МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Самарский государственный социально-педагогический университет»

Кафедра информационно-коммуникационных технологий в образовании

УТВЕРЖДАЮ
Проректор по УМР и КО,
председатель УМС СГСПУ
_____Н.Н. Кислова

МОДУЛЬ "ОРГАНИЗАЦИЯ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ"
Информационная безопасность и защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационно-коммуникационных технологий в образовании**

Учебный план ФНО-б18НВв(5г6м)АБ.plx
Педагогическое образование (с двумя профилями подготовки)

С изменениями:
протокол №4 от 30.11.2018

Квалификация **бакалавр**

Форма обучения **очно-заочная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 18
самостоятельная работа 90

Виды контроля в семестрах:
экзамены 9

Распределение часов дисциплины по семестрам

Семестр(Курс.Номер семестра на курсе)	**9(5.1)**		Итого	
Вид занятий	УП	РПД	УП	РПД
Лекции	6	6	6	6
Практические	10	10	10	10
Консультация перед экзаменом	2	2	2	2
В том числе инт.	4	4	4	4
Итого ауд.	18	18	18	18
Контактная работа	18	18	18	18
Сам. работа	90	90	90	90
Итого	108	108	108	108

Программу составил(и):

М.А. Воронина

При наличии обучающихся из числа лиц с ограниченными возможностями здоровья, которым необходим особый порядок освоения дисциплины (модуля), по их желанию разрабатывается адаптированная к ограничениям их здоровья рабочая программа дисциплины (модуля).

Рабочая программа дисциплины

Информационная безопасность и защита информации

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 44.03.05 ПЕДАГОГИЧЕСКОЕ ОБРАЗОВАНИЕ
(С ДВУМЯ ПРОФИЛЯМИ ПОДГОТОВКИ) (уровень бакалавриата) (приказ Минобрнауки России от 09.02.2016г. №91)

составлена на основании учебного плана:

Педагогическое образование (с двумя профилями подготовки)

С изменениями:
протокол №4 от 30.11.2018
утвержденного учёным советом вуза от 29.08.2017 протокол № 1.

Рабочая программа одобрена на заседании кафедры

Информационно-коммуникационных технологий в образовании

Протокол от 28.08.2018 г. № 1
Зав. кафедрой Брыксина О.Ф.

Начальник УОП

Н.А. Доманина

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Цель дисциплины – обеспечить технологическую и правовую готовность к созданию безопасной информационно-образовательной среды и использованию различных методов и средств защиты информации; профессиональную готовность к реализации образовательных внеурочной деятельности в соответствии с требованиями образовательных стандартов, формированию у обучающихся навыков защиты информации и безопасного использования программных средств при работе с информационными ресурсами.
Курс предполагает подготовку студентов к решению следующих задач: готовность к формированию у обучающихся знаний в области теоретических основ информационной безопасности, ознакомлению с моделями возможных угроз безопасности информации и современными методами защиты информации и программного обеспечения; освоение правовых основ и способов проектирования профессиональной сетевой среды на основе современных методов и средств защиты информации; постановка и решения исследовательских задач в области современной теории и практике защиты информации.
Область профессиональной деятельности: образование.
Объектами профессиональной деятельности являются обучение, воспитание, развитие, просвещение.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.06
2.1	**Требования к предварительной подготовке обучающегося:**
Содержание дисциплины базируется на материале	
Информационно-коммуникационные технологии во внеурочной деятельности в области начального образования	
Информационно-коммуникационные технологии в образовании	
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы	
Производственная практика (преддипломная практика)	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОК-3: способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве
Знать:
основные виды угроз информационной безопасности; последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций; нормативно-правовую и законодательную базу по обеспечению информационной безопасности; понятие и виды компьютерных вирусов, их разрушительные действия; методы защиты от компьютерных вирусов
Уметь:
указать сильные и слабые стороны различных подходов к обеспечению безопасности; проводить экспертную оценку электронных образовательных ресурсов с точки зрения эффективности реализации методов и средств защиты информации; описывать правовые основы обеспечения конфиденциальности; прогнозировать действие вирусов и атак, направленных на вызов отказа в обслуживании
Владеть:
навыками устранения отказов программного и аппаратного обеспечения; навыками работы с антивирусным программным обеспечением

ПК-10: способностью проектировать траектории своего профессионального роста и личностного развития
Знать:
методы и устройства обеспечения безопасности информации в профессиональной сетевой среде; нормативно-правовую и законодательную базу, технологические стратегии по обеспечению информационной безопасности при взаимодействии в компьютерных сетях
Уметь:
выработать политику и реализовать на практике механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения)
Владеть:
навыками применения методов и средств организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения)

ПК-12: способностью руководить учебно-исследовательской деятельностью обучающихся
Знать:
актуальные проблемы для проведения учебно-исследовательской деятельности обучающихся в области информационной безопасности

Уметь:
провести классификацию угроз, выделить наиболее распространенные угрозы доступности; основные угрозы целостности; основные угрозы конфиденциальности; объяснить проблемы и проводить сравнительный анализ угроз безопасности и методов и средств защиты; описывать тенденции в обеспечении конфиденциальности на технологических примерах
Владеть:
навыками анализа исторических аспектов и современных тенденций развития предметной области

