МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
_____ И.М. Ажмухамедов

_____

«06» июня 2024 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой ИБ
_____ Т.Г. Гурская
протокол заседания кафедры № 9
«06» июня 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Безопасность мобильных приложений

Составитель	**Демина Р.Ю., к.т.н., доц., доцент кафедры ИБ**
Направление подготовки	**09.04.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ**
Направленность (профиль) ОПОП	**Разработка мобильных приложений**
Квалификация (степень)	**магистр**
Форма обучения	**очно-заочная**
Год приема	**2022**
Курс	**3**
Семестр	**5**

Астрахань – 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Целями освоения дисциплины «Безопасность мобильных приложений» являются: формирование у студентов знаний и умений в области обеспечения безопасности информации мобильных приложениях, а также навыков работы со встроенными средствами защиты.

1.2. Задачи освоения дисциплины:

- изучение основных встроенных механизмов защиты информации в мобильных приложениях;
- приобретение практических навыков выбора и обоснованием рационального решения по защите информации мобильных приложений с учетом заданных требований.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина Б1.Д.03.01 «Безопасность мобильных приложений» относится к части, формируемой участниками образовательных отношений и осваивается в 5 семестре.

2.2. Для изучения данной дисциплины студенту необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами:

– *Модели информационных процессов и систем:* изучены методы формализации и схематизации задач, используемые для построения моделей информационных процессов и систем; приобретены необходимые теоретические знания и практические навыки, относящиеся к реализации моделей информационных процессов и систем в виде программ для имитационного моделирования на ЭВМ.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

- Выпускная квалификационная работа
- Научно-исследовательская работа
- Производственная практика

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки:

профессиональных (ПК):

ПК-2. Способен разрабатывать, вводить в действие и обслуживать базы данных; дополнять, модифицировать и совершенствовать базы данных и другие хранилища информации.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	**Уметь (2)**	**Владеть (3)**
ПК-2 Способен разрабатывать, вводить в действие и обслуживать базы данных; дополнять, модифицировать и совершенствовать базы данных и другие хранилища информации	ИПК.2.1.1 современные тенденции, технологии и регламенты интеграции БД на новые платформыи версии ПО.	ИПК 2.2.1 проводить анализ системных проблем обработки информации на уровне БД ИПК 2.2.1 формировать предложения по перспективному развитию БД, осуществлять контроль обновлений БД.	ИПК 2.3.1. навыками внедрения в практику администрирования новыхтехнологий работы с БД, осуществлять их обслуживание

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Объем дисциплины (модуля) 3 з.е., 108 часов, 33 часа выделено на контактную работу обучающихся с преподавателем (лекции – 11, лабораторные работы – 22), 75 часа – на самостоятельную работу обучающихся.

Таблица 2– Структура и содержание дисциплины

№ п/п	Наименование раздела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)*
				Л	ПЗ	ЛР	КР	СР	
1	Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	4	1	1		3		9	Лабораторная работа №1, устный опрос
2	Тема 2. Построение системы защиты информации в организации	4	1	1		3		9	Тест, устный опрос
3	Тема 3. Современные методики анализа и управления рисками информационной безопасности	4	2	1		3		9	Лабораторная работа №2, устный опрос
4	Тема 4. Классификация и методы оценки угроз информационной безопасности от	4	3	1		3		9	Контрольная работа №1, устный опрос

	мобильных устройств								
5	Тема 5. Защита мобильных устройств	4	4	1		3		9	Лабораторная работа №3, устный опрос
6	Тема 6. Внедрение систем MDM (Mobile Device Management), как составная часть стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств	4	4	2		3		9	Лабораторная работа №4, устный опрос
7	Тема 7. Решение типовых проблем защиты мобильных устройств в корпоративной среде на примере использования Trend Micro Mobile Security	4	5	2		4		9	Лабораторная работа № 5, устный опрос
8	Тема 8. Современные тенденции и направления развития методов и средств защиты от мобильных угроз	4	6	2		4		12	Контрольная работа №2, устный опрос
ИТОГО		**108**		**11**		**22**		**75**	**ЗАЧЕТ**

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Темы дисциплины	**Кол-во часов**	**Компетенции**	**Σ общее кол-во компетенций**
		ПК-2	
Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасностиРФ	13	+	1
Тема 2. Построение системы защиты информации в организации	13	+	1
Тема 3. Современные методики анализа и	13	+	1

управления рисками информационной безопасности			
Тема 4. Классификация иметоды оценки угроз информационной безопасности от мобильных устройств	13	+	1
Тема 5. Защита мобильных устройств	13	+	1
Тема 6. Внедрение систем MDM (Mobile Device Management), как составная часть стратегии обеспечениябезопасности конфиденциальной информации при использовании мобильных устройств	14	+	1
Тема 7. Решение типовых проблем защиты мобильныхустройств в корпоративной среде на примере использования Trend Micro Mobile Security	15	+	1
Тема 8. Современные тенденции и направления развития методов и средств защиты от мобильных угроз	18	+	1
ИТОГО:	**108**		

