АТПЗ/Так/РАСЧ -51.В.ДВ.5.2 - 05/04/2019

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
Нижегородский государственный технический университет им. Р.Е. Алексеева

Дзержинский политехнический институт (филиал)

Кафедра «Автоматизация, энергетика, математика и информационные системы»

УТВЕРЖДАЮ:
Директор института
_____ О.А Казанцев
«_05__» _____04_____2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации и информационная безопасность

наименование дисциплины

Направление подготовки

15.03.04 Автоматизация технологических процессов и производств

код и название направления

Направленность (профиль)

Разработка автоматизированных систем управления

Уровень образования

бакалавриат

Форма обучения

заочная

(очная, очно-заочная, заочная)

Дзержинск, 2019

Составители рабочей программы дисциплины:

Ст. преподаватель, к.т.н. _____ /__Наумова Е.Г.__/

(подпись) (Ф. И. О.)

Рабочая программа принята на заседании кафедры «Автоматизация, энергетика, математика и информационные системы»

«_04_»_____04_____ 2019__ г. Протокол заседания №___6_____

Заведующий кафедрой
«_05__»_____04_____2019_г. _____ /__Л.Ю. Вадова__/

(подпись) (Ф. И. О.)

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой
Автоматизация, энергетика, математика и информационные системы

(наименование кафедры)

_____ Л.Ю. Вадова

(подпись) (расшифровка подписи)

Декан факультета
Инженерно-технологический

(наименование)

_____ Г.В. Пастухова

(подпись) (расшифровка подписи)

Председатель методической комиссии по профилю подготовки
Автоматизация технологических процессов и производств

(наименование)

_____ Л.Ю. Вадова

(подпись) (расшифровка подписи)

Заместитель начальника отдела УМБО

_____ Е.Г. Воробьева-Дурнакина

(подпись) (расшифровка подписи)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СОДЕРЖАНИЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. Наименование дисциплины

Дисциплина Б1.В.ДВ.5.2 «Защита информации и информационная безопасность» - это дисциплина по направлению подготовки 15.03.04 «Автоматизация технологических процессов и производств», уровень образования - бакалавриат.

Профильным для данной дисциплины является вид профессиональной деятельности: научно-исследовательский.

Объектом профессиональной деятельности являются средства технологического оснащения автоматизации, управления, контроля, диагностирования, испытаний основного и вспомогательного производств, их математическое, программное, информационное и техническое обеспечение, а также методы, способы и средства их проектирования, изготовления, отладки, производственных испытаний, эксплуатации и научного исследования в различных отраслях национального хозяйства.

Данная дисциплина готовит к решению следующих задач профессиональной деятельности: изучение научно-технической информации, отечественного и зарубежного опыта по направлению исследований в области автоматизации технологических процессов и производств, автоматизированного управления жизненным циклом продукции, компьютерных систем управления ее качеством; участие в разработке алгоритмического и программного обеспечения средств и систем автоматизации и управления.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы (компетенции выпускников).

2.1. Дисциплина обеспечивает частичное формирование компетенции:

ОПК-2 – Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности;

ПК-18 – Способность аккумулировать научно-техническую информацию, отечественный и зарубежный опыт в области автоматизации технологических процессов и производств, автоматизированного управления жизненным циклом продукции, компьютерных систем управления ее качеством.

Признаки и уровни освоения компетенций приведены в табл. 2.1.

Таблица 2.1 – Признаки и уровни освоения компетенций

Код и содержание компетенций	Формулировка дисциплинарной части компетенции	Уровень формирования компетенций
ОПК-2 – Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	Способность решать задачи защиты информации на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	Продвинутый уровень формирования компетенции Формируется частично в составе дисциплин (табл.3.1) Итоговый контроль сформированности компетенции ОПК-2 осуществляется в ходе подготовки и защиты ВКР
ПК-18 – Способность аккумулировать научно-техническую информацию, отечественный и зарубежный опыт в области автоматизации технологических процессов и производств, автоматизированного управления жизненным циклом продукции, компьютерных систем управления ее качеством	Способность аккумулировать научно-техническую информацию, отечественный и зарубежный опыт в области обеспечения информационной безопасности	Углублённый уровень формирования компетенции Формируется частично в составе дисциплин (табл.3.1) Итоговый контроль сформированности компетенции ПК-18 осуществляется в ходе подготовки и защиты ВКР

2.2. В результате изучения дисциплины бакалавр должен овладеть следующими знаниями, умениями и навыками в рамках формируемых компетенций (табл. 2.2):

Таблица 2.2 - Планируемые результаты обучения

Уровень освоения компетенции	Описание признаков проявления компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)		
		Знать	**Уметь**	**Владеть**
1. **Компетенция ОПК-2**				
углублённый	понимает и может объяснить полученные знания в области защиты информации и информационной безопасности	возможные угрозы безопасности информации, методы и средства защиты информации, методы разработки внутренней политики безопасности фирмы, программные и аппаратные средства, используемые для обеспечения безопасности информации	проводить анализ объекта защиты, проектировать, настраивать и эксплуатировать систему защиты информации	навыками работы в проектировании системы защиты, навыками работы с программными средствами, используемыми для обеспечения безопасности информации
2. **Компетенция ПК-18**				
начальный	понимает и может объяснить полученные знания в области защиты информации и информационной безопасности	основные требования к информационной безопасности; методы разработки внутренней политики безопасности организаций; методы передачи конфиденциальной информации по открытым каналам связи; методы защиты сетевой информации	разрабатывать политику безопасности организации; использовать современные информационные технологии, технику, прикладные программные средства при решении задач профессиональной деятельности	навыками в разработке политики безопасности предприятия, представлением об особенностях построения систем защиты на разных уровнях

При наличии лиц с ограниченными возможностями здоровья устанавливается особый порядок освоения дисциплины, предусматривающий возможность достижения ими планируемых результатов обучения с учетом состояния здоровья и имеющихся заболеваний.

3. Место дисциплины в структуре образовательной программы бакалавриата

3.1. Дисциплина реализуется в рамках дисциплин по выбору вариативной части Блока 1 «Дисциплины (модули)» (Б1.В.ДВ.5.2).

3.2 Дисциплина (модуль) изучается на 4 курсе в 8-ом семестре.

3.3. Требования к входным знаниям, умениям и владениям студентов:

Для освоения дисциплины Б1.В.ДВ.5.2 «Защита информации и информационная безопасность» студент должен:

- *знать* основные понятия и определения теории информации, способы представления, хранения и передачи информации*;*
- *уметь* работать в качестве пользователя персонального компьютера, работать с операционными системами, уметь работать в сетях*;*
- *владеть навыками* представления информации в информационных системах.

Этапы формирования компетенций и ожидаемые результаты обучения, определяющие уровень сформированности компетенций, указаны в табл. 3.1, 3.2.

