МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

ОДОБРЕНО:
Руководитель ОП
_____ С.А. Зайцева
(подпись)
«21» июня 2023 г.

Рабочая программа дисциплины
ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Уровень высшего образования:	магистратура
Квалификация выпускника:	магистр
Направление подготовки:	44.04.01 Педагогическое образование
Направленность (профиль) образовательной программы:	Информационные технологии в профессиональной деятельности педагога

Шуя

1. Цели освоения дисциплины: приобретение знаний о информационной безопасности кибернетических систем, в том числе обеспечение безопасности автоматизированных систем управления технологическими процессами в системе образования.

2. Место дисциплины в структуре ОП

Дисциплина «Основы кибербезопасности» является факультативной дисциплиной.

Успешное освоение данной дисциплины будет способствовать подготовке обучающихся к сдаче и сдаче государственного экзамена, выполнению и защите выпускной квалификационной работы. Студент, приступающий к изучению данной дисциплины, должен:

Знать:

- программно-аппаратные средства реализации ИКТ в педагогическом процессе;
- теоретико-методологические основы самооценки, саморазвития, самореализации;
- направления и источники саморазвития и самореализации.

Уметь:

- оценивать пригодность и качество образовательных ресурсов для организации учебно-воспитательного процесса;
- определять личностные и профессиональные приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.

Владеть:

- методами анализа эффективности использования ИКТ в образовательном процессе;

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

3.1. Компетенции, формированию которых способствует данная дисциплина

При реализации дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

а) универсальные компетенции (УК) и индикаторы их достижения:

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Код и наименование индикатора достижения универсальной компетенции
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6. Способен определять и реализовать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.	УК-6.1. Применяет рефлексивные методы в процессе оценки разнообразных ресурсов (личностных, психофизиологических, ситуативных, временных и т.д.), используемых для решения задач самоорганизации и саморазвития. УК-6.2. Определяет приоритеты собственной деятельности, выстраивает планы их достижения. УК-6.3. Формулирует цели собственной деятельности, определяет пути их достижения с учетом ресурсов, условий, средств, временной перспективы развития деятельности и планируемых результатов. УК-6.4. Критически оценивает эффективность использования

		времени и других ресурсов для совершенствования своей деятельности. УК-6.5. Демонстрирует интерес к учебе и использует предоставляемые возможности для приобретения новых знаний и навыков с целью совершенствования своей деятельности.

б) общепрофессиональные компетенции (ОПК) и индикаторы их достижения:

–

в) профессиональные компетенции (ОПК) и индикаторы их достижения:

Код и наименование профессиональной компетенции выпускника	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ опыта)
Тип задач профессиональной деятельности: педагогический		
ПК-1. Способен применять средства информационно-коммуникационных технологий в решении педагогических задач.	ПК-1.1. Знает: основы методики преподавания с использованием дистанционных образовательных технологий и электронного обучения. ПК-1.2. Умеет: адекватно оценивать портфель образовательных ИКТ-решений для учебного процесса; эффективно использовать стандартные компьютерные приложения и интегрировать современные ИКТ в образовательный процесс; выявлять и внедрять ИКТ-инновации в образовательный процесс. ПК-1.3. Владеет: методиками организации и осуществления образовательного процесса с использованием ИКТ; современными ИКТ, необходимыми для построения эффективных коммуникаций между участниками образовательного процесса; методами анализа эффективности использования ИКТ в образовательном процессе.	Профессиональный стандарт 01.001 «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)»

3.2. Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

- теоретические основы и технологии организации учебно-воспитательного процесса с использованием ИКТ (ПК-1 (индикаторы – 1, 2, 3);
- программно-аппаратные средства реализации ИКТ в педагогическом процессе (ПК-1 (индикаторы – 1, 2, 3);
- способы самоорганизации собственной деятельности и ее совершенствования (УК-6 (индикаторы – 1, 2, 3, 4, 5).

Уметь:

- оценивать пригодность и качество образовательных ресурсов для организации учебно-воспитательного процесса (ПК-1 (индикаторы – 1, 2, 3);

- использовать стандартные компьютерные приложения и интегрировать современные ИКТ в образовательный процесс (ПК-1 (индикаторы – 1, 2, 3);

Владеть:

- методиками организации и осуществления образовательного процесса с использованием ИКТ (ПК-1 (индикаторы – 1, 2, 3);

4. Объём и содержание дисциплины

Очная форма обучения

Объем дисциплины составляет 1 зачетную единицу (27 час.)

Контактная работа 10,75 час.

Самостоятельная работа 16,25 час.