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
основные виды угроз информационной безопасности; последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций; нормативно-правовую и законодательную базу по обеспечению информационной безопасности; понятие и виды компьютерных вирусов, их разрушительные действия; методы защиты от компьютерных вирусов; методы и устройства обеспечения безопасности информации в профессиональной сетевой среде; нормативно-правовую и законодательную базу, технологические стратегии по обеспечению информационной безопасности при взаимодействии в компьютерных сетях; актуальные проблемы для проведения учебно-исследовательской деятельности обучающихся в области информационной безопасности	
3.2	**Уметь:**
указать сильные и слабые стороны различных подходов к обеспечению безопасности; проводить экспертную оценку электронных образовательных ресурсов с точки зрения эффективности реализации методов и средств защиты информации; описывать правовые основы обеспечения конфиденциальности; прогнозировать действие вирусов и атак, направленных на вызов отказа в обслуживании; выработать политику и реализовать на практике механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения); провести классификацию угроз, выделить наиболее распространенные угрозы доступности; основные угрозы целостности; основные угрозы конфиденциальности; объяснить проблемы и проводить сравнительный анализ угроз безопасности и методов и средств защиты; описывать тенденции в обеспечении конфиденциальности на технологических примерах	
3.3	**Владеть:**
навыками устранения отказов программного и аппаратного обеспечения; навыками работы с антивирусным программным обеспечением; навыками применения методов и средств организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения); навыками анализа исторических аспектов и современных тенденций развития предметной области	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Интеракт.
	Раздел 1. Введение в информационную безопасность			
1.1	Основные понятия информационной безопасности /Лек/	9	1	1
1.2	Основные понятия информационной безопасности /Пр/	9	2	1
1.3	Основные понятия информационной безопасности /Ср/	9	15	0
1.4	Угрозы безопасности информации, их классификация /Лек/	9	1	1
1.5	Угрозы безопасности информации, их классификация /Пр/	9	2	0
1.6	Угрозы безопасности информации, их классификация /Ср/	9	13	0
	Раздел 2. Защита информации			
2.1	Современные методы защиты информации /Лек/	9	2	0
2.2	Современные методы защиты информации /Пр/	9	2	0
2.3	Современные методы защиты информации /Ср/	9	22	0
2.4	Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов» /Лек/	9	1	0
2.5	Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов» /Пр/	9	2	1
2.6	Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов» /Ср/	9	23	0
2.7	Криптографические методы информационной безопасности /Лек/	9	1	0
2.8	Криптографические методы информационной безопасности /Пр/	9	2	0
2.9	Криптографические методы информационной безопасности /Ср/	9	17	0
2.10	Консультация перед экзаменом	9	2	0

5. Оценочные и методические материалы по дисциплине (модулю)

5.1. Содержание аудиторной работы по дисциплине (модулю)

Лекция. Тема 1. Основные понятия информационной безопасности (2 ч.)

Вопросы:
• Понятие информационной безопасности и защищенной системы.
• Актуальность защиты информационных систем и телекоммуникаций.
• Информационная безопасность в условиях функционирования глобальных сетей.
• Нормативно-правовые и законодательные акты в области информационной безопасности.
Лекция. Тема 2. Угрозы безопасности информации, их классификация (2 ч.)
Вопросы:
• Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы.
• Анализ угроз информационной безопасности.
• Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).
• Свойства информации: конфиденциальность, доступность, целостность.
• Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб.
• Примеры реализации угроз информационной безопасности.
• Причины, виды и каналы утечки конфиденциальной информации.
• Методы и средства несанкционированного доступа к компьютерным ресурсам и программным средствам.
Лекция. Тема 3. Современные методы защиты информации. (2 ч.)
Вопросы:
• Основные задачи обеспечения защиты информации.
• Основные методы и средства защиты информационных систем.
• Классификация способов и средств комплексной защиты информации.
• Понятие политики безопасности информационных систем.
• Разработка и реализация политики безопасности.
• Идентификация и аутентификация. Парольные схемы аутентификации. Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей.
• Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.
• Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.
Лекция. Тема 4. Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов». (2 ч.)
Вопросы:
• Понятие и основные этапы жизненного цикла «компьютерных вирусов»; факторы, влияющие на их распространение.
• Объекты внедрения, функции и режимы функционирования вирусов.
• Схемы заражения файлов и загрузчиков. Способы маскировки, используемые вирусами.
• Классификация «компьютерных вирусов».
• Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля.
• Антивирусное программное обеспечение.
• Защита системы электронной почты. Спам, борьба со спамом.
• Технология гарантированного восстановление вычислительной системы после заражения «компьютерными вирусами».
Лекция. Тема 5. Криптографические методы информационной безопасности (2 ч.)
Вопросы:
• Методы криптографии. Средства криптографической защиты информации (СКЗИ).
• Криптографические преобразования. Шифрование и дешифрование информации.
• Использование криптографических средств для решения задач идентификации и аутентификации.
• Электронная подпись (ЭП), принципы ее формирования и использования.
• Подтверждение подлинности объектов и субъектов информационной системы.
• Контроль целостности информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.
• Лицензирование и сертификация в области информационной безопасности.
• Критерии безопасности компьютерных систем.
Практическое занятие. Основные понятия информационной безопасности (4 ч.)
Вопросы и задания:
• Понятие информационной безопасности.
• Нормативно-правовые и законодательные акты России в области информационной безопасности.
• Справочные правовые системы.
• Практическая работа по теме «Политики государств в области информационной безопасности»
Практическое занятие. Угрозы безопасности информации, их классификация (2 ч.)
Вопросы и задания:
• Основные виды угроз информационной безопасности.
• Последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций.
• Практическая работа по теме «Угрозы безопасности информации
Практическое занятие. Современные методы защиты информации (4 ч.)