Таблица 3.1 – Дисциплины, участвующие в формировании компетенций ОПК-2, ПК-18 вместе с дисциплиной Б1.В.ДВ.5.2 «Защита информации и информационная безопасность»

Код компетенции	Названия учебных дисциплин, модулей, практик, участвующих в формировании компетенции вместе с данной дисциплиной	Курсы / семестры обучения									
		1 курс		2 курс		3 курс		4 курс		5 курс	
		семестр		семестр		семестр		семестр		семестр	
		1	2	3	4	5	6	7	8	9	10
ОПК-2	Информатика	x	x								
	Вычислительные машины, системы и сети						x				
	Метрология, стандартизация и сертификация						x				
	Практика по получению первичных профессиональных умений и навыков, в т.ч. первичных умений и навыков научно-исследовательской деятельности						x				
	Системы технической безопасности								x		
	Защита информации и информационная безопасность								x		
	Практика по получению профессиональных умений и опыта профессиональной деятельности								x		
	Технические средства автоматизации									x	
	Технические измерения и приборы									x	
	Подготовка и защита ВКР										x
ПК-18	Системы технической безопасности								x		
	Защита информации и информационная безопасность								x		
	Научно-исследовательская работа								x		
	Проектирование автоматизированных систем									x	
	Автоматизация управления жизненным циклом продукции										x
	Управление качеством										x
	Преддипломная практика										x
	Подготовка и защита ВКР										x

Таблица 3.2 – Этапы формирования компетенций ОПК-2, ПК-18 вместе с дисциплиной Б1.В.ДВ.5.2 «Защита информации и информационная безопасность»

Код	Наименование компетенции (дисциплинарной части компетенции)	Наименования дисциплин		
		Начальный этап (пороговый уровень)	Основной этап (углубленный уровень)	Завершающий этап (продвинутый уровень)
ОПК-2	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	1. Информатика	1. Вычислительные машины, системы и сети 2. Метрология, стандартизация и сертификация 3. Практика по получению первичных профессиональных умений и навыков, в т.ч. первичных умений и навыков научно-исследовательской деятельности 4. Системы технической безопасности 5. Защита информации и информационная безопасность	1. Технические измерения и приборы 2. Технические средства автоматизации 3. Подготовка и защита ВКР

			6. Практика по получению профессиональных умений и опыта профессиональной деятельности	
ПК-18	Способность аккумулировать научно-техническую информацию, отечественный и зарубежный опыт в области автоматизации технологических процессов и производств, автоматизированного управления жизненным циклом продукции, компьютерных систем управления ее качеством	1. Системы технической безопасности 2. Защита информации и информационная безопасность 3. Научно-исследовательская работа	1. Проектирование автоматизированных систем	1. Автоматизация управления жизненным циклом продукции 2. Управление качеством 3. Преддипломная практика 4. Подготовка и защита ВКР

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Объем дисциплины (общая трудоемкость) составляет 4 зачетных единиц (з.е), в часах это 144 академических часов, в том числе контактная работа обучающихся с преподавателем 18 часов, самостоятельная работа обучающихся 122 часов.

В табл. 4.1 представлена структура дисциплины.

Таблица 4.1- Структура дисциплины

Вид учебной работы	**Всего часов**	**Семестр**
		8
1. Контактная работа обучающихся с преподавателем (по видам учебных занятий) **(всего),** в том числе:	**18**	**18**
1.1. Аудиторные занятия (всего), в том числе:	**14**	**14**
- лекции (Л)	**6**	**6**
- лабораторные работы (ЛР)	**8**	**8**
- практические занятия (ПЗ)		
- практикумы (П)		
1.2. Внеаудиторные занятия (всего), в том числе:	**4**	**4**
- групповые консультации по дисциплине	**4**	**4**
- групповые консультации по промежуточной аттестации (экзамен)		
- индивидуальная работа преподавателя с обучающимся: - по проектированию: проект (работа) - по выполнению РГР - по выполнению КР - по составлению реферата, доклада, эссе		
2. Самостоятельная работа студента (СРС) **(всего)**	**122**	**122**
Вид промежуточной аттестации (зачёт с оценкой)	**Зачёт с оценкой, 4**	**Зачёт с оценкой, 4**
Общая трудоемкость, часы/зачетные единицы	**144/4**	**144/4**

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий

5.1. Разделы дисциплин и виды занятий

Распределение учебной нагрузки по разделам дисциплины приведено в табл. 5.1.

Тематическое содержание разделов дисциплины с перечислением содержащихся в них дидактических единиц приведено в табл. 5.2.

Темы лабораторных занятий приведены в табл. 5.4, виды самостоятельной работы – в табл. 5.5.

Таблица 5.1 - Распределение учебной нагрузки по разделам дисциплины

Номер раздела	Наименование раздела дисциплины	Виды занятий и их трудоемкость, часы						
		Всего часов (без экзамена)	Лекции	Практические занятия	Лабораторные работы	Внеаудиторная контактная работа	СРС	Формируемые компетенции
1	Общие вопросы информационной безопасности	21	0,5	–	0,5	–	20	ОПК-2 ПК-18
2	Правовые средства защиты	21	0,5	–	0,5	–	20	ОПК-2 ПК-18
3	Криптографическая защита информации	25	1	–	4	–	20	ОПК-2 ПК-18
4	Техническая защита информации	36	2	–	2	–	32	ОПК-2 ПК-18
5	Физическая защита информации	33	2	–	1	–	30	ОПК-2 ПК-18
6	Групповые консультации по дисциплине	4	–	–	–	4	–	ОПК-2 ПК-18
	Итого	**144**	**6**	–	**8**	**4**	**122**	

Таблица 5.2 - Содержание разделов дисциплины (по лекциям)

№ разде-л	Наименование раздела	Код компетенции	Содержание темы (наименование темы, перечисление дидактических единиц)	Трудоемкость (час.)	Технология оценивания
1	Общие вопросы информационной безопасности	ОПК-2 ПК-18	Тема 1.1. Основные понятия	0,2	Участие в групповых обсуждениях
			Тема 1.2. Угрозы	0,2	
			Тема 1.3. Классификация средств защиты	0,1	
2	Правовые средства защиты	ОПК-2 ПК-18	Тема 2.1. Отечественное правовое обеспечение	0,3	Участие в групповых обсуждениях
			Тема 2.2. Зарубежная и международная политика безопасности	0,2	
3	Криптографическая защита информации	ОПК-2 ПК-18	Тема 3.1. Криптография, стеганография	0,2	Участие в групповых обсуждениях. Выполнение индивидуальных заданий
			Тема 3.2. Симметричные и асимметричные алгоритмы	0,4	
			Тема 3.3. Хэширование	0,2	
			Тема 3.4. Электронная подпись	0,2	
4	Техническая защита информации	ОПК-2 ПК-18	Тема 4.1. Защита ВС	0,5	Участие в групповых обсуждениях. Выполнение индивидуальных заданий
			Тема 4.2. Защита ИС	0,5	
			Тема 4.3. Защита данных	0,5	
			Тема 4.4. Защита в сети	0,5	
5	Физическая защита информации	ОПК-2 ПК-18	Тема 5.1. Организационные средства защиты	1	Участие в групповых обсуждениях. Выполнение индивидуальных заданий
			Тема 5.2. Программно-технические средства защиты	1	
			итого	6	