Содержание дисциплины

Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ

Основные положения теории информационной безопасности: информация и информационные отношения; субъекты информационных отношений, их безопасность. Три вида возможных нарушений ИС. Определение требований к защищенности информации. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения». ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем». ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»

Тема 2. Построение системы защиты информации в организации

Понятие угрозы. Защита. Классификация угроз и мер защиты информации. Таксономия нарушений ИБ вычислительной системы и причины, обуславливающие их существование. Состав и содержание средств защиты, объекты и элементы защиты. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем». ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Тема 3. Современные методики анализа и управления рисками информационной безопасности

Классификация каналов проникновения в систему и утечки информации. Неформальная модель нарушителя в АС. Виды противников или «нарушителей». Анализ

способов нарушений ИБ. Понятия о видах вирусов. ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования». ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности». ISO/IEC 27000:2009 – СУИБ: определения и основные принципы.

Тема 4. Классификация и методы оценки угроз информационной безопасности от мобильных устройств

Задачи системы безопасности. Меры противодействия угрозам безопасности. Классификация мер. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные механизмы защиты АС. Модели безопасности и их применение. ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001–2006 – требования к СУИБ ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799–2005 – практические правила управления ИБ. ISO/IEC 27003:2010 – руководство по внедрению СУИБ. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004–2011 – оценка функционирования СУИБ.

Тема 5. Защита мобильных устройств

Основные технологии построения защищенных ЭИС. Место ИБ экономических систем в национальной безопасности страны. Концепция ИБ. Особенности работы с персоналом, владеющим конфиденциальной информацией. Технологические основы обработки конфиденциальных документов. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010 – управление рисками ИБ. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006–2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ. ISO/IEC 27011:2008 – руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002

Тема 6. Внедрение систем MDM (Mobile Device Management), как составная часть стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств

Методы криптографии. Классификация шифров по различным признакам. Шифры перестановки. Шифры замены. Шифры гаммирования. Надежность шифров. ISO/IEC 27033 – управление безопасностью сетей. ISO/IEC 27035:2011 – управление инцидентами ИБ. ISO/IEC 27037 – руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме. ISO/IEC 13335 – методы и средства обеспечения безопасности информационных технологий. ISO/IEC 15408 и ISO/IEC 18045:2008 – общие критерии и методология оценки безопасности информационных технологий. ISO 19011:2011 и ГОСТ Р ИСО 19011–2003 – рекомендации по аудиту систем менеджмента

Тема 7. Решение типовых проблем защиты мобильных устройств в корпоративной среде на примере использования Trend Micro Mobile Security

Международные стандарты информационного обмена. ИБ в условиях функционирования в России глобальных сетей. Назначение и задачи в сфере обеспечения ИБ на уровне государства. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса. СТО БР ИББС-1.0 – общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации. СТО БР ИББС-1.1 – аудит ИБ 78. СТО БР ИББС-1.2 – методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. Рекомендации по стандартизации Р 50.1.053-2005.

Тема 8. Современные тенденции и направления развития методов и средств защиты от мобильных угроз

Информационные технологии. Основные термины и определения в области технической защиты информации. (утв. Приказом Ростехрегулирования от 06.04.2005 № 77-ст). Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 29.12.2005 №

479-ст).

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

Для успешного освоения дисциплины является обязательным посещение всех занятий, выполнение домашнего задания и иных форм самостоятельной работы, которые назначаются преподавателем.

Особенность изучения дисциплины состоит из лекций с элементами беседы. Такая лекции эффективны тем, что предусматривают использование вопросно-ответной формы подачи материала, то есть преподаватель использует приемы скрытого диалога, когда лектор с помощью студентов отвечает на поставленные проблемные вопросы. А также выполнение комплекса лабораторных работ, главной задачей которых является получение навыков самостоятельной работы на компьютерах с использованием современных информационных систем и программного обеспечения для решения различных учебных и профессиональных задач.

Методическая поддержка дисциплины обеспечивается использованием дистанционных технологий. Студентам предлагается информационный ресурс, расположенный по адресу: http://moodle.asu.edu.ru, на сервере дистанционного обучения АГУ. Доступ студентов к учебным ресурсам осуществляется по учетной записи и паролю после регистрации на курс «Инженерия информационных систем» на период обучения по данной дисциплине.

На сервере размещен методический материал по данной дисциплине, в содержание которого входит:

- теоретический материал;
- мультимедийные презентации по тематикам лекций;
- задания и указания по выполнению лабораторно-практических работ, требования к содержанию и их оформлению, рекомендации по их защите;
- тестовые вопросы, предназначенные всех видов контроля, включая самоконтроль освоения учебного материала;
- вопросы к экзамену.

Аудиторные занятия проводятся на основе теоретического материала, опубликованного на образовательном портале, это позволяет студентам изучить пропущенный материал или самостоятельно разобраться с темой, не освоенной на занятии.

Для исключения отрыва студентов от учебного процесса проводится учет посещаемости аудиторных занятий.