Вопросы и задания:
• Парольные методы защиты информации. Программные средства для хранения паролей.
• Основные методы и средства защиты информационных систем. Классификация способов и средств комплексной защиты информации.
• Защита Интернет-подключений, функции и назначение межсетевых экранов (брандмауэров).
• Выполнение двух лабораторно-практических работ «Особенности защиты информации в локальных и глобальных компьютерных сетях».
Практическое занятие. Понятие и классификация «компьютерных вирусов». (2 ч.)
Вопросы и задания:
• Классификация «компьютерных вирусов». Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля.
• Антивирусное программное обеспечение.
• Выполнение лабораторно-практической работы «Компьютерные вирусы».
Практическое занятие. Защита от «компьютерных вирусов». (2 ч.)
Вопросы и задания:
• Классификация «компьютерных вирусов». Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля.
• Антивирусное программное обеспечение.
• Выполнение лабораторно-практической работы «Антивирусные средства защиты».
Практическое занятие. Криптографические методы информационной безопасности. (4 ч.)
Вопросы и задания:
• Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Использование криптографических средств для решения задач идентификации и аутентификации.
• Выполнение трех лабораторно-практических работ «Принципы криптографической защиты информации».

5.2. Содержание самостоятельной работы по дисциплине (модулю)

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1.	Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности	Домашняя работа поисково-аналитического характера по теме «Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности».	Глог по теме «Информационная безопасность в РФ» (с помощью сервиса glogster.com)
2.	Угрозы безопасности информации, их классификация	Самостоятельное структурирование учебного материала по существующим угрозам безопасности информации.	• Составление google-таблицы с: ○ классификаций угроз безопасности информации по различным признакам, ○ классификацией компьютерных преступлений, ○ и др.
3.	Современные методы защиты информации.	Самостоятельное обучение в Интернет-университете http://www.intuit.ru/studies/courses/680/536/info Курс «Основы информационной безопасности при работе на компьютере»	Сертификат
4.	Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов».	Классификация «компьютерных вирусов» и антивирусных программных средств.	Составление ментальной карты (кластера, фишбоун и др.) по теме.
5.	Криптографические методы информационной безопасности	Самостоятельное изучение законодательных и нормативно-правовых актов в сфере электронной подписи, цифровых сертификатов, лицензирования деятельности удостоверяющих центров.	Коллективный Google-документ, отражающий состояние нормативно-правовой базы по изучаемой теме в РФ.
6.	Современные методы защиты информации.	Упорядочивание, приведение в единую систему знаний о современных методах защиты информации. Выявление причинно-следственных связей.	Создание гугл-сайта по выбранной теме.

Содержание самостоятельной работы по дисциплине на выбор студента

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1.	Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности	Домашняя работа поисково-аналитического характера по теме «Информационная безопасность: концептуальные, практические, системотехнические, экономические, правовые, криптологические, математические, психологические, физические, программные и информационные основы».	Составление словаря терминов в области информационной безопасности и перечня нормативных документов по информационной безопасности (Google-документ).
2.	Угрозы безопасности информации, их классификация	Подготовка мультимедийной презентации об источниках угроз информационной безопасности и способах совершения компьютерных преступлений	Мультимедийная презентация. Публичное выступление
3.	Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов».	Подготовка мультимедийной презентации о классификации и схемах функционирования компьютерных вирусов или антивирусных программных средствах	Презентация MS Power Point
4.	Современные методы защиты информации.	Эссе рефлексивного характера по одной из проблем курса: «Как я лично понимаю термин *информационная безопасность*?», «Защита информации: основные подходы», «Использование методов социальной инженерии для получения доступа к информации», «Особенности парольной защиты информации»	Публикация в Google-группе
5.	Криптографические методы информационной безопасности	Создание индивидуального блога с обзором правовых и технологических аспектов электронной цифровой подписи и электронных сертификатов.	Блог
6.	Все темы	Составление аннотированного каталога Интернет-ресурсов по теме (по выбору студента)	Аннотированный каталог (Google-документ)

5.3.Образовательные технологии
При организации изучения дисциплины будут использованы следующие образовательные технологии: информационно-коммуникационные технологии, технология организации самостоятельной работы, технология рефлексивного обучения, технология модульного обучения, технология игрового обучения, технологии групповой дискуссии, интерактивные технологии, технология проблемного обучения, технология организации учебно-исследовательской деятельности, технология проектного обучения, технология развития критического мышления.
5.4. Текущий контроль, промежуточный контроль и промежуточная аттестация
Балльно-рейтинговая карта дисциплины оформлена как приложение к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине оформлен отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ			
6.1. Рекомендуемая литература			
6.1.1. Основная литература			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Аверченков В. И. , Рытов М. Ю. , Кондрашин Г. В. ,Рудановский М.	Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов http://biblioclub.ru/index.php? page=book_view_red&book_id=93351	М.: ФЛИНТА, 2011
Л1.2	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации: учебное пособие http://biblioclub.ru/index.php?page=book&id=276557	М.; Берлин: Директ-Медиа, 2015
Л1.3	Прохорова О. В.	Информационная безопасность и защита информации: учебник http://biblioclub.ru/index.php? page=book_view_red&book_id=438331	Самара: СГАСУ, 2014
6.1.2. Дополнительная литература			