Таблица 5.3 – Темы практических занятий

№ раздела	Наименование раздела	Код компетенции	Темы практических занятий	Трудоемкость (час.)	Технология оценивания
			Не предусмотрены		
			итого		

Таблица 5.4 - Темы лабораторных работ

№ раздела	Наименование раздела	Код компетенции	Темы лабораторных работ	Трудоемкость (час.)	Технология оценивания
3	Криптографическая защита информации	ОПК-2 ПК-18	Криптоанализ	1	Выполнение индивидуальных заданий
3	Криптографическая защита информации	ОПК-2 ПК-18	Создание программы шифрования, дешифрования	3	Выполнение индивидуальных заданий
4	Техническая защита информации	ОПК-2 ПК-18	Управление доступом	2	Выполнение индивидуальных заданий
1	Общие вопросы информационной безопасности	ОПК-2 ПК-18	Анализ объекта защиты	0,5	Выполнение индивидуальных заданий
2	Правовые средства защиты			0,5	
5	Физическая защита информации			1	
			итого	8	

Таблица 5.5 - Самостоятельная работа студентов

№ раздела	Наименование темы	Код Компетенции	Виды самостоятельной работы (детализация видов самостоятельной работы по каждому разделу)	Трудоемкость (час.)	Технология оценивания
1	Тема 1.1. Основные понятия	ОПК-2 ПК-18	- изучение основной и дополнительной литературы, рекомендованной по курсу - подготовка к ответу на вопросы по теме	5 5	Участие в групповых обсуждениях
	Тема 1.2. Угрозы	ОПК-2 ПК-18	- изучение основной и дополнительной литературы, рекомендованной по курсу - подготовка к ответу на вопросы по теме	5 5	
2	Тема 2.1. Отечественное правовое обеспечение Тема 2.2. Зарубежная и международная политика безопасности	ОПК-2 ПК-18	- изучение основной и дополнительной литературы, рекомендованной по курсу - подготовка к ответу на вопросы по теме	10 10	Участие в групповых обсуждениях
3	Тема 3.4. Электронная подпись	ОПК-2 ПК-18	- изучение основной и дополнительной литературы, рекомендованной по курсу - подготовка к ответу на вопросы по теме	10 10	Участие в групповых обсуждениях
4	Тема 4.3. Защита данных	ОПК-2 ПК-18	- изучение основной и дополнительной литературы, рекомендованной по курсу - подготовка к ответу на вопросы по теме	10 5	Участие в групповых обсуждениях
	Тема 4.4. Защита в сети	ОПК-2 ПК-18	- изучение основной и дополнительной литературы, рекомендованной по курсу - подготовка к ответу на вопросы по теме	12 5	Участие в групповых обсуждениях
5	Тема 5.2. Программно-технические средства защиты	ОПК-2 ПК-18	- изучение основной и дополнительной литературы, рекомендованной по курсу - подготовка к ответу на вопросы по теме	20 10	Участие в групповых обсуждениях
			итого:	**158**	

5.2. Примерная тематика рефератов (докладов, эссе)

Не предусмотрено

5.3. Примерная тематика курсовых проектов (работ)

Не предусмотрено учебным планом

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Темы и содержание учебных занятий в форме самостоятельной работы представлены в табл. 6.1.

Таблица 6.1. - Темы и содержание учебных занятий в форме самостоятельной работы

Раздел	Тема	Содержание занятий	Кол-во час
1.	Темы 1.1 – 1.3	1. Чтение основного учебника: Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова. — Ростов-на-Дону : ЮФУ, 2016. — 74 с. — ISBN 978-5-9275-2364-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114462 - разделы 1.1, 1.2, 2 2. Чтение дополнительного учебника: Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 - разделы 1.1, 1.2 3. Работа с контрольными вопросами	**20**
2.	Темы 2.1 – 2.2	1. Чтение основного учебника: Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова. — Ростов-на-Дону : ЮФУ, 2016. — 74 с. — ISBN 978-5-9275-2364-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114462 - раздел 3 2. Чтение дополнительного учебника: Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 - раздел 3 3. Работа с контрольными вопросами	**20**
3.	Темы3.1-3.4	1. Чтение основного учебника: Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова. — Ростов-на-Дону : ЮФУ, 2016. — 74 с. — ISBN 978-5-9275-2364-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114462 - раздел 9.1, 9.2, 9.5 2. Чтение дополнительного учебника: Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 - раздел 6 3. Работа с контрольными вопросами	**20**
4.	Тема 4.1-4.4	1. Чтение основного учебника: Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова. — Ростов-на-Дону : ЮФУ, 2016. — 74 с. — ISBN 978-5-9275-2364-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114462 - раздел 7, 10, 11 2. Чтение дополнительного учебника: Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 - раздел 7, 10. 11 3. Работа с контрольными вопросами	**28**

5	Тема 5.1-5.2	1. Чтение основного учебника: Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова. — Ростов-на-Дону : ЮФУ, 2016. — 74 с. — ISBN 978-5-9275-2364-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114462 - раздел 5 2. Чтение дополнительного учебника: Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 - раздел 2 Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 2-е изд. — Москва : ИНТУИТ, 2016. — 266 с. — ISBN 978-5-94774-821-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100295 - раздел 6 3. Работа с контрольными вопросами	**20**

6.2. Список литературы для самостоятельной работы

Список литературы для самостоятельной работы представлен в табл. 6.2.

Таблица 6.2 - Список литературы для самостоятельной работы

№ пп	Наименование источника
1	Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова. — Ростов-на-Дону : ЮФУ, 2016. — 74 с. — ISBN 978-5-9275-2364-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114462
2	Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 (дата обращения: 01.04.2019).
3	Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 2-е изд. — Москва : ИНТУИТ, 2016. — 266 с. — ISBN 978-5-94774-821-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100295 (дата обращения: 01.04.2019).

6.3 Методическое сопровождение самостоятельной работы

Проведение самостоятельной работы по дисциплине регламентируется:

1. Методическими рекомендациями по организации и планированию самостоятельной работы студентов по дисциплине. Приняты Учебно-методическим советом НГТУ им. Р.Е. Алексеева, протокол № 2 от 22 апреля 2013 г. Электронный адрес: http://www.nntu.ru/RUS/otd_sl/ymy/metod_dokym_obraz/met_rekom_organiz_samoct_rab.pdf?20

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Этапы формирования компетенций (с указанием дисциплин, формирующих компетенции совместно с дисциплиной Б1.В.ДВ.5.2 «Защита информации и информационная безопасность») отражены в разделе 3 (таблицы 3.1 и 3.2)

Зная этапы формирования компетенций и место дисциплины Б1.В.ДВ.1.1 «Прикладное программное обеспечение» в этой ценностной цепочке создаем систему оценки уровней сформированности компетенций и результатов обучения по данной дисциплине. Для этого планируемые результаты обучения (знать, уметь и владеть) оцениваем, применив определенные критерии оценки, для чего формируем шкалу и процедуры оценивания (табл. 7.1).

