Департамент образования администрации Владимирской области
Государственное автономное образовательное учреждение дополнительного профессионального образования Владимирской области «Владимирский институт развития образования имени Л.И. Новиковой»

Кафедра цифрового образования и информационной безопасности

«УТВЕРЖДАЮ»

«__» _____ 2021

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА-ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Основы кибербезопасности

Владимир
2021

Организация - разработчик: ГАОУ ДПО ВО «Владимирский институт развития образования имени Л.И. Новиковой»

Составители (разработчики):

Мишин Д.В., к.т.н., заведующий кафедрой цифрового образования и информационной безопасности ГАОУ ДПО ВО ВИРО

Программа рекомендована кафедрой цифрового образования и информационной безопасности ГАОУ ДПО ВО ВИРО к использованию в учебном процессе для повышения квалификации сотрудников образовательных организаций в сфере безопасного применения цифровых технологий и Интернет при решении широкого круга задач.

Протокол №22 от «3» марта 2021 г.

Зав.кафедрой _____ Д.В.Мишин

I. Общая характеристика программы

1.1. Нормативно-правовые основания разработки программы

Нормативную правовую основу разработки программы составляют:

- Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях по защите информации»;
- Федеральный закон от с 01.01.2008 г. № 152-ФЗ РФ «О персональных данных»;
- Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию";
- Федеральный закон от 27.07.2010 г. № 210 «Об организации предоставления государственных и муниципальных услуг»
- Доктрина информационной безопасности Российской Федерации от 05.12.2016 № 646 (утверждённая указом Президента РФ);
- Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы";
- Государственная программа РФ «Развитие образования» на 2018-2025 гг. (Утверждено постановлением правительства РФ 26.12.2017.№1642);
- Паспорт национального проекта «Образование» (УТВЕРЖДЕН президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол от 3 сентября 2018 г. №10);
- Постановление Правительства РФ от 26.12 2017 г. № 1642 "Об утверждении государственной программы Российской Федерации "Развитие образования";
- Распоряжение Правительства Российской Федерации от 25.10.2014 г. № 2125-р «Об утверждении Концепции создания единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»;
- Распоряжение Правительства РФ от 14.02.2015 г. №236-р «Об утверждении плана мероприятий ("дорожной карты") по созданию единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»;
- Приказ Минобрнауки России от 1.07.2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Приказ Минобрнауки России от 15.01.2013 №10 «Федеральные государственные требования к минимуму содержания дополнительных профессиональных образовательных программ профессиональной переподготовки и повышения квалификации педагогических работников, а также к уровню профессиональной переподготовки педагогических работников»;
- Приказ Министерства образования и науки РФ от 23.08.2017 г. № 816 "Об утверждении Порядка применения организациями осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ";
- Приказ Минтруда России от 18.10.2013 N 544н (ред. от 05.08.2016) Об утверждении профессионального стандарта "Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель);
- Приказ Министерства образования и науки РФ от 6.10.2009 г. N 373 "Об утверждении и введении в действие федерального государственного образовательного стандарта начального общего образования" (с изменениями и дополнениями);

- Приказ Министерства образования и науки РФ от 17.122010 г. № 1897 "Об утверждении и введении в действие федерального государственного образовательного стандарта основного общего образования» (с изменениями и дополнениями);
- Приказ Министерства образования и науки РФ от 17.05 2012 г. № 413 "Об утверждении и введении в действие федерального государственного образовательного стандарта среднего общего образования» (с изменениями и дополнениями);
- Приказ департамента образования администрации Владимирской области от 7.05.2014 г. № 675 «О введении в рабочую эксплуатацию АИС «Информационный портал системы образования Владимирской области»;
- Приказ департамента образования администрации Владимирской области от 31.12.2014 г. № 1688 «Об утверждении Концепции создания и развития регионального информационного портала Владимирской области»;
- Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (утв. Минобрнауки России от 22.01.2015 г. № ДЛ-1/ 05 ВН);
- Методические рекомендации-разъяснения по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки России от 22.04.2015 г. № ВК-1030/ 06);
- Государственная программа Владимирской области «Информационное общество (2014-2020 годы)»;
- СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях».

Локальные акты

- Положение об итоговой аттестации слушателей по программам повышения квалификации в ГАОУ ДПО ВО ВИРО.
- Положение об организации дополнительного профессионального образования слушателей ГАОУ ДПО ВО ВИРО.

