

# РУКОН ЦЕЛЬ

МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

Автономная некоммерческая организация  
дополнительного профессионального образования  
«Многопрофильный центр квалификаций «Цель»

**УТВЕРЖДАЮ**

Директор АНО ДПО «МЦК «Цель»

О. В. Самоварова

Приказ №3п/2023-БО

от «03» апреля 2023 г.

Одобрена на заседании  
педагогического совета

Протокол №3 от «03» апреля 2023 г



**ДОПУЩЕНО**

Председатель президиума ЭНМС

Ю.И. Глаголева

подпись

2023 г.



Дополнительная общеобразовательная  
общеразвивающая программа

**«КИБЕРЗАЩИТНИК I уровень»**

(5 акад. час.)

Автор-составитель:

Сойманова Светлана Викторовна, методист

г. Санкт-Петербург, 2023 г.

## 1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная общеразвивающая программа «Киберзащитник I уровень» АНО ДПО «МЦК «Цель» (далее – Программа) имеет техническую направленность.

**1.1. Нормативно-правовую основу** разработки Программы составляют:

- Конституция Российской Федерации;
- Федеральный закон "Об образовании в Российской Федерации" от 29.12.2012 N 273-ФЗ;
- Приказ Министерства просвещения РФ от 27 июля 2022 г. N 629 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам";
- Приказ Минобрнауки России от 23.08.2017 N 816 "Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ";
- Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 г. № 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 N 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";
- Концепция развития дополнительного образования детей до 2030 года (утверждена распоряжением Правительства Российской Федерации от 31 марта 2022 г. № 678-р);

- Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы) (Приложение к письму Департамента государственной политики в сфере воспитания детей и молодежи Министерства образования и науки РФ от 18.11.2015 № 09-3242);

- Устав Автономной некоммерческой организации дополнительного профессионального образования «Многопрофильный центр квалификаций «Цель».

## **1.2. Актуальность программы**

В современном мире информационная безопасность является одной из самых актуальных и важных тем. Все больше людей используют интернет для своих повседневных задач, а также для работы и учебы. С одной стороны, это дает огромные возможности для получения знаний и общения с людьми со всего мира. С другой стороны, в интернете есть множество угроз и опасностей, таких как вирусы, хакеры, мошенничество и многие другие.

Изучение навыков компьютерной безопасности важно для учащихся по многим причинам:

1. Защита личной информации. В цифровую эпоху все больше личной информации о людях хранится в цифровом формате. Злоумышленники могут использовать эту информацию для мошенничества, кражи личности и других преступлений. Изучение навыков компьютерной безопасности поможет старшеклассникам защитить свою личную информацию и избежать негативных последствий.

2. Защита компьютерных систем. Компьютерные системы используются в различных областях, и их защита очень важна. учащиеся могут изучать навыки компьютерной безопасности, чтобы защитить компьютерные системы своей школы, колледжа или университета от вредоносных программ и кибератак.

3. **Карьерные возможности.** Навыки компьютерной безопасности являются очень востребованными на рынке труда, и изучение их может помочь учащимся получить конкурентные преимущества при поступлении в университет или при поиске работы в области технологий.

4. **Понимание технологического мира.** Сегодня технологии окружают нас повсюду, и понимание, как они работают, может быть полезным для жизни и карьеры старшеклассников. Изучение навыков компьютерной безопасности поможет им понять, как работают различные программы и как они могут быть защищены от вредоносных программ и кибератак.

В целом, изучение навыков компьютерной безопасности может быть полезным для учащихся в различных аспектах их жизни, от личной безопасности до карьерных возможностей.

### **1.3. Новизна программы**

Все знают правила поведения в интернете и за компьютером. О том что нельзя переходить на подозрительные сайты, открывать письма от неизвестных отправителей, иметь на своем рабочем компьютере и телефоне антивирус. Но никто, никогда не объяснял почему нужно вести себя именно так. Мы говорим “Вирус”, но не понимаем как он работает, говорим хакер, но не знаем кто это и чем именно занимается. На данном курсе мы не только расскажем о методах противодействия хакерским атакам, интернет-мошенникам и вредоносному программному обеспечению, но и покажем как происходит хакерская атака на сайт, как злоумышленник ищет уязвимости в обороне сайта и как пользуется в полученной информацией, как работает вирус и чем он в действительности опасен. Курс расскажет не только о том как определить зараженные или вредоносные ресурсы в сети интернет, но что делать, если вы все таки на них попали. В рамках данного курса будет развенчан романтический образ хакеров и показан реальный ущерб от действий хакеров.

