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.03(Пд) Производственная практика (преддипломная)

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: 2028/2029 **Семестр(ы):** В

9.Цель практики:

- проведение систематизации, расширения, закрепление и углубления теоретических профессиональных знаний, полученных в результате изучения дисциплин направления и специальных дисциплин профильной программы подготовки;
- выполнение выпускной квалификационной работы;
- формирование у студентов навыков ведения самостоятельной научной работы, исследования и экспериментирования.

Задачи практики:

Основной задачей производственной практики преддипломной является приобретение опыта в исследовании актуальной научной проблемы, а также подбор необходимых материалов для выполнения выпускной квалификационной работы.

Во время 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.О.03(Пд)
№	**Код**	**Наименование**
Для успешного прохождения учебной практики обучающиеся используют знания, умения, сформированные в ходе изучения дисциплин		
1	Б1.О.35	Объектно-ориентированное программирование
2	Б1.О.37	Методы программирования
3	Б1.О.41	Защита в операционных системах
4	Б1.О.44	Защита программ и данных
5	Б1.О.57.04	Современные технологии защиты информации компьютерных систем и сетей
6	Б1.О.57.01	Инженерия программного обеспечения
7	Б1.В.10	Комплексное обеспечение безопасности компьютерных систем и сетей
8	Б2.О.02(Н)	Производственная практика (научно-исследовательская работа)
9	Б2.О.05(П)	Производственная практика (проектно-эксплуатационная)
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее		
10	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-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;	*Знать:* – основные способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; – основы физической защиты объектов информатизации. *Уметь:* – анализировать и оценивать угрозы информационной безопасности объекта *Владеть:* – методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации.
		ОПК-9.17	владеет методами расчета и инструментального контроля показателей эффективности технической защиты информации.	
ОПК-13.	*Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности*	*ОПК-13.2*	владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств	*Знать:* – общие принципы построения и использования современных языков программирования высокого уровня; – современные технологии программирования; – показатели качества программного обеспечения; – базовые структуры данных; – программные методы предотвращения несанкционированного доступа к данным; – основные программные методы защиты данных от несанкционированного доступа. *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 программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;
		ОПК-13.5	умеет работать с интегрированными средами разработки программного обеспечения;	
		ОПК-13.6	владеет навыками разработки, отладки, документирования и тестирования программ;	
		ОПК-13.9	знает показатели качества программного обеспечения;	
		ОПК-13.10	знает базовые структуры данных;	
		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	– навыками разработки, отладки, документирования и тестирования программ; – методами оценки качества готового программного обеспечения; – навыками разработки алгоритмов для решения типовых профессиональных задач.
ОПК-4.1.	*Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения)*	*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;	*<u>Знать:</u>* – языки и системы программирования, инструментальные средства применяемые при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач. *<u>Уметь:</u>* – использовать языки и системы программирования, инструментальные средства при обеспечении защиты информации в компьютерных системах при решении различных профессиональных, исследовательских и прикладных задач. *<u>Владеть:</u>* навыками применения аналитических и компьютерных моделей объектов информатизации при создании систем защиты информации.
		ОПК-4.1.5	владеет навыками применения аналитических и компьютерных моделей объектов информатизации при создании систем защиты информации;	
ОПК-4.2.	*Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения)*	*ОПК-4.2.3*	владеет навыками проведения анализа защищенности, мониторинга, аудита и обеспечения контрольных проверок функционирования и безопасности компьютерных систем и сетей;	*<u>Владеть:</u>* 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-4.3.5*	способен применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности;	*<u>Знать:</u>* – программные средства прикладного, системного и специального назначения используемые при разработке и анализе политики информационной безопасности. *<u>Уметь:</u>* – применять программные средства прикладного, системного и специального назначения при разработке и анализе политики информационной безопасности. *<u>Владеть:</u>* программными средствами прикладного, системного и специального назначения применяемыми при разработке и анализе политик 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-1.3*	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;	*<u>Знать:</u>* – 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. *<u>Уметь:</u>* – 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. *<u>Владеть:</u>* технологиями 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;	*Знать:* – методы и средства проведения анализа, теоретического и прикладного исследования уровней защищенности 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 теоретические и прикладное исследование уровней защищенности компьютерных систем и сетей. *Владеть:* навыками проведения анализа 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-3.2;*	знает методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов;	*Знать:* – методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов *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; – выполнять проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация мероприятий по обеспечению кибербезопасности; *Владеть:* навыками проведения анализа безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности.
		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;	
		ПК-3.5	выполняет проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация мероприятий по обеспечению кибербезопасности;	

