МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

Авторы-составители: **Пенский Олег Геннадьевич**
Карпов Михаил Юрьевич

Рабочая программа дисциплины

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Код УМК 91350

Утверждено
Протокол №1
от «31» августа 2020 г.

Пермь, 2020

1. Наименование дисциплины

Основы кибербезопасности

2. Место дисциплины в структуре образовательной программы

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

Направление: **44.03.01** Педагогическое образование

направленность Русская филология

3. Планируемые результаты обучения по дисциплине

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

44.03.01 Педагогическое образование (направленность : Русская филология)

ОК.10 понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

ПК.2 способность использовать современные методы и технологии обучения и диагностики

4. Объем и содержание дисциплины

Направления подготовки	44.03.01 Педагогическое образование (направленность: Русская филология)
форма обучения	заочная
№№ триместров, выделенных для изучения дисциплины	11,12
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	10
Проведение лекционных занятий	6
Проведение практических занятий, семинаров	4
Самостоятельная работа (ак.час.)	98
Формы текущего контроля	Защищаемое контрольное мероприятие (2) Письменное контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (12 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Кибербезопасность в системе национальной безопасности РФ

Студенты должны усвоить то, что компьютерная безопасность является частью информационной безопасности государства, должны понять общие принципы построения СЗИ и формализацию в подходе построения СЗИ, студенты должны научиться применять при построении оценки эффективности СЗИ правила четкой и нечеткой математики, уметь использовать методы экспертных оценок при создании СЗИ, должны создать СЗИ ПК и оценить ее эффективность с помощью всех изученных методов и применении метода экспертного оценивания DELPHI, должны понять общие принципы работы хакеров в сети Интернет и уметь работать в сети с наибольшей вероятностью предохранения от утечек информации, должны усвоить принципы организации работы СЗИ в банковских структурах и узнать современные основные угрозы ИС, должны узнать об основных типах сетей и классификации СЗИ этих сетей. При рассмотрении данной темы необходимо дать характеристики следующим неопределенностям, влияющим на адекватность работы СЗИ:

☐ Неясное представление целей СЗИ;

☐ Неясное представление угроз и ущерба от наступающих угроз;

☐ Отсутствие точных методов оценки эффективности СЗИ.

Информационная война, методы и средства её ведения

При рассмотрении данной темы необходимо сформировать у студентов твердые навыки по использованию матрицы знаний при создании СЗИ. Студент должен разработать программу, позволяющую заполнять элементы матрицы знаний в ходе создания СЗИ. На лекции преподаватель рассказывает о структуре матрицы знаний и контроле создания СЗИ на основе этой матрицы знаний. При рассмотрении данной темы необходимо сформировать у студентов практические навыки построения матрицы знаний, как основном механизме планирования создания СЗИ. Студентам в качестве практического задания предлагается разработать компьютерную программу, формирующую матрицу знаний для ПК. Текущим контролем усвоения материалов темы является защита плана построения СЗИ ПК с помощью матрицы знаний перед аудиторией.

Критерии защищенности компьютерных систем

Студент должен понять общие свойства большинства математических моделей и методов оценки эффективности СЗИ. Он должен знать то, все методы носят оценочный и приближенный характер, часто использующий экспертное оценивание и, как нечеткие, так и четкие характеристики. Студенты должны понять, что, исходя из этого, матмодели СЗИ делятся на три типа: основанные на теории четкой математики, нечеткой математики и использующие смешанные основы.

Студент, основываясь на знаниях теории вероятностей и понятиях теории нечетких множеств, должен освоить методы построения функции ущерба СЗИ и вычислять численные значения этой функции для конкретных СЗИ. Студент должени уметь применять расчеты для определения наиболее эффективной СЗИ из заданных СЗИ.

Защита информации, обрабатываемой в автоматизированных системах

Студент должен получить твердые навыки при создании СЗИ с оценкой их эффективности с помощью математических моделей. Преподаватель на лекции рассказывает пример создания простейшей СЗИ ПК с использование математических моделей. Он обращает особое внимание на оценку экономических затрат создания и функционирования СЗИ, как основном факторе, определяющим выбор при внедрении СЗИ.