#### **1.4. Отличительные особенности программы**

Отличительными особенностями данной программы является ориентированность на практическое подтверждение доводимой до учащихся информации. Все что учащиеся увидят в рамках данного курса будет подкреплено реальными живыми примерами. Также данный курс покажет реальный ущерб от хакерских атак и противоправных действий в области информационной безопасности, разрушающий миф о романтизме хакерства. В процессе обучения учащиеся узнают о том как неосмотрительные действия школьника при использовании устройств и сети интернет могут повлиять не только него самого, но и на окружающих.

Преподаватели курса являются действующими специалистами ведущих компаний страны в области информационной безопасности. Они имеют огромный опыт и возможность продемонстрировать тот или иной пример с различных точек зрения. Благодаря этому примеры, демонстрируемые преподавателями, становятся более понятными и живыми, что повышает интерес обучающихся к занятиям.

#### **1.5. Цель программы**

Знакомство учащегося с потенциальными угрозами при использовании современного программного обеспечения и сети интернет, способами их выявления и устранения при использовании информационных систем. Начальная профориентация учащегося.

#### **1.6. Задачи программы**

***Обучающие:***

- формирование навыков по оценке уязвимости компьютерных сервисов;
- знакомство с методами и инструментами киберзащиты.

***Развивающие:***

- развитие познавательных умений (поиск и выделение необходимой информации, структурирование знаний, самостоятельное создание

алгоритмов деятельности при решении проблем творческого и поискового характера);

- развитие регулятивных умений (ставить цели, планировать собственную деятельность и способы достижения результата, осуществлять контроль и коррекцию деятельности);

- развитие коммуникативных умений (планирование учебного сотрудничества, умение полно и точно выражать свои мысли в соответствии с задачами коммуникации, умения в разрешении конфликтов и т.д.);

- развитие технических способностей обучающегося, внимания, мышления, памяти, воображения, мотивации к дальнейшему изучению программирования;

- развитие индивидуальных творческих способностей.

***Воспитательные:***

- формирование навыков коллективной работы учащихся;

- формирование у учащихся самостоятельности, ответственности, социальной активности;

- формирование готовности учащихся к сознательному выбору направления своей профессиональной деятельности в соответствии с личными интересами и способностями, с учетом социокультурной и экономической ситуации в регионе и стране.

**1.7. Планируемые результаты обучения**

В результате освоения программы, учащиеся будут обладать набором определенных предметных, метапредметных и личностных компетенций

***Предметные:***

- у учащихся будет сформирована система знаний в области анализа и оценки уязвимости компьютерных сервисов;

- учащиеся приобретут знания методики киберзащиты и освоят инструменты по предотвращению компьютерных угроз.

***Метапредметные:***

- у учащихся разовьется творческий потенциал;
- у учащихся разовьется культура речи, обогатится словарный запас;
- учащиеся научатся анализировать, логически и образно мыслить.

**Личностные:**

- у учащихся сформируются навыки коллективной работы;
- у учащихся сформируется самостоятельность, ответственность, социальная активность;
- у учащихся сформируется готовность к сознательному выбору направления своей профессиональной деятельности в соответствии с личными интересами и способностями, с учетом социокультурной и экономической ситуации в регионе и стране.

**1.8. Содержание** Программы представлено общей характеристикой, учебным планом, календарным учебным графиком, содержанием тем, планируемыми результатами освоения Программы, условиями реализации и системой оценки результатов освоения Программы.

**1.9. Категория обучающихся**

Программа рассчитана на учащихся в возрасте от 12 до 18 лет.

**1.10. Форма обучения:** очно-заочная с применением электронного обучения и дистанционных образовательных технологий

**1.11. Режим занятий**

Учебная нагрузка по программе составляет не более 5 учебных занятий в неделю. Продолжительность занятия – 30 минут. Занятия проводятся по группам, подгруппам или индивидуально.

