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

УТВЕРЖДАЮ

декан факультета прикладной
математики, информатики
и механики
С.Н. Медведев
26.05.2023

ПРОГРАММА ПРАКТИКИ
Б2.О.02(Н) Производственная практика (научно-исследовательская работа)

Код и наименование(тип) практики/НИР в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем и сетей

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию практики: Кибербезопасности информационных систем

6. Составители программы: Сафонов Виталий Владимирович, к.т.н., доцент

(ФИО, ученая степень, ученое звание)

7. Рекомендована: Научно-методическим советом факультета прикладной математики, информатики и механики 26.05.2023 г., протокол №9

(наименование рекомендующей структуры, дата, номер протокола,

_____

отметки о продлении вносятся вручную)

---

8. Учебный год: 2027/2028 **Семестр(ы):** 9

9.Цель практики:

− подготовка студента к решению задач, относящихся к различным проблемам комплексного обеспечения информационной безопасности, а также к решению отдельных фундаментальных проблем, связанных с компьютерной безопасностью;

− углубление и закрепление теоретических знаний, полученных студентами при изучении общепрофессиональных и специальных дисциплин;

− приобретение и совершенствование студентами профессиональных навыков и умений, закрепляющих полученные теоретические знания;

− развитие у студентов интереса к научно-исследовательской работе, привитие им навыков проведения исследований;

− проведение исследований, непосредственно связанных с выпускной квалификационной работой (ВКР).

Задачи практики:

Основной задачей научно-исследовательской работы является приобретение опыта в исследовании актуальной научной проблемы, а также подбор необходимых материалов для выполнения выпускной квалификационной работы.

Во время научно-исследовательской практики студент должен:

изучить:

− информационные источники по разрабатываемой теме с целью их использования при выполнении выпускной квалификационной работы;

− методы моделирования и исследования вопросов информационной безопасности;

− методы анализа и обработки данных, являющихся входными для проведения научного исследования;

− информационные технологии, применяемые в научных исследованиях, программные продукты, относящиеся к профессиональной сфере;

− требования к оформлению научно-технической документации;

выполнить:

− анализ, систематизацию и обобщение информации по теме исследований;

− сравнение результатов исследования объекта разработки с отечественными и зарубежными аналогами;

− анализ научной и практической значимости проводимых исследований.

10. Место практики в структуре ООП: *обязательная часть блока Б2.*

Цикл (раздел) ООП: Б2		код дисциплины в УП: Б2.Б.02(Н)
№	**Код**	**Наименование**
Для успешного прохождения учебной практики обучающиеся используют знания, умения, сформированные в ходе изучения дисциплин		
1	Б1.О.28	Методы оптимизации
2	Б1.О.35	Объектно-ориентированное программирование
3	Б1.О.37	Методы программирования
4	Б1.О.40	Модели безопасности компьютерных систем
5	Б1.О.42	Основы построения защищенных компьютерных сетей
6	Б1.О.43	Основы построения защищенных баз данных
7	Б1.О.44	Защита программ и данных
8	Б1.О.51	Защита информации от утечки по техническим каналам
9	Б1.О.57.01	Инженерия программного обеспечения
10	Б1.О.57.03	Разработка прикладного программного обеспечения для компьютерных систем
11	Б1.О.57.06	Современные проблемы информационной безопасности
12	ФТД.01	Анализ данных компьютерных систем и сетей
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее		
13	Б2.О.03(Пд)	Производственная практика (преддипломная)

14	Б2.О.04(Н)	Производственная практика (экспериментально-исследовательская)
15	Б2.О.05(П)	Производственная практика (проектно-эксплуатационная)
16	Б3.01(Д)	Подготовка к процедуре защиты и защита выпускной квалификационной работы

11. Вид практики, способ и форма ее проведения

Вид практики: *производственная*.
Способ проведения практики: *стационарная*.
Форма проведения практики: *дискретная.*
Реализуется частично в форме практической подготовки (ПП).
Производственная практика проводится в структурных подразделениях университета и в организациях на основе договоров, заключаемых между Университетом и организациями, деятельность которых соответствует направленности реализуемой образовательной программы по соответствующему профилю.

12. Планируемые результаты обучения при прохождении практики (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-7.	*Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ*	*ОПК-7.5*	умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач	Знать: – общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения; – необходимые и достаточные условия оптимальности задачи математического программирования. Уметь: – разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач; – применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.
		ОПК-7.9	знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения	
		ОПК-7.10	умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач;	
		ОПК-7.12	Знает необходимые и достаточные условия оптимальности задачи математического программирования.	
ОПК-8.	*Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей*	*ОПК-8.11*	владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах	Уметь: – применять методы экспериментального исследования при решении профессиональных задач. Владеть: – способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.
		ОПК-8.14	умеет применять методы экспериментального исследования при решении профессиональных задач	