	Авторы, составители	Заглавие	Издательство, год
Л2.1	А.М. Голиков	Защита информации в инфокоммуникационных системах и сетях: учебное пособие http://biblioclub.ru/index.php?page=book&id=480637	Томск : Томский государственный университет систем управления и радиоэлектроники,
Л2.2	И.В. Ефремов, В.А. Солопова	Информационные технологии в сфере безопасности: практикум: учебное пособие http://biblioclub.ru/index.php?page=book&id=259178	Оренбург : ОГУ, 2013
Л2.3	Л.В. Котова	Сборник задач по дисциплине «Методы и средства защиты информации»: учебное пособие http://biblioclub.ru/index.php?page=book&id=469877	Москва : МПГУ, 2015
Л2.4	С.А. Нестеров	Основы информационной безопасности : учебное пособие http://biblioclub.ru/index.php?page=book&id=363040	Санкт-Петербург : Издательство Политехнического университета, 2014
Л2.5	Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.	Организация безопасной работы информационных систем : учебное пособие http://biblioclub.ru/index.php?page=book&id=277794	Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014
Л2.6	В.И. Петренко	Теоретические основы защиты информации: учебное пособие http://biblioclub.ru/index.php?page=book&id=458204	Ставрополь : СКФУ, 2015

6.2 Перечень программного обеспечения

- Acrobat Reader DC
- Dr.Web Desktop Security Suite, Dr.Web Server Security Suite
- GIMP
- Microsoft Office 2016 Professional Plus (Пакет программ Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher)
- Microsoft Office 365 Pro Plus - subscription license (12 month) (Пакет программ Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher, Skype for Business, OneDrive, SharePoint Online)
- Microsoft Windows 10 Education
- Microsoft Windows 7/8.1 Professional
- XnView
- Архиватор 7-Zip
- Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»

6.3 Перечень информационных справочных систем

- Elsevier (база данных «Freedom Collection» и коллекции электронных книг «Freedom Collection eBook collection», национальная подписка на полнотекстовые ресурсы)
- SCOPUS издательства Elsevier
- SpringerNature (национальная подписка на полнотекстовые ресурсы)
- База данных международных индексов научного цитирования Web of Science
- БД «Polpred.com. Обзор СМИ»
- УИС РОССИЯ
- ЭБС «E-LIBRARY.RU»
- ЭБС «ЛАНЬ»
- ЭБС «РУКОНТ» (Контекстум)
- ЭБС «Университетская библиотека онлайн»
- ЭБС «ЮРАЙТ» (Коллекция Легендарные книги)
- Информационно-образовательная программа «Росметод»
- СПС «ГАРАНТ-Аналитик»
- СПС «Консультант-Плюс»

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Наименование специального помещения: учебная аудитория для проведения занятий лекционного типа, практических занятий, групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации. Оснащенность: Комплект учебной мебели, меловая доска, ноутбук, проекционное оборудование (мультимедийный проектор и экран), портативное звукоусиливающее оборудование.
7.2	Наименование специального помещения: помещение для самостоятельной работы, Читальный зал. Оснащенность: ПК-1шт., Принтер-1шт., Телефон-1шт., Письменный стол-4 шт., Парта-2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические рекомендации для преподавателей по организации изучения дисциплины

Дисциплине «Информационная безопасность и защита информации» отводится существенная роль в профессиональной подготовке будущего специалиста.

Лекционный курс должен строиться таким образом, чтобы, приступая к изучению каждой новой темы, студенты знали, какие вопросы ранее изученного материала будут использованы при изучении нового. Каждая лекция должна носить проблемный характер. Студенты должны привлекаться к постановке проблемы, к поиску путей ее решения, обоснованию каждого утверждения. Используемые методы должны ориентировать будущего специалиста на их усвоение и применение в будущей профессиональной деятельности.

В начале каждой лекции необходимо уяснить цель, которую лектор ставит перед собой и перед студентами. Необходимо ориентировать студентов на сравнение того, что он слышит на лекции с тем, что им было изучено ранее, укладывать новую информацию в собственную, уже имеющуюся у него систему знаний. По ходу лекции целесообразно подчеркивать новые понятия, выяснять их смысл. Разъяснять, как основные положения дисциплины находят практическое применение в обеспечении безопасности при решении конкретных задач.

На лекции важная роль должна быть отведена дискуссии. С этой целью в процессе подготовки к лекции целесообразно продумать систему вопросов, на которые должны ответить студенты, с полным обоснованием своих утверждений.

В конце лекции вместе со студентами целесообразно подвести ее итоги и убедиться, что поставленная цель достигнута.

Каждое практическое занятие целесообразно начинать с повторения теоретического материала, который будет использован на нем. Для этого очень важно четко сформулировать цель занятия и основные знания, умения и навыки, которые студент должен приобрести в течение занятия.

Методические рекомендации для студентов по организации изучения дисциплины

Студенту необходимо научиться работать на лекциях, на практических занятиях и организовывать самостоятельную внеаудиторную деятельность. В ходе самостоятельной подготовки к практическим занятиям необходимо прочитать составленный ранее конспект лекции, подчеркнуть наиболее важные моменты, пополнить словарь новых терминов, составить план ответа на каждый из предлагаемых для изучения вопросов. Для более глубокого усвоения темы необходимо прочесть рекомендованный преподавателем материал из учебной литературы.

Важнейшей особенностью обучения в высшей школе является высокий уровень самостоятельности студентов в ходе образовательного процесса. Эффективность самостоятельной работы зависит от таких факторов как:

• уровень мотивации студентов к овладению конкретными знаниями и умениями;
• наличие навыка самостоятельной работы, сформированного на предыдущих этапах обучения;
• наличие четких ориентиров самостоятельной работы.

