МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Волгоградский государственный социально-педагогический университет»
Факультет математики, информатики и физики
Кафедра информатики и методики преподавания информатики

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____ Ю. А. Жадаев
« 31 » мая 2019 г.

Информационная безопасность

Программа учебной дисциплины

Направление 09.03.03 «Прикладная информатика»

Профиль «Прикладная информатика»

очная форма обучения

Волгоград
2019

Обсуждена на заседании кафедры информатики и методики преподавания информатики
«26» 02 2019 г., протокол № 7

Заведующий кафедрой _____ Сергеев А.Н. «26» 02 2019 г.
(подпись) (зав. кафедрой) (дата)

Рассмотрена и одобрена на заседании учёного совета факультета математики, информатики и физики «02» 04 2019 г. , протокол № 7

Председатель учёного совета Сергеев А.Н. _____ «02» 04 2019 г.
(подпись) (дата)

Утверждена на заседании учёного совета ФГБОУ ВО «ВГСПУ»
«31» 05 2019 г. , протокол № 10

Отметки о внесении изменений в программу:

Лист изменений № _____ _____ _____ _____
(подпись) (руководитель ОПОП) (дата)

Лист изменений № _____ _____ _____ _____
(подпись) (руководитель ОПОП) (дата)

Лист изменений № _____ _____ _____ _____
(подпись) (руководитель ОПОП) (дата)

Разработчики:
Карякина Татьяна Ивановна, кандидат педагогических наук, доцент кафедры информатики и методики преподавания информатики ФГБОУ ВО «ВГСПУ».

Программа дисциплины «Информационная безопасность» соответствует требованиям ФГОС ВО по направлению подготовки 09.03.03 «Прикладная информатика» (утверждён приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 922) и базовому учебному плану по направлению подготовки 09.03.03 «Прикладная информатика» (профиль «Прикладная информатика»), утверждённому Учёным советом ФГБОУ ВО «ВГСПУ» (от 31 мая 2019 г., протокол № 10).

1. Цель освоения дисциплины

Сформировать систему компетенций бакалавра прикладной информатики в области обеспечении качества автоматизации и информатизации решения прикладных задач и создания информационных систем для решения задач обеспечения информационной безопасности компьютерных систем в проектной и производственно-технологической профессиональной деятельности.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» относится к базовой части блока дисциплин.

Для освоения дисциплины «Информационная безопасность» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Алгоритмизация и программирование», «Безопасность жизнедеятельности», «Вычислительные системы, сети и телекоммуникации», «Информационные системы и технологии», «Теория вероятностей и математическая статистика», «Экономика фирмы (предприятия)».

Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин «Менеджмент», «Программная инженерия», «Проектирование информационных систем», прохождения практик «Ознакомительная практика», «Технологическая (проектно-технологическая) практика».

3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:

– способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

– способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4).

В результате изучения дисциплины обучающийся должен:

знать

– терминологию и основные понятия теории защиты информации;

– содержание основных нормативных документов в области защиты компьютерной информации;

– виды угроз информационным системам;

– цели и задачи административного уровня обеспечения информационной безопасности;

– причины и источники случайных воздействий на информационные системы;

– классы функциональных требований и требований доверия;

– виды систем шифрования данных по способу их функционирования;

уметь

– использовать основные концептуальные положения системы защиты информации;
– квалифицировать нарушения в сфере информационной безопасности;
– выявлять угрозы информационной безопасности;
– определить политику безопасности организации;
– определять каналы несанкционированного доступа к информации;
– использовать стандарт для оценки защищенности информационных систем;
– классифицировать методы криптографического преобразования информации;

владеть
– распределением задач информационной безопасности по уровням ее обеспечения;
– навыками определения ответственности за нарушения в сфере информационной безопасности;
– навыками обосновывать организационно-технические мероприятия по защите информации в информационных системах;
– направлениями разработки политики безопасности;
– навыками выявления и классифицирования угрозы информационной безопасности;
– отличием функциональных требований от требований доверия;
– общей технологией использования метода шифрования.

