МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Институт математики и механики им. Н.И. Лобачевского

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____
"___"_____20___ г.

Программа дисциплины

Основы информационной безопасности Б1.В.ДВ.7

Направление подготовки: 44.03.05 - Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Математика, информатика и информационные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Шафигуллин И.К.

Рецензент(ы):
Насибуллин Р.Г.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Авхадиев Ф. Г.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института математики и механики им. Н.И. Лобачевского :
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) ассистент, к.н. Шафигуллин И.К. Кафедра теории функций и приближений отделение математики , Ilnar.Shafigullin@kpfu.ru

1. Цели освоения дисциплины

Выпускник, освоивший дисциплину:

Должен демонстрировать способность и готовность:

Решать стандартные задачи профессиональной деятельности, связанные с информационной безопасностью систем, включая:

1) настройку безопасности на уровне операционной системы и приложений,

2) применение антивирусного программного обеспечения,

3) принципы криптографической защиты информации,

4) использование профессиональные программные и аппаратные средства защиты информации.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел 'Б1.В.ДВ.7 Дисциплины (модули)' основной профессиональной образовательной программы 44.03.05 'Педагогическое образование (с двумя профилями подготовки) (не предусмотрено)' и относится к дисциплинам по выбору.

Осваивается на 5 курсе в 9 семестре.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-11 (профессиональные компетенции)	готовностью использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования
СПК-11 (профессиональные компетенции)	владеет современными формализованными математическими, информационно-логическими и логико-семантическими моделями и методами представления, сбора и обработки информации для учебных целей
СПК-13 (профессиональные компетенции)	способен создавать и использовать современные информационные и коммуникационные технологии для создания, формирования и администрирования электронных образовательных ресурсов
СПК-15 (профессиональные компетенции)	способен создавать и размещать информацию в компьютерной сети
СПК-2 (профессиональные компетенции)	понимает, что фундаментальное знание является основой компьютерных наук готов применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов
СПК-16 (профессиональные компетенции)	способен ориентироваться в информационном потоке, использовать рациональные способы получения, преобразования, систематизации и хранения информации, актуализировать ее в необходимых ситуациях интеллектуально-познавательной деятельности, способен структурировать информацию, организовывать ее поиск и защиту

В результате освоения дисциплины студент:

4. должен демонстрировать способность и готовность:

Решать стандартные задачи профессиональной деятельности, связанные с информационной безопасностью систем, включая:

1) настройку безопасности на уровне операционной системы и приложений,

2) применение антивирусного программного обеспечения,

3) принципы криптографической защиты информации,

4) использование профессиональные программные и аппаратные средства защиты информации.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 9 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
1.	Тема 1. Тема 1. Настройки безопасности операционной системы Windows	10		0	0	3	
2.	Тема 2. Тема 2. Настройки безопасности приложений Microsoft Office	10		0	0	3	
3.	Тема 3. Тема 3. Настройки безопасности Интернет-обозревателей	10		0	0	3	
4.	Тема 4. Тема 4. Антивирусное программное обеспечение	10		0	0	4	
5.	Тема 5. Тема 5. Классификация вредоносного ПО	10		0	0	3	
6.	Тема 6. Тема 6. Основы криптографической защиты информации	10		0	0	4	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
7.	Тема 7. Тема 7. Профессиональные программные и аппаратные средства защиты информации	10		0	0	4	
.	Тема . Итоговая форма контроля	9		0	0	0	Зачет
	Итого			0	0	24	

4.2 Содержание дисциплины

Тема 1. Тема 1. Настройки безопасности операционной системы Windows

лабораторная работа (3 часа(ов)):

Изучение настроек безопасности операционной системы Windows. Изучение списка политик безопасности ОС. Настройки брандмауэра Windows. Распределение прав доступа в рамках учётных записей. Решение задач по изучаемой теме.

Тема 2. Тема 2. Настройки безопасности приложений Microsoft Office

лабораторная работа (3 часа(ов)):

Рассмотрение пакета программ Microsoft Office. Понятие макросов и макровирусов. Цифровые подписи и цифровые сертификаты макроса. решение задач по изучаемой теме

Тема 3. Тема 3. Настройки безопасности Интернет-обозревателей

лабораторная работа (3 часа(ов)):

Обзор наиболее актуальных Интернет-обозревателей. Файлы Cookie. Блокирование и разрешение файлов Cookie в зависимости от их типа. Решение задач по изучаемой теме

Тема 4. Тема 4. Антивирусное программное обеспечение

лабораторная работа (4 часа(ов)):

Рассмотрение классификации антивирусного ПО. Основные производители антивирусного ПО. Онлайн проверка файлов на вирусы.Решение задач по изучаемой теме.

Тема 5. Тема 5. Классификация вредоносного ПО

лабораторная работа (3 часа(ов)):

Рассмотрение принципов работы основных типов вредоносного программного обеспечения. Сетевые черви, троянские программы, key logger, почтовые черви,черви для файлообменных сетей, фарминг

Тема 6. Тема 6. Основы криптографической защиты информации

лабораторная работа (4 часа(ов)):

Обзор истории развития криптографических систем. Симметричное шифрование, шифрование методом перестановки, шифрование методом замены, поточное шифрование. Решение задач по изучаемой теме

Тема 7. Тема 7. Профессиональные программные и аппаратные средства защиты информации

лабораторная работа (4 часа(ов)):

Рассмотрение криптографического пакета PGP Desktop, стеганографический пакет Steganos Security Suite. Решение задач по изучаемой теме