Занятия начинаются не ранее 8.00 часов утра и заканчиваются не позднее 18.00 часов.

**1.12. Трудоемкость программы**

Нормативная трудоемкость обучения по Программе – 5 академических часов, включая все виды аудиторной и внеаудиторной учебной работы учащихся.

**1.13. Форма документа, выдаваемого по результатам освоения программы**

По результатам освоения программы учащимся выдается сертификат о прохождении обучения установленного образовательной организацией образца.



## 2. СОДЕРЖАНИЕ ПРОГРАММЫ

### 2.1. УЧЕБНЫЙ ПЛАН ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «КИБЕРЗАЩИТНИК I уровень»

№ п/п	Наименование тем	Количество часов (ак. час)				Формы аттестации/ контроля
		Всего	Теория	Практика	Самостоятел ьная работа	
1	2	3	4	5	6	7
1.	Противодействие хакерским атакам	1	2/3	-	1/3	Опрос
2.	Защита сайта от взлома	1	2/3	-	1/3	Опрос
3.	Безопасность личных данных	1	2/3	-	1/3	Опрос
4.	Доступные методы и инструменты киберзащиты	1	2/3	-	1/3	Опрос
5.	Итоговое тестирование	1	1/3	-	2/3	Тест
	<b>Итого часов</b>	<b>5</b>	<b>3</b>	<b>-</b>	<b>2</b>	

## 2.2. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Наименование тем	Аудиторные занятия		Всего часов
	1 день	2 день	
1. Противодействие хакерским атакам	Т 2/3 (ДОТ)	СР 1/3 (ДОТ)	1
2. Защита сайта от взлома	Т 2/3 (ДОТ)	СР 1/3 (ДОТ)	1
3. Безопасность личных данных	Т 2/3 (ДОТ)	СР 1/3 (ДОТ)	1
4. Доступные методы и инструменты киберзащиты	Т 2/3 (ДОТ)	СР 1/3 (ДОТ)	1
5. Итоговое тестирование	СР 2/3 (ДОТ)	Т 1/3 (ДОТ)	1
Всего часов	3 <sup>1/3</sup>	1 <sup>2/3</sup>	5

*Примечание:*

«Т1» - теоретическая подготовка, 2/3 час.; «СР» - самостоятельная работа, 1/3 час.; «ДОТ» - дистанционные образовательные технологии.

### 2.3. СОДЕРЖАНИЕ ТЕМ

#### Тема 1. Противодействие хакерским атакам (1 час)

*Теория.* Методы и способы цели хакерских атак. Влияние хакерских атак на общество. Потенциальные жертвы хакеров и возможные последствия. Развенчание романтического образа хакера. Невольные соучастники хакерских атак. Как не стать соучастником выгоды хакерских атак, риски и последствия в результате неудачи. Сравнение выгод и рисков.

*Самостоятельная работа.* Закрепление пройденного материала

#### Тема 2. Защита сайта от взлома (1 час)

*Теория.* Демонстрация реального взлома демонстрационного сайта. Основные методы и подходы к взлому сайтов. Пострадавшие и последствия. Выстраивание обороны сайта и противодействие атакам. Чек лист проверки сайта на устойчивость к базовым методам взлома.

*Самостоятельная работа.* Закрепление пройденного материала

#### Тема 3. Безопасность личных данных (1 час)

*Теория.* Какие данные необходимо защищать. Как "утекают" личные данные. Способы использования личных данных. Влияние утечки ваших личных на окружающих. Как защитить свои личные данные и окружающих.

*Самостоятельная работа.* Закрепление пройденного материала

#### Тема 4. Доступные методы и инструменты киберзащиты (1 час)

*Теория.* Демонстрация ошибочных действий пользователя при взаимодействии с компьютером и в сети интернет. Демонстрация последствий таких действий для себя и окружающих. Демонстрация скорости подбора паролей в зависимости от требований к их сложности. Как без навыков программирования распознать потенциально вредоносный сервис. Что делать если вы уже использовали вредоносный сервис.

