с 17 лет.