4. Объём дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестры
		4
Аудиторные занятия (всего)	44	44
В том числе:		
Лекции (Л)	18	18
Практические занятия (ПЗ)	–	–
Лабораторные работы (ЛР)	26	26
Самостоятельная работа	64	64
Контроль	–	–
Вид промежуточной аттестации		ЗЧО
Общая трудоемкость часы	108	108
зачётные единицы	3	3

5. Содержание дисциплины
5.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Понятия информационной безопасности, защиты информации	Основные задачи информационной безопасности. Предмет защиты информации, его свойства. Объект защиты информации. Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности.
2	Информация как правовая категория, ее особенности	Государственная политика информационной безопасности. Органы обеспечения информационной безопасности. Лицензирование деятельности в области информационной безопасности. Структура и состав информационного законодательства в РФ. Ответственность за нарушения в сфере

		информационной безопасности. Стандарты информационной безопасности.
3	Основные источники угроз безопасности информации	Классификация угроз информационной безопасности. Виды злоумышленников по отношению к автоматизированной системе. Компьютерные вирусы как угроза информационной безопасности. Классификация антивирусных программ. Профилактика компьютерных вирусов.
4	Уровни формирования режима информационной безопасности	Цели и задачи административного уровня обеспечения информационной безопасности. Основные направления разработки политики информационной безопасности организации. Группы сведений, содержащиеся в документации по политике безопасности организации. Программно-технический уровень обеспечения информационной безопасности. Инженерно-техническая защита информации.
5	Методы и средства защиты информации в компьютерных системах	Пути достижения требуемой достоверности обработки информации. Общие принципы и методы выявления технических каналов утечки информации. Организационные и инженерно-технические меры и мероприятия по обеспечению конфиденциальности информации в автоматизированных системах. Рубежи защиты и компоненты системы охраны объекта. Разграничение доступа в автоматизированных системах. Организационные и аппаратно-программные методы повышения сохранности информации.
6	Особенности защиты информации в распределенных компьютерных системах	Функциональные требования и требования доверия, изложенные в «Общих критериях». Сервисы безопасности и администрирование средств безопасности в вычислительных сетях в соответствии с «Рекомендациями X.800». Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных компьютерных системах. Защита информации в каналах связи. Межсетевое экранирование. Подтверждение подлинности взаимодействующих процессов. Подтверждение подлинности информации, получаемой по коммуникационной подсети. Электронная цифровая подпись. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика.
7	Классификация методов криптографического преобразования информации	Шифрование. Методы шифрования с симметричным ключом. Методы замены. Методы перестановки. Аналитические методы шифрования. Аддитивные методы шифрования. Системы шифрования с открытым ключом. Российский стандарт на шифрование информации ГОСТ 28147-89.

5.2. Количество часов и виды учебных занятий по разделам дисциплины

№ п/п	Наименование раздела дисциплины	Лекц.	Практ. зан.	Лаб. зан.	СРС	**Всего**

1	Понятия информационной безопасности, защиты информации	2	–	3	9	14
2	Информация как правовая категория, ее особенности	2	–	3	9	14
3	Основные источники угроз безопасности информации	2	–	4	10	16
4	Уровни формирования режима информационной безопасности	3	–	4	9	16
5	Методы и средства защиты информации в компьютерных системах	3	–	4	9	16
6	Особенности защиты информации в распределенных компьютерных системах	3	–	4	9	16
7	Классификация методов криптографического преобразования информации	3	–	4	9	16

6. Перечень основной и дополнительной учебной литературы

6.1. Основная литература

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html (дата обращения: 27.12.2019). — Режим доступа: для авторизир. пользователей.

2. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — ISBN 978-5-94774-821-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/52209.html (дата обращения: 27.12.2019). — Режим доступа: для авторизир. пользователей.

3. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/10677.html (дата обращения: 27.12.2019). — Режим доступа: для авторизир. пользователей.

6.2. Дополнительная литература

1. Креопалов, В. В. Технические средства и методы защиты информации : учебное пособие / В. В. Креопалов. — Москва : Евразийский открытый институт, 2011. — 278 с. — ISBN 978-5-374-00507-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/10871.html (дата обращения: 27.12.2019). — Режим доступа: для авторизир. пользователей.

2. Федин, Ф. О. Информационная безопасность : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин. — Москва : Московский городской педагогический университет, 2011. — 260 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/26486.html (дата обращения: 27.12.2019). — Режим доступа: для авторизир. пользователей.

3. Хорев П. Б. Методы и средства защиты информации в компьютерных системах :

учеб. пособие для студентов вузов, обучающихся по направлению 230100 (654600) "Информатика и вычислит. техника" / П. Б. Хорев. - М. : Академия, 2005. - 254,[1] с. : ил. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 251-252 (28 назв.). - ISBN 5-7695-1839-1; 35 экз. : 183-33.

