Министерство науки и высшего образования Российской Федерации

Муромский институт (филиал)

федерального государственного бюджетного образовательного учреждения высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(МИ ВлГУ)

Кафедра *ФПМ*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
16.06.2020

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Направление подготовки *10.03.01 Информационная безопасность*

Профиль подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*

Квалификация (степень) выпускника *Бакалавр*

Семестр	Трудоемкость, час./зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контр. (экз., зач., зач. с оц.)
4	**144 / 4**	**32**	**16**		**5,2**	**0,35**	**53,55**	**63,8**	**Экз.(26,65)**
Итого	**144 / 4**	**32**	**16**		**5,2**	**0,35**	**53,55**	**63,8**	**26,65**

Муром, 2020 г.

1. Цель освоения дисциплины

Цель дисциплины: дать понятие о существующих угрозах информационной безопасности и их источниках;

дать понятие о существующих средствах обеспечения информационной безопасности и тенденциях их развития.

научить анализировать имеющуюся ситуацию на предприятии;

научить определять круг мер и средств для повышения информационной безопасности.

2. Место дисциплины в структуре ОПОП ВО (Цикл (Б1.О.13))

Базовые дисциплины: Введение в специальность, Математика, Дискретная математика.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах.

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.

Результатом освоения дисциплины является достижение следующих индикаторов:

ОПК-1.1.3 Владеть навыками разработки и реализации политики управления доступом в компьютерных системах.

ОПК-1.2 Уметь оценивать роль и значение информации, информационных технологий и информационной безопасности.

ОПК-2.2 Знать основные методы и средства обеспечения информационной безопасности.

ОПК-2.7 Уметь решать задачи профессиональной деятельности на основе существующих компьютерных технологий.

ОПК-2.9 Уметь ориентироваться в актуальных проблемах информационной безопасности.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

4.1. Форма обучения: очная

Уровень базового образования: среднее общее.
Срок обучения 4г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Семинары	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР	Консультация	Контроль	
1	Основы информационной безопасности	4	32		16			63,8				Устный опрос, тестирование
Всего за семестр		144	32		16			63,8		5,2	0,35	Экз.(26,65)
Итого		144	32		16			63,8		5,2	0,35	26,65

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 4

Раздел 1. Основы информационной безопасности

Лекция 1.

Актуальность проблемы информационной безопасности. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Основные понятия и определения (2 часа).

Лекция 2.

Политика государства в области информационной безопасности. Правовые основы обеспечения информационной безопасности (2 часа).

Лекция 3.

Угрозы безопасности информации. Источники угроз (2 часа).

Лекция 4.

Модель угроз безопасности информации. Модель нарушителя безопасности информации (2 часа).

Лекция 5.

Меры и методы обеспечения защиты информации. Организационные(процедурные, административные) меры защиты информации (2 часа).

Лекция 6.

Инженерно-технические меры защиты информации (2 часа).

Лекция 7.

Идентификация и аутентификация. Управление доступом (2 часа).

Лекция 8.

Межсетевое экранирование. Обеспечение высокой доступности (2 часа).

Лекция 9.

Протоколирование и аудит. Системы обнаружения и предотвращения компьютерных атак (2 часа).

Лекция 10.

Криптографические методы защиты информации. Электронная цифровая подпись. Контроль целостности (2 часа).

Лекция 11.

Вредоносные программы и защита от них. Защита информации в компьютерных сетях. Тестирование на проникновение. Социальная инженерия (2 часа).

Лекция 12.

Меры по обеспечению безопасности данных при их обработке в информационных системах персональных данных и государственных информационных системах (2 часа).

Лекция 13.

Лицензирование и сертификация в области ИБ (2 часа).

Лекция 14.

Аттестация объектов информатизации. Выбор средств ИБ. Управление рисками ИБ (2 часа).

Лекция 15.

Компьютерные преступления, инциденты ИБ и их расследование. Форензика (2 часа).

Лекция 16.

Основные стандарты и спецификации в области информационной безопасности. Цифровая гигиена (2 часа).