1.2. Область применения программы

Настоящая программа предназначена для повышения квалификации учителей информатики, технологии, ОБЖ, руководителей ОО, администраторов ИБ ОО и ответственных за обеспечение безопасности ПДн в ОО.

1.3. Требования к обучающимся

Высшее профессиональное образование или среднее профессиональное образование по направлениям подготовки «Образование и педагогика» или в области, соответствующей преподаваемому предмету, либо высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательной организации.

1.4. Цель и планируемые результаты освоения программы

Формирование и развитие профессиональных компетенций учителей информатики, технологии, ОБЖ, администраторов ИБ ОО и ответственных за обеспечение безопасности ПДн в сфере цифровых технологий, безопасности в Интернет, получение практики решения вопросов в основных направлениях кибербезопасности.

Обучающийся в результате освоения программы должен владеть:

Обучающийся в результате освоения программы должен владеть:

Код ТФ	ТФ	Практический опыт (Трудовые действия)	Умения	Знания
A/01.6	Педагогическая деятельность по проектированию и реализации образовательного процесса в образовательных организациях дошкольного, начального общего, основного общего, среднего общего образования Общепедагогическая функция. Обучение	– Осуществление профессиональной деятельности в соответствии с требованиями федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего образования – Планирование и проведение учебных занятий – Систематический анализ эффективности учебных занятий и подходов к обучению – Организация, осуществление контроля и оценки учебных достижений, текущих и итоговых результатов освоения основной образовательной программы обучающимися – Формирование навыков, связанных с информационно-коммуникационными технологиями (далее - ИКТ) – Объективная оценка знаний обучающихся на основе тестирования и других методов контроля в соответствии с реальными учебными возможностями детей	– Объективно оценивать знания обучающихся на основе тестирования и других методов контроля в соответствии с реальными учебными возможностями детей – Разрабатывать (осваивать) и применять современные психолого-педагогические технологии, основанные на знании законов развития личности и поведения в реальной и виртуальной среде – Использовать и апробировать специальные подходы к обучению в целях включения в образовательный процесс всех обучающихся, в том числе с особыми потребностями в образовании: обучающихся, проявивших выдающиеся способности; обучающихся, для которых русский язык не является родным; обучающихся с ограниченными возможностями здоровья – Владеть ИКТ-компетентностями: • общепользовательская ИКТ-компетентность; • общепедагогическая ИКТ-компетентность; • предметно-педагогическая ИКТ-компетентность (отражающая профессиональную ИКТ-компетентность соответствующей области человеческой деятельности)	– Преподаваемый предмет в пределах требований ФГОС и основной общеобразовательной программы – Пути достижения образовательных результатов и способы оценки результатов обучения – Основы методики преподавания, основные принципы деятельностного подхода, виды и приемы современных педагогических технологий – Рабочая программа и методика обучения по данному предмету – Приоритетные направления развития образовательной системы Российской Федерации, законов и иных нормативных правовых актов, регламентирующих образовательную деятельность в Российской Федерации, нормативных документов по вопросам обучения и воспитания детей и молодежи, ФГОС начального общего, основного общего, среднего общего образования, законодательства о правах ребенка, трудового законодательства

Сокращения:

ОО – образовательная организация

ИБ – информационная безопасность

СДО – среда дистанционного обучения

Cisco NetAcad - среда дистанционного обучения международной сетевой академии Cisco

1.5. **Форма обучения:** с применением ЭО и ДОТ

Срок обучения: 48 часов.

Режим занятий: индивидуально в соответствии с графиком курса.

1.6. Форма документа, выдаваемого по результатам освоения программы: лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдается сертификат о повышении квалификации.

2. Учебный план

№ п.п	Наименование разделов	Инвариантная часть	Вариативная часть	Всего	Форма аттестации
1.	**Модуль 1.** Знакомство с СДО Cisco NetAcad. Актуальность задачи и содержание основных направлений кибербезопасности	**4**	-	**4**	Практическая работа
2.	**Модуль 2.** Триада ИБ и куб кибербезопасности	**8**	-	**8**	Тестирование, Практическая работа
3.	**Модуль 3.** Понятие угрозы, атаки, риска кибербезопасности	**8**	-	**8**	Тестирование, Практическая работа
4.	**Модуль 4.** Способы обеспечения конфиденциальности цифровой информации	**8**	-	**8**	Тестирование, Практическая работа
5.	**Модуль 5.** Способы обеспечения целостности цифровой информации	**8**	-	**8**	Тестирование, Практическая работа
6.	**Модуль 6.** Способы обеспечения доступности цифровой информации	**8**		**8**	Тестирование, Практическая работа
7.	**Итоговая аттестация. Рефлексия.**	**4**		**4**	Итоговое тестирование
8.	**Итого**	**48**		**48**	