Для каждого результата обучения выделим 4 критерия, соответствующих степени сформированности данной компетенции (или ее части).

Эталонный планируемый результат соответствует критерию 4 (точность, правильность, соответствие).

Критерии 1-3 – показатели «отклонений от эталона».

Критерий 2 – минимальный приемлемый уровень сформированности компетенции (или ее части).

Таблица 7.1. – Шкалы оценивания на этапе промежуточной аттестации по дисциплине

№ пп	Наименование этапа	Технология оценивания	Шкала (уровень) оценивания (j – уровень оценивания)				Этапы контроля
			ниже порогового К1	Пороговый К2	Углубленный К3	Продвинутый К4	
1	Усвоение материала дисциплины	Знаниевая компонента	Отсутствие усвоения	Не полное усвоение	Хорошее усвоение	Отличное усвоение	Зачёт с оценкой
		Деятельностная компонента (Задачи, задания)	Отсутствие решения	Решение с ошибками	Правильное решение с отдельными недочетами	Правильное решение без ошибок	

Критерии для определения уровня сформированности компетенции в рамках дисциплины при промежуточной аттестации зачет с оценкой:

Знаниевый компонент включает в себя планирование знаний на следующих уровнях:

- ✓ уровень знакомства с теоретическими основами-$З_1$,
- ✓ уровень воспроизведения -$З_2$,
- ✓ уровень извлечения новых знаний- $З_3$.

Деятельностный компонент (умения и навыки) планируется на следующих уровнях:

- ✓ умение решать типовые задачи с выбором известного метода, способа -$У_1$,
- ✓ умение решать задачи путем комбинации известных методов, способов, -$У_2$
- ✓ умение решать нестандартные задачи -$У_3$.

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формировании, описание шкал оценивания (табл. 7.2)

Таблица 7.2 – Показатели достижений заданного уровня освоения компетенций в зависимости от этапа формирования

Планируемые результаты обучения по дисциплине	**Критерии оценивания результатов обучения (уровень усвоения)**				**Процедуры оценивания**
	1. Отсутствие усвоения	**2. Неполное усвоение**	**3. Хорошее усвоение**	**4. Отличное усвоение**	
Знать ОПК-2					
$З_1$ - уровень знакомства с теоретическими основами	Не знает основные понятия дисциплины, возможные угрозы безопасности информации	Показывает неуверенные знания основных понятий дисциплины	Знает основные понятия дисциплины, возможные угрозы безопасности информации	Уверенно оперирует основными понятиями дисциплины, знает возможные угрозы безопасности информации	Выполнение индивидуального задания по лабораторной работе, участие в групповых обсуждениях
$З_2$ - уровень воспроизведения	Не знает методы и средства защиты информации	Показывает неуверенные знания средств защиты	Знает основы средства защиты, но может допускать ошибки при выборе методов защиты	Уверенно ориентируется в методах и средствах защиты информации	
$З_3$ - уровень извлечения новых знаний	Не знаком с методами разработки внутренней политики безопасности фирмы	Допускает ошибки при выборе программных и аппаратных средств, используемые для обеспечения безопасности информации	Способен определять необходимое ПО для разработки внутренней политики безопасности фирмы	Может аргументировано определять необходимый набор и состав средств для обеспечения информационной безопасности	

Планируемые результаты обучения по дисциплине	Критерии оценивания результатов обучения (уровень усвоения)				Процедуры оценивания
	1. Отсутствие усвоения	2. Неполное усвоение	3. Хорошее усвоение	4. Отличное усвоение	
Знать ПК-18					
З$_1$ - уровень знакомства с теоретическими основами	Не знает основные требования к информационной безопасности	Показывает неуверенные знания требований к информационной безопасности	Знает основные требования к информационной безопасности,	Знает основные требования к информационной безопасности и может соотнести их с объектами защиты	Выполнение индивидуального задания по лабораторной работе, участие в групповых обсуждениях
З$_2$ - уровень воспроизведения	Не знает методы передачи конфиденциальной информации по открытым каналам связи; методы защиты сетевой информации	Имеет общее представление о методах защиты сетевой информации	Знает методы защиты сетевой информации	Знает методы передачи конфиденциальной информации по открытым каналам связи; методы защиты сетевой информации	
З$_3$ - уровень извлечения новых знаний	Не знаком с методами разработки внутренней политики безопасности фирмы	Допускает ошибки при выборе программных и аппаратных средств, используемые для обеспечения безопасности информации	Способен определять необходимое ПО для разработки внутренней политики безопасности фирмы	Может аргументировано определять необходимый набор и состав средств для обеспечения информационной безопасности	
Уметь ОПК-2					
У$_1$ – умение решать типовые задачи с выбором известного метода, способа	Не может выполнить анализ объекта защиты	Испытывает затруднения при анализе объекта защиты	Способен выполнить общий анализ объекта защиты	Способен выполнить подробный анализ объекта защиты	Выполнение индивидуального задания по лабораторной работе, участие в групповых обсуждениях
У$_2$ – умение решать задачи путем комбинации известных методов, способов	Не может подобрать средства защиты	Может определить только направление защиты	Способен определять направления и средства защиты объекта	Аргументировано ведёт определение методов и средств защиты	
У$_3$ – умение решать нестандартные задачи	Не может настраивать и эксплуатировать систему защиты информации	Не уверенно эксплуатирует систему защиты информации	Способен эксплуатировать систему защиты информации	Способен настраивать и эксплуатировать систему защиты информации	
Уметь ПК-18					
У$_1$ – умение решать типовые задачи с выбором известного метода, способа	Не знаком с методами разработки внутренней политики безопасности организации	Имеет общее представление о внутренней политики безопасности организации	Способен формулировать общие положения политики безопасности организации	Способен разрабатывать политику безопасности организации	Выполнение индивидуального задания по лабораторной работе, участие в групповых обсуждениях
У$_2$ – умение решать задачи путем комбинации известных методов, способов	Не может подобрать средства защиты	Может определить только направление защиты	Способен определять направления и средства защиты объекта	Аргументировано ведёт определение методов и средств защиты	

Планируемые результаты обучения по дисциплине	Критерии оценивания результатов обучения (уровень усвоения)				Процедуры оценивания
	1. Отсутствие усвоения	2. Неполное усвоение	3. Хорошее усвоение	4. Отличное усвоение	
$У_3$ – умение решать нестандартные задачи	Не может использовать современные средства при решении задач обеспечения безопасности	Испытывает затруднения при использовании программных для решения профессиональных задач	Способен применять современные прикладные программные средства для решения задач обеспечения информации	Умеет применять современные информационные технологии, технику, прикладные программные средства	

7.3. Материалы для текущей аттестации

Шкалы оценивания этапа текущей аттестации приведены в табл. 7.3.