7. Ресурсы Интернета

Перечень ресурсов Интернета, необходимых для освоения дисциплины:

1. Электронная библиотечная система IPRbooks. URL: http://iprbookshop.ru.

8. Информационные технологии и программное обеспечение

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости):

1. Пакет офисных приложений (редактор текстовых документов, презентаций, электронных таблиц).

9. Материально-техническая база

Для проведения учебных занятий по дисциплине «Информационная безопасность» необходимо следующее материально-техническое обеспечение:

1. Компьютерный класс для самостоятельной работы студентов, оборудованный необходимым количеством персональных компьютеров, подключённых к единой локальной сети с возможностью централизованного хранения данных и выхода в Интернет, использования офисных приложений и CASE-средств.
2. Аудитория для проведения учебных занятий, оснащенная аудиторной доской, стационарным или переносным комплексом мультимедийного презентационного оборудования, имеющего доступ к Интернету и локальной сети.

10. Методические указания для обучающихся по освоению дисциплины

Дисциплина «Информационная безопасность» относится к базовой части блока дисциплин. Программой дисциплины предусмотрено чтение лекций и проведение лабораторных работ. Промежуточная аттестация проводится в форме аттестации с оценкой.

Лекционные занятия направлены на формирование глубоких, систематизированных знаний по разделам дисциплины. В ходе лекций преподаватель раскрывает основные, наиболее сложные понятия дисциплины, а также связанные с ними теоретические и практические проблемы, даёт рекомендации по практическому освоению изучаемого материала. В целях качественного освоения лекционного материала обучающимся рекомендуется составлять конспекты лекций, использовать эти конспекты при подготовке к практическим занятиям, промежуточной и итоговой аттестации.

Лабораторная работа представляет собой особый вид индивидуальных практических занятий обучающихся, в ходе которых используются теоретические знания на практике, применяются специальные технические средства, различные инструменты и оборудование. Такие работы призваны углубить профессиональные знания обучающихся, сформировать умения и навыки практической работы в соответствующей отрасли наук. В процессе лабораторной работы обучающийся изучает практическую реализацию тех или иных процессов, сопоставляет полученные результаты с положениями теории, осуществляет интерпретацию результатов работы, оценивает возможность применения полученных знаний на практике.

При подготовке к лабораторным работам следует внимательно ознакомиться с

теоретическим материалом по изучаемым темам. Необходимым условием допуска к лабораторным работам, предполагающим использованием специального оборудования и материалов, является освоение правил безопасного поведения при проведении соответствующих работ. В ходе самой работы необходимо строго придерживаться плана работы, предложенного преподавателем, фиксировать промежуточные результаты работы для отчета по лабораторной работе.

Контроль за качеством обучения и ходом освоения дисциплины осуществляется на основе рейтинговой системы текущего контроля успеваемости и промежуточной аттестации студентов. Рейтинговая система предполагает 100-балльную оценку успеваемости студента по учебной дисциплине в течение семестра, 60 из которых отводится на текущий контроль, а 40 – на промежуточную аттестацию по дисциплине. Критериальная база рейтинговой оценки, типовые контрольные задания, а также методические материалы по их применению описаны в фонде оценочных средств по дисциплине, являющемся приложением к данной программе.

11. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа обучающихся является неотъемлемой частью процесса обучения в вузе. Правильная организация самостоятельной работы позволяет обучающимся развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, способствует формированию навыков совершенствования профессионального мастерства.

Самостоятельная работа обучающихся во внеаудиторное время включает в себя подготовку к аудиторным занятиям, а также изучение отдельных тем, расширяющих и углубляющих представления обучающихся по разделам изучаемой дисциплины. Такая работа может предполагать проработку теоретического материала, работу с научной литературой, выполнение практических заданий, подготовку ко всем видам контрольных испытаний, выполнение творческих работ.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине представлено в рабочей программе и включает в себя:

– рекомендуемую основную и дополнительную литературу;

– информационно-справочные и образовательные ресурсы Интернета;

– оценочные средства для проведения текущего контроля и промежуточной аттестации по дисциплине.

Конкретные рекомендации по планированию и проведению самостоятельной работы по дисциплине «Информационная безопасность» представлены в методических указаниях для обучающихся, а также в методических материалах фондов оценочных средств.

12. Фонд оценочных средств

Фонд оценочных средств, включающий перечень компетенций с указанием этапов их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания, типовые контрольные задания и методические материалы является приложением к программе учебной дисциплины.