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ**

#### **3.1. МАТЕРИАЛЬНО – ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ**

С целью реализации Программы с применением исключительно электронного обучения, дистанционных образовательных технологий в образовательной организации созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся.

##### **Требуемое оборудование**

Каждому участнику образовательного процесса необходимо иметь персональный компьютер с доступом в сеть Интернет.

##### **Требуемое программное обеспечение (для учащихся)**

Рекомендовано: браузер Yandex, ОС Astra Linux, офисный пакет Р7-Офис для Astra Linux.

##### **Наименование систем, ресурсов, программ, оборудования, используемых в образовательном процессе**

###### **1. Информационно-коммуникационные системы:**

- Операционная система: Astra Linux;
- Среда виртуализации VirtualBox;
- браузер Yandex.

###### **2. Система дистанционного обучения (СДО):**

- Вебинар.Ру.

### 3.2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ (ЛИТЕРАТУРА)

Учебно-методическое обеспечение учебного процесса с применением электронного обучения, дистанционных образовательных технологий включает электронные информационные образовательные ресурсы (ЭИОР), размещенные на электронных носителях и/или в электронной среде поддержки обучения.

№ п/п	Наименование темы	Перечень электронных информационных ресурсов (электронно-библиотечных ресурсов и систем, информационно-справочных систем)	Перечень электронных образовательных ресурсов
1.	Противодействие хакерским атакам	<p>Центр кибербезопасности. АНО «Центр реагирования на компьютерные инциденты»: официальный сайт. - Москва. - URL: <a href="https://www.cert.ru/">https://www.cert.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>Журнал "Хакер" [Электронный ресурс]. ИП Югай Александр Олегович: официальный сайт. – г. Волгоград. - URL: <a href="https://xakep.ru/">https://xakep.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>Центр обеспечения безопасности информации "Лаборатория Касперского". АО «Лаборатория Касперского»: официальный сайт. - Москва. - URL: <a href="https://www.kaspersky.ru/">https://www.kaspersky.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://habr.com/ru/hub/security/">https://habr.com/ru/hub/security/</a></p>	<p>Журнал "Хакер" [Электронный ресурс]. ИП Югай Александр Олегович: официальный сайт. – г. Волгоград. - URL: <a href="https://xakep.ru/">https://xakep.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>Security News: Информационно-аналитическое издание по техническим средствам и системам безопасности: официальный сайт. – Издательство «Секьюрити Фокус». Москва. - URL: <a href="https://www.secnews.ru/">https://www.secnews.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>"SecurityLab.ru": официальный сайт. Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://www.securitylab.ru/">https://www.securitylab.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p>

		(дата обращения: 31.03.2023). – Текст: электронный.	
2.	Защита сайта от взлома	<p>Центр кибербезопасности. АНО «Центр реагирования на компьютерные инциденты»: официальный сайт. - Москва. - URL: <a href="https://www.cert.ru/">https://www.cert.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>Журнал "Хакер" [Электронный ресурс]. ИП Югай Александр Олегович: официальный сайт. – г. Волгоград. - URL: <a href="https://xakep.ru/">https://xakep.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>"SecurityLab.ru": официальный сайт. Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://www.securitylab.ru/">https://www.securitylab.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://habr.com/ru/hub/security/">https://habr.com/ru/hub/security/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p>	<p>Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://habr.com/ru/hub/security/">https://habr.com/ru/hub/security/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>"SecurityLab.ru": официальный сайт. Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://www.securitylab.ru/">https://www.securitylab.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>Pentestit.ru. ООО «ПентестИТ»: официальный сайт. – г. Орел. - URL: <a href="https://pentestit.ru/">https://pentestit.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p>
3.	Безопасность личных данных	<p>Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор): официальный сайт. – Москва. - URL: <a href="https://rkn.gov.ru/">https://rkn.gov.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p> <p>Национальный координационный центр по компьютерным инцидентам. Федеральная служба безопасности Российской Федерации: официальный сайт. – Москва. - URL: <a href="https://cert.gov.ru/">https://cert.gov.ru/</a> (дата обращения: 31.03.2023). –</p>	<p>Центр кибербезопасности. АНО «Центр реагирования на компьютерные инциденты»: официальный сайт. - Москва. - URL: <a href="https://www.cert.ru/">https://www.cert.ru/</a> (дата обращения: 31.03.2023). – Текст: электронный.</p>