Приступая к самостоятельной работе, студенту необходимо четко представлять:

• цель изучения конкретного учебного материала;
• место изучаемого материала в системе знаний, необходимых для формирования специалиста;
• перечень знаний и умений, которыми должен овладеть студент;
• порядок изучения учебного материала;
• источники информации;
• наличие контрольных заданий;
• форму и способ фиксации результатов выполнения учебных заданий;
• сроки выполнения самостоятельной работы.

При выполнении самостоятельной работы студентам рекомендуется:

• записывать ключевые слова и основные термины,
• составлять словарь основных понятий.

После изучения учебного материала необходимо проверить усвоение учебного материала с помощью предлагаемых тестов текущего контроля и при необходимости повторить учебный материал.

В процессе подготовки к зачету необходимо систематизировать, запомнить учебный материал, научиться применять его при решении конкретных задач по обеспечению безопасности.

Приобретение новых знаний должно идти поэтапно:

• знакомство;
• понимание, уяснение основных закономерностей строения и функционирования изучаемого объекта, выявление связей между его элементами и другими подобными объектами;
• фиксация новых знаний в системе имеющихся знаний;
• запоминание и последующее воспроизведение;
• использование полученных знаний для приобретения новых знаний, умений и навыков и т.д.

Приобретение новых знаний требует от обучающегося определенных усилий и активной работы на каждом этапе формирования знаний. Знания, приобретенные учащимся в ходе активной самостоятельной работы, являются более глубокими и прочными.

В ходе обучения студент сталкивается с необходимостью понять и запомнить большой по объему учебный материал. Важнейшим условием для успешного формирования прочных знаний является их упорядочивание, приведение их в единую систему. Это осуществляется в ходе выполнения обучающимся следующих видов работ по самостоятельному структурированию учебного материала:

• запись ключевых слов,
• составление словаря терминов,
• составление классификаций по различным признакам,

• выявление причинно-следственных связей,
• составление коротких рефератов, учебных текстов,
• составление опорных схем и конспектов,
• составление плана выступления.

Практическое занятие должно ориентировать студента на организацию самостоятельной работы. С этой целью на каждом занятии должна быть предусмотрена самостоятельная работа студентов под контролем преподавателя, во время выполнения которой студент может обратиться к преподавателю с вопросом, получить на него ответ. Сам процесс организации самостоятельной работы на занятии должен служить образцом организации самостоятельной деятельности студента. Очень полезна организация самостоятельной работы со взаимопроверкой студентами работ друг друга. Это развивает умение осуществлять контроль и коррекцию результатов своего собственного труда.

Материал лабораторной работы включает:

• основные понятия;
• основные приемы работы, а именно, описание последовательности команд для реализации основных задач. Все задания должны выполняться последовательно, так как они расположены в порядке возрастания сложности;
• упражнения и проекты для самостоятельного выполнения.

Зачёт является итоговой аттестацией и проверкой уровня знаний по всем темам. При этом учитываются приобретённые практические навыки работы на персональном компьютере, итоговый продукт, умение самостоятельно выбрать оптимальный вариант решения, полнота использования изученных возможностей программного обеспечения.

Курс «Информационная безопасность и защита информации» носит практический характер, поэтому студенты самостоятельно выполняют лабораторные работы, в ходе которых изучают основы программного обеспечения и сетевых технологий. После этого студенты выполняют индивидуальные практические задания творческого характера, которые способствуют развитию креативных способностей, воображения, образного мышления.

Деятельность студента в течение семестра оценивается по критериально-оценочной шкале и фиксируется как в рабочем журнале преподавателя, так и в листе индивидуальных образовательных достижений.

Приложение

Балльно-рейтинговая карта дисциплины
«Информационная безопасность и защита информации»
Направление подготовки: 44.03.05 Педагогическое образование
Профили: "Начальное образование" и "Организация внеурочной деятельности"

4 курс
8 семестр

Вид контроля		Минимальное количество баллов	Максимальное количество баллов
Модуль 1. Введение в информационную безопасность			
Текущий контроль по модулю:			
1	Аудиторная работа	8	10
2	Самостоятельная работа (специальные обязательные формы)	8	10
3	Самостоятельная работа (специальные формы на выбор студента)	4	8
Контрольное мероприятие по модулю		4	12
Промежуточный контроль		**24**	**40**
Модуль 2. Защита информации			
Текущий контроль по модулю:			
1	Аудиторная работа	8	18
2	Самостоятельная работа (специальные обязательные формы)	10	20
3	Самостоятельная работа (специальные формы на выбор студента)	8	14
Контрольное мероприятие по модулю		6	8
Промежуточный контроль		**32**	**60**
Промежуточная аттестация		56	**100**

