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»

«18» дек 2020

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА-
ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Введение в кибербезопасность (*Introduction to Cybersecurity*)

Владимир

2020

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 школ в сфере применения автоматизированных информационных систем в условиях оказания государственных и муниципальных услуг в электронном виде, являющихся администраторами АИС «Электронная школа».

Протокол №2 от «5» февраля 2020г.

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, руководителей образовательных организаций, 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:

Код ТФ	ТФ	Практический опыт (Трудовые действия)	Умения	Знания
1	2	3	4	5
A/01.7.2	Разработка общей стратегии образовательной организации	Анализировать внутреннюю и внешнюю среду образовательной организации. Выявлять и оценивать возможности и угрозы для организации со стороны внешнего окружения. Принимать, согласовывать и утверждать стратегические решения, разрабатывать принципы функциональных политик.	Анализировать деятельность образовательной организации. Анализировать изменения во внутренней и внешней среде образовательной организации. Оценивать риски. Прогнозировать развитие событий. Управлять проектами с использованием информационных технологий. Формировать организационную стратегию, определять показатели и индикаторы ее достижения.	Методы анализа и взаимодействия образовательной организации и внешней среды. Принципы, методы, технологии анализа факторов внешней среды организации. Принципы, методы, технологии анализа рисков. Информационная открытость системы образования. Мониторинг в системе образования. Законодательство Российской Федерации в сфере образования.
A/07.7.2	Минимизирует риски изменения позиции образовательной организации на рынке образовательных услуг	Анализировать хозяйственно - финансовую деятельность организации (в том числе с участием контрольных организаций). Контролировать расходование средств в соответствии со стратегией организации.	Анализировать деятельность и текущую ситуацию. Вести письменные коммуникации. Аргументировать и отстаивать свое мнение в инновационных проектах.	Методы управления рисками.
B/09.7.1	Управляет основными (технологическими)	Организовывать реализацию планов внедрения новой	Владеть методами оценки эффективности комплекса работ,	Порядок оформления операций и организацию

	процессами	технологии, проведения организационно - технических мероприятий, научно - исследовательских и опытно - конструкторских работ.	отдельных проектов и работ, программ и деловых процессов. Выявлять и анализировать значимые проблемы в сфере своей компетенции для их решения.	документооборота по участкам учета. Правила приема и сдачи оборудования после ремонта. Специализацию подразделений и связи между ними.

Сокращения:

ОО – образовательная организация

ИБ – информационная безопасность

СДО – среда дистанционного обучения

Cisco NetAcad - среда дистанционного обучения международной сетевой академии Cisco

1.5. **Форма обучения:** дистанционная.

Срок обучения: 36 часов (дистанционно).

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	**8**	-	**8**	Тестирование
2.	**Модуль 2.** Понятие угрозы, атаки, риска кибербезопасности	**8**	-	**8**	Тестирование
3.	**Модуль 3.** Методы и средства защиты конфиденциальной информации при использовании Интернет	**8**	-	**8**	Тестирование
4.	**Модуль 4.** Методы и средства обеспечения кибербезопасности в организации	**8**	-	**8**	Тестирование
5.	Прохождение итогового тестирования	**4**	-	**4**	Итоговое тестирование
6.	**Итого**	**36**		**36**	

3. Календарный учебный график

Компоненты программы	**Дни недели**			
	1 д	2 д	3 д	4 д
Модуль 1-4	Л/П	Л/П	Л/П	Л/П
Практика (учебная)	-	-	-	-
Итоговая аттестация				+

