МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
прикладной математики, информатики,
физики и методики их преподавания

_____ Е.А. Позднова

04.02.2016 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ОД.19 Информационная безопасность

1. Шифр и наименование направления подготовки / специальности:

44.03.01 Педагогическое образование

2. Профиль подготовки:

Информатика и информационные технологии в образовании

3. Квалификация выпускника:

Бакалавр

4. Форма обучения:

Заочная

5. Кафедра, отвечающая за реализацию дисциплины:

кафедра прикладной математики, информатики, физики и методики их преподавания

6. Составитель программы:

Позднова Е.А., кандидат педагогических наук, доцент

7. Рекомендована:

кафедрой прикладной математики, информатики, физики и методики их преподавания (протокол № 8 от 04.02.2016)

8. Учебный год: 2011/2012 **Семестр:** 5

9. Цели и задачи учебной дисциплины:

Целью дисциплины является становление профессиональной компетенции педагога через формирование целостного представления о роли информационных технологий в современной образовательной среде и педагогической деятельности на основе овладения комплексными методами и современными средствами защиты компьютерных систем и их компонентов от различных угроз безопасности

В ходе изучения дисциплины ставятся **задачи**:

- дать теоретические основы знаний в области принципов и физических основ, используемых для защиты информации, алгоритмов их работы и методик применения;
- выработка у студентов умений формулировать и обосновывать технические требования к средствам защиты информации, осуществлять обоснованный выбор комплекса СЗИ для конкретных компьютерных систем и использовать их в практической деятельности;
- формирование у студентов представлений об особенностях, тенденциях, проблемах и перспективах развития средств защиты информации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Информационная безопасность» является обязательной дисциплиной вариативной части ООП.

Областью профессиональной деятельности бакалавров, на которую ориентирует дисциплина, является школьное образование.

Профильной для данной дисциплины является педагогическая и культурно-просветительская профессиональная деятельность бакалавров. Дисциплина готовит к решению следующих задач профессиональной деятельности:

в области педагогической деятельности:

- использование возможностей образовательной среды для обеспечения качества образования, в том числе с использованием информационных технологий;
- осуществление профессионального самообразования и личностного роста, проектирование дальнейшего образовательного маршрута и профессиональной карьеры.

в области культурно-просветительской деятельности:

- популяризация профессиональной области знаний общества.

Для освоения дисциплины «Информационная безопасность» студенты используют знания, умения, навыки, сформированные в ходе изучения дисциплины «Информатика».

Изучение данной дисциплины может являться основой для последующего изучения дисциплин: «Правовые аспекты защиты информации», «Методика обучения и воспитания», «Основы криптографической защиты информации» вариативной части профессионального цикла, для последующего прохождения учебной и производственной практик.

11. Компетенции обучающегося, формируемые в результате освоения дисциплины:

а) общекультурные (ОК): ОК-3;

б) общепрофессиональные(ОПК) ОПК-4;

в) специальные (СК): ПК-4.

В результате изучения дисциплины студент должен

знать:

- основные понятия теории информационной безопасности;
- направления разработки и применения средств защиты информации;
- методы и средства защиты информации;
- основные нормативные документы в сфере обеспечения информационной безопасности;

уметь:

- уметь применять правовые, программные и технические средства для защиты информации в информационных системах;
- уметь пользоваться различными методами и средствами защиты информации в различных видах деятельности;

владеть:

- навыками обеспечения информационной безопасность на различных уровнях;
- способами осуществления выбора различных мер и средств обеспечения информационной безопасности в учебном процессе с учетом реального оснащения образовательного учреждения.

12. Структура и содержание учебной дисциплины

12.1 Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом: 2/72.

12.2 Виды учебной работы

Вид учебной работы	Трудоемкость (часы)		
	Всего	В том числе в интерактивной форме	По семестрам
			2 сем.
Аудиторные занятия	12	4	12
в том числе: лекции	6	2	6
практические			
лабораторные	6	2	6
Самостоятельная работа	56		56
Контроль	4		
Итого:	72	4	72
Форма промежуточной аттестации			Зачет

12.3. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Угрозы информационной безопасности	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. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.