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		
		В		
		ч.	ч., в форме ПП	
Всего часов	288	288	217	
в том числе:				
Контактная работа (включая НИС)	2	2	2	

Самостоятельная работа	286	286	215	
Итого:	288	288	217	

15. Содержание практики (или НИР)

п/п	Разделы (этапы) практики	Виды учебной работы	Объем учебной работы, ч	
			Контактные часы	Самостоятельная работа
1.	*Подготовительный этап*	Инструктаж по общим вопросам, по технике безопасности, составление плана работ.	0,5	10
2.	*Научно-исследовательский этап*	Выбор темы исследования; определение проблемы, объекта и предмета исследования; формулирование цели и задач исследования; теоретический анализ литературы и исследований по проблеме, подбор необходимых источников по теме (патентные материалы, научные отчеты, техническая документация и др.); составление библиографии; формулирование рабочей гипотезы.	0,5	100
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 учебной научной задачи, исследований и экспериментов.	0,5	100
4.	*Этап оформления отчёта по итогам практики*	Описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.	0,5	76

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-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;*	*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.*

		ПК-3.4 способен проводить анализ и формализацию поставленных задач в области безопасности компьютерных систем и сетей.	
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;* *ПК-3.2 знает методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов.*	*ОПК-4.1.5 владеет навыками применения аналитических и компьютерных моделей объектов информатизации при создании систем защиты информации.*
3	*Контрольно-аналитический*	*ПК-3.5 выполняет проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация мероприятий по обеспечению кибербезопасности.*	
4	*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.	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. — (Вопросы управления информационной безопасностью; Кн.1). — ISBN 978-5-9912-0361-6.
4.	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. — ISBN 978-5-241-00925-8.
5.	Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации: [учебное пособие для студ. вузов, обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян. — М.: ФОРУМ, 2009. — 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.
6.	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. — ISBN 5-9706-0019-9: 449.10 р. — URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117.
7.	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: / Э. Скудис. — Москва : ДМК Пресс, 2009 .— 512 с. — ISBN 5-94074-170-3 : 176-00 .— URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112.
8.	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. — URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf.
9.	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. — 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.
10.	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors: Обнаружение и защита / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. - 304 с.
11.	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: / Шаньгин В. Ф. — Москва: ДМК Пресс, 2010. — 544 с. — Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника». — ISBN 978-5-94074-518-1. — URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122.
12.	Астанин, Иван Константинович. Защита информации: учебное пособие для вузов / И.К. Астанин, Н.И. Астанин; Воронеж. гос. ун-т, Лискинский филиал. — Воронеж: Воронеж. гос. ун-т, 2006. — ISBN 5-9273-1080-x.

б) дополнительная литература:

№ п/п	Источник
13.	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва: Флинта: Наука, 2014. — 108 с.
14.	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.
15.	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.
16.	Системы и средства информатики: Ежегодник / Гл. ред. И.А. Соколов. — Москва: ИПИ РАН. – 2010.– Вып. 20. – № 2. — 350 с.
17.	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.
18.	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.
19.	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).
20.	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.
21.	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.
22.	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
23.	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.
24.	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.
25.	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.
26.	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. — ISBN 5-7695-2592-4.
27.	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб.: БХВ-Петербург, 2006. - 464 с.
28.	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html.
29.	Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб. : Питер, 2005. — 991 с.
30.	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.
31.	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков. — Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
32.	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). — ISBN 5-7695-2592-4.
33.	Андрианов В.И."Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие / В.А. Бородин, А.В. Соколов. – С-Пб.: Лань, 1996.
34.	Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И. Абалмазов. – М.: Гротек, 1997.
35.	Брусницин Н.А. Открытость и шпионаж / Н.А. Брусницин. – М.: Воениздат, 1991.
36.	Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В. Василевский. – М.: НПЦ "Нелк", 1998.
37.	Хорев А.А., Способы и средства ЗИ / А.А. Хорев. – МО РФ, 1998.
38.	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.
39.	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
40.	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
41.	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