Закон РФ о государственной тайне

Рассматривается закон РФ о гостайне. В частности, изучаются вопросы, касающиеся засекречивания и рассекречивания информации, общих принципов составления перечня закрытых тем, служебных

полномочий структур по засекречиванию информации, возможности отрытых публикаций и патентов.

Безопасность сети интернет

Интернет.

Студент должен изучить следующие вопросы:

1. Интернет в структуре информационно-аналитического обеспечения.
2. Основные протоколы Интернет и их использование злоумышленниками.
3. Аутентификация в Интернет.
4. Легкость наблюдения за передаваемыми данными.
5. Потенциальные проблемы с электронной почтой.

Компьютерные вирусы и антивирусные продукты

Понятие компьютерного вируса. Признаки заражения компьютера. История возникновения вирусов. Классификации компьютерных вирусов. Пути проникновения вирусов на компьютер. Методы защиты от компьютерных вирусов. Антивирусные программы

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. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/33430

2. Горев, А. И. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. — Омск : Омская академия МВД России, 2016. — 88 c. — ISBN 978-5-88651-642-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/72856.html

Дополнительная:

1. Расторгуев С. П. Информационная война. Проблемы и модели. Экзистенциальная математика:учеб. пособие для студентов вузов/С. П. Расторгуев.-М.:Гелиос АРВ,2006, ISBN 5-85438-145-1.-240.-Библиогр.: с. 234-235

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. https://www.urait.ru/bcode/422772

3. Государственная тайна и ее защита в Российской Федерации:Учеб.-метод. пособие/Аникин П. П. [и др.]ред.: Вус М. А., Федоров А. В..-СПб.:Юрид. центр Пресс,2003, ISBN 5-94201-276-8.-610.

4. Савицкий, А. Г. Национальная безопасность. Россия в мире : учебник для студентов вузов / А. Г. Савицкий. — Москва : ЮНИТИ-ДАНА, 2017. — 463 c. — ISBN 978-5-238-02307-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/81509.html

5. Ермаков Д. Г. Применение антивирусных программ для обеспечения информационной безопасности:учебное пособие/Ермаков Д. Г..-Екатеринбург:Уральский федеральный университет, ЭБС АСВ,2013.-64. http://www.iprbookshop.ru/66577.html

6. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 581 c. — ISBN 978-5-4497-0560-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/94863.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

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:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «AdobeAcrobatReader DC»;
- офисный пакет приложений «LibreOffice», AltLinux

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

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения практических занятий - компьютерный класс. Состав оборудования определен в Паспорте компьютерного класса.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

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 и критерии их оценивания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОК.10 понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Знать основные понятия в области кибербезопасности. Знать основные требования нормативных документов по безопасности информации. Уметь анализировать показатели качества систем кибербезопасности. Владеть методикой создания систем кибербезопасности. Владеть критериями оценки систем кибербезопасности.	**Неудовлетворител** Знает менее 50% основных понятий в области кибербезопасности Не знает основные требования нормативных документов по безопасности информации Не знает методику создания систем кибербезопасности; Не может представить анализ показатели качества и критерии оценки системкибербезопасности Не знает основные требования по порядку оформления документации Не может оформить (с отдельными ошибками)полученные результаты исследовательских работ Не может сделать оценку защищенности системы кибербезопасностина основании полученных результатов исследований. **Удовлетворительн** Знает не менее 50% основных понятий в области кибербезопасности; Знает основные требования нормативных документов по безопасности информации; Частично знает методику создания систем кибербезопасности; Может в общих чертах представить анализ показатели качества и критерии оценки системкибербезопасности; Знает основные требования по порядку оформления документации; Может оформить (с отдельными ошибками) полученные результаты исследовательских работ; Не может сделать оценку защищенности системы кибербезопасности на основании полученных результатов исследований;