3. Календарный учебный график

Компоненты программы	**Модули**						
	1 м	2 м	3 м	4 м	5 м	6 м	7 м
Модуль 1-7	Л/П	Л/П	Л/П	Л/П	Л/П	Л/П	П
Практика (учебная)	-	-	-	-	-	-	-
Итоговая аттестация							+

4.Рабочие программы учебных модулей

Наименование модулей, практики, тем программы	**Вид учебного занятия**	**Содержание учебного материала**	**Всего часов**
<u>Наименование компонента программы:</u> ***Модуль 1. Знакомство с СДО Cisco NetAcad. Актуальность задачи и содержание основных направлений кибербезопасности***			
Тема 1.1. Знакомство с СДО netacad. Категории защищаемой информации.	Практическое занятие	Информация для учащихся. Описание содержания курса. Описание среды обучения netacad.com —важной части общего взаимодействия между студентами и преподавателями во время обучения в Сетевой академии. Описание принципов и методики обучения в СДО netacad.com Объясняется, что представляет собой кибербезопасность, что такое организационные данные, ПДн и другие	2

		конфиденциальные данные, почему их важно защищать.	
Тема 1.2. Типы киберзлоумышленников и специализации по кибербезопасности. Понятие киберпреступлений, кибервойна	Лекция	Разбирается, кто такие киберпреступники и какие цели они преследуют. Дается классификация киберпреступников. Объясняется, что такое кибервойны и почему в ОО нужны грамотные в вопросах кибербезопасности сотрудники.	2
<u>Наименование компонента программы:</u> ***Модуль 2. Триада ИБ и куб кибербезопасности***			
Тема 2.1. Триада «КЦД». Куб кибер-безопасности	Лекция	Три грани куба кибербезопасности. Принципы информационной безопасности. Триада «КЦД». Состояние данных. Обрабатываемые данные.	2
	Практическое занятие		2
Тема 2.1. Архитектура управления ИБ цифровой среды	Лекция	Средства противодействия угрозам безопасности. Политики и процедуры кибербезопасности. Образовательные и учебные мероприятия по кибербезопасности. Архитектура управления безопасностью ИТ-среды. Модель кибербезопасности ISO.	2
	Практическое занятие		2
<u>Наименование компонента программы:</u> ***Модуль 3. Понятие угрозы, атаки, риска кибербезопасности***			
Тема 3.1. Кибератаки. Классификация и признаки кибератак.	Лекция	Рассматриваются способы анализа последствий кибератаки экспертами по кибербезопасности. Также затрагиваются проблемы уязвимости аппаратного и программного обеспечения и разные категории уязвимости в системе безопасности.	2
	Практическое занятие		2
Тема 3.2. Методы и средства выявления и противодействия кибератакам	Лекция	Приводятся разные типы вредоносного ПО и его симптомы. Рассказывается о разных способах, которые применяют злоумышленники для проникновения в системы, а также описываются атаки типа «Отказ в обслуживании».	2
	Практическое занятие		2
<u>Наименование компонента программы:</u> ***Модуль 4. Способы обеспечения конфиденциальности цифровой информации***			
Тема 4.1. Основы криптографии.	Лекция	Шифрование с закрытым ключом. Процесс симметричного шифрования. Шифрование с открытым ключом. Алгоритмы асимметричного шифрования.	2
	Практическое занятие		2
Тема 4.2. Основы управления доступом	Лекция	Функции управления доступом. Типы средств разграничения доступа. Системы разграничения физического доступа. Идентификация. Методы аутентификации. Типы средств контроля безопасности. Превентивные средства контроля	2
	Практическое занятие		2
<u>Наименование компонента программы:</u> ***Модуль 5. Способы обеспечения целостности цифровой информации***			
Тема 5.1. Электронная	Лекция	Виды средств контроля целостности	2