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 20 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.	*Подготовительный этап*	*ОПК-9*	*ОПК-9.15*	Отчет по практике.
2.	*Научно-исследовательский этап*	*ОПК-13*	*ОПК-13.10*	Отчет по практике. Защита отчета по практике.
			ОПК-13.13	
			ОПК-13.14	
			ОПК-13.15	
			ОПК-13.17	
			ОПК-13.18	
			ОПК-13.19	
			ОПК-13.21	
		ОПК-4.1	*ОПК-4.1.3*	
		ОПК-4.3	*ОПК-4.3.5*	
		ПК-1	*ПК-1.3*	
		ПК-2	*ПК-2.2*	
			ПК-2.5	
		ПК-3	*ПК-3.2*	
			ПК-3.3	
			ПК-3.4	
3.	*Этап выполнения исследовательских работ по индивидуальному плану*	*ОПК-9*	*ОПК-9.17*	Отчет по практике. Защита отчета по практике.
		ОПК-13	*ОПК-13.2*	
			ОПК-13.5	
			ОПК-13.16	
			ОПК-13.23	
		ОПК-4.1	*ОПК-4.1.5*	
		ОПК-4.2	*ОПК-4.2.3*	
		ПК-1	*ПК-1.3*	
		ПК-2	*ПК-2.2*	
			ПК-2.5	
		ПК-3	*ПК-3.5*	
4.	*Этап оформления отчёта по итогам практики*	*ОПК-13*	*ОПК-13.6*	Отчет по практике.
			ОПК-13.9	
			ОПК-13.12	
		ПК-3	*ПК-3.4*	
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.

1. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
2. Биометрические средства идентификации и аутентификации пользователей.
3. Аутентификация субъектов в распределенных системах, проблемы и решения.
4. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
5. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
6. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
7. Метод прогонки.
8. Метод наименьших квадратов.
9. Сравнить метод Рунге-Кутты и метод Адамса заданного порядка точности.

10. Критерии оценки безопасности компьютерных систем. Структура требований безопасности. Классы защищенности.

11. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.

12. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).

13. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Отчет по практике

Оценка знаний, умений и навыков, характеризующих этапы формирования компетенций, при прохождении практики проводится в ходе промежуточной аттестаций. Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Темы индивидуальных проектов

1. Принципы построения систем защиты информации.
2. Актуальность проблемы обеспечения безопасности в информационном обществе.
3. Средства обеспечения информационной безопасности в корпоративных информационных системах
4. Аппаратные средства обеспечения информационной безопасности
5. Информационные уязвимости объектов
6. Программные средства обеспечения информационной безопасности
7. Антропогенные информационные уязвимости
8. Техногенные информационные уязвимости
9. Организационно-правовые средства обеспечения информационной безопасности
10. Угрозы информационной безопасности и их источники
11. Организационно-административные средства защиты информации
12. Основные причины утечки информации.
13. Политика безопасности. Основные типы политики безопасности.
14. Меры защиты персональных данных в информационных системах.
15. Использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
16. Научно-технические проблемы защиты информационных ресурсов, информационных и телекоммуникационных систем;
17. Общеметодологические проблемы кадрового обеспечения информационной безопасности;
18. Нарушение законных ограничений на распространение информации;
19. Противоправные сбор и использование информации;
20. Адаптивные системы защиты информации.

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»:

- 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 – 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 %.