Вид контроля		Примеры заданий, критерии оценки и количество баллов	Темы для изучения и образовательные результаты
Модуль 1. Введение в информационную безопасность			
Текущий контроль по модулю			
1	Аудиторная работа	**Практическая работа по теме «Политика государства в области информационной безопасности» (6 баллов)** • Продемонстрировано знание теоретического материала; • С помощью технологии SWOT-анализа определены сильные и слабые стороны, возможности и угрозы информационной безопасности; • Оформление задания соответствует требованиям *Каждый критерий оценивается в 2 балла*	Тема 1. Основные понятия информационной безопасности. Понятие информационной безопасности. Нормативно-правовые и законодательные акты в области информационной безопасности. Справочные правовые системы. Знает: o основные понятия информационной безопасности; • нормативно-правовую и законодательную базу по обеспечению информационной безопасности; Умеет: • разъяснить понятие информационной безопасности; основные составляющие информационной безопасности; • указать сильные и слабые стороны различных подходов к обеспечению безопасности; • описывать правовые основы обеспечения конфиденциальности; Владеет: • терминологическим аппаратом.
		Практическая работа по теме «Угрозы безопасности информации (4 балла) • Владение терминологическим аппаратом, понимание сущности основных видов угроз безопасности; • Владение навыками структурирования информации по теме и представления в виде ментальной карты (фишбоун, кластера); • Использование сетевых сервисов для создания вышеназванных продуктов; • Результат представлен в лаконичной форме, удобной для восприятия аудиторией. *Каждый критерий оценивается в 1 балл*	Тема 2. Угрозы безопасности информации, их классификация. Знает: • основные виды угроз информационной безопасности; • последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций; Умеет: • проводить классификацию угроз, выделять наиболее распространенные угрозы доступности; основные угрозы целостности; основные угрозы конфиденциальности; Владеет: • навыками определения и выявления вид угроз конфиденциальности, возникающих в связи с применением компьютеров и компьютерных сетей.
2	Самостоятельная работа (обязательная)	**Домашняя работа поисково-аналитического характера по теме «Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности» (6 баллов)** • Содержание представленной информации осмысленно и интерпретировано в соответствии с поставленной задачей • Результат представлен в лаконичной форме, удобной для восприятия.	Тема 1. Основные понятия информационной безопасности. Знает: • нормативно-правовую и законодательную базу по обеспечению информационной безопасности; Умеет: • детализировать и интерпретировать нормативно-правовую информацию в области информационной безопасности; Владеет:

		• Визуализированы результаты работы (составлен глог по теме «Информационная безопасность в РФ» например, с помощью сервиса glogster.com); *Каждый критерий оценивается по следующему правилу: 0 баллов - критерий не выполнен; 1 балл – выполнен частично; 2 балла – выполнен полностью* **Практическая работа по теме «Угрозы безопасности информации. Компьютерные преступления» (4 балла)** • Составлена google-таблица с (2 балла): o классификаций угроз безопасности информации по различным признакам, o классификацией компьютерных преступлений, o и др. • Материал структурирован, информация полная, адекватная и актуальная (1 балл); • Оформление задания соответствует требованиям (1 балл).	• навыками информационного анализа информации по теме. Тема 2. Угрозы безопасности информации, их классификация. Знает: • основные виды компьютерных преступлений; • последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций; Умеет: • приводить примеры реализации угроз информационной безопасности; Владеет: • навыками определения причин, видов и каналов утечки конфиденциальной информации.
3	Самостоятельная работа (на выбор)	Домашняя работа поисково-аналитического характера по теме «Информационная безопасность: концептуальные, практические, системотехнические, экономические, правовые, криптологические, математические, психологические, физические, программные и информационные основы». Составление словаря терминов в области информационной безопасности и перечня нормативных документов по информационной безопасности (Google-документ) (4 балла). • Наполнение терминологического словаря (2 балла); • Корректность цитирования источников (1 балл); • Грамотность содержания и оформления (1 балл).	Тема 1. Основные понятия информационной безопасности. Знает: • основные понятия информационной безопасности; • нормативно-правовую и законодательную базу по обеспечению информационной безопасности; Умеет: • детализировать и интерпретировать нормативно-правовую информацию в области информационной безопасности; Владеет: навыками информационного анализа информации по теме.
		Подготовка мультимедийной презентации и сообщения об источниках угроз информационной безопасности и способах совершения компьютерных преступлений (4 балла) • Информационная (содержательная) насыщенность продукта; • Авторская интерпретация содержания; • Уровень структуризации информации; • Адекватный выбор выразительных средств; • Выбор адекватного сервиса для представления презентации; • Корректность цитирования источников; • Реализация технологических возможностей сервиса • Размещение на серверах	Тема 2. Угрозы безопасности информации, их классификация Знает: • основные виды компьютерных преступлений; • последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций; Умеет: • приводить примеры реализации угроз информационной безопасности; Владеет: • навыками определения причин, видов и каналов утечки конфиденциальной информации.

		www.slideshare.net,www.slideboom.com; создание Google-презентаций; использование сервиса www.prezy.com и т.п. *Каждый критерий оценивается в 0,5 балла*	
Контрольное мероприятие по модулю		**Контрольный тест №1 (12 баллов)** **Минимальное количество баллов по модулю – 30, максимальное - 51**	
Вид контроля		**Примеры заданий, критерии оценки и количество баллов**	**Темы для изучения и образовательные результаты**
Модуль 2. Защита информации			
Текущий контроль по модулю			
1	Аудиторная работа	Выполнение лабораторно-практических работ «Особенности защиты информации в локальных и глобальных компьютерных сетях». *Выполнение лабораторной работы – 4 балла * 2 работы=8.* Отчёт о выполнении лабораторной работы. *Критерии:* • *отчёт содержит полную информацию по изучаемым вопросам;* • *студент чётко и ясно объясняет методы защиты;* • *студент демонстрирует знания программных средств защиты информации при работе в компьютерных сетях;* • *студент демонстрирует навыки организации защиты при работе в компьютерных сетях.* *Каждый критерий – 0,25 балла*	**Тема 3.** Современные методы защиты информации. Парольные методы защиты информации. Программные средства для хранения паролей. Основные методы и средства защиты информационных систем. Классификация способов и средств комплексной защиты информации. Защита Интернет-подключений, функции и назначение межсетевых экранов (брандмауэров). **Знает**: • программные и программно-аппаратные методы и средства обеспечения информационной безопасности; **Умеет:** • защищать информацию с использованием паролей, противостоять методам социальной инженерии; • применять методы защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации; **Владеет:** • навыками применения методов защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации. • навыками применения методов и средств организационно-правовой защиты информации; • навыками применения методов и средств инженерно-технической защиты;
2		Выполнение лабораторно-практических работ «Компьютерные вирусы», «Антивирусные средства защиты». *Критерии: выполнение лабораторной работы – 2 балла * 2 работы =4* Отчёт о выполнении лабораторной работы. *Критерии:* • *отчёт содержит полные ответы на контрольные вопросы;* • *студент чётко и ясно объясняет алгоритм действий пользователя при заражении компьютера вирусами;*	**Тема 4.** Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов». Классификация «компьютерных вирусов». Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля. Антивирусное программное обеспечение. **Знает:** • понятие и виды компьютерных вирусов, их разрушительные действия; • методы защиты от компьютерных вирусов;