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Знает не менее 60% основных понятий в области информационной безопасности На хорошем уровне знает основные требования нормативных документов по безопасности информации Знает требования по порядку оформления документации На хорошем уровне может представить анализ показатели качества и критерии оценки системкибербезопасности Может оформить (с отдельными ошибками) полученные результаты исследовательских работ; Может сделать оценку защищенности системы кибербезопасности на основании полученных результатов исследований. **Отлично** Знает основные понятия в области информационной безопасности На отличном уровне знает основные требования нормативных документов по безопасности информации умеет их интерпретировать; Знает в деталях требования по порядку оформления документаци; Досконально знает и может представить подробный анализ показатели качества и критерии оценки системкибербезопасности; Может оформить полученные результаты исследовательских работ; Может сделать оценку защищенности системы кибербезопасности на основании полученных результатов исследований.
ПК.2 способность использовать современные методы и технологии обучения и диагностики	Знать основные понятия в области кибербезопасности. Знать основные требования нормативных документов по безопасности информации. Уметь представить анализ показателей качества и критерий оценки систем кибербезопасности.	**Неудовлетворител** Знает менее 50% основных понятий в области кибербезопасности Не знает основные требования нормативных документов по безопасности информации Не знает методику создания систем кибербезопасности; Не может представить анализ показатели качества и критерии оценки систем

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
	Владеть современными методами и технологиями обучения и диагностики.	**Неудовлетворител** кибербезопасности **Удовлетворительн** Знает не менее 50% основных понятий в области кибербезопасности; Знает основные требования нормативных документов по безопасности информации; Частично знает методику создания систем кибербезопасности; Умеет (с ошибками) представить анализ показатели качества и критерии оценки систем кибербезопасности; **Хорошо** Знает не менее 70% основных понятий в области информационной безопасности На хорошем уровне знает основные требования нормативных документов по безопасности информации Знает методику создания систем кибербезопасности; Умеет представить анализ показатели качества и критерии оценки систем кибербезопасности; **Отлично** Знает основные понятия в области информационной безопасности На отличном уровне знает основные требования нормативных документов по безопасности информации умеет их интерпретировать; Знает отлично методику создания систем кибербезопасности; Умеет представить анализ показатели качества и критерии оценки систем кибербезопасности;

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : заочная

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 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.2 способность использовать современные методы и технологии обучения и диагностики **ОК.10** понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Закон РФ о государственной тайне **Письменное контрольное мероприятие**	Письменная контрольная работа (тест), включающая в себя основные термины по проблематике кибербезопасности; требования нормативных документов регламентирующие технические и программные меры обеспечения кибербезопасности; особенности обеспечения кибербезопасности компьютерных систем при обработке информации, составляющей государственную тайну;
ПК.2 способность использовать современные методы и технологии обучения и диагностики	Безопасность сети интернет **Защищаемое контрольное мероприятие**	Письменная контрольная работа (тест), включающая в себя общие принципы работы хакеров в сети Интернет, аутентификация в Интернет, проблемы с передачей данных по электронной почте.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.2 способность использовать современные методы и технологии обучения и диагностики **ОК.10** понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Компьютерные вирусы и антивирусные продукты **Защищаемое контрольное мероприятие**	Письменная контрольная работа (тест), включающая в себя вопросы вторжения в компьютерную систему методами удаленного доступа, вторжения в систему при наличии локального доступа; вторжения в мобильные устройства, новые тенденции; антивирусные программы, их достоинства и недостатки, особенности применения.

Спецификация мероприятий текущего контроля

Закон РФ о государственной тайне

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.3**

Показатели оценивания	Баллы
Знать основные понятия и определения из нормативных документов РФ по кибербезопасности	10
Знать общие положения законодательства по защите государственной тайны, перечень сведений, подлежащих засекречиванию, порядок рассекречивания документов	10
Знать общеметодологические принципы теории кибербезопасности. Роль кибербезопасности в обеспечении национальной безопасности государства	10

Безопасность сети интернет

Продолжительность проведения мероприятия промежуточной аттестации: **16 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.3**

Показатели оценивания	Баллы
Знать общие принципы работы хакеров в сети Интернет	10
Знать методы воздействия на компьютерную систему	10
Знать методы нарушения конфиденциальности, целостности и доступности информации; причины, виды, каналы утечки и искажения информации	10

Компьютерные вирусы и антивирусные продукты

Продолжительность проведения мероприятия промежуточной аттестации: **16 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **16.4**

Показатели оценивания	Баллы
Антивирусные программы, обоснование лучших вариантов защиты	20
Знать методы вторжения злоумышленников в компьютерную систему методами удаленного доступа, вторжения в систему при наличии локального доступа, вторжения в мобильные устройства, новые тенденции.	20