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*	*Удовлетвори-тельно*
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.	–	*Неудовлетвори-тельно*

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

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-9.17 владеет методами расчета и инструментального контроля показателей эффективности технической защиты информации.

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

ОПК-13.2 владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств

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

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

ОПК-13.9 знает показатели качества программного обеспечения;

ОПК-13.10 знает базовые структуры данных;

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 (по областям применения)

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-4.1.5 владеет навыками применения аналитических и компьютерных моделей объектов информатизации при создании систем защиты информации;

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

ОПК-4.2.3 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-4.3.5 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-1.3 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-3.2 знает методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов;

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;

ПК-3.5 выполняет проверку устойчивости приложений к внешнему несанкционированному доступу, в том числе проверка устойчивости веб-приложений к атакам, применение средств контроля безопасности, управление криптографическими средствами, а также организация мероприятий по обеспечению кибербезопасности.

Вопросы с вариантами ответов

1. Объект защиты информации это…

А) информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности

Б) информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации

В) объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности

Г) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

2. Как называется доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами?

- мандатный доступ;
- атака;
- **несанкционированный доступ.**

3. Как называется способ защиты информации от утечки через ПЭМИН, основанный на локализации электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами?

- **экранирование;**
- подавление;
- зашумление.

4. Как называются методы защиты акустической информации, предусматривающие подавление технических средств разведки?

- пассивные;
- **проактивные;**
- **активные.**

5. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

- Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- **Улучшить контроль за безопасностью этой информации**
- Снизить уровень классификации этой информации

6. Где применяются средства контроля динамической целостности?

- **анализе потока финансовых сообщений**
- обработке данных
- **при выявлении кражи, дублирования отдельных сообщений**

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

- с глобальным хищением информации
- с появлением интернета

- **с недостаточной образованностью в области безопасности**

8. Нестандартность, разнообразность - это общие требования к защите информации (1) или требование, предъявляемое к системе безопасности информации (2), или условие, которому должна удовлетворять система защиты информации (3)?
- (1).
- (2).
- **(3).**
- Ни одно из этих понятий.

9. Комплексность - это общие требования к защите информации (1) или требование, предъявляемое к системе безопасности информации (2), или условие, которому должна удовлетворять система защиты информации (3)?
- **(1).**
- (2).
- (3).
- Ни одно из этих понятий.

10. Какие цели преследует защита информации?
цели защиты информации - недопущение "взлома" данных, хранящихся в компьютере.
- **целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при их разработке, производстве и применении информационных систем, технологии и средств их обеспечения**

11. Является ли данное свойство особенностью информации?
- **размерность.**
- непрерывность.
- дискретность.
- наглядность.
- **ценность.**

12. Что является составной частью концепции и структуры защиты информации?
- **Развитый ассортимент технических средств защиты информации, производимых на промышленной основе.**
- **Значительное число имеющих необходимые лицензии организаций, специализирующихся на решении вопросов защиты информации.**
- **Большой практический опыт решения проблем в рассматриваемой области.**

13. Какой атаки на ARP протокол не существует?
- ARP Spoofing;
- **ARP Stuffing;**
- ARP Sniffing.

14. Расположите в порядке следование модели OSI типы атак
- **DNS Sniffing;**
- ARP Spoofing;
- **XSS.**

15. Используется ли условная вероятность в методах обнаружения злоупотреблений?

- **да;**
- нет.

16. Является ли система обнаружения вторжений активным компонентом по защите от угроз?
- да;
- **нет.**

17. В перечень этапов проведения аудита ИС входит:
- **выработка рекомендаций**
- **сбор информации для аудита**
- выявление недостатков при обработке информации
- **выработка рекомендаций**

18. Результаты проведения аудита подразделяются на:
- **организационные**
- **технические**
- программные
- **методологические**

19. Оценка рисков для ИС производится с помощью следующих шкал**:**
- **количественной**
- **логарифмической**
- **качественной**
- матричной

20. Отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью – это:
- **целостность;**
- единство;
- синтез;
- полнота.