ОПК-9.	*Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации*	*ОПК-9.15*	умеет анализировать и оценивать угрозы информационной безопасности объекта;	Уметь: – анализировать и оценивать угрозы информационной безопасности объекта.
ОПК-13.	*Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности*	*ОПК-13.5*	умеет работать с интегрированными средами разработки программного обеспечения;	Уметь: – работать с интегрированными средами разработки программного обеспечения; – формализовать поставленную задачу; – разрабатывать эффективные алгоритмы и программы; – проводить оценку вычислительной сложности алгоритма; – планировать разработку сложного программного обеспечения; – применять средства и методы анализа программного обеспечения для выявления закладок; – применять методы анализа проектных решений для обеспечения защищенности компьютерных систем; – применять современные средства обеспечения информационной безопасности программ и данных; – проводить анализ программных средств, применяемых для контроля и защиты информации. Владеть: – навыками разработки, отладки, документирования и тестирования программ; – методами оценки качества готового программного обеспечения; – навыками разработки алгоритмов для решения типовых профессиональных задач.
		ОПК-13.6	владеет навыками разработки, отладки, документирования и тестирования программ;	
		ОПК-13.12	умеет формализовать поставленную задачу;	
		ОПК-13.13	умеет разрабатывать эффективные алгоритмы и программы;	
		ОПК-13.14	умеет проводить оценку вычислительной сложности алгоритма;	
		ОПК-13.15	умеет планировать разработку сложного программного обеспечения;	
		ОПК-13.16	владеет методами оценки качества готового программного обеспечения;	
		ОПК-13.17	владеет навыками разработки алгоритмов для решения типовых профессиональных задач;	
		ОПК-13.18	Умеет применять средства и методы анализа программного обеспечения для выявления закладок	
		ОПК-13.19	Умеет применять методы анализа проектных решений для обеспечения защищенности компьютерных систем.	
		ОПК-13.21	Уметь применять современные средства обеспечения информационной безопасности программ и данных	
		ОПК-13.23	Умеет проводить анализ программных средств, применяемых для контроля и защиты информации	
ОПК-4.1	Способен организовывать защиту информации в компьютерных	ОПК-4.1.3	способен использовать языки и системы программирования, инструментальные	Уметь: – использовать языки и системы программирования, инструментальные средства при обеспечении защиты

	системах и сетях		средства при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач;	информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач – выполнять разработку и внедрение системы обеспечения информационной безопасности компьютерных систем, анализировать и оценивать ее отказоустойчивость и вырабатывать меры по ее улучшению. Владеть: – языками и системами программирования, инструментальными средствами при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач.
		ОПК-4.1.4	способен выполнять разработку и внедрение системы обеспечения информационной безопасности компьютерных систем, анализировать и оценивать ее отказоустойчивость и вырабатывать меры по ее улучшению;	
ОПК-4.2	Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения)	ОПК-4.2.2	знает назначение и основные задачи аудита, мониторинга и контрольных проверок функционирования и защищенности компьютерных систем и сетей;	Знать: – назначение и основные задачи аудита, мониторинга и контрольных проверок функционирования и защищенности компьютерных систем и сетей. Владеть: – навыками проведения анализа защищенности, мониторинга, аудита и обеспечения контрольных проверок функционирования и безопасности компьютерных систем и сетей.
		ОПК-4.2.3	владеет навыками проведения анализа защищенности, мониторинга, аудита и обеспечения контрольных проверок функционирования и безопасности компьютерных систем и сетей;	
ОПК-4.3	Способен разрабатывать и анализировать корректность политики информационной безопасности компьютерных систем и сетей (по областям применения)	ОПК-4.3.3	способен разрабатывать формальные модели политик безопасности и политики управления доступом, формировать политику информационной безопасности, анализировать ее корректность, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности компьютерных систем и сетей;	Уметь: – разрабатывать формальные модели политик безопасности и политики управления доступом, формировать политику информационной безопасности, анализировать ее корректность, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности компьютерных систем и сетей – применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности. Владеть: – программными средствами прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности.
		ОПК-4.3.5	способен применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности;	
ПК-1	Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации	ПК-1.1	применяет современные методы разработки программного обеспечения и технологии программирования;	Уметь: – применять современные методы разработки программного обеспечения и технологии программирования; – использовать принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения. Владеть: – современными методами разработки программного обеспечения и технологии программирования.
		ПК-1.3	использует принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с	

			использованием современных методов и средств разработки программного обеспечения;	
ПК-2	Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях	ПК-2.2	способен проводить анализ компьютерных систем с целью определения уровня защищённости и доверия с последующим обобщением и обработкой информации, полученной в ходе исследований;	Уметь: – проводить анализ компьютерных систем с целью определения уровня защищённости и доверия с последующим обобщением и обработкой информации, полученной в ходе исследований; – проводить теоретическое и прикладное исследование уровней защищенности компьютерных систем и сетей.
		ПК-2.5	проводит теоретические и прикладное исследование уровней защищенности компьютерных систем и сетей;	
ПК-3	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач	ПК-3.3	способен проводить анализ безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности;	Уметь: – проводить анализ безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности; – проводить анализ и формализацию поставленных задач в области безопасности компьютерных систем и сетей.
		ПК-3.4	способен проводить анализ и формализацию поставленных задач в области безопасности компьютерных систем и сетей;	

13. Объем практики в зачетных единицах / ак. час. (*в соответствии с учебным планом)* — 8/288.

Форма промежуточной аттестации *зачет с оценкой.*

14. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		9		
		ч.	ч., в форме ПП	
Всего часов	288	288	203	
в том числе:				
Контактная работа (включая НИС)	4	4	3	
Самостоятельная работа	284	284	200	
Итого:	288	288	203	

15. Содержание практики (или НИР)

п/п	Разделы (этапы) практики	Виды учебной работы	Объем учебной работы, ч	
			Контактные часы	Самостоятельная работа
1.	*Организационно-подготовительный этап*	проведение собрания по организации практики; установочный инструктаж по задачам, срокам и требуемой отчетности; инструктаж по технике безопасности работы; формулировка задач для решения в ходе практики;	1	24

		подготовка документов, подтверждающих факт направления на практику; получение задания от руководителя практики; производственный инструктаж		
2.	*Научно-исследовательский этап*	1) выбор темы исследования; определение проблемы, объекта и предмета исследования; 2) формулирование цели и задач исследования (анализ исходных данных для решения поставленной задачи; локализация проблематики, объекта и предмета исследования); 3) теоретический анализ литературы и исследований по проблеме, подбор необходимых источников по теме (патентные материалы, научные отчеты, техническая документация и др.); составление библиографии; 4) формулирование рабочей гипотезы; выбор оборудования для решения поставленной задачи; 5) разработка математического, алгоритмического или программного обеспечения необходимого для решения поставленной задачи основываясь на тезисах рабочей гипотезы	1	90
3.	*Этап выполнения исследовательских работ по индивидуальному плану*	определение проблемы, объекта и предмета исследования, формулирование цели и задач исследования, теоретический анализ литературы и исследований по проблеме, проведение обзора и выбор современных информационных технологий, специального программного обеспечения и оборудования для решения поставленной задачи по анализу защищенности объекта информатизации; проведение самостоятельного решения сформулированной научной задачи, исследований и экспериментов	1	90
4.	*Оформление отчёта по итогам практики*	описание проделанной работы с самооценкой результатов выполнения НИР; формулирование выводов и предложений по организации НИР	1	80

Содержание практической подготовки при проведении практики устанавливается исходя из содержания и направленности образовательной программы, содержания практики, ее целей и задач. Практическая подготовка при проведении практики направлена на формирование умений и навыков в соответствии с трудовыми действиями и (или) трудовыми функциями по профилю образовательной программы.