		<p>Текст: электронный. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://habr.com/ru/hub/security/">https://habr.com/ru/hub/security/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный. Центр кибербезопасности. АНО «Центр реагирования на компьютерные инциденты»: официальный сайт. - Москва. - URL: <a href="https://www.cert.ru/">https://www.cert.ru/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный.</p>	
4.	Доступные методы и инструменты киберзащиты	<p>Центр кибербезопасности. АНО «Центр реагирования на компьютерные инциденты»: официальный сайт. - Москва. - URL: <a href="https://www.cert.ru/">https://www.cert.ru/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный. Журнал "Хакер" [Электронный ресурс]. ИП Югай Александр Олегович: официальный сайт. – г. Волгоград. - URL: <a href="https://xakep.ru/">https://xakep.ru/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный. Национальный координационный центр по компьютерным инцидентам. Федеральная служба безопасности Российской Федерации: официальный сайт. – Москва. - URL: <a href="https://cert.gov.ru/">https://cert.gov.ru/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный. "SecurityLab.ru": официальный сайт. Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://www.securitylab.ru/">https://www.securitylab.ru/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. -</p>	<p>Интернет-портал. Безопасность пользователей в сети интернет. Национальный координационный центр по компьютерным инцидентам: официальный сайт. - Москва. - URL: <a href="https://safe-surf.ru/">https://safe-surf.ru/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный. "SecurityLab.ru": официальный сайт. Positive Technologies: официальный сайт. - Москва. - URL: <a href="https://www.securitylab.ru/">https://www.securitylab.ru/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный. Интернет-портал. ISO27000.RU. ООО «Максимастер»: официальный сайт. – Москва. - URL: <a href="https://maximaster.ru/portfolio/site/iso27000/">https://maximaster.ru/portfolio/site/iso27000/</a> (дата обращения: 31.03.2023). –</p> <p>Текст: электронный.</p>

		URL: <a href="https://habr.com/ru/hub/security/">https://habr.com/ru/hub/security/</a> (дата обращения: 31.03.2023). – Текст: электронный.	
--	--	---	--

**Примечание:**

Перечень учебной литературы определяется образовательным учреждением. Список рекомендуемой литературы представлен в Приложении 3.

**3.3. ИНФОРМАЦИОННО-МЕТОДИЧЕСКИЕ УСЛОВИЯ  
РЕАЛИЗАЦИИ ПРОГРАММЫ ВКЛЮЧАЮТ:**

1. учебный план;
2. календарный учебный график;
3. образовательную программу;
4. методические материалы и разработки;
5. расписание занятий.

**3.4. КАДРОВОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ**

Педагогическая деятельность по реализации Программы осуществляется лицами, имеющими среднее профессиональное или высшее образование (в том числе по направлению, соответствующему направлению дополнительной общеобразовательной программы) и отвечающим требованиям профессионального стандарта "Педагог дополнительного образования детей и взрослых", утвержденного приказом Минтруда России от 5 мая 2018 г. N 298н.

Персональный состав педагогических работников, обеспечивающих реализацию образовательного процесса, отражен в Приложении 2.

**4. ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ  
ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА**



Обучение по программе осуществляется в очно-заочной форме с применением электронного обучения и дистанционных образовательных технологий.

Образовательный процесс осуществляется как в режиме онлайн, в форме вебинаров, так и в режиме оффлайн в форме самостоятельной работы учащихся.

Образовательная деятельность учащихся предусматривает следующий вид учебных занятий: лекции, самостоятельную работу, определенные учебным планом.

При реализации Программы используются различные образовательные технологии во время проведения аудиторных (онлайн) занятий: технология «перевернутого класса», геймификация, кейс-технология, онлайн-конференция и т.д.

## **5. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ**

Оценка качества освоения программы осуществляется в виде текущего контроля знаний обучающихся, итогового тестирования.

Текущий контроль знаний осуществляется преподавателем в форме опроса. Перечень вопросов текущего контроля знаний обучающихся представлен в Приложении 1.

Итоговое тестирование состоит из 10 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала. (Приложение 1).

