МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Авторы-составители: **Радионова Марина Владимировна**
Ильин Иван Вадимович

Рабочая программа дисциплины

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Код УМК 101544

Утверждено
Протокол №8
от «17» апреля 2024 г.

Пермь, 2024

1. Наименование дисциплины

Основы кибербезопасности

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « Б.1 » образовательной программы по направлениям подготовки (специальностям):

Направление подготовки: **38.03.05** Бизнес-информатика

направленность Бизнес-аналитика

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Основы кибербезопасности** у обучающегося должны быть сформированы следующие компетенции:

38.03.05 Бизнес-информатика (направленность : Бизнес-аналитика)

ОПК.1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности

Индикаторы

ОПК.1.1 Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук

ОПК.4 Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

Индикаторы

ОПК.4.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности

4. Объем и содержание дисциплины

Направление подготовки	38.03.05 Бизнес-информатика (направленность: Бизнес-аналитика)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	10
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (2)
Формы промежуточной аттестации	Зачет (10 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Основы кибербезопасности [для экономистов]

Тема 1. Концепция информационной безопасности

Международные стандарты информационного обмена. Концептуальная модель информационной безопасности. Объекты угроз. Правовое регулирование защиты информации. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Законодательство РФ в области защиты информации.

Тема 2. Вредоносные программы и антивирусная профилактика

Тема 2. Вредоносные программы и антивирусная профилактика
Вредоносные программы. Разновидности вредоносных программ. Социальная инженерия. Характерные особенности программ удаленного администрирования. Внедрение и запуск кода. Антивирусное программное обеспечение. Организационно-технические мероприятия по созданию и поддержанию функционирования комплексной системы защиты.

Тема 3. Криптографические методы защиты данных

Понятие и классификация криптографических методов и средств защиты информации. Шифрование и кодирование. Ключ. Криптостойкость шифра. Симметричные и асимметричные (с открытым ключом) криптосистемы. Системы электронно-цифровой подписи.

Тема 4. Методы и аппаратно-программные средства защиты информации

Требования к программно-аппаратным средствам защиты информации. Проблема целостности и проблема конфиденциальности информации на магнитных носителях. Способы восстановления информации на внешних носителях. Методы защиты информации. Принципы защиты информации. Характеристики средств защиты информации, создаваемые аппаратно-программными средствами. Аутентификация, авторизации, аудит. Защита сетей и использование межсетевых экранов. Межсетевой экран (МЭ), Firewall, брандмауэр. Основные компоненты МЭ. Фильтрующий маршрутизатор. Прокси-серверы. Функции прокси-сервера. Политика межсетевого взаимодействия. Политика сетевой безопасности.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Информационные технологии в экономике и управлении : учебник для вузов / В. В. Трофимов [и др.] ; ответственный редактор В. В. Трофимов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 556 с. — (Высшее образование). — ISBN 978-5-534-18678-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. https://urait.ru/bcode/545322

2. Информационная безопасность. Правовые основы информационной безопасности. 10-11 классы : учебник / М. С. Цветкова, С. В. Голубчиков, В. К. Новиков [и др.] ; под редакцией М. С. Цветковой. — 2-е изд. — Москва : Просвещение, 2022. — 112 с. — ISBN 978-5-09-101618-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. https://profspo.ru/books/132252

Дополнительная:

1. Информационные технологии в экономике и управлении в 2 ч. Часть 1 : учебник для вузов / В. В. Трофимов [и др.] ; под редакцией В. В. Трофимова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 269 с. — (Высшее образование). — ISBN 978-5-534-09083-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. https://www.urait.ru/bcode/475056

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

При освоении дисциплины использование ресурсов сети Интернет не предусмотрено.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Основы кибербезопасности** предполагает использование следующего программного обеспечения и информационных справочных систем:
1) презентационные материалы (слайды по темам лекционных занятий);
2) доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
3) доступ в электронную информационно-образовательной среду университета;
4) интернет-сервисы и электронные ресурсы.
Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:
1. Приложения, позволяющее просматривать и воспроизводить медиаконтент PDF-файлов;
2. Офисные пакеты приложений;
3. Браузер

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Материально-техническая база обеспечивается наличием:
1. Лекционные занятия – аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
2. Практические занятия – аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
3. Лабораторные занятия – компьютерный класс, оснащенный персональными ЭВМ и соответствующим программным обеспечением. Состав оборудования определен в Паспорте компьютерного класса
4. Самостоятельная работа – аудитория для самостоятельной работы, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченная доступом в электронную информационно-образовательную среду университета. Помещения Научной библиотеки ПГНИУ.
5. Текущий контроль, групповые и индивидуальные консультации, промежуточная аттестация – аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Основы кибербезопасности

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.1

Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.1.1 Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук	Применяет знания основных положений и концепций в области информационной безопасности	**Неудовлетворител** НЕУДОВЛЕТВОРИТЕЛЬНО выставляется студенту, который не знает основных положений и концепций в области информационной безопасности. Заявленная часть компетенции в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических задач. Требуется повторное обучение. **Удовлетворительн** УДОВЛЕТВОРИТЕЛЬНО выставляется студенту, который не уверенно знает основных положений и концепций в области информационной безопасности. Сформированность заявленной части компетенции соответствует минимальным требованиям. **Хорошо** ХОРОШО выставляется студенту, который в целом хорошо знает основных положений и концепций в области информационной безопасности. Сформировано умение использовать соответствующие программные инструменты в стандартных ситуациях. Компетенция в целом соответствует требованиям. **Отлично** ОТЛИЧНО выставляется студенту, который отлично знает основных положений и концепций в области информационной безопасности. Обучающийся свободно справляется с практическими задачами, владеет разносторонними приемами выполнения соответствующий видов работ. Сформированность заявленной части

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично компетенции превышает стандартные требования. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для применения творческого подхода к решению сложных практических задач.