2	Информационные системы и их компоненты как объекты защиты	Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы, влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.
3	Направления разработки и применения средств защиты информации	Системные принципы информационной безопасности Выработка политики безопасности Направления применения методов и средств защиты информации
4	Методика построения защищенных информационных систем	Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
5	Организационно-правовые меры и средства защиты информации	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Информационная безопасность образовательной организации.
6	Технические и программные средства защиты информации	Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.
7	Технические средства контроля доступа к компонентам информационных систем	Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.
8	Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.	Требования к защите электропитания различных компонентов КС. Выбор политики защиты электропитания КС Выборочная защита. Частичная защита.Полная защита Основные варианты организации защиты ЭП асчет мощности UPS Устройства бесперебойного электропитания Управление UPS Пример: управляемый APC

		Smart-UPS D. Технические характеристики. Технология автоматического выключения нескольких серверов с разными операционными системами.
9	Методы и средства уничтожения информации	Особенности хранения компьютерной информации на физических носителях Способы уничтожения информации без разрушения носителя: программные и физические. Способы уничтожения информации с разрушением носителя: механические, термические, химические радиационные.
10	Криптографические методы защиты информации	Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. Изучение устройства и принципа работы шифровальной машины Энигма. Стандарт симметричного шифрования AES Rijndael. Генерация простых чисел, используемых в асимметричных системах шифрования. Электронная цифровая подпись. Шифрование методом скользящей перестановки. Корректирующие коды. Методы сжатия.

12.4 Междисциплинарные связи

№ п/п	Наименование дисциплин учебного плана, с которым организована взаимосвязь дисциплины рабочей программы	№№ разделов дисциплины рабочей программы, связанных с указанными дисциплинами
1	Информатика	1-3
2	Правовые аспекты защиты информации	5
3	Методика обучения и воспитания	1-9
4	Основы криптографической защиты информации	3-4, 10

12.5. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Угрозы информационной безопасности	1			6	7
2	Информационные системы и их компоненты как объекты защиты				6	6
3	Направления разработки и применения средств защиты информации	1			6	7
4	Методика построения защищенных информационных систем	1			6	7
5	Организационно-правовые меры и средства защиты информации				8	8
6	Технические и программные средства защиты информации	1			6	7
7	Технические средства контроля доступа к компонентам информационных систем	1			6	7

8	Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.	1			6	7
9	Методы и средства уничтожения информации				6	6
10	Криптографические методы защиты информации			6		6
	Зачет					4
	Итого:	6		6	56	72

13. Учебно-методическое и информационное обеспечение дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ 7.1–2003, используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Башлы, П.Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. - М. : Евразийский открытый институт, 2011. - 375 с. - ISBN 978-5-374-00301-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90539
2	Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

б) дополнительная литература:

№ п/п	Источник
3	Партыка, Татьяна Леонидовна. Информационная безопасность : учебное пособие для студентов учреждений среднего профессионального образования / Т.Л. Партыка, И.И. Попов .– 2-е изд., испр. и доп .— М. : ФОРУМ: ИНФРА-М, 2007 .— 368с. : ил. — (Профессиональное образование)
4	Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для студентов вузов.- 3-е изд., стер.- М.: Академия, 2007
5	Липин Ю.Н. Базы данных и знаний. Управление базами и защита информации: учебное пособие.- Пермь : ПермГТУ, 2008
6	Щекочихин О.В. Введение в комплексную защиту объектов информатизации: учеб. пос.- Кострома: Изд-во Костром. гос. технол. ун-та, 2010

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
7	Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. - СПб.: СПбГУ ИТМО, 2010. - 98 с. То же [Электронный ресурс]. - URL: http://window.edu.ru/resource/984/71984

14. Материально-техническое обеспечение дисциплины:

Компьютерный класс, мультимедиа проектор.

15. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю):

- Microsoft Office 2010;
- ОС Microsoft Windows 7;
- Borlan Dev Studio (или Borland Delphi 5).

16. Формы организации самостоятельной работы:

- составление опорных конспектов;

- подготовка докладов и рефератов.

17. Перечень учебно-методического обеспечения для организации самостоятельной работы обучающихся по дисциплине (модулю):

- методические указания к лабораторным работам по дисциплине «Информационная безопасность»;
- вопросы к зачету по дисциплине «Информационная безопасность»;
- перечень вопросов для самостоятельно изучения «Информационная безопасность».

18. Критерии аттестации по итогам освоения дисциплины:

- оценка **«зачтено»** выставляется студенту, если студент ориентируется в теоретическом материале; имеет представление об основных подходах к излагаемому материалу; знает определения основных теоретических понятий излагаемой темы, умеет применять теоретические сведения для анализа практического материала, в основном демонстрирует готовность применять теоретические знания в практической деятельности и освоение большинства показателей формируемых компетенций;
- оценка **«не зачтено»** выставляется студенту, если студент не ориентируется в теоретическом материале; не знает основных понятий излагаемой темы, не умеет применять теоретические сведения для анализа практического материала, не демонстрирует готовность применять теоретические знания в практической деятельности и освоение показателей формируемых компетенций.