### ***Критерии оценки результатов выполнения итогового тестирования***

По результатам прохождения итогового тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев:

отметка «зачтено» – 30% и более правильных ответов;

отметка «не зачтено» – менее 30% правильных ответов.

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

### Примеры вопросов текущего контроля знаний

1. Что такое кибербезопасность и зачем она нужна?
2. Что такое хакерство и какие существуют виды хакерских атак?
3. Какие виды киберугроз существуют?
4. Что такое вирусы и как они распространяются?
5. Какие есть способы защиты своего компьютера от вирусов?
6. Что такое "фишинг" и как от него защититься?
7. Какие есть способы создания надежного пароля?
8. Какие существуют методы шифрования данных и зачем они нужны?
9. Что такое двухфакторная аутентификация и как она работает?
10. Какие есть основные правила безопасности при работе в интернете?
11. Что делать, если ваша учетная запись была взломана?
12. Какие есть программы для обнаружения и удаления вирусов?
13. Как работает защита сайтов от взлома и какие меры безопасности нужно принимать при создании сайта?
14. Какие есть виды атак на сайты и как от них защититься?
15. Что такое "бэкап" и зачем он нужен для защиты данных?

### Примеры вопросов итогового тестирования

1. Какого типа тестирования безопасности приложений не существует?
  1. Black-box
  2. White-box
  3. Red-box
  4. Grey-box

**2. В чем заключаются task-based CTF соревнования?**

1. Противостояние команд Red Cell (взломщиков) и Blue Cell (защитников)
2. Поиск флага в процессе заданий на хакинг
3. Проведение тестирования безопасности реальных систем
4. Анализ веб-приложения на уязвимости

**3. Как называется атака перебора пароля по словарю?**

1. Bug bounty
2. Фаззинг
3. Brute-force
4. XSS

**4. Какое средство защиты чаще всего используют для веб-приложений?**

1. Web Application Firewall
2. Web Scanner
3. Host-based Firewall
4. Vulnerability Scanner

**5. Какой категории персональных данных не существует?**

1. Общедоступные
2. Иные
3. Личные
4. Биометрические

**6. Какой инструмент используется для перехвата и анализа трафика в сети?**

1. Burp Suite Intruder
2. Burp Suite Repeater
3. Wireshark
4. Hydra

**7. Главный документ, определяющий законодательство в сфере ПДн в Российской Федерации?**

1. Постановление Правительства №1119
2. Федеральный закон №152
3. Приказ ФСТЭК №21
4. Федеральный закон №149

**8. Что такое хеш пароля?**

1. Значение, зависимое от логина и пароля вместе
2. Результат взлома пароля
3. Строка, применяемая для авторизации вместо пароля
4. Набор символов после применения к паролю математической функции

**9. Зачем нужен SSL-сертификат сайта?**

1. Для шифрования подключений
2. Для подтверждения подлинности сайта
3. Для использования средств защиты
4. Для удаленного подключения к серверу

**10. Выставьте в верном порядке приведенные пароли от самого безопасного (1) до самого небезопасного (4). (Пример ответа - abcd)**

1. \$p0ngeB0b
2. SecurePassworD
3. lJ6SFg1wc5
4. K6%7NZ#EQh^\*EZ8

**ПЕРСОНАЛЬНЫЙ СОСТАВ ПЕДАГОГИЧЕСКИХ  
РАБОТНИКОВ**

№ п/п	ФИО	Занимаемая должность	Сведения об уровне образования	Квалификация	Наименование направления подготовки и (или) специальности	Сведения об имеющихся: ученой степени, ученом звании	Сведения о повышении квалификации и (или) профессиональной переподготовке	Общий стаж работы	Стаж работы по специальности	Преподаваемые темы
1.	Почаевец Андрей Андреевич	Программный директор АНО ДПО МЦК "Цель", преподаватель линейки программ 1С	Высшее профессиональное;  Среднее профессиональное	Инженер;  Техник	Информационные системы и технологии  Программное обеспечение вычислительной техники и автоматизированных систем	-	2021 Luxoft training Luxoft training, REQ-065 Управление требованиями в Agile; 2020 Первый Бит Первый Бит, Управленческий учет в "1С:Зарплата и управление персоналом КОРП"; 2020 Первый Бит Первый Бит, Кадровый учет в "1С:Зарплата и управление персоналом 3.1"; 2020 ИнфоСтарт	19 лет	1 год	Тема 2