Виды учебных занятий и формы промежуточной аттестации	3 сем.	
	Контактная работа с преподавателем	Самостоятельная работа обучающегося
Практические занятия	10,5	16,25
Зачёт	0,25	-
Всего	10,75	16,25

Заочная форма обучения

Объем дисциплины составляет 1 зачетную единицу (27 час.)

Контактная работа 3,25 час.

Самостоятельная работа 23,75 час.

Виды учебных занятий и формы промежуточной аттестации	2 курс	
	Контактная работа с преподавателем	Самостоятельная работа обучающегося
Практические занятия	3	21
Зачёт	0,25	2,75
Всего	3,25	23,75

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и объемом учебных занятий

Очная форма обучения

№ п/п	Раздел (тема) дисциплины	Семестр	Виды учебных занятий, включая самостоятельную работу обучающихся и объем (в часах)				Формы текущего контроля успеваемости Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа		Самостоятельная работа обучающегося	
				Лаб.	Пр.		
1.	Введение в проблему	4			4,5	7	Практические

	кибербезопасности.						задания
2.	Требования к системам защиты информации.	4			6	9,25	Практические задания
ИТОГО					10,5	16,25	Зачёт

Заочная форма обучения

№ п/п	Раздел (тема) дисциплины	Курс	Виды учебных занятий, включая самостоятельную работу обучающихся и объем (в часах)				Формы текущего контроля успеваемости Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа		Самостоятельная работа обучающегося	
				Лаб.	Пр.		
1	Введение в проблему кибербезопасности.	2			1,5	12	Практические задания
2.	Требования к системам защиты информации.	2			1,5	11	Практические задания
ИТОГО					3	21	Зачёт

4.2. Развернутое описание содержания учебного материала по разделам (темам)

Тема 1 – Введение в проблему кибербезопасности.

Понятие кибербезопасности. Роль человека в кибернетических системах. Проблема информационной безопасности в кибернетических системах. Понятие доверенной информационной системы. Отношения доверия в информационных системах. Internet вещей, smart things – коммуникация и принятие решений без участия человека. Требования к обеспечению безопасности.

Тема 2 – Требования к системам защиты информации.

Определение систем реального времени с точки зрения информационной безопасности. Виды идентификации применяемы в современных информационных системах. Понятие идентификационной сущности. Проблема хранения идентификационной сущности. Процедуры идентификации без участия человека. Криптографические методы идентификации.

5. Образовательные технологии, в том числе перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Для изучения дисциплины предлагается сочетание традиционных образовательных технологий в форме интерактивных практических занятий с информационными технологиями при выполнении лабораторных работ.

В рамках курса предусмотрены три основных вида практических занятий:

- письменные и интерактивные упражнения, которые привязаны к отдельным темам курса, и предназначены, в основном, для самостоятельного изучения и самоконтроля;
- лабораторные работы в специально оборудованном и настроенном классе (аудитории);
- лабораторные работы в виртуальной среде, которые могут выполняться студентами самостоятельно или под руководством преподавателя в специализированной компьютерной среде для проектирования, моделирования работы и анализа

компьютерных сетей.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Учебная дисциплина обеспечена электронным учебно-методическим комплексом, который доступен в полном объеме зарегистрированному инструктору Сетевой академии Cisco и включает следующие компоненты:

Для магистрантов:

- интерактивный учебник по всем темам курса, содержащий анимационные и видеоролики, компьютерные тесты, мультимедийные практические задания;
- компьютерная среда для проектирования, моделирования работы и анализа компьютерных сетей packettracer;
- методические рекомендации по выполнению лабораторных работ в виртуальной среде - packettracer;
- интерактивные тесты;
- методические рекомендации по выполнению лабораторных работ с реальным оборудованием.

Для преподавателя:

- руководство для преподавателя, включающее методические указания по организации учебного процесса;
- методические рекомендации по выполнению лабораторных работ с реальным оборудованием (версия для инструкторов);
- методические рекомендации по выполнению лабораторных работ в виртуальной среде - packettracer (версия для инструкторов);
- подробный учебно-тематический план с указанием рекомендаций по выполнению практических занятий и лабораторных работ;
- общее описание курса для размещения на сайте образовательного учреждения;
- слайд–лекции по всем раздела курса (на английском языке);
- регулярные обновления учебных курсов, связанные с появлением новых технологий и развитием систем сертификаций (на английском языке);
- дополнительные материалы.

Помимо основных материалов по курсу всем преподавателям доступны ресурсы, представленные в форуме преподавателей Сетевых академий Cisco, на специализированных порталах сообществ инструкторов.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине

Для текущего контроля успеваемости применяются:

- практические аудиторные задания – 25 баллов практические задания (пять заданий по 5 баллов);
- подготовка доклада по предложенной теме –15 баллов;
- выполнение самостоятельного проектного задания – 25 баллов.