Практическая подготовка проводится путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью, способствующих формированию, закреплению и развитию практических навыков и компетенций по профилю соответствующей образовательной программы.

№ п/п	Типы задач профессиональной деятельности	Формируемые профессиональные компетенции	Формируемые общепрофессиональные компетенции специализации
1	*Научно-исследовательский*	*ПК-1.1 применяет современные методы разработки программного обеспечения и технологии программирования;* *ПК-2.2 способен проводить анализ компьютерных систем с целью определения уровня защищённости и доверия с последующим обобщением и обработкой информации, полученной в ходе исследований;* *ПК-2.5 проводит теоретические и прикладное исследование уровней защищенности компьютерных систем и сетей;* *ПК-3.3 способен проводить анализ безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности;* *ПК-3.4 способен проводить анализ и формализацию поставленных задач в области безопасности компьютерных систем и сетей.*	*ОПК-4.1.3 способен использовать языки и системы программирования, инструментальные средства при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач;* *ОПК-4.3.5 способен применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности.*
2	*Проектный*	*ПК-1.3 использует принципы*	

		комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения;	
3	*Контрольно-аналитический*		*ОПК-4.1.4 способен выполнять разработку и внедрение системы обеспечения информационной безопасности компьютерных систем, анализировать и оценивать ее отказоустойчивость и вырабатывать меры по ее улучшению. ОПК-4.2.2 знает назначение и основные задачи аудита, мониторинга и контрольных проверок функционирования и защищенности компьютерных систем и сетей;*
4	*Организационно-управленческий*		*ОПК-4.3.3 способен разрабатывать формальные модели политик безопасности и политики управления доступом, формировать политику информационной безопасности, анализировать ее корректность, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности компьютерных систем и сетей.*
5	*Эксплуатационный*		*ОПК-4.2.3 владеет навыками проведения анализа защищенности, мониторинга, аудита и обеспечения контрольных проверок функционирования и безопасности компьютерных систем и сетей.*

16. Перечень учебной литературы, ресурсов сети «Интернет», необходимых для прохождения практики *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1.	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва: Дашков и Ко, 2012. — 244 с. URL:http://biblioclub.ru/index.php?page=book&id=112247.
2.	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с. URL:http://www.methodolog.ru/books/mni.pdf.
3.	Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. - М.: Академия, 2007. – 330 с.
4.	Основы управления информационной безопасностью: [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.]. — 2-е изд., испр. — Москва: Горячая линия-Телеком, 2014. — 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
5.	Краковский, Ю.М. Информационная безопасность и защита информации: учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский. — М.; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
6.	Олейник П. П. Корпоративные информационные системы: для бакалавров и специалистов: учебник для студ. вузов, обуч. по направл. 080800 "Прикладная информатика (по областям)" и др. экон. спец. – СПб.: Питер, 2012. – 176 с.
7.	Фостер, Джеймс. Защита от взлома: сокеты, эксплойты, shell-код: / Дж. Фостер, М. Прайс ; пер. с англ. А. А. Слинкина .— Москва : ДМК Пресс, 2008 .— 784 с. : ил. — (Информационная безопасность).— ISBN 5-9706-0019-9 : 449.10 р. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
8.	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите/ Э. Скудис. — Москва: ДМК Пресс, 2009. — 512 с. : ил. — (Защита и администрирование) .— ISBN 5-94074-170-3 : 176-00 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112>.
9.	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения:

	учебное пособие для вузов / В.А. Голуб; Воронеж. гос. ун-т.— Воронеж: ЛОП ВГУ, 2006. — 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
10.	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок/ М. Ховард, Д. Лебланк, Дж. Виега; авт. предисл. А. Йоран. — Москва: ДМК Пресс, 2009. — 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
11.	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors: Обнаружение и защита / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. - 304 с.
12.	Проскурин В. Г. Защита программ и данных - М.: Академия, 2011. – 198 с.
13.	Управление внедрением информационных систем: курс лекций: учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. технологий / В.И. Грекул, Г. Н. Денищенко, Н.Л. Коровкина. – М.: Интернет-Ун-т информ. технологий, 2008. [Электронный ресурс] URL: http://www.intuit.ru/studies/courses/2196/267/info/.
14.	Юрин И.Ю. Теоретические и практические основы защиты информации. 2012. http://library.sgu.ru/uch_lit/620.pdf.

б) дополнительная литература:

№ п/п	Источник
15.	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва: Флинта: Наука, 2014. — 108 с.
16.	Кручинин, В.В. Компьютерные технологии в научных исследованиях: учебно-методическое пособие / В.В. Кручинин. – Москва: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269.
17.	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В. Барвиненко, В.С. Верба. — Москва: Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348.
18.	Системы и средства информатики: Ежегодник / Гл. ред. И.А. Соколов. — Москва: ИПИ РАН. – 2010.– Вып. 20. – № 2. — 350 с.
19.	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
20.	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451.
21.	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст).
22.	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
23.	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
24.	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
25.	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
26.	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
27.	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.