							ИнфоСтарт, DevOps для 1С			
2.	Бердашкевич Артём Эдуардович	Генеральный директор ИТ-компании "Tiger- Tag"	Высшее	Магистр	Информационная безопасность	-	Анализ рисков информационной безопасности предприятия. Безопасность IoT устройств. Построение защищенных информационных систем. Этический хаккинг и тестирование на проникновение	6 лет	1 год	Тема 1
3.	Лукьянцев Игорь Сергеевич	Специалист по информационной безопасности	Среднее профессиональное	Техник-программист	Программирование в компьютерных системах	-	-	2 года	2 года	Тема 3
4.	Яицкий Антон Андреевич	Специалист по информационной безопасности	Высшее	Магистр	Информационная безопасность	-	Администрирование ОС Astra Linux: Расширенное администрирование - РусБИТех-Астра QA School - Digital Design; Программирование и автоматизация	1 год	1 год	Тема 4

							Python - повышен ие квалифик ации Универс итет ИТМО			
--	--	--	--	--	--	--	--	--	--	--



## СПИСОК ЛИТЕРАТУРЫ

### Литература для педагога

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учебное пособие / В.Ф. Шаньгин – М.: ИД Форум-Инфра-М, 2023.- 416 с.-ISBN 978-5-8199-0754-2 (ИД «Форум»).
2. Глушаков, С.В., Тесленко, Н.С., Бабенко, М.И. Секреты хакера: защита и атака [Текст] / С.В. Глушаков, Н.С. Тесленко, М.И. Бабенко – М.: АСТ, 2008 -544 с. - ISBN: 978-5-17-050954-6.
3. Скембрей, Джоел, Шема, Майк. Секреты хакеров. Безопасность Web-приложений - готовые решения [Текст] / Джоел Скембрей, Майк Шема – М.: Вильямс, 2003. - 384 с. - ISBN: 5845904102.
4. Малюк, А.А. Защита информации в информационном обществе [Текст]: учебное пособие для вузов / А.А. Малюк. – М.: Горячая Линия - Телеком, 2015. - 230 с. - ISBN: 978-5-9912-0481-1.
5. Бабаш, А.В., Баранова, Е.К. Основы информационной безопасности [Текст]: учебник / А.В. Бабаш, Е.К. Баранова – М.: ИЦ РИОР, 2022.- 202 с. - ISBN: 978-5-369-01806-4.

### Литература для обучающихся

1. Маккарти, Б. Кибердзюцу: кибербезопасность для современных ниндзя [Текст] / Б. Маккарти – СПб: Питер, 2022. - 224 с. - ISBN: 978-5-4461-2958-4.
2. Диогенес, Ю., Озкайя, Э. Кибербезопасность. Стратегии атак и обороны [Текст] / Ю. Диогенес, Э. Озкайя – М.: ДМК Пресс, 2020. - 326 с. ISBN: 978-5-97060-709-1.
3. Коллинз, М. Защита сетей: подход на основе анализа данных : практическое руководство / М. Коллинз ; пер. с англ. А. В. Добровольской. - М: ДМК Пресс, 2020. - 308 с. - ISBN 978-5-97060-649-0. - Текст:

электронный. - URL: <https://znanium.com/catalog/product/1908080> (дата обращения: 30.03.2023).

4. Ломакин, П., Шрейн, Д. Антихакинг [Текст] / П. Ломакин, Д. Шрейн – М.: Майор, 2002. - 512 с. ISBN: 5-901321-45-6.

5. Бирюков, А.А. Информационная безопасность: защита и нападение [Текст] / А.А. Бирюков – М.: ДМК Пресс, 2017. - 536 с. ISBN: 978-5-97060-435-9.

6. Фленов, М.Е. Web-сервер глазами хакера. [Текст] / М.Е. Фленов - 3-е издание, переработанное и дополненное. – М.: БХВ, 2021. - 256 с. ISBN: 978-5-9775-6795-4.