Таблица 7.3 – Этап текущей аттестации по дисциплине Б1.В.ДВ.5.2 «Защита информации и информационная безопасность»

Вид оценивания аудиторных занятий	Технология оценивания		Шкала (уровень) оценивания на этапе текущего контроля			
			1.Отсутствие усвоения	2.Неполное усвоение	3.Хорошее усвоение	4.Отличное усвоение
Работа на лекциях	Участие в групповых обсуждениях	***1***	отсутствие участия **1.1**	единичное высказывание **1.2**	активное участие в обсуждении **1.3**	Высказывание суждений с обоснованием точки зрения **1.4**
	Выполнение тестов	***2***	выполнение менее 55% **2.1**	выполнение выше 55% **2.2**	выполнение более 70% **2.3**	выполнение более 86 % **2.4**
Работа на лабораторных занятиях	Выполнение индивидуальных заданий на лабораторных работах, составление отчета по лабораторным работа	***3***	неправильное выполнение **3.1**	выполнение с ошибками **3.2**	правильное выполнение без ошибок с отдельными замечаниями **3.3**	правильное выполнение без ошибок **3.4**
		Оценка:	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

Критериальная оценка:

Пороговый уровень	оценка «удовлетворительно»	**1.2 + 2.2+3.2** или **1.1+2.2+3.2**
Углубленный уровень	оценка «хорошо»	**1.3 + 2.3 +3.3** или **1.2+2.3+3.3**
Продвинутый уровень	оценка «отлично»	**1.4 + 2.4 +3.4** или **1.3+2.4+3.4**

7.4 Материалы для промежуточной аттестации

Формой промежуточной аттестации по дисциплине является экзамен

Шкала оценивания этапа промежуточной аттестации (*экзамен)* приведена в табл. 7.4.

Таблица 7.4. – Этап промежуточной аттестации по дисциплине

Наименование этапа оценивания	Технология оценивания		Шкала (уровень) оценивания на этапе промежуточной аттестации				
			1.Отсутствие усвоения	2.Не полное усвоение	3.Хорошее усвоение	4.Отличное усвоение	Этапы контроля
Выполнение лабораторных работ (ЛР)	Защита отчёта		Невыполнение ЛР	Защита неуверенная	Хорошая защита с небольшими неточностями	Уверенная защита	Защита работы
Отработка пропущенных занятий	Ответ на контрольные вопросы		Незнание материала	неполное усвоение	хорошее усвоение	отличное усвоение	Опрос на лекции
Усвоение материала дисциплины	Знаниевая компонента	**З**	Невыполнение заданий, ЛР **З1**	неполное усвоение **З2**	хорошее усвоение **З3**	отличное усвоение **З4**	**Экзамен**
	Деятельностная (задания)	**У**	отсутствие отчета по лабораторным работам, ответов на вопросы **У1**	выполнение с ошибками **У2**	правильное выполнение с отдельными замечаниями **У3**	верное выполнение без ошибок **У4**	
Оценка:			Неудовлетворительно	Удовлетворительно	хорошо	отлично	

Критериальная оценка

Пороговый уровень	оценка «удовлетворительно»	**З2 + У2** или **З3 + У2**
Углубленный уровень	оценка «хорошо»	**З3 + У3** или **З4 + У3 или З2+У4**
Продвинутый уровень	оценка «отлично»	**З4+ У4 или З3+У4**

Оценки "отлично" заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, умение свободно выполнять практические задания, предусмотренные программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой.

Оценки "хорошо" заслуживает обучающийся, обнаруживший полное знание учебного материала, успешно выполняющий предусмотренные в программе практические задания, усвоивший основную литературу, рекомендованную в программе. Оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

Оценки "удовлетворительно" заслуживает обучающийся, обнаруживший знания основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющийся с выполнением практических заданий, предусмотренных программой, знакомых с основной литературой, рекомендованной программой. Оценка "удовлетворительно" выставляется обучающимся, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.

Оценка "неудовлетворительно" выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой практических заданий. Оценка "неудовлетворительно" ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании образовательного учреждения без дополнительных занятий по соответствующей дисциплине.

7.5. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной деятельности

7.5.1. Конкретная технология оценивания, оценочные средства

Конкретная технология оценивания, в зависимости от вида учебной работы, представлена в табл. 5.2 - 5.5, оценочные средства указаны в табл. 7.5.

Для выполнения процедур оценивания составлен паспорт оценочных средств (табл. 7.5)

Таблица 7.5 - Паспорт оценочных средств

№ п/п	Тематика для контроля	Код контролируемой компетенции (или ее части)	Количество тестовых заданий	Другие оценочные средства	
				вид	Количество
1	Тема 1.1. Тема 1.2. Тема 1.3.	ОПК-2 ПК-18	10	Контрольный вопрос	7
2	Тема 2.1. Тема 2.2	ОПК-2 ПК-18	10	Контрольный вопрос	4
3	Тема 3.1. Тема 3.2. Тема 3.3 Тема 3.4	ОПК-2 ПК-18	10	Отчёт по лабораторной работе Контрольный вопрос	2 7
4	Тема 4.1. Тема 4.2. Тема 4.3 Тема 4.4	ОПК-2 ПК-18	10	Отчёт по лабораторной работе Контрольный вопрос	1 24
5	Тема 5.1 Тема 5.2	ОПК-2 ПК-18	10	Отчёт по лабораторной работе Контрольный вопрос	1 4

7.5.2. Комплект оценочных материалов, предназначенных для оценивания уровня сформированности компетенций на определенных этапах обучения

7.5.2.1. Комплект оценочных материалов для текущей аттестации

Таблица 7.6 - Оценочные средства дисциплины для текущей аттестации

	Код формируемой компетенции	Вопросы (номера вопросов)	Задания (номера заданий)
1	ОПК-2	Раздел 1: вопросы 1 - 7 Раздел 2: вопросы 8 -11 Раздел 3: вопросы 12 - 18 Раздел 4: вопросы 19 - 42 Раздел 5: вопросы 43 - 46	Тестирование
2	ПК-18		

7.5.2.2. Критерии оценивания курсовой работы

Не предусмотрено учебным планом.

7.5.2.3. Комплект оценочных материалов для промежуточной аттестации

Таблица 7.7 - Оценочные средства дисциплины для промежуточной аттестации

	Код формируемой компетенции	Вопросы (номера вопросов)	Задания (номера заданий)
1	ОПК-2	Раздел 1: вопросы 1 - 7 Раздел 2: вопросы 8 -11 Раздел 3: вопросы 12 - 18 Раздел 4: вопросы 19 - 42 Раздел 5: вопросы 43 - 46	Тестирование
2	ПК-18		

Образцы оценочных средств

Тематика лабораторных работ приведена в табл. 5.4.