28.	Ермошкин Н.Н., Тарасов А.А. Стратегия информационных технологий предприятия. М.: Изд-во Московского гуманитарного университета, 2003.
29.	Корнеев И.К., Степанов Е.А. Защита информации в офисе. – "Издательство Проспект", 2008. – 333 с.
30.	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html.
31.	Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб.: Питер, 2005. — 991 с.
32.	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века: матер. XII международ. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.
33.	Партыка Т.Л. Информационная безопасность М.: ФОРУМ, 2007.
34.	Мельников, Владимир Павлович. Информационная безопасность и защита информации: учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. — М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника). — Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
35.	Андрианов В.И."Шпионские штучки" и устройства для защиты объектов, и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.
36.	Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И.Абалмазов. – М.: Гротек, 1997.
37.	Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В.Василевский. – М.: НПЦ "Нелк", 1998.
38.	Хорев А.А., Способы и средства ЗИ / А.А.Хорев. – МО РФ, 1998.
39.	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
40.	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
41.	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
42.	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1.	ЭБС Лань
2.	ЭБС «Университетская библиотека online»
3.	ЭБС «Электронная библиотека технического ВУЗа» (ЭБС «Консультант студента»)
4.	ЭБС ЮРАЙТ
5.	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
6.	http://www.cryptopro.ru
7.	http://www.infotecs.ru
8.	http://www.lissi-crypto.ru/
9.	http://www.signal-com.ru
10.	http://www.shipka.ru

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы и т.д.

17. Образовательные технологии, применяемые при проведении практики и методические указания для обучающихся по прохождению практики

НИР - самостоятельное исследование студента, оформленное в виде научного отчета. НИР является обязательной частью учебного плана.

Основными задачами НИР являются:

1) дать возможность студенту провести самостоятельное научное исследование, углубить знания по специальным дисциплинам;

2) определить способность студента выполнять научное исследование на уровне, соответствующем квалификации.

НИР содержат следующие основные части: введение, теория, эксперимент, результаты, обсуждение результатов, выводы, заключение, замечания, список литературы. Аннотация объемом не более 0,5 страницы расположена после титульного листа и предшествует «Содержанию». Список буквенных обозначений и сокращений следует за «Содержанием». Рисунки и таблицы располагаются по тексту после ссылок на них. Работу необходимо написать аккуратно, грамотным научным языком. Жесткие требования к объему работы отсутствуют. Ориентировочно можно посоветовать объем НИР в пределах 30-50 страниц.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. Представленный отчет по практике оценивается на соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Структура отчета по практике

1. Отчет по практике должен включать титульный лист, содержание, введение, описание теоретических и практических аспектов выполненной работы, заключение, список использованных источников, приложения.

2. На титульном листе должна быть представлена тема практики, группа и фамилия студента, данные о предприятии, на базе которого выполнялась практика, фамилия руководителя.

3. Во введении студенты должны дать краткое описание задачи, решаемой в рамках практики.

4. В основной части отчета студенты приводят подробное описание проделанной теоретической и (или) практической работы, включая описание и обоснование выбранных решений, описание программ и т.д.

5. В заключении дается краткая характеристика проделанной работы, и приводятся ее основные результаты.

6. В приложениях приводятся непосредственные результаты разработки: тексты программ, графики и диаграммы, и т.д.

Требования к оформлению отчета

1. Отчет оформляется в печатном виде, на листах формата А4.

2. Основной текст отчета выполняется шрифтом 14 пунктов, с интервалом 1,5 между строками. Текст разбивается на абзацы, каждый из которых включает отступ и выравнивание по ширине.

3. Текст в приложениях может быть выполнен более мелким шрифтом.

4. Отчет разбивается на главы, пункты и подпункты, включающие десятичную нумерацию.

5. Рисунки и таблицы в отчете должны иметь отдельную нумерацию и названия.

6. Весь отчет должен быть оформлен в едином стиле: везде в отчете для заголовков одного уровня, основного текста и подписей должен использоваться одинаковый шрифт.

7.Страницы отчета нумеруются, начиная с титульного листа. Номера страниц проставляются в правом верхнем углу для всего отчета кроме титульного листа.

8. Содержание отчета должно включать перечень всех глав, пунктов и подпунктов, с указанием номера страницы для каждого элемента содержания.

9. Ссылки на литературу и другие использованные источники оформляются в основном тексте, а сами источники перечисляются в списке использованных источников.

10. Объем отчета по практике должен быть не менее 30 страниц.

18. Материально-техническое обеспечение практики:

г. Воронеж, ул. Университетская площадь, д.1, главный учебный корпус, ауд.214

Компьютер в составе: системный блок: процессор Intel(R) Core(TM) i5, оперативная память 8Гб, HDD 500Гб; монитор: LG FLATRON. Мультимедиапроектор BenQ. Экран настенный для проектора. Аудио колонки Creative A60. Коммутатор.

г. Воронеж, ул. Университетская площадь, д.1, учебный корпус 1б, ауд.407

Компьютер в составе: процессор Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz, оперативная память 16 Гб, SSD 256 Гб, HDD 1Тб, видеокарта NVIDIA GeForce GTX 1080 Ti; монитор DELL S2419HN. Компьютер в составе (1 шт.): процессор Intel(R) Core(TM) i7-7800X CPU @ 3.50GHz, оперативная память 96 Гб, SSD 1Тб, HDD 4Тб, видеокарта NVIDIA GeForce RTX 2080 Ti (2 шт.); монитор DELL S2419HN. Источник бесперебойного питания APC Back-UPS BV1000I-GR, line-interactive, мощность:1000ВА, 600Вт (16 шт.). Источник бесперебойного питания Legrand KEOR LINE RT 1500ВА (1 шт.). Коммутатор HP 2530-24G Switch (Managed, 24*10/100/1000 + 4 SFP, 19"). Интерактивная доска SMART SBM685 (87 дюймов, ПО SMART SLS) с пассивным лотком. Проектор Vivitek DH758UST (ультракороткофокусный, DLP, Full HD 1080p (1920 x 1080) , 3500 ANS, 10000:1, полная поддержка 3D).