		• *студент демонстрирует знания способов профилактики заражения компьютера вирусами, многообразия антивирусных средств, их возможностей и особенностей приобретения, установки и использования;* • *студент демонстрирует навыки работы с антивирусной программой.* *Каждый критерий – 0,5 балла*	**Умеет:** • прогнозировать действие вирусов и атак, направленных на вызов отказа в обслуживании; • объяснить угрозы безопасности из-за компьютерных вирусов и атак, направленных на инициирование отказов в обслуживании; **Владеет:** • навыками работы с антивирусным программным обеспечением.
		Выполнение лабораторно-практических работ «Принципы криптографической защиты информации». *Критерии: выполнение лабораторной работы – 2 балла * 3 работы =6* Отчёт о выполнении лабораторных работ в MS Excel. *Критерии:* • *отчёт содержит полные ответы на контрольные вопросы;* • *студент чётко и ясно объясняет изучаемый алгоритм (метод) шифрования;* • *студент демонстрирует примеры выполненных практических заданий в MS Excel.* *Каждый критерий оценивается в 1 балл*	**Тема 5.** Криптографические методы информационной безопасности. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Использование криптографических средств для решения задач идентификации и аутентификации. **Знает:** • возможности и ограничения широко распространенных криптографических методов; • понятия криптография, криптоанализ, криптостойкость; • понятия шифрование и цифровая подпись, требования к алгоритму шифрования. **Умеет:** • объяснить принципы симметричного и асимметричного шифрования; • особенности криптографических стандартов. **Владеет:** • основами технологии криптографической защиты информации.
3	Самостоятельная работа (обязательная)	Самостоятельное обучение в Интернет-университете http://www.intuit.ru/studies/courses/680/536/info Курс «Основы информационной безопасности при работе на компьютере» Курс обучает правильному обеспечению безопасности персональных данных. В курсе рассмотрены общие понятия в области защиты персональных данных, а также методы их защиты от злоумышленников. *Сертификат – 5 баллов.*	**Тема 3.** Современные методы защиты информации Примеры реализации угроз информационной безопасности. Причины, виды и каналы утечки конфиденциальной информации. Методы и средства несанкционированного доступа к компьютерным ресурсам и программным средствам. Аппаратные и программные средства защиты информации. Компьютерные вирусы. Действия вирусов. Разновидности вирусов. Профилактика и лечение. Антивирусные программы и их виды. Использование файерволов. Противодействие методам социальной инженерии. Безопасность банковских карт. Безопасность работы в интернете. **Знает:** • правовые нормы организации информационного пространства на основе сетевых технологий; • основные обязанности по обеспечению и защите авторского права в процессе информационного обмена в профессиональной деятельности; **Умеет:** • использовать методы и программно-аппаратные средства защиты информации в процессе профессиональной деятельности; **Владеет:**

			• основными технологиями обеспечения защиты информации как на локальном компьютере, так и в процессе сетевого взаимодействия.
		Составление ментальной карты (кластера, фишбоун и др.) по теме «Понятие и классификация компьютерных вирусов. Защита от компьютерных вирусов». Оценка достижений – максимум **3 балла** 1. Работа как результат изученного в аудитории материала – **1 балл** 2. Использован материал, не рассмотренный на практических занятиях на уроке. – **2 балла** 3. Работа с элементами новизны и оригинальности – **3 балла**	**Тема 4.** Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов». Классификация «компьютерных вирусов». Способы заражения компьютерными вирусами. Методы защиты от компьютерных вирусов. **Знает:** • классификацию компьютерных вирусов по различным признакам; • методы защиты от компьютерных вирусов; **Умеет:** • компьютерных вирусов и атак, направленных на инициирование отказов в обслуживании.
		Создание коллективного Google-документа о состоянии нормативно-правовой базы в сфере электронной цифровой подписи, цифровых сертификатов, лицензирования деятельности удостоверяющих центров. Оценка достижений – максимум **2 балла.** *Критерии (каждый критерий – 1 балл):* • *тема раскрыта полностью;* • *студент владеет материалом и демонстрирует знания при ответе на вопросы.*	**Тема 5.** Криптографические методы информационной безопасности. Электронная подпись. Электронный сертификат. Удостоверяющий центр. Открытый и закрытый ключи. Лицензирование. **Знает:** • понятия электронной подписи, электронного сертификата, удостоверяющего центра; **Умеет:** • объяснить особенности сертификации средств электронной подписи. **Владеет:** • навыками самостоятельного поиска и структурирования информации.
4	1. **2.** **3.**	Создание Google-сайта (10 баллов) Контент (содержание) – 5 баллов • Ясно ли предназначение сайта? • Присутствует ли информация на всех страницах (во всех разделах) сайта? • Ориентирован ли сайт на целевую аудиторию? • Соответствует ли содержание сайта (текстовое, графическое) его тематике? • Есть ли грамматические или синтаксические ошибки? Эргономичность использования – 2 балла • Организовано ли содержание логически? • Насколько проста и понятна навигация? • Расположена ли навигация в одном и том же месте на всех страницах? • Позволяет ли навигация вернуться на предыдущие подуровни? Внешний вид (дизайн) – 3 балла	**Тема 3.** Современные методы защиты информации. Защита информации при работе в компьютерных сетях. Парольная защита информации. Разграничение доступа. **Знает:** • способы защиты информации при работе в компьютерных сетях; **Умеет:** • структурировать информацию по изучаемой теме; • открывать для доступа (защищать) размещаемую в сети информацию.