Перечень вопросов, необходимых для проведения текущего и промежуточного контроля

1. Основные понятия защиты информации и информационной безопасности
2. Модель безопасности информации
3. Классификация угроз безопасности компьютерных систем
4. Угрозы доступности
5. Угрозы конфиденциальности
6. Угрозы доступности
7. Основные направления защиты информации
8. Законодательство РФ в области информационной безопасности
9. Отечественные стандарты безопасности
10. Международные стандарты безопасности
11. Политика безопасности РФ
12. Криптографическая защита информации.
13. Симметричные криптосистемы.
14. Система шифрования с открытым ключом.
15. Гибридные технологии шифрования
16. Электронная цифровая подпись (ЭП). Формирование и получение сообщения с ЭП.
17. Хэш-функция. Хэширование
18. Электронная цифровая подпись. Системы сертификации.
19. Процедуры идентификации.
20. Классификация видов аутентификации
21. Методы аутентификации, использующие пароли и PIN-коды.
22. Методы аутентификации, основанные на владении предметом.
23. Биометрическая аутентификация пользователя.
24. Управление доступом.
25. Защита ОС
26. Резервное копирование данных, репликация.
27. Безопасное хранение данных.
28. Функции межсетевых экранов
29. Фильтрующие маршрутизаторы
30. Шлюзы сетевого и прикладного уровня.
31. Основные схемы сетевой защиты на брандмауэрах.
32. Проблемы безопасности межсетевых экранов
33. Формирование политики межсетевого взаимодействия
34. Основные понятия и функции виртуальных частных сетей

35. Построение виртуальных частных сетей. Среда передачи данных, оборудование удаленных объектов, протоколы VPN.
36. Организация VPN-канала. Инкапсуляция и туннелирование.
37. Основные варианты архитектуры VPN.
38. Компьютерные вирусы. Внешние признаки проявления деятельности вирусов
39. Классификация вирусов.
40. Жизненный цикл вирусов.
41. Методы обнаружения вирусов
42. Виды антивирусных программ
43. Организационные средства защиты
44. Формирование политики безопасности организации
45. Угрозы на инженерно-техническом уровне
46. Программно-технические средства защиты территории, помещений

Образцы тестов

1. Суть компрометации информации

– внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

– несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

– *внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений*

2. Основные угрозы доступности информации:

– непреднамеренные ошибки пользователей
– злонамеренное изменение данных
– хакерская атака
– *отказ программного и аппаратно обеспечения*
– перехват данных

3. К формам защиты информации не относится…

– *аналитическая*
– правовая
– организационно-техническая
– криптографическая

4. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …

– *обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации*
– реализацию права на доступ к информации
– соблюдение норм международного права в сфере информационной безопасности
– выявление нарушителей и привлечение их к ответственности
– разработку методов и усовершенствование средств информационной безопасности

5. Кто является основным ответственным за определение уровня классификации информации?

– Руководитель среднего звена
– Высшее руководство
– *Владелец*
– Пользователь

6. Основные угрозы доступности информации:

– отказ персонала в использовании нового ПО
– хакерская атака
– *разрушение или повреждение помещений*
– случайное изменение данных
– перехват данных

7. Утечка информации – это …

– несанкционированный процесс переноса информации от источника к злоумышленнику
– *процесс раскрытия секретной информации*
– процесс уничтожения информации
– непреднамеренная утрата носителя информации

8. К посторонним лицам-нарушителям информационной безопасности относится:

– персонал, обслуживающий технические средства;
– технический персонал, обслуживающий здание;
– сотрудники службы безопасности
– *представители конкурирующих организаций.*
– лица, нарушившие пропускной режим

9. Преднамеренная угроза безопасности информации

– *кража*
– наводнение
– повреждение кабеля, по которому идет передача, в связи с погодными условиями
– ошибка разработчика

10. К естественным угрозам безопасности информации

– кража
– *наводнение*
– преднамеренное повреждение кабеля, по которому идет передача
– ошибка разработчика

11. Что самое главное должно продумать руководство при классификации данных?

– Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
– *Необходимый уровень доступности, целостности и конфиденциальности*
– Оценить уровень риска и отменить контрмеры
– Управление доступом, которое должно защищать данные

12. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

– Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
– Когда риски не могут быть приняты во внимание по политическим соображениям
– Когда необходимые защитные меры слишком сложны
– *Когда стоимость контрмер превышает ценность актива и потенциальные потери*

13. Что не относится к технической радиоэлектронной разведке:

– *фотографическая*
– радиотехническая
– радиолокационная
– разведка ПЭМИН

14. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:

– Антивирус
– Замок
– *Брандма́уэр*
– Криптография
– Экспертная система

15. По какой причине удостоверяющий центр отзывает сертификат?
– если открытый ключ пользователя скомпрометирован
– если пользователь переходит на использование модели pem, которая использует сеть доверия
– *если закрытый ключ пользователя скомпрометирован*
– если пользователь переходит работать в другой офис

16. В чем состоит криптографическая задача обеспечения целостности?
– гарантирование невозможности внесения случайных ошибок в процессе передачи по каналам связи;
– *гарантирование невозможности несанкционированного изменения информации;*
– оба ответа верны.

17. Какие методы разрабатываются с целью обеспечения аутентификации?
– *методы подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия;*
– методы присвоения уникального идентификатора взаимодействующим сторонам и самой информации в процессе информационного взаимодействия;
– оба ответа верны.

18. Преимущества эвристического метода антивирусной проверки над методом сравнения с эталоном
– более надежный
– существенно менее требователен к ресурсам
– не требует регулярного обновления антивирусных баз
– *позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы*

19. Это защищает информационные активы предприятия от региональных рисков, связанных с чрезвычайными ситуациями (катастрофами):
– Инкрементное резервное копирование
– *Удаленная репликация*
– Полное резервное копирование
– Дупликация данных
– Локальная репликация

20. Запись определенных событий в журнал безопасности сервера называется:
– Идентификацией
– *Аудитом*
– Аутентификацией
– Администрированием
– Авторизацией

Пример экзаменационного билета (оценочные средства в полном объеме хранятся на кафедре «Автоматизация, транспортные и информационные системы»)

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Нижегородский государственный технический университет им. Р.Е.Алексеева» (НГТУ)
ДЗЕРЖИНСКИЙ ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ (ФИЛИАЛ) (ДПИ НГТУ)

Факультет **ИТ**
Кафедра _____
Дисциплина **«Информационная безопасность и защита информации»**

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Шифрование по таблице Вижинера. Ключ: Билет
2. лщффдпльеёй_рцэбжкмтъсюесйц_увнибны
3. пъщуфогрдгцнш_срчппюя_рты_зшйщтнюйфьюкбэсищуф

Зав. кафедрой **Экзаменатор**
«___»_____ 20__ г

7.6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Методические материалы представлены ниже:

- Положение о фонде оценочных средств для установления уровня сформированности компетенций обучающихся и выпускников на соответствие требованиям ФГОС ВО о от 5 декабря 2014 г. http://www.nntu.ru/RUS/otd_sl/ymy/norm_dokym_ngty/pologo_fonde_ocen_sredstv.pdf ;
- Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся НГТУ http://www.nntu.ru/RUS/otd_sl/ymy/norm_dokym___ngty/polog kontrol_yspev.pdf ;
- Методические указания по разработке курсовой работы по дисциплине http://www.nntu.ru/ineyl/osnovn_obrazovat_programm_ychebn_plan.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Карта обеспеченности дисциплины учебно-методической литературой

Код по учебному плану Б1.В.ДВ.5.2 Защита информации и информационная безопасность	К какой части Б1 относится дисциплина			
(*полное название дисциплины*)		обязательная		базовая часть цикла
	x	по выбору студента	x	вариативная часть цикла

15.03.04	Автоматизация технологических процессов и производств
(*код направления / специальности*)	(*полное название направления подготовки / специальности*)

АТПП	Уровень подготовки		Форма обучения	
(*аббревиатура направления / специальности*)		специалист		очная
	x	бакалавр	x	заочная
		магистр		очно-заочная

2019 год (*год утверждения учебного плана ОПОП*)

Семестр(ы) 8

Количество групп 1

Количество студентов 20

Составители программы
1) ФИО, институт, кафедра, телефон, e-mail
Наумова Е.Г., ДПИ НГТУ, кафедра АЭМИС, (8313) 34-47-30

СПИСОК ИЗДАНИЙ

№	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
	1 Основная литература	
1	Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова. — Ростов-на-Дону : ЮФУ, 2016. — 74 с. — ISBN 978-5-9275-2364-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114462 (дата обращения: 25.12.2019).	Эл. ресурс
2	Мельников, В.П. Информационная безопасность и защита информации: учебное пособие для вузов / В.П. Мельников. – М.: Академия, 2009	13
3	Информационная безопасность : учебное пособие / составители Е. Р. Кирколуп [и др.]. — Барнаул : АлтГПУ, 2017. — 316 с. — ISBN 978-5-88210-898-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112164 (дата обращения: 25.12.2019).	Эл. ресурс
	2 Дополнительная литература	
1	Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 (дата обращения: 25.12.2019).	Эл. ресурс
2	Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 2-е изд. — Москва : ИНТУИТ, 2016. — 266 с. — ISBN 978-5-94774-821-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100295 (дата обращения: 25.12.2019).	Эл. ресурс
3	Райкин, И.Л. Информационная безопасность и защита информации: учебное пособие для вузов / И.Л. Райкин. – Н.Новгород, 2011	5

4	Капранов, С.Н. Основы информационной безопасности : учебное пособие для вузов / С.Н. Капранов. - Н.Новгород, 2012.	Электронные текстовые данные
5	Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. — 2-е изд. — Москва : ФЛИНТА, 2015. — 182 с. — ISBN 978-5-9765-1904-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/62972 (дата обращения: 25.12.2019).	Электронные текстовые данные
6	**Криптографические методы шифрования данных**: метод. указания к лабораторным работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направлений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова, Н.И. Кечкина.– Дзержинск, 2018. - 24 с.	Эл. ресурс
7	**Парольная система защиты**: метод. указания к лабораторным работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направлений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова.– Дзержинск, 2018. - 8 с.	Эл. ресурс
8	**Анализ объекта защиты с целью обеспечения информационной безопасности**: метод. указания к лабораторным работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направлений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова.– Дзержинск, 2018. - 9 с.	Эл. ресурс

Основные данные об обеспеченности на

(*дата составления рабочей программы*)

основная литература [x] обеспечена [ ] не обеспечена

дополнительная литература [x] обеспечена [ ] не обеспечена

Данные об обеспеченности на _____

(*дата составления рабочей программы*)

основная литература [x] обеспечена [ ] не обеспечена

дополнительная литература [x] обеспечена [ ] не обеспечена

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

9.1. Ресурсы системы федеральных образовательных порталов:

1. Федеральный портал. Российское образование. http://www.edu.ru/
2. Российский образовательный портал. http://www.school.edu.ru/default.asp
3. Естественный научно-образовательный портал. http://www.en.edu.ru/

4. Федеральный правовой портал. Юридическая Россия. http://www.law.edu.ru/
5. Информационно-коммуникационные технологии в образовании. http://www.ict.edu.ru/
6. Федеральный образовательный портал. Социально-гуманитарное и политическое образование. http://www.humanities.edu.ru/
7. Российский портал открытого образования. http://www.openet.edu.ru/
8. Федеральный образовательный портал. Инженерное образование. http://www.techno.edu.ru/
9. Федеральный образовательный портал. Здоровье и образование. http://www.valeo.edu.ru/
10. Федеральный образовательный портал. Международное образование. http://www.international.edu.ru/
11. Федеральный образовательный портал. Непрерывная подготовка преподавателей. http://www.neo.edu.ru/wps/portal
12. Государственное учреждение «Центр исследований и статистики науки» ЦИСН. Официальный сайт: http://www.csrs.ru/about/default.htm.
13. Официальный сайт Федеральной службы государственной статистики РФ. Электронный ресурс: http://www.gks.ru.
- Зарубежные сетевые ресурсы
14. Архив научных журналов издательства http://iopscience.iop.org/и т.д.

9.2. Научно-техническая библиотека НГТУ им. Р.Е Алексеева http://www.nntu.ru/RUS/biblioteka/bibl.html

9.2.1. Электронные библиотечные системы

Электронно-библиотечная система ООО «Издательство Лань»:
Электронный каталог книг ***http://library.nntu.nnov.ru/***
Электронный каталог периодических изданий ***http://library.nntu.nnov.ru/***
Информационная система доступа к каталогам библиотек сферы образования и науки ЭКБСОН ***http://www.vlibrary.ru/***
Электронная библиотечная система «Университетская библиотека ONLINE НГТУ»
http://biblioclub.ru/index.php?page=main_ub
Электронная библиотека "Айбукс" **http://ibooks.ru/**
Реферативные наукометрические базы
*WebofScience****http://apps.webofknowledge.com/UA_GeneralSearch_input.do***
Scopus ***http://www.scopus.com/***
Реферативные журналы **http://www.nntu.ru/RUS/biblioteka/resyrs/ref_gyrnal_14.htm**
Госты Нормы, правила, стандарты и законодательство России
http://www.nntu.ru/RUS/biblioteka/resyrs/norma.htm
База данных гостов РосИнформ Вологодского ЦНТИ
http://www.nntu.ru/RUS/biblioteka/resyrs/baza_gost.htm
Бюллетени новых поступлений литературы в библиотеку
http://www.nntu.ru/RUS/biblioteka/index.htm
Ресурсы Интернет **http://www.nntu.ru/RUS/biblioteka/index.htm**
Персональные библиографические указатели ученых НГТУ
http://www.nntu.ru/RUS/biblioteka/bibl_ych.html
Доступ онлайн
Научные журналы НЭИКОН
ЭБС BOOK.ru.
База данных зарубежных диссертаций "ProQuestDissertation&ThesesGlobal"
ЭБС ZNANIUM.COM
ЭБС издательства "Лань"
ЭБС"Айбукс"
База данных Scopus издательства Elsevier; База данных WebofScienceCoreCollection
База данных Polpred.com Обзор СМИ
Электронная библиотека eLIBRARY.RU **http://www.nntu.ru/RUS/biblioteka/news.html**

9.3. Центр дистанционных образовательных технологий НГТУ им. Р.Е. Алексеева
Электронная библиотека http://cdot-nntu.ru/?page_id=312
Другое, что вы используете в качестве ресурсов сети «Интернет».