г. Воронеж, ул. Университетская площадь, д.1, главный учебный корпус, ауд.124

Компьютер в составе: системный блок: процессор AMD Ryzen 7 3800X 8-Core Processor, оперативная память 32Гб, HDD 1Тб, SSD 256Гб, видеокарта NVIDIA GeForce GTX 1050; монитор: Dell S2419H. Интерактивная доска SMART SBM685 (87 дюймов). Мультимедиапроектор Vivitek ультракороткофокусный. Источник бесперебойного питания Legrand Keor SPX 1000 BA IEC C13 (16 шт.). Источник бесперебойного питания Legrand Keor Line RT 1000 BA (1 шт.). Коммутатор HP 2530-48G Switch (1 шт.).

г. Воронеж, ул. Университетская площадь, д.1, главный учебный корпус, ауд.226

Моноблок HP: процессор Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz, оперативная память 8Гб, SSD 250Гб. Мультимедиапроектор Epson. Аудио колонки EV (2 шт.). Микрофон. Экран для проектора. Маркерные панели Askell (2 шт.).

г. Воронеж, ул. Университетская площадь, д.1, учебный корпус 1, ауд.2/25

Учебный стенд "Программные средства криптографии", SCRYPTO в составе:
каркас моноблока (1 шт.); интегрированный вычислительный узел 3 шт.) в составе: процессор Intel: два ядра с тактовой частотой 2700 МГц, ОЗУ: объём 4 Гб тип DDR-3, твердотельный накопитель SSD объемом 60 Гб, блок питания мощностью 300 Вт, 2 сетевых интерфейса GigabitEthernet; переключатель KBM-типа D-Link (1 шт.); неуправляемый коммутатор D-Link (1 шт.); модуль питания, контроля и интеграции стенда в общую лабораторию (1 шт.); монитор Philips(1 шт.); комплект консоли рабочего места обучаемого (1 шт.) в составе: клавиатура Oklick, мышь Oklick; комплект учебно-методических пособий (1 к-т.); статистическое программное обеспечение управления модулем питания (1 шт.); флэш-диск восстановления ОС на интегрированных ПК (3 шт.) с операционной системой ArchLinux; флэш-диск мультимедийного методического пособия (1 шт.); группа коммутационных портов (2 шт.).

Типовой комплект учебного оборудования "Сетевая безопасность", SECURITY в составе: управляемый коммутатор третьего уровня D-Link (1 шт.); управляемый коммутатор второго уровня D-Link (1 шт.); аппаратно-программный эмулятор устройства локальной сети (1 шт.); неуправляемый коммутатор D-Link (2 шт.); маршрутизатор беспроводной D-Link (2 шт.); брандмауэр D-Link (2 шт.); модуль питания, контроля и интеграции стенда в общую лабораторию (1 шт.); коммутационная панель (1 шт.); вычислительный узел (4 шт.) в составе: процессор Intel: два ядра с тактовой частотой 2700 МГц, ОЗУ: объём 4 Гб тип DDR-3, твердотельный накопитель SSD объемом 60 Гб, блок питания мощностью 300 Вт, 2 сетевых интерфейса GigabitEthernet, 1 беспроводной сетевой интерфейс; моноблок (1 шт.); статистическое программное обеспечение управления модулем питания, контроля и интеграции (1 шт.); программная система восстановления U-Profi (R) (4 флэш-диска объемом 8 Гб) (1 шт.); удлинитель USB (4 шт.); кабель VGA (2 шт.); патч-корд (10 шт.); методическое пособие (2 к-та.).

Учебно-практический стенд «Системы контроля и управления доступом», ФЗИ-СКУД в составе: модель стены (1 шт.); ноутбук Lenovo (1 шт.): экран с диагональю 15.6" (разрешение 1366x768), ОЗУ объемом 2048 Мб, накопитель объемом 120 Гб, процессор Intel два ядра с тактовой частотой 1,4 ГГц, веб-камера; сканер линейных и двумерных штрих-кодов (1 шт.); светодиод (1 шт.); электромеханический замок (1 шт.); сетевой контроллер СКУД (2 шт.); мультимедийный терминал многофакторной идентификации, в том числе распознавание лиц (1 шт.); настольное устройство чтения и записи смарт-карт (1 шт.); контактная смарт-карта с объёмом памяти 256 байт (5 шт.); USB ключ тип e-token (1 шт.); комплект ПО и конвертор (1 шт.); программатор карт Mifare настольный (1 шт.); считыватель бесконтактных карт Em-Marine (1 шт.); считыватель бесконтактных карт Mifare (1 шт.); смарт-карта тип Mifare (5 шт.); смарт-карта тип Em-Marine (5 шт.); ключ iButton (Touch-Memory) (5 шт.); программатор ключей Touch-

Memory (1 шт.); модуль согласования интерфейсов (1 шт.); электромагнитный замок (1 шт.); считыватель ключей TouchMemory (1 шт.); сетевой контроллер TouchMemory (1 шт.); блок питания (1 шт.); программа распознавания автомобильных номеров (1 шт.); макет номера ТС РФ (5 шт.); сетевое реле (1 шт.); IP-камера (1 шт.); коммутатор неуправляемый D-Link (1 шт.); модуль питания, контроля и интеграции комплекта в общую лабораторию (1 шт.); статистическое программное обеспечение управления модулем питания, контроля и интеграции (1 шт.); программный эмулятор физических объектов доступа (1 шт.); методическое пособие (2 шт.).