ОПК.4

Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.4.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Реализует выбор ИКТ и использует их в профессиональной деятельности с учетом требований ИБ	**Неудовлетворител** НЕУДОВЛЕТВОРИТЕЛЬНО выставляется студенту, который не знает методы обеспечения ИБ. Заявленная часть компетенции в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических задач. Требуется повторное обучение. **Удовлетворительн** УДОВЛЕТВОРИТЕЛЬНО выставляется студенту, который не уверенно знает методы обеспечения ИБ. Сформированы знания и умения в области ИБ, необходимые для дальнейшего обучения. Сформированность заявленной части компетенции соответствует минимальным требованиям. **Хорошо** ХОРОШО выставляется студенту, который в целом хорошо знает методы обеспечения ИБ. Сформировано умение использовать соответствующие программные инструменты в стандартных ситуациях. Компетенция в целом соответствует требованиям. **Отлично** ОТЛИЧНО выставляется студенту, который отлично знает методы обеспечения ИБ. Сформированы систематические знания и умения в области ИБ. Обучающийся свободно справляется с практическими задачами, владеет разносторонними

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично приемами выполнения соответствующий видов работ. Сформированность заявленной части компетенции превышает стандартные требования. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для применения творческого подхода к решению сложных практических задач.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 50 до 60
«неудовлетворительно» / «незачтено» менее 50 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Тема 1. Концепция информационной безопасности **Входное тестирование**	остаточные знания студента по всем разделам курса "Информатика и ИКТ"
ОПК.1.1 Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук	Тема 2. Вредоносные программы и антивирусная профилактика **Письменное контрольное мероприятие**	Тема Вредоносные программы и антивирусная профилактика
ОПК.4.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Тема 3. Криптографические методы защиты данных **Письменное контрольное мероприятие**	тема Криптографические методы защиты данных

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.1.1 Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук **ОПК.4.2** Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Тема 4. Методы и аппаратно-программные средства защиты информации **Итоговое контрольное мероприятие**	все темы курса

Спецификация мероприятий текущего контроля

Тема 1. Концепция информационной безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
На «10 баллов» оценивается глубокие остаточные знания студента по всем разделам курса "Информатика и ИКТ", владеет разносторонними навыками и приемами выполнения практических работ и решения задач.	10
На «7 баллов» оценивается поверхностные остаточные знания студента по всем разделам курса "Информатика и ИКТ", владеет некоторыми навыками и приемами выполнения практических работ и решения задач.	7
На «5 баллов» оцениваются слабые остаточные знания студента по всем разделам курса "Информатика и ИКТ". Студент не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушение последовательности в изложении материала и испытывает трудности в выполнении практических заданий.	5

Тема 2. Вредоносные программы и антивирусная профилактика

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **15**

Показатели оценивания	Баллы

«30 баллов» выставляется за сданные все практические и контрольные работы (темы Вредоносные программы и антивирусная профилактика). Возможно добавление / снижение баллов за качество выполненных заданий	30
«20 баллов» выставляется за частично сданные практические и контрольные работы (темы Вредоносные программы и антивирусная профилактика). Возможно добавление / снижение баллов за качество выполненных заданий	20
«15 баллов» выставляется за минимальный набор сданных практических и контрольных работ (темы Вредоносные программы и антивирусная профилактика). Возможно добавление / снижение баллов за качество выполненных заданий	15

Тема 3. Криптографические методы защиты данных

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **15**

Показатели оценивания	Баллы
«30 баллов» выставляется за сданные все практические и контрольные работы (темы Криптографические методы защиты данных). Возможно добавление / снижение баллов за качество выполненных заданий	30
«20 баллов» выставляется за частично сданные практические и контрольные работы (темы Криптографические методы защиты данных). Возможно добавление / снижение баллов за качество выполненных заданий	20
«15 баллов» выставляется за минимальный набор сданных практических и контрольных работ (темы Криптографические методы защиты данных). Возможно добавление / снижение баллов за качество выполненных заданий	15

Тема 4. Методы и аппаратно-программные средства защиты информации

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **20**

Показатели оценивания	Баллы
«40 баллов» выставляется за сданные все практические и контрольные работы (темы включают все содержательные линии дисциплины). Возможно добавление / снижение баллов за качество выполненных заданий. А также за 80 % выполненных тестовых заданий	40
«30 баллов» выставляется за 60 % выполненных тестовых заданий. Также за частично сданные практические и контрольные работы (темы включают все содержательные линии дисциплины). Возможно добавление / снижение баллов за качество выполненных заданий	30
«20 баллов» выставляется за минимальный набор сданных практических и контрольных работ (темы включают все содержательные линии дисциплины). Возможно добавление / снижение баллов за качество выполненных заданий. А также за 50 % выполненных тестовых заданий	20