9.4 Научно-техническая библиотека ДПИ НГТУ http://http://www.dpi-ngtu.ru/

9.4.1. Электронные библиотечные системы

Электронно-библиотечная система ООО «Издательство Лань»: *http://e.lanbook.com/*
Электронно-библиотечная система издательства «ЮРАЙТ» http://biblio-online.at/home?1
Информационная система «Единое окно доступа к информационным ресурсам» http://window.edu. ru/catalog/
Госты Нормы, правила, стандарты и законодательство России **http://gost-rf.ru/**
Электронная библиотека eLIBRARY.RU http://elibrary.ru/defaultx.asp

9.4.2. Информационные ресурсы библиотеки ДПИ НГТУ

Электронный каталог - локально
Электронная библиотека - локально
База выполненных запросов - локально
Реферативные журналы Falcon 2.0 - локально
Справочно-поисковая система «КонсультантПлюс» - локально
Виртуальная выставка трудов преподавателей ДПИ НГТУ http: //www.dpi-ngtu.ru/aboutlibrary/1115—2015
Виртуальная выставка трудов преподавателей ДПИ НГТУ (Архив) http://www.dpi-ngtu.ru/aboutlibrary/862-virtvistavkaprepoddpingtu
Библиографические указатели преподавателей ДПИ НГТУ http://www.dpi-ngtu.ru/aboutlibrary/798-biblukazateliprepodovdpi
Бюллетень новых поступлений http://dpi-ngtu.ru/doc_for_load/novie_postuplenia.pdf
Периодические издания: «Периодические издания ДПИ НГТУ»; «Сводный список журналов»;
«Журналы в интернете» http://www.dpi-ngtu.ru/aboutlibrary/periodizdaniya
Виртуальные выставки http://www.dpi-ngtu.ru/aboutlibrary/virtvistavki
Научно-техническая библиотека НГТУ им. РЕ. Алексеева http://www.nntu.rii/RUS/biblioteka/bilt.html

9.4.3. Интернет-ресурсы http://www.dpi-ngtu.ru/aboutlibrary/resourses

Официальные сайты
Образовательные ресурсы
Библиотеки в интернете
Патенты и стандарты
Информационные центры
Энциклопедии, справочники, словари

9.4.4. Материалы в помощь студентам: http://www.dpi-ngtu.ru/aboutlibrary/resourses

10 Методические указания для обучающихся по освоению дисциплины

10.1. Методические рекомендации разработанные преподавателем:

— **Криптографические методы шифрования данных: метод. указания к лабораторным** работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направлений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологи-

ческих процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова, Н.И. Кечкина.– Дзержинск, 2018. - 24 с.

— Парольная система защиты: метод. указания к лабораторным работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направлений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова.– Дзержинск, 2018. - 8 с.

— Анализ объекта защиты с целью обеспечения информационной безопасности: метод. указания к лабораторным работам по дисциплине «Информационная безопасность и защита информации» для обучающихся направлений подготовки 09.03.02 «Информационные системы и технологии», 01.03.04 «Прикладная математика» всех форм обучения, по дисциплине «Защита информации и информационная безопасность» для обучающихся направления подготовки 15.03.04 «Автоматизация технологических процессов и производств» всех форм обучения, по дисциплине «Хранение и защита компьютерной информации» для обучающихся направления подготовки 15.04.04 «Автоматизация технологических процессов и производств» всех форм обучения / ДПИ НГТУ; сост.: Е.Г. Наумова.– Дзержинск, 2018. - 9 с.

10.2. Методические рекомендации НГТУ им. Р.Е.Алексеева:

— Методические рекомендации по организации аудиторной работы. Приняты Учебно-методическим советом НГТУ им. Р.Е. Алексеева, протокол № 2 от 22 апреля 2013 г. Электронный адрес: http://www.nntu.ru/RUS/otd_sl/ymy/metod_dokym_obraz/met_rekom_aydit_rab.pdf?20. Дата обращения 23.09.2015.

— Методические рекомендации по организации и планированию самостоятельной работы студентов по дисциплине. Приняты Учебно-методическим советом НГТУ им. Р.Е. Алексеева, протокол № 2 от 22 апреля 2013 г. Электронный адрес: http://www.nntu.ru/RUS/otd_sl /ymy/metod_dokym_obraz/met_rekom_organiz_samoct_rab.pdf?20. Учебное пособие «Проведение занятий с применением интерактивных форм и методов обучения», Ермакова Т.И., Ивашкин Е.Г., 2013 г. Электронный адрес: http://www.nntu.ru/RUS/otd_sl/ymy/metod_dokym_obraz/provedenie-zanyatij-s-primeneniem-interakt.pdf.

— Учебное пособие «Организация аудиторной работы в образовательных организациях высшего образования», Ивашкин Е.Г., Жукова Л.П., 2014 г. Электронный адрес: http://www.nntu.ru/RUS/otd_sl/ymy/metod_dokym_obraz/organizaciya-auditornoj-raboty.pdf.

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

Дисциплина, относится к группе дисциплин, в рамках которых предполагается использование информационных технологий как вспомогательного инструмента для выполнения задач, таких как:

- оформление отчетов по лабораторному занятию;

- использование электронной образовательной среды института;
- использование специализированного программного обеспечения;
- организация взаимодействия с обучающимися посредством электронной почты;
- использование видеоконференцсвязи;
- компьютерное тестирование.

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используется следующее программное обеспечение:

- Microsoft Office стандартный (Word, Power Point, Access, Excel); Adobe Reader; Microsoft Visual Studio,
- Портал электронного обучения ДПИ НГТУ.

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

Таблица 12.1 – Сведения о помещениях

№ ауд	Наименование аудитории	Площадь, $м^2$	Количество посадочных мест
1328	Аудитория лекционных занятий	74	60
1440	Вычислительный центр	110	14

Таблица 12.2 – Программные продукты, используемые при проведении лабораторных работ по дисциплине

№ п/п	№ ауд.	Вид учебного занятия	Наименование программного продукта
1.	1440	Лабораторные работы	Приложения офисного пакета MS Office; Adobe Reader MS Visual Studio