19. Оценочные средства для проведения текущей и промежуточной аттестации обучающихся по практике

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	*Организационно-подготовительный этап*	*ОПК-13*	*ОПК-13.12*	Отчет по практике.
2.	*Научно-исследовательский этап*	*ОПК-7*	*ОПК-7.5*	Отчет по практике. Защита отчета по практике.
			ОПК-7.9	
			ОПК-7.10	
			ОПК-7.12	
		ОПК-13	*ОПК-13.13*	
			ОПК-13.14	
			ОПК-13.15	
			ОПК-13.17	
			ОПК-13.21	
			ОПК-13.23	
		ОПК-8	*ОПК-8.11*	
			ОПК-8.14	
		ОПК-4.1	ОПК-4.1.3	
		ОПК-4.2	ОПК-4.2.3	
			ОПК-4.2.2	
		ОПК-4.3	ОПК-4.3.3	
			ОПК-4.3.5	
		ПК-1	ПК-1.1	
			ПК-1.3	
		ПК-2	ПК-2.2	
		ПК-3	ПК-3.3	
			ПК-3.4	
3.	*Этап выполнения исследовательских работ по индивидуальному плану*	*ОПК-9*	*ОПК-9.15*	Отчет по практике. Защита отчета по практике.
		ОПК-13	*ОПК-13.6*	
			ОПК-13.18	
			ОПК-13.19	
		ОПК-4.1	ОПК-4.1.4	
		ПК-2	ПК-2.5	
		ПК-3	ПК-3.4	
4.	*Оформление отчёта по итогам практики*	*ОПК-13*	*ОПК-13.5*	Отчет по практике.
			ОПК-13.6	
			ОПК-13.12	
			ОПК-13.16	
			ОПК-13.18	
Промежуточная аттестация форма контроля – зачет с оценкой				Индивидуальное задание

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Индивидуальные задания

Перечень индивидуальных заданий

Перечень индивидуальных заданий

Провести анализ поставленной задачи с точки зрения обеспечения максимально эффективной защиты информации в инфраструктуре организации (рассмотреть теоретические аспекты, на основании анализа построить модель безопасности).

1. Автоматизированная система в защищенном исполнении организации (или предприятия любой формы собственности).
2. Анализ уязвимостей и организация защиты информации в локальной сети организации (или предприятия любой формы собственности).
3. Анализ уязвимостей и эффективности средств и способов защиты информации в автоматизированной системе организации (или предприятия любой формы собственности).
4. Инструментальный мониторинг защищенности автоматизированной системы организации (или предприятия любой формы собственности).
5. Информационная система персональных данных организации (или предприятия любой формы собственности).
6. Комплексная защита информации в локальной сети организации (или предприятия любой формы собственности).
7. Подготовка к аттестации информационной системы персональных данных в организации (или предприятии любой формы собственности).
8. Сбор и анализ исходных данных для проектирования системы защиты информации организации (или предприятия любой формы собственности).
9. Система контроля и управления доступом в организации (или на предприятии любой формы собственности).
10. Система управления информационной безопасностью автоматизированной системы организации (или предприятия любой формы собственности).

Требования к выполнению заданий

Провести анализ поставленной задачи с точки зрения обеспечения нахождения эффективного решения опираясь на существующую инфраструктуру организации (рассмотреть теоретические аспекты, на основании анализа построить модель решения и т.д.).

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Отчет по практике

Темы проектов

1. Средства обеспечения информационной безопасности в корпоративных информационных системах
2. Аппаратные средства обеспечения информационной безопасности
3. Информационные уязвимости объектов
4. Программные средства обеспечения информационной безопасности
5. Антропогенные информационные уязвимости
6. Техногенные информационные уязвимости
7. Организационно-правовые средства обеспечения информационной безопасности
8. Угрозы информационной безопасности и их источники
9. Организационно-административные средства защиты информации
10. Основные причины утечки информации и возможности противодействия утечкам информации.
11. Меры защиты персональных данных в информационных системах персональных данных.
12. Подтверждение подлинности объектов и субъектов информационной системы.
13. Контроль целостности информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

14. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
15. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
16. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
17. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
18. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
19. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
20. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
21. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
22. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
23. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
24. Биометрические средства идентификации и аутентификации пользователей.
25. Аутентификация субъектов в распределенных системах, проблемы и решения.
26. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
27. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
28. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
29. Критерии оценки безопасности компьютерных систем. Структура требований безопасности. Классы защищенности.
30. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
31. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
32. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
33. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
34. Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.
35. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
36. Применение средств Windows для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
37. Разграничение доступа к данным в ОС семейства UNIX.
38. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
39. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
40. Понятие атаки на систему информационной безопасности. Особенности локальных атак.

41. Распределенные информационные системы. Удаленные атаки на информационную систему.

42. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.

43. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.

44. Виртуальные частные сети, их функции и назначение.

45. Сетевые войны: цели, задачи, сценарии и средства их проведения, оценка перспектив развития и противодействия в контексте обеспечения информационной безопасности государства.

46. Социальные сети как инструмент организации протестов и «революций»: способы и средства возмущения социума, сценарий ослабления и свержения власти, меры противодействия в контексте обеспечения информационной безопасности государства.

47. Статистический анализ всевозможных классов и типов атак на информационные инфо-системы: цели, частота атак и величина ущербов от их реализации, соответствующая
оценка рисков в динамике развития сферы информационной безопасности, выводы относительно опасности и возможностей противодействия.

48. Анализ и подготовка обзора научно-технических материалов по гетерогенным сетям в контексте обеспечения их безопасности.

49. Развитие научно-методического обеспечения теории ветвящихся процессов на анализ распространения вредоносного программного обеспечения в сетевых структурах.

50. Развитие научно-методического обеспечения теории случайных графов на анализ живучести сетевых структур.

51. Опасность DDOS-атак и риск-моделирование их разновидностей в контексте противодействия.

Промежуточная аттестация по практике включает подготовку и защиту отчета.

Отчет содержит следующие составляющие: обработанный и систематизированный материал по тематике практики; экспериментальную часть, включающую основные методы проведения исследования и статистической обработки, обсуждение полученных результатов; заключение, выводы и список литературных источников. Отчет обязательно подписывается (заверяется) руководителем практики. Результаты прохождения практики докладываются обучающимся в виде устного сообщения с демонстрацией презентации на заседании кафедры (заключительной конференции).