4.1.2.2. Перечень практических занятий

Семестр 4

Раздел 1. Основы информационной безопасности

Практическое занятие 1

Реализация дискреционной модели политики безопасности (2 часа).

Практическое занятие 2

Простые симметричные криптосистемы (2 часа).

Практическое занятие 3

Простые симметричные криптосистемы (2 часа).

Практическое занятие 4

Алгоритм XOR. Одноразовый блокнот (2 часа).

Практическое занятие 5

Протокол Фиата-Шамира (2 часа).

Практическое занятие 6

Защита от копирования (2 часа).

Практическое занятие 7

Контроль целостности (2 часа).

Практическое занятие 8

Хэш-функции (2 часа).

Методические указания по практическим работам приведены в электронном курсе "Основы информационной безопасности" Информационно-образовательного портала МИ ВлГУ и доступны по ссылке - https://www.mivlgu.ru/iop/course/view.php?id=1217&topic=0#section-6

4.1.2.3. Перечень лабораторных работ

Не планируется.

4.1.2.4. Перечень учебно-методического обеспечения для самостоятельной работы

Методические указания для самостоятельной работы размещены на информационно-образовательном портале института по ссылке https://www.mivlgu.ru/iop/course/view.php?id=5058.

Для самостоятельной работы также используются издания из списка приведенной ниже основной и дополнительной литературы.

Перечень тем, вынесенных на самостоятельное изучение:

1. Объединение блочных шифров.
2. Криптосистемы на эллиптических кривых.
3. Совершенные шифры.
4. Близкие к совершенным шифры.
5. Экстремальные шифры.
6. Аппаратные средства защиты.
7. Программные и аппаратные средства сетевой защиты в различных операционных системах.
8. Протоколы защищенной передачи информации в сети.
9. Корпоративные системы обеспечения информационной безопасности.

4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В процессе изучения дисциплины применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). Задачи решаются синхронно со студентами с пояснением шагов решения.

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

Фонды оценочных средств приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины Основы информационной безопасности

7.1. Основная учебно-методическая литература по дисциплине

1. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 c. — ISBN 978-5-4497-0863-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/101992.html. — Режим доступа: для авторизир. пользователей - https://www.iprbookshop.ru/101992.html

2. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие - Санкт-Петербург: СПб: Университет ИТМО, 2015, 2015. - 93 с. - http://books.ifmo.ru/file/pdf/1763.pdf

3. Маркина Т.А. Основные механизмы защиты в ОС MS Windows. Методические рекомендации по выполнению лабораторных работ. Учебно-методическое пособие - Санкт-Петербург: СПб: Университет ИТМО, 2015, 2015. - 48 с. - http://books.ifmo.ru/file/pdf/1766.pdf

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Камышев, Э.Н. Информационная безопасность и защита информации: Учебное пособие. - Томск: ТПУ, 2009. - 95 с. - http://window.edu.ru/resource/033/75033/files/InfoBesop.pdf

2. Ожиганов А.А. Криптографические системы с секретным и открытым ключом: учебное пособие - Санкт-Петербург: СПб.: Университет ИТМО, 2015. - 64 с. - 100 экз. - http://books.ifmo.ru/file/pdf/1730.pdf

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

1) Информационно-поисковая система Консультант Плюс (http://www.consultant.ru)

2) Информационный портал Совета Безопасности Российской Федерации (http://www.scrf.gov.ru/documents/6/)

3) Информационно-аналитический портал ISO27000.RU / ЗАЩИТА-ИНФОРМАЦИИ.SU (http://iso27000.ru)

4) Каталог решений и услуг по Информационной Безопасности (http://www.ru-ib.ru)

Программное обеспечение:

LibreOffice (Mozilla Public License v2.0)

Microsoft Windows 10 Professional (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Microsoft Visual Studio (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

iprbookshop.ru
books.ifmo.ru
window.edu.ru
consultant.ru
scrf.gov.ru
iso27000.ru
ru-ib.ru
mivlgu.ru/iop

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лаборатория программно-аппаратных средств защиты информации

Программно-аппаратный комплекс RadioInspector WIFI 2 ; портативный RFID считыватель cipherLab 1862; компьютер для проведения мультимедиалекций Raspberry; персональный компьютер Mini PC Android MK808 B; ПК CPU-Intel Core i5-4460 BOX - 12 шт.; экран DRAPPER Apex STAR; видеопроектор SANYO PDG-DSU20; коммутатор. Доступ к сети Интернет.