		• Выдержаны ли цвета, шрифты, графика в едином стиле? • Сбалансированы ли цвета дизайна страниц? • Сбалансирован ли макет страницы (наличие сетки)? • Не перегружена ли страница информацией (особенно касается главных станиц)? • Качественна ли графика и сочетается ли она с остальными составляющими страницы? • Не мешает ли графика пользователю воспринимать информацию	
5	Самостоятельная работа (на выбор)	Подготовка мультимедийной презентации о классификации и схемах функционирования компьютерных вирусов или антивирусных программных средствах. *Оценивание – 5 баллов.* *Критерии:* 1. Полнота раскрытия темы - 1 б. 2. Актуальность материалов, отражающих современный уровень состояния вопроса - 1 б. 3. Оригинальность изложения идеи, наличие интересных фактов - 1 б. 4. Дизайн оформления визуального ряда (презентации и т.д.) - 0,5 б. 5. Логичность, последовательность изложения, отсутствие информации, не относящейся к теме - 1 б. 6. Отсутствие синтаксических, стилистических и орфографических ошибок - 0,5 б.	**Тема 4.** Понятие и классификация «компьютерных вирусов». Защита от «компьютерных вирусов». Классификация «компьютерных вирусов». Способы заражения компьютерными вирусами. Методы защиты от компьютерных вирусов. **Знает:** • классификацию компьютерных вирусов по различным признакам; • методы защиты от компьютерных вирусов; **Умеет:** • применять на практике методы защиты от компьютерных вирусов.
		Эссе рефлексивного характера по одной из проблем курса: «Как я лично понимаю термин *информационная безопасность*?», «Защита информации: основные подходы», «Использование методов социальной инженерии для получения доступа к информации», «Особенности парольной защиты информации» **(2 балла).** • Отражена глубина изучения проблемы, проведен ее многофакторный анализ; • Работа отражает личное видение автора проблемы и пути ее решения; • Соответствие стилю эссе; • Содержание эссе размещено в Google-группе *Каждый критерий оценивается в 0,5 балла*	**Тема 3.** Современные методы защиты информации. Парольные методы защиты информации. Программные средства для хранения паролей. Основные методы и средства защиты информационных систем. Классификация способов и средств комплексной защиты информации. Защита Интернет-подключений, функции и назначение межсетевых экранов (брандмауэров). **Знает**: • терминологический аппарат науки; **Умеет:** • применять методы защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации; • формулировать критерии и проводить рациональный поиск информации в соответствии с поставленными целями; • критически оценивать информацию с точки зрения ее качества, достоверности и релевантности; **Владеет:**

			• навыками применения методов защиты данных в процессе решения практических задач получения, хранения, обработки и передачи информации.
6		Создание индивидуального *блога* с обзором правовых и технологических аспектов электронной цифровой подписи и электронных сертификатов.– *5 баллов* *Критерии* оценки блога • *Технологичность (наличие навигационных элементов (облако тегов, аннотация содержания и пр., целесообразность используемых дополнений, расширений, гаджетов и т.п.) – 3 балла* • *Социальность (блог ориентирован на профессиональную сферу) – 2 балла*	**Тема 5.** Криптографические методы информационной безопасности. Электронная подпись. Электронный сертификат. Удостоверяющий центр. Открытый и закрытый ключи. Лицензирование. **Знает:** • понятия электронной подписи, электронного сертификата, удостоверяющего центра; **Умеет:** • объяснить особенности сертификации средств электронной подписи. **Владеет:** • навыками самостоятельного поиска и структурирования информации.
		Составление аннотированного каталога Интернет-ресурсов по теме (по выбору студента) (2 балла -10-15 ресурсов) • Репрезентативность ресурсов, • Соответствие выбранной тематике, • Научная новизна, доступность изложения, • Качество оформления каталога, выбор средств для его тиражирования. *Каждый критерий оценивается в 0,5 балла*	**Тема 3.** Современные методы защиты информации Основные методы и средства защиты информационных систем. Понятие политики безопасности информационных систем. Парольные схемы аутентификации. Защита Интернет-подключений, функции и назначение межсетевых экранов. Знает: • основные понятия информационной безопасности; • нормативно-правовую и законодательную базу по обеспечению информационной безопасности; Умеет: • разъяснить понятие информационной безопасности; основные составляющие информационной безопасности; • указать сильные и слабые стороны различных подходов к обеспечению безопасности; • описывать правовые основы обеспечения конфиденциальности; Владеет: • терминологическим аппаратом.
Контрольное мероприятие по модулю		**Контрольный тест №1 (8 баллов)** **Минимальное количество баллов по модулю – 30, максимальное - 49**	

Ст. преподаватель кафедры ИКТ в образовании М.А. Воронина