19. Методические указания для обучающихся по освоению дисциплины (модуля):

Приступая к изучению учебной дисциплины, прежде всего обучающиеся должны ознакомиться с учебной программой дисциплины. Вводная лекция содержит информацию об основных разделах рабочей программы дисциплины; электронный вариант рабочей программы размещён на сайте БФ ВГУ.

Обучающиеся должны иметь четкое представление о:

- перечне и содержании компетенций, на формирование которых направлена дисциплина;
- основных целях и задачах дисциплины;
- планируемых результатах, представленных в виде знаний, умений и навыков, которые должны быть сформированы в процессе изучения дисциплины;
- количестве часов, предусмотренных учебным планом на изучение дисциплины, форму промежуточной аттестации;
- количестве часов, отведенных на аудиторные занятия и на самостоятельную работу;
- формах аудиторных занятий и самостоятельной работы;
- структуре дисциплины, основных разделах и темах;
- системе оценивания ваших учебных достижений;
- учебно-методическом и информационном обеспечении дисциплины.

Знание основных положений, отраженных в рабочей программе дисциплины, поможет обучающимся ориентироваться в изучаемом курсе, осознавать место и роль изучаемой дисциплины, строить свою работу в соответствии с требованиями, заложенными в программе.

Основными формами аудиторных занятий по дисциплине являются лекции и лабораторные работы, посещение которых обязательно для всех студентов (кроме студентов, обучающихся по индивидуальному плану).

В ходе лекционных занятий следует не только слушать излагаемый материал и кратко его конспектировать, но очень важно участвовать в анализе примеров, предлагаемых преподавателем, в рассмотрении и решении проблемных вопросов, выносимых на обсуждение. Необходимо критически осмысливать предлагаемый материал, задавать вопросы как уточняющего характера, помогающие уяснить отдельные излагаемые положения, так и вопросы продуктивного типа, направленные на расширение и углубление сведений по изучаемой теме, на выявление недостаточно освещенных вопросов, слабых мест в аргументации и т.п.

В процессе конспектирования лекционного материала лучше использовать одну сторону тетрадного разворота (например, левую), оставив другую (правую) для внесения вопросов, замечаний, дополнительной информации, которая может появиться при изучении учебной или научной литературы во время подготовки к практическим занятиям. Не следует дословно записывать лекцию, лучше попытаться понять логику изложения и выделить наиболее важные положения лекции в виде опорного конспекта или ментальной карты (для составления ментальной карты или опорного конспекта можно использовать разворот тетради или отдельный чистый лист А4, который затем можно вклеить в тетрадь для конспектов). Основные определения важнейших понятий, особенно при отсутствии единства в трактовке тех или иных понятий среди ученых, лучше записать. Не следует пренебрегать примерами, зачастую именно записанные примеры помогают наполнить опорный конспект живым содержанием и облегчают его понимание.

Рекомендуется использовать различные формы выделения наиболее сложного, нового, непонятного материала, который требует дополнительной проработки: можно пометить его знаком вопроса (или записать на полях сам вопрос), цветом, размером букв и т.п. – это поможет быстро найти материал, вызвавший трудности, и в конце лекции (или сразу же, попутно) задать вопрос преподавателю (не следует оставлять непонятый материал без дополнительной проработки, без него иногда бывает невозможно понять последующие темы). Материал, уже знакомый или понятный, нуждается в меньшей детализации – это поможет сэкономить усилия во время конспектирования.

Следует отметить, что рекомендации по составлению конспектов лекций так же распространяются и на составление опорных конспектов.

В ходе выполнения лабораторных работ студент выполняет задания, содержащиеся в методическом пособии дисциплины в соответствии с имеющимися указаниями. Далее студент самостоятельно выполняет индивидуальное задание.

Обязательно следует познакомиться с критериями оценивания каждой формы контроля (реферата, теста, проекта и т.д.) – это поможет избежать недочетов, снижающих оценку за работу.

При подготовке к промежуточной аттестации необходимо повторить пройденный материал в соответствии с учебной программой, примерным перечнем вопросов, выносящихся на зачет. Рекомендуется использовать конспекты лекций и источники, перечисленные в списке литературы в рабочей программе дисциплины, а также ресурсы электронно-библиотечных систем. Необходимо обратить особое внимание на темы учебных занятий, пропущенных по разным причинам. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.