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями.

На практических занятиях пройденный теоретический материал подкрепляется решением задач по основным темам дисциплины. Занятия проводятся в компьютерном классе, используя специальное программное обеспечение. Каждой подгруппе обучающихся преподаватель выдает задачу, связанную с разработкой и программной реализацией алгоритмов обработки информации. В конце занятия обучающие демонстрируют полученные результаты преподавателю и при необходимости делают работу над ошибками.

Выполнение самостоятельной работы студентом основано на ознакомлении с материалами, расширяющими знания по темам, вынесенным на СРС, в источниках литературы и интернет ресурсах, рекомендованных преподавателем.

Форма заключительного контроля при промежуточной аттестации – экзамен. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *10.03.01 Информационная безопасность* и профилю подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*
Рабочую программу составил *к.т.н., доцент Астафьев А.В.*_____
Рецензент(ы) *Директор обособленного подразделения ООО "Ред Софт Центр" Гуреев А. П.* _____
(Подпись)

Программа рассмотрена и одобрена на заседании кафедры *ФПМ* протокол №_____ от _____2020 года.
Заведующий кафедрой *ФПМ* _____*Орлов А.А.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета

протокол №_____ от _____2020 года.
Председатель комиссии _____ _____ _____
(Подпись) (Ф.И.О.)

Программа переутверждена:
на_____учебный год. Протокол заседания кафедры № _____от _____20__ года.
Заведующий кафедрой_____ _____ _____
(Подпись) (Ф.И.О.)

Программа переутверждена:
на_____учебный год. Протокол заседания кафедры № _____от _____20__ года.
Заведующий кафедрой_____ _____ _____
(Подпись) (Ф.И.О.)

Программа переутверждена:
на_____учебный год. Протокол заседания кафедры № _____от _____20__ года.
Заведующий кафедрой_____ _____ _____
(Подпись) (Ф.И.О.)

РЕЦЕНЗИЯ
на рабочую программу дисциплины
«Основы информационной безопасности»
по направлению подготовки 10.03.01 Информационная безопасность

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с требованиями федерального государственного образовательного стандарта по направлению подготовки 10.03.01 Информационная безопасность.

На изучение данного курса по учебному плану отводится 144 час. (4ЗЕТ). Формой итогового контроля изучения дисциплины является экзамен.

Цель дисциплины: дать понятие о существующих угрозах информационной безопасности и их источниках;

дать понятие о существующих средствах обеспечения информационной безопасности и тенденциях их развития.

научить анализировать имеющуюся ситуацию на предприятии;

научить определять круг мер и средств для повышения информационной безопасности.

Содержание занятий соответствуют требованиям образовательного стандарта. Имеется перечень вопросов для самостоятельной работы студентов, способствующий более глубокому изучению дисциплины.

Освоение дисциплины позволит студентам приобрести теоретические и практические знания, необходимые при решении задач в будущей практической деятельности.

Предлагаемые фонды оценочных средств для выявления уровня знаний и умений обучаемых полностью охватывает содержание курса и соответствуют ФГОС.

Перечень учебно-методической литературы достаточен для изучения дисциплины. Имеются ссылки на электронно-библиотечные системы.

Рабочая программа дисциплины «Основы информационной безопасности» рекомендуется для использования в учебном процессе по направлению подготовки 10.03.01 Информационная безопасность.

Рецензент:
Директор обособленного подразделения ООО "Ред Софт Центр" — Гуреев А. П.

16.06.2020 г.