подпись. Хэш	Практическое занятие	данных. Алгоритмы хеширования. HMAC. Электронные подписи. Подписи и законодательство.	2
Тема 5.2. Сертификаты	Лекция	Базовые сведения о цифровых сертификатах. Использование цифровых сертификатов. Создание цифрового сертификата.	2
	Практическое занятие		2
Наименование компонента программы: ***Модуль 6. Способы обеспечения доступности цифровой информации***			
Тема 6.1. Меры повышения доступности	Лекция	Высокая доступность. Пять девяток. Сферы, в которых реализация концепции «пять девяток» обязательна. Меры по повышению доступности. Многоуровневая защита	2
	Практическое занятие		2
Тема 6.2. Реагирование на инциденты ИБ	Лекция	Реагирование на инциденты. Этапы реагирования на инциденты. Технологии реагирования на инциденты. Системы обнаружения вторжений. Аварийное восстановление. Планирование аварийного восстановления	2
	Практическое занятие		2
Наименование компонента программы: ***Модуль 7. Итоговая аттестация. Рефлексия.***			
Тема 7.1. Итоговое тестирование - Final Exam.	Практическое занятие	Прохождение итогового тестирования	3
Тема 7.2. Отзыв о курсе - End of Course.	Практическое занятие	Рефлексия	1

Требования к итоговому тестированию: Для успешного завершения курса обучающимся необходимо дать не менее 70% правильных ответов в рамках итогового теста.

5.Организационно-педагогические условия реализации программы

5.1. Организация образовательного процесса

Реализация программы подразумевает наличие базового уровня ИКТ компетентности слушателей.

Программой предусмотрена итоговая аттестация в форме итогового тестирования.

Индивидуальные и групповые консультации проходят при непосредственном общении преподавателя и обучающихся средствами СДО.

5.1. Материально-техническое обеспечение

Реализация программы требует наличия:

- технических средств обучения**:** компьютер, подключенный к сети Интернет (для дистанционной формы), актуальные версии браузера.

5.3. Информационное обеспечение обучения

Основные источники:

1. Диогенес, Озкайя: Кибербезопасность. Стратегии атак и обороны Издательство: ДМК-Пресс, 2020 г.
2. Владимир Шаньгин: Информационная безопасность и защита информации. Издательство: ДМК-Пресс, 2017 г.

3. Йован Курбалийя Управление интернетом Проблемы, субъекты, преграды 2017
4. Хранение и защита компьютерной информации : учеб. пособие /Л. Г. Акулов, В. Ю. Наумов ; ВолгГТУ. – Волгоград,2015. – 64 с.ISBN 978–5–9948–1819–0
5. Буряк В. В. Цифровая экономика, хактивизм и кибербезопасность:Монография / В. В. Буряк.–Симферополь:ИП Зуева Т.В., 2019. –140с. ISBN978-5-6041634-3-6

Интернет ресурсы:

1. Материалы курса Cybersecurity Essentional https://www.netacad.com/ru/courses/security/cybersecurity

5.4. Кадровое обеспечение образовательного процесса

Педагогические работники, реализующие дополнительную профессиональную программу, должны удовлетворять квалификационным требованиям, указанным в квалификационных справочниках по соответствующим должностям.

6. Контроль и оценка результатов освоения программы

6.1. Промежуточная аттестация: промежуточная аттестация слушателей предусматривает прохождение тестирования и выполнение практических работ по результатам изучения модулей.

6.2. Итоговая аттестация: итоговая аттестация слушателей проводится после освоения всех модулей программы в форме зачета по совокупности результатов выполнения практических работ и прохождения итогового тестирования.

Оценивание: «зачет/незачет».

Результаты	**Основные показатели оценки результата**
Сформированы навыки, связанные с решением организационных и технических вопросов кибербезопасности **в ОО,** практикой применения средств защиты в ОО.	В ходе тестирования проходит проверка полученных знаний: – в сфере ИКТ, цифровых технологий и кибербезопасности; – о наиболее распространенных рисках, угрозах, атаках и уязвимостях современной киберсреды, – о мерах и средствах защиты ОО от типовых киберугроз. – об основных правилах поведения в сети для обеспечения безопасности Слушатели, успешно освоившие Программу, должны **уметь**: – идентифицировать киберугрозы – описывать разные типы вредоносного ПО и атак – уметь производить простейшую настройку средств защиты – формировать стратегию защиты, используемую ОО для борьбы с атаками