4.Рабочие программы учебных модулей

Наименование модулей, практики, тем программы	Вид учебного занятия	Содержание учебного материала	Всего часов
Наименование компонента программы: ***Модуль 1. Знакомство с СДО Cisco Netacad. Актуальность задачи и содержание основных направлений кибербезопасности***			
Тема 1.1. Знакомство со средой дистанционного обучения курса «Введение в кибербез-опасность».	Лекция	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	-
	Практическое занятие		1
Тема 1.2. Категории защищаемой информации	Лекция	Объясняется, что представляет собой кибербезопасность, что такое организационные данные, ПДн и другие конфиденциальные данные, почему их важно защищать.	1
	Практическое занятие		1
Тема 1.3. Типы киберзлоумышленнико в и специализации по кибербезопасности	Лекция	Разбирается, кто такие киберпреступники и какие цели они преследуют. Дается классификация киберпреступников.	1
	Практическое занятие		2
Тема 1.4. Понятие киберпреступлений, кибервойна	Лекция	Объясняется, что такое кибервойны и почему в ОО нужны грамотные в вопросах кибербезопасности сотрудники.	2
	Практическое занятие		-
Наименование компонента программы: ***Модуль 2. Понятие угрозы, атаки, риска кибербезопасности***			
Тема 2.1. 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 2.2. 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
Наименование компонента программы: ***Модуль 3. Методы и средства защиты конфиденциальной информации при использовании Интернет***			
Тема 3.1. Методы и средства защиты конфиденциальной информации	Лекция	Кратко описываются техники аутентификации, которые помогут обеспечить безопасность данных. Приводятся способы повышения безопасности данных в Интернете и	2
	Практическое занятие		2

		правила поведения в сети.	
Тема 3.2. Методы и средства защиты ПДн при работе в Интернет	Лекция	Рассказывается о персональных устройствах и персональных данных. Даются советы по защите устройств, созданию надежных паролей и безопасного пользования беспроводными сетями. Также рассматривается вопрос обеспечения безопасности данных.	2
	Практическое занятие		2
Наименование компонента программы: ***Модуль 4. Методы и средства обеспечения кибербезопасности в организации***			
Тема 4.1. Межсетевое экранирование	Лекция	Описываются технологии и процессы, используемые экспертами по кибербезопасности для защиты сети, оборудования и данных организации. Приводится краткий обзор нескольких типов используемых в настоящее время межсетевых экранов, устройств обеспечения безопасности и программного обеспечения, а также лучших практических рекомендаций.	1
	Практическое занятие		1
Тема 4.2. Анализ информационных потоков	Лекция	Объясняется, что такое ботнеты, убийственная цепочка (kill chain), безопасность на основе поведения и как использовать NetFlow для мониторинга сети.	1
	Практическое занятие		1
Тема 4.3. Методы и средства обнаружения инцидентов безопасности	Лекция	Обсуждается подход Cisco к кибербезопасности, включая команду CSIRT и сборник сценариев по безопасности. Также кратко рассматриваются инструменты, используемые экспертами по кибербезопасности для обнаружения и предотвращения сетевых атак.	1
	Практическое занятие		1
Тема 4.4. Образование в области информационной и кибербезопасности	Лекция	Рассматриваются современные международные программы в области кибербезопасности, направления дальнейшего повышения квалификации.	1
	Практическое занятие		1
Наименование компонента программы: ***Модуль 5. Итоговая аттестация. Рефлексия.***			
Тема 5.1. Итоговая аттестация.	Практическое занятие	Прохождение итогового тестирования	3.
Тема 5.2. Отзыв о курсе - End of Course.	Практическое занятие	Рефлексия	1

Требования к итоговому тестированию: Для успешного завершения курса обучающимся необходимо дать не менее 75% 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, флеш плеера и java.

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 Безопасность (Introduction to Cybersecurity) https://www.netacad.com/ru/courses/security/introduction-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 по результатам каждого модуля.

6.2. Итоговая аттестация: итоговая аттестация слушателей предусматривает прохождение итогового тестирования.

Оценивание: «зачет/незачет».

Итоговая аттестация проводится после освоения всех модулей программы.

Результаты	**Основные показатели оценки результата**
Сформированы навыки, связанные с решением	В ходе тестирования проходит проверка полученных знаний:

организационных и технических вопросов кибербезопасности **в ОО,** практикой применения средств защиты в ОО.	– 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

Харчевникова Елена Львовна

Подписано цифровой подписью: Харчевникова Елена Львовна
Дата: 2021.10.21 09:42:39 +03'00'