Помимо этого учитывается:

- посещаемость (отсутствие пропусков занятий) – 5 баллов.

На зачете по дисциплине «Основы кибербезопасности» контролируемые знания, умения и владения, характеризующие этапы формирования компетенций в процессе освоения образовательной программы. Зачет проводится в форме презентации авторского электронного теста по материалам дисциплины – 30 баллов. Тест проектируется и реализуется до зачета в процессе самостоятельной работы по дисциплине.

По желанию, студенты могут сдавать зачет в форме собеседования (устного ответа на предложенные вопросы). Примерные задания для организации собеседования содержатся в Приложении 1 к данной рабочей программе. Общая накопительная оценка складывается из баллов текущей успеваемости в семестре по предмету и баллов, полученных студентами на зачете.

Оценка на зачете выставляется по следующей шкале:

Шкала оценки результатов по дисциплине «Основы кибербезопасности»

Повышенный уровень	Базовый уровень	Пороговый уровень	Ниже порогового уровня
зачтено	зачтено	зачтено	не зачтено
85-100 баллов	71-84 балла	61-70 баллов	60 и менее баллов

Фонд оценочных средств по дисциплине «Основы кибербезопасности» в полном объёме представлен в Приложении 2 к рабочей программе.

8. Учебно-методическое и информационное обеспечение дисциплины

Учебная и учебно-методическая литература:

– ***основная литература:***

1. Загинайлов, Ю. Н. Основы информационной безопасности : курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=362895 (дата обращения: 05.07.2023). – Библиогр. в кн. – ISBN 978-5-4475-3947-4. – DOI 10.23681/362895. – Текст : электронный.
2. Петров, С. В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.
3. Прохорова, О. В. Информационная безопасность и защита информации : учебник : [16+] / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 05.07.2023). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.
4. Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с.

– ***дополнительная литература:***

1. Галатенко, В. А. Основы информационной безопасности : курс лекций : учебное пособие / В. А. Галатенко ; Интернет университет информационных технологий ; под ред. В. Б. Бетелина. - 2-е изд. ; испр. - Москва : Интернет-Университет Информационных Технологий, 2004. - 264 с.
2. Гашков, С. Б. Криптографические методы защиты информации : учебное пособие для студентов вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва : Академия, 2010. - 304 с.
3. Гершензон, В. Е. Информационные технологии в управлении качеством среды обитания : учебное пособие / В. Е. Гершензон, Е. В. Смирнова, В. В. Элиас ; под ред. В. Е. Гершензона. - Москва : Академия, 2003. - 288 с.

4. Исаев, Г. Н. Проектирование информационных систем : учебное пособие / Г. Н. Исаев. - Москва : Омега-Л, 2013. - 424 с. : ил.
5. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : курс лекций : учебное пособие / О. Р. Лапонина ; под ред. В. А. Сухомлина. - Москва : Интернет-Университет Информационных технологий, 2005. - 608 с.
6. Попов, В. Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности : учебное пособие / В. Б. Попов. - Москва : Финансы и статистика, 2005. - 176 с. : ил.
7. Расторгуев, С. П. Основы информационной безопасности : учебное пособие для студентов высших учебных заведений / С. П. Расторгуев. - Москва : Академия, 2007. - 192 с.
8. Ярочкин, В. И. Информационная безопасность / В. И. Ярочкин. - Москва : Академический Проект : Гаудеамус, 2004. - 544 с.

Интернет-ресурсы:

1. Google-диск. -. https://drive.google.com;
2. Google-документы. - https://docs.google.com;
3. Образовательный онлайн-ресурс для проведения электронного тестирования и генерирования заданий. -. www.yaklass.ru;
4. Сетевая академия Cisco. – https://www.cisco.com

Современные профессиональные базы данных и информационно-справочные системы:

1. ЭБС «Университетская библиотека онлайн»;
2. Коллекция Шуйского филиала ИвГУ на национальном цифровом ресурсе «Руконт»;
3. Консультант Плюс http://www.consultant.ru;
4. Портал общероссийской системы оценки качества образования. - http://www.osoko.edu.ru/;
5. Словари и энциклопедии на Академике. - https://dic.academic.ru

Программное обеспечение:

Программное обеспечение:

В процессе изучения дисциплины используются офисные пакеты Microsoft Office, Open Office, программа для просмотра и чтения файлов PDF Adobe Acrobat Reader DC, программа для воспроизведения флэш-анимации в браузерах Adobe Flash Player, вэб-обозреватели Google Chrome, Opera, Антивирус Касперского, 1С университет, Packet Tracer — симулятор сети передачи данных, выпускаемый фирмой Cisco Systems.

9. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий семинарского типа, укомплектованная специализированной мебелью и техническими средствами обучения.
2. Учебная аудитория для проведения текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью и техническими средствами обучения.
3. Помещение для самостоятельной работы, оснащенное специализированной мебелью, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Автор рабочей программы дисциплины: А.В. Ермошин, доцент кафедры математики, информатики и методики обучения, кандидат технических наук, доцент.

Программа рассмотрена на заседании кафедры математики, информатики и методики обучения «15» мая 2019 г., протокол № 8

Программа обновлена
протокол заседания кафедры № 5 от «21» февраля 2020 г.
Согласовано:
Руководитель ОП
_____ С.А. Зайцева
(подпись)

Программа обновлена
протокол заседания кафедры № 10 от «07» июня 2021 г.
Согласовано:
Руководитель ОП
_____ С.А. Зайцева
(подпись)

Программа обновлена
протокол заседания кафедры № 7 от «18» февраля 2022 г.
Согласовано:
Руководитель ОП
_____ С.А. Зайцева
(подпись)

Программа обновлена
протокол заседания кафедры № 11 от «21» июня 2023 г.
Согласовано:
Руководитель ОП
_____ С.А. Зайцева
(подпись)

Приложение 1.

Методические указания для обучающихся по освоению дисциплины

На самостоятельную работу студентов по курсу «Основы кибербезопасности» отводится более 50% учебного времени от общей трудоемкости курса. Сопровождение самостоятельной работы студентов по данному курсу может быть организовано в следующих формах:

– согласование индивидуальных заданий (виды и темы заданий, сроки представления результатов) самостоятельной работы студента в пределах часов, отведенных на самостоятельную работу;

– консультации (индивидуальные и групповые), в том числе с применением дистанционных технологий взаимодействия;

– промежуточный контроль хода выполнения заданий, строящихся на основе различных способов самостоятельной информационной деятельности в открытой информационной среде.

Преподаватель определяет содержание самостоятельной работы, график её выполнения; создает сетевую информационную и коммуникационную среду для организации самостоятельной работы.

В процессе организации самостоятельной работы особое внимание уделяется не только развитию информационной культуры, но и формированию готовности к кооперации, к работе в коллективе в сетевом пространстве, для чего целесообразно стимулировать студентов к совместной деятельности в малых группах.

Одной из важнейших особенностей заданий для самостоятельной работы по курсу «Основы кибербезопасности» является их ориентация на формирование способности оценивать уровень угрозы и обеспечивать безопасность в различных системах.

К типовым заданиям для самостоятельной работы студентов относятся:

- выполнение практических заданий по организации информационной и кибербезопасности;
- составление инструкции и заданий по организации информационной и кибербезопасности.

ПРАКТИЧЕСКОЕ ПРОЕКТНОЕ ЗАДАНИЕ

(25 баллов)

Разработать концепцию информационной безопасности образовательного учреждения по следующему примерному плану.

1) Цели системы информационной безопасности
2) Задачи системы информационной безопасности.
3) Объекты информационной безопасности.
4) Вероятные нарушители.
5) Основные виды угроз информационной безопасности.
6) Классификация угроз.
    a. Основные непреднамеренные искусственные угрозы.
    b. Основные преднамеренные искусственные угрозы.
7) Мероприятия по обеспечению информационной безопасности.
8) Средства защиты от потенциальных угроз.
9) Разработайте вариант политики паролей
10) Предложите ПО для антивирусной защиты (проведя сравнительный анализ цен, возможностей и пр.)

Критерии оценки проекта

Оценки в баллах	Критерии
4	Самостоятельность в подготовке материала
6	Аргументированность и полнота материала
4	Использование современной и актуальной литературы
6	Практическая ценность проекта
5	Качество презентации и аргументированность выводов
25	**Итого**

ДОКЛАД

Примерная проблематика докладов

1. Влияние киберустройств на повседневную жизнь человека
2. требования к информационной безопасности в системах реального времени
3. определение политики безопасности для аварийного режиме работы АСУТП
4. Методы авторизации безучастия человека

Критерии оценки доклада

Оценки в баллах	Критерии
3	Самостоятельность в подготовке материала
3	Аргументированность и полнота материала
3	Использование современной и актуальной литературы
3	Обобщение опыта организации информационной безопасности
3	Качество презентации
15	**Итого**