По результатам доклада с учетом характеристики руководителя и качества представленных отчетных материалов обучающемуся выставляется соответствующая оценка (дифференцированный зачет по итогам практики выставляется обучающимся руководителем практики на основании доклада и отчетных материалов, представленных обучающимся).

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя от предприятия, выступления с презентацией и ответов на вопросы по итогам практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. При защите отчета по практике оценивается соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках

выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя практики от кафедры.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок. Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

− требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов). Соответствует оценке - «отлично»;

− результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; соответствует оценке - «хорошо»;

− результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; соответствует оценке - «удовлетворительно»;

− результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

− выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов. Соответствует оценке - «отлично»;

− выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

− выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для аттестации студент предъявляет дневник практики, задание руководителя на прохождение практики и оформляет результаты практики в виде отчета и готовит выступление с презентацией по результатам практики.

Для оценивания результатов обучения на зачете с оценкой используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Знать: результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный. «Уметь» и «Владеть»: выполнены все требования к выполнению, написанию и защите отчета.	*Повышенный уровень*	*Отлично*

Знать: результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки). «Уметь» и «Владеть»: выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно	*Базовый уровень*	*Хорошо*
Знать: результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) «Уметь» и «Владеть»: выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление.	*Пороговый уровень*	*Удовлетворительно*
Знать: результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия. «Уметь» и «Владеть»: требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены.	–	*Неудовлетворительно*

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

ОПК-7.5 умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач

ОПК-7.9 знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения

ОПК-7.10 умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач;

ОПК-7.12 Знает необходимые и достаточные условия оптимальности задачи математического программирования.

ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

ОПК-8.11 владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах

ОПК-8.14 умеет применять методы экспериментального исследования при решении профессиональных задач

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

ОПК-9.15 умеет анализировать и оценивать угрозы информационной безопасности объекта;

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

ОПК-13.5 умеет работать с интегрированными средами разработки программного обеспечения;

ОПК-13.6 владеет навыками разработки, отладки, документирования и тестирования программ;

ОПК-13.12 умеет формализовать поставленную задачу;

ОПК-13.13 умеет разрабатывать эффективные алгоритмы и программы;

ОПК-13.14 умеет проводить оценку вычислительной сложности алгоритма;

ОПК-13.15 умеет планировать разработку сложного программного обеспечения;

ОПК-13.16 владеет методами оценки качества готового программного обеспечения;

ОПК-13.17 владеет навыками разработки алгоритмов для решения типовых профессиональных задач;

ОПК-13.18 Умеет применять средства и методы анализа программного обеспечения для выявления закладок

ОПК-13.19 Умеет применять методы анализа проектных решений для обеспечения защищенности компьютерных систем.

ОПК-13.21 Уметь применять современные средства обеспечения информационной безопасности программ и данных

ОПК-13.23 Умеет проводить анализ программных средств, применяемых для контроля и защиты информации

ОПК-4.1 Способен организовывать защиту информации в компьютерных системах и сетях

ОПК-4.1.3 способен использовать языки и системы программирования, инструментальные средства при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач;

ОПК-4.1.4 способен выполнять разработку и внедрение системы обеспечения информационной безопасности компьютерных систем, анализировать и оценивать ее отказоустойчивость и вырабатывать меры по ее улучшению;

ОПК-4.2 Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения)

ОПК-4.2.2 знает назначение и основные задачи аудита, мониторинга и контрольных проверок функционирования и защищенности компьютерных систем и сетей;

ОПК-4.2.3 владеет навыками проведения анализа защищенности, мониторинга, аудита и обеспечения контрольных проверок функционирования и безопасности компьютерных систем и сетей;

ОПК-4.3 Способен разрабатывать и анализировать корректность политики информационной безопасности компьютерных систем и сетей (по областям применения)

ОПК-4.3.3 способен разрабатывать формальные модели политик безопасности и политики управления доступом, формировать политику информационной безопасности, анализировать ее корректность, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности компьютерных систем и сетей;

ОПК-4.3.5 способен применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности;

ПК-1 Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации

ПК-1.1 применяет современные методы разработки программного обеспечения и технологии программирования;

ПК-1.3 использует принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения;

ПК-2 Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях

ПК-2.2 способен проводить анализ компьютерных систем с целью определения уровня защищённости и доверия с последующим обобщением и обработкой информации, полученной в ходе исследований;

ПК-2.5 проводит теоретические и прикладное исследование уровней защищенности компьютерных систем и сетей;

ПК-3 Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач

ПК-3.3 способен проводить анализ безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности;

ПК-3.4 способен проводить анализ и формализацию поставленных задач в области безопасности компьютерных систем и сетей.

Вопросы с вариантами ответов

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

- пользователь;
- **владелец;**
- руководитель предприятия

2. ISO 17799 не охватывает
- Политику безопасности
- Организационная безопасность
- Классификация и контроль имущества
- Безопасность персонала
- Физическая безопасность и безопасность среды
- Управление коммуникациями и операциями
- Контроль доступа
- Разработка и поддержка систем
- Поддержка непрерывности деловых процессов
- Соответствие политике
- **Охватывает все**

3. Обязано ли лицо, осуществляющее обработку персональных данных по поручению оператора, получать согласие субъекта персональных данных на обработку его персональных данных:
- **не обязано;**
- обязано;
- не обязано только в случаях, предусмотренных законом.

4. К какой из составляющих системы защиты информации относятся средства пожарной сигнализации и пожаротушения:
- организационной
- программной
- **технической**
- информационно-лингвистической

5. Используемые средства защиты информации в АСОД на начальном этапе:
- материальные
- морально-этические
- неформальные
- **формальные**

6. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
- анализ рисков
- **анализ затрат / выгоды**
- результаты аттестации

7. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется
- системой угроз;
- **системой защиты;**
- системой безопасности;
- системой уничтожения.