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел дисциплины	Се-мест	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
1.	Тема 1. Тема 1. Настройки безопасности операционной системы Windows	10		Демонстрация навыков по проведению соответствующих настроек систем безопасности.	6	Выполнение заданий преподавателя про проведению настроек системы безопасности.
2.	Тема 2. Тема 2. Настройки безопасности приложений Microsoft Office	10		Демонстрация навыков по проведению соответствующих настроек систем безопасности.	4	Выполнение заданий преподавателя про проведению настроек системы безопасности.
3.	Тема 3. Тема 3. Настройки безопасности Интернет-обозревателей	10		Демонстрация навыков по проведению соответствующих настроек систем безопасности.	4	Выполнение заданий преподавателя про проведению настроек системы безопасности.
4.	Тема 4. Тема 4. Антивирусное программное обеспечение	10		Демонстрация навыков по проведению соответствующих настроек систем безопасности.	6	Выполнение заданий преподавателя про проведению настроек системы безопасности.
5.	Тема 5. Тема 5. Классификация вредоносного ПО	10		Демонстрация навыков по проведению соответствующих настроек систем безопасности.	4	Выполнение заданий преподавателя про проведению настроек системы безопасности.
6.	Тема 6. Тема 6. Основы криптографической защиты информации	10		Демонстрация навыков по проведению соответствующих настроек систем безопасности.	6	Выполнение заданий преподавателя про проведению настроек системы безопасности.

N	Раздел дисциплины	Се-мест	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
7.	Тема 7. Тема 7. Профессиональные программные и аппаратные средства защиты информации	10		Демонстрация навыков по проведению соответствующих настроек систем безопасности.	6	Выполнение заданий преподавателя про проведению настроек системы безопасности.
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в компьютерном классе.

Преподаватель демонстрирует на интерактивной доске основные возможности настройки систем безопасности, а студенты выполняют соответствующие настройки на своих ПК.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Тема 1. Настройки безопасности операционной системы Windows

Выполнение заданий преподавателя про проведению настроек системы безопасности. , примерные вопросы:

Пример задания: 1. Создать цифровой сертификат с автоподписью, подписать им любой макрос, закрыть документ с сохранением, затем вновь открыть и проверить цифровой сертификат макроса. По ходу выполнения задания составить отчёт с копиями окон.

Тема 2. Тема 2. Настройки безопасности приложений Microsoft Office

Выполнение заданий преподавателя про проведению настроек системы безопасности. , примерные вопросы:

Пример задания: 2. Блокировать файлы Cookie для конкретных веб-узлов для указанных Интернет-обозревателей.

Тема 3. Тема 3. Настройки безопасности Интернет-обозревателей

Выполнение заданий преподавателя про проведению настроек системы безопасности. , примерные вопросы:

Пример задания: 3. Принципы работы Key Logger программ.

Тема 4. Тема 4. Антивирусное программное обеспечение

Выполнение заданий преподавателя про проведению настроек системы безопасности. , примерные вопросы:

Пример задания: 4. Установка бесплатного антивирусного программного обеспечения на локальном компьютере.

Тема 5. Тема 5. Классификация вредоносного ПО

Выполнение заданий преподавателя про проведению настроек системы безопасности. , примерные вопросы:

Пример задания: 5. Зашифровать вручную свои данные методом перестановки, например: "Фамилия, имя и отчество" по ключам предоставленным в задании.

Тема 6. Тема 6. Основы криптографической защиты информации

Выполнение заданий преподавателя про проведению настроек системы безопасности. , примерные вопросы:

Пример задания: 6. Составить программу для шифрования методом перестановки

Тема 7. Тема 7. Профессиональные программные и аппаратные средства защиты информации

Выполнение заданий преподавателя про проведению настроек системы безопасности. , примерные вопросы:

Пример задания: 7. Настроить одну из систем защиты информации.

Итоговая форма контроля

зачет (в 9 семестре)

Примерные вопросы к итоговой форме контроля

На зачете студентам предлагается провести настройки систем, которые были произведены в течение семестра.

7.1. Основная литература:

1.Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - (Высшее образование) ISBN 978-5-369-01450-9 Режим доступа: http://znanium.com/bookread2.php?book=495249

2. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. Режим доступа: http://znanium.com/bookread.php?book=402686

3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. Режим доступа: http://znanium.com/bookread.php?book=405000

7.2. Дополнительная литература:

1. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс]: учеб. пособие / С.А. Нестеров. - Электрон. дан. - Санкт-Петербург: Лань, 2018. - 324 с. - Режим доступа: https://e.lanbook.com/book/103908

2. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие. - Казань: Казанский университет, 2012. - 138 с. - Режим доступа: http://kpfu.ru/docs/F366166681/mzi.pdf

7.3. Интернет-ресурсы:

Интернет-университет "Интуит" - https://www.intuit.ru/

Интернет-университет "Интуит" - https://www.intuit.ru/

Информационно-правовой портал ГАРАНТ.РУ - http://www.garant.ru/

Открытые курсы Массачусетского технологического института США - https://ocw.mit.edu/index.htm

Открытые курсы Массачусетского технологического института США - https://ocw.mit.edu/index.htm

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Основы информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Требуется наличие прав Администратора на машинах, на которых будет производиться обучение.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 44.03.05 "Педагогическое образование (с двумя профилями подготовки)" и профилю подготовки Математика, информатика и информационные технологии .

Автор(ы):
Шафигуллин И.К. _____
"__" _____ 201 __ г.

Рецензент(ы):
Насибуллин Р.Г. _____
"__" _____ 201 __ г.