21. Какой из методов основан на добавлении избыточной информации к передаваемому слову?
- **метод Хемминга;**
- метод Давида Слепянина;
- метод Хоквингема.

22. К полиалфавитным шифрам относятся:
- шифр Плейфера;
- шифр Хилла;
- шифр Бофора;
- **все перечисленные шифры.**

23. Какой нормативный акт является основным в сфере регулирования электронной под-писи:
- федеральный закон №1-ФЗ от 10.01.2002 «Об электронной цифровой подписи»;
- ***федеральный закон №63-ФЗ от 06.04.2011 «Об электронной подписи»;***
- постановление Правительства Российской Федерации № 111 от 9 февраля 2012 г. «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой».

24. В каких типах криптоатак используется метод "опробования"? (Укажите несколько верных вариантов ответа.)

а) криптоатака с использованием криптограмм;

б) криптоатака с использованием открытых текстов и соответствующих криптограмм;

в) криптоатака с использованием выбираемых криптоаналитиком открытых текстов и соответствующих криптограмм;

г) все ответы верны.

25. Время, затрачиваемое алгоритмом для решения задачи, рассматриваемое как функция размера задачи или количества входных данных, – это:

а) временная сложность;

б) время воспроизведения алгоритма;
в) время решения алгоритма.

26. Отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью – это:

а) целостность;
б) единство;
в) синтез;
г) полнота.

27. Двойной DES не используется, потому что

(1) недостаточна длина ключа
(2) существует атака «встреча посередине», которая позволяет снизить стойкость алгоритма до стойкости простого DES
(3) слишком увеличивается сложность вычислений

28. Атака "вмешательство" — это угроза:

(1) готовности
(2) целостности
(3) конфиденциальности
(4) секретности

29. В DES последний раунд при первом способе шифрования и обратного дешифрования отличается от других:

(1) применением смесителя
(2) отсутствием устройства замены
(3) применением устройства замены и смесителя
(4) применением устройства замены

30. Протоколирование и аудит могут использоваться для:

(1) предупреждения нарушений ИБ
(2) обнаружения нарушений
(3) восстановления режима ИБ

31. Сигнатурный метод выявления атак хорош тем, что он:

(1) поднимает мало ложных тревог
(2) способен обнаруживать неизвестные атаки
(3) прост в настройке и эксплуатации

32. Для чего используются средства создания хэщ-сумм файлов и данных при расследовании компьютерных инцидентов?

- для обнаружения несанкционированного доступа на чтение;
- **для обнаружения нарушения целостности;**
- для обнаружения нарушения доступности.

33 На какой класс SOC по локализации функций следует ориентироваться компании для развертывания SOC в течение нескольких месяцев?

- Внутренний
- **Внешний**
- Гибридный
- Любой из вышеперечисленных

34 Какую модель рекомендуется использовать при реагировании на инциденты кибербезопасности?

- ITIL
- COBIT
- **Cyber Kill-Chain**
- TIP

35 Протоколирование – это

a) Сбор и накопление информации о событиях ИС
b) Ведение документов
c) Все из перечисленного
d) Ничего из перечисленного

36. На основании чего разрабатывается Положение о реагировании на инциденты?

- на основании модели угроз безопасности;
- на основании модели производственных процессов и активов;

- **на основании политики информационной безопасности.**

37. Чем определяется процедура и методы расследования компьютерных инцидентов в организации?
- требованиями уголовно-процессуального кодекса РФ;
- **утвержденными внутренними регламентами организации;**
- техническими возможностями организации.

38. Какие из средств обеспечивают наиболее полное расследование компьютерных инцидентов?
- **системы обнаружения и предотвращения вторжений;**
- списки управления доступом на маршрутизаторах;
- системы шифрования трафика.

39. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
1. Внедрение управления механизмами безопасности
2. Классификацию данных после внедрения механизмов безопасности
3. **Уровень доверия, обеспечиваемый механизмом безопасности**
4. Соотношение затрат / выгод

40. Система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения – криптосисема ...

+ асимметричная
+ с открытым ключом

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).