8.Обеспечение информационной безопасности есть обеспечение…
- *Независимости информации*
- *Изменения информации*
- *Копирования информации*
- ***Сохранности информации***
- *Преобразования информации*

9. Искусственные угрозы безопасности информации вызваны:
- **деятельностью человека**
- ошибками при проектировании системы безопасности, ее элементов или разработке программного обеспечения
- ошибками при действиях персонала
- корыстными устремлениями злоумышленников

10. При каком типе атаки степень активности криптоаналитика наивысшая?
- **криптоатака с использованием криптограмм;**

- криптоатака с использованием открытых текстов и соответствующих криптограмм;
- **криптоатака с использованием выбираемых криптоаналитиком открытых текстов и соответствующих криптограмм**

1. Дифференциальный криптоанализ относится к атакам:
   a) На основе шифртекста
   b) На основе открытых текстов
   c) На основе подобранного открытого текста
   d) На основе адаптивно подобранного открытого текста
2. Способ защиты информации, при котором конкурент вводится в заблуждение относительно деятельности и намерений:
   1. кодирование
   2. криптография
   3. управление
   4. маскировка
3. Перечислите виды электронной подписи:
   а) простая, сложная, комбинированная;
   б) простая, квалифицированная, сложная;
   в) простая, квалифицированная, неквалифицированная.
4. Идентификация это:
   а) процесс предъявления пользователем идентификатора;
   б) процесс подтверждения подлинности;
   в) сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов.
5. Какую роль играют центры сертификации ключей:
   а) они играют роль доверенной третьей стороны для доказывания факта передачи информации;
   б) они служат для регистрации абонентов, изготовления сертификатов открытых ключей, хранения изготовленных сертификатов, поддержания в актуальном состоянии справочника действующих сертификатов и выпуска списка досрочно отозванных сертификатов;

16. Моделями типа «черный ящик» являются
    a. Модели мышления
    b. Модели, описывающие зависимость параметров состояния объекта от входных параметров
    c. **Модели, описывающие входные и выходные параметры объекта без учета внутренней структуры объекта**
    d. Модели «аварийного» ящика на самолетах
17. Моделями типа «белый ящик» являются
    a. Модели мышления
    b. **Модели, описывающие зависимость параметров состояния объекта от входных параметров**
    c. Модели, описывающие входные и выходные параметры объекта с учетом внутренней структуры объекта
    d. Модели, описывающие выходные данные в программе
18. Установите соответствие
    1. Полный взлом
    2. Глобальная дедукция
    3. Частичная дедукция
    4. Информационная дедукция

    1. криптоаналитик разрабатывает функциональный эквивалент исследуемого алгоритма, позволяющий зашифровывать и расшифровывать информацию без знания ключа.
    2. криптоаналитику удается расшифровать или зашифровать некоторые сообщения.
    3. криптоаналитик извлекает секретный ключ.
    4. криптоаналитик получает некоторую информацию об открытом тексте или ключе.

    Ответ: 1-3, 2-1, 3-2, 4-4

19 Какие из перечисленных киберугроз являются ключевыми на ближайшее будущее? Выберите все правильные ответы.

- **Устройства IoT как площадка для реализации атак**

- Спам
- **Программы-вымогатели**
- **Criminal-as-a-service (переход киберпреступников на сервисную модель)**
- Программы-шпионы
- **«Призраки интернета прошлого» (угрозы от устаревшего программного и программно-аппаратного обеспечения, которое находится в интернете)**
- Программы-майнеры
- Скимминг

20. Что такое несанкционированный доступ (нсд)?

1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

2) Создание резервных копий в организации

3) Правила и положения, выработанные в организации для обхода парольной защиты

4) Вход в систему без согласования с руководителем организации

5) Удаление не нужной информации

21. В чем заключается основная причина потерь информации, связанной с ПК?

1) с глобальным хищением информации

2) с появлением интернета

3) с недостаточной образованностью в области безопасности

22. Протоколирование и аудит могут использоваться для:

(1) предупреждения нарушений ИБ

(2) обнаружения нарушений

(3) восстановления режима ИБ

23. Аутентификация на основе пароля, переданного по сети в открытом виде, плоха, потому что не обеспечивает защиты от:

(1) перехвата

(2) воспроизведения

(3) атак на доступность

24. Виртуальная реальность подразумевает …

A. созданный техническими средствами мир, передаваемый человеку через его ощущения: зрение, слух, осязание и пр.

B. виртуальные объекты, интегрированные в восприятие пользователя, как часть реальной окружающей картины мира в режиме реального времени.

C. объединение реального и виртуального миров для создания новых окружений и визуализаций, где физический и цифровой объекты сосуществуют и взаимодействуют в реальном времени.

D. создание виртуального цифрового сценария для воспроизведения на любом медиа-устройстве.

25. Какие технические средства могут быть использованы для доказательства вины человека?

(1) журналы доступа

(2) биометрические ключи

(3) видеонаблюдение

26. Сверточное кодирование

Ответ: При свёрточном кодировании преобразование информационных последовательностей в выходные и кодовые происходит непрерывно. Кодер двоичного свёрточного кода содержит сдвигающий регистр из m разрядов и сумматоры по модулю 2 для образования кодовых символов в выходной последовательности. Входы сумматоров соединены с определёнными разрядами регистра. Коммутатор на выходе устанавливает очередность посылки кодовых символов в канал связи.

2. Для какого источника открытых текстов вероятности появления k -грамм в тексте зависят от их места в тексте?

Ответ Нестационарный

3. Какая криптоатака основана на знании открытого текста для случайных фрагментов шифротекста?

Ответ: на основе открытых текстов

Критерии и шкалы оценивания заданий ФОС:

Для оценивания выполнения заданий используется балльная шкала:

1) закрытые задания (тестовые с вариантами ответов, средний уровень сложности):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ (полностью или частично неверный).

2) открытые задания (тестовые с кратким текстовым ответом, повышенный уровень сложности):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ (полностью или частично неверный).

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).

6.