5.1. Указания для обучающихся по освоению дисциплины (модуля)

Самостоятельная работа по освоению дисциплины включает:

– для овладения знаниями: изучение дополнительной учебной литературы и посещение Интернет-ресурсов;

- для закрепления и систематизации знаний: работа с материалами лекций (обработка текста), самоконтроль изученного теоретического материала, подготовка к тестированию и промежуточной аттестации (экзамену (2 семестр));

Планирование времени, необходимого на изучение дисциплин, студентам лучше всего осуществлять весь семестр, предусматривая при этом регулярное повторение материала.

При изучении дисциплины сначала необходимо по каждой теме прочитать рекомендованную литературу и составить краткий конспект основных положений,

терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме для освоения последующих тем курса. Для расширения знания по дисциплине рекомендуется использовать Интернет-ресурсы; проводить поиски в различных системах и использовать материалы сайтов, рекомендованных преподавателем.

Содержание самостоятельной работы обучающегося приведено в таблице 4.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер раздела (темы)	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
1	Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	9	Изучение учебной литературы и материалов лекций, самоконтроль
2	Тема 2. Построение системы защиты информации в организации	9	Изучение учебной литературы и материалов лекций, самоконтроль
3	Тема 3. Современные методики анализа и управления рисками информационной безопасности	9	Изучение учебной литературы и материалов лекций, самоконтроль
4	Тема 4. Классификация и методы оценки угроз информационной безопасности от мобильных устройств	9	Изучение учебной литературы и материалов лекций, самоконтроль
5	Тема 5. Защита мобильных устройств	9	Изучение учебной литературы и материалов лекций, самоконтроль
6	Тема 6. Внедрение систем MDM (Mobile Device Management), как составная часть стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств	9	Изучение учебной литературы и материалов лекций, самоконтроль
7	Тема 7. Решение типовых проблем защиты мобильных устройств в корпоративной среде на примере использования Trend Micro Mobile Security	9	Изучение учебной литературы и материалов лекций, самоконтроль
8	Тема 8. Современные тенденции и направления развития методов и средств защиты от мобильных угроз	12	Изучение учебной литературы и материалов лекций, самоконтроль

5.2. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно:

Одним из видов письменных работ является самостоятельное подготовка отчетов по выполненным лабораторным работам. Отчет оформляется с помощью любого текстового редактора и должен содержать: описание процесса выполнения работы с предоставлением промежуточных и итоговых результатов. Результаты должны быть представлены, как в текстовом, так и в графическом виде.

Также в процессе обучения студенты выполняют группой проект. Отчет по проекту должен оформляться в электронном и печатном виде на листах формата А4 и содержать задание, краткие необходимые теоретические сведения, полученные по каждому пункту задания результаты и выводы. К оформлению отчета предъявляются стандартные требования.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Лекционные занятия организуются с применением традиционных и инновационных технологий организации учебной деятельности студентов.

На лекциях рассматриваются теоретические основы информатики и вычислительной техники, примеры решения практических задач. Обеспечивается демонстрационная поддержка изложения курса в форме компьютерной презентации. Это способствует передаче большего количества учебного материала обучающимся во время аудиторных занятий и более доходчивому его освоению. В то же время, для студентов первого курса рекомендуется практические примеры разбирать, пользуясь традиционной технологией «доски и мела», поскольку это позволяет включить обучаемого в процесс решения задачи.

Лабораторные работы выполняются студентами с применением ПК и ориентированы на формирование деятельностных компетентностей. Они заключаются в выполнении сквозного цикла лабораторных работ. В процессе выполнения лабораторных работ достигаются следующие цели:

- изучаются программные средства и технологии обработки информации;
- формируются практические навыки обработки информации различного вида и формы при решении конкретных практических задач;
- формируется навык выявления ошибочных и нештатных ситуаций и реагирования на них.

На лабораторных занятиях студент вначале знакомится с содержанием работы, пользуясь электронными методическими материалами, размещенными на http://moodle.asu.edu.ru, затем выполняет задание и показывает результаты преподавателю. Лабораторные работы, выполняются студентом самостоятельно, возникающие при их выполнении проблемы разрешаются в рамках учебного времени и индивидуальных и групповых консультаций. Для выставления баллов по итогам выполнения ЛР, студенты прикрепляют файлы с выполненными работами и отчеты на образовательный портал.

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы, устный опрос
Тема 2. Построение системы защиты информации в организации	Лекция - презентация	Не предусмотрено	Выполнение теста, устный опрос
Тема 3. Современные методики анализа и управления рисками информационной безопасности	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы, устный опрос
Тема 4. Классификация и методы оценки угроз	Обзорная лекция	Не предусмотрено	выполнение контрольной

информационной безопасности от мобильных устройств			работы, устный опрос
Тема 5. Защита мобильных устройств	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы,устный опрос
Тема 6. Внедрение систем MDM(Mobile Device Management), каксоставная часть стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы,устный опрос
Тема 7. Решение типовых проблем защиты мобильных устройств в корпоративной среде на примере использования Trend Micro Mobile Security	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы,устный опрос
Тема 8. Современные тенденции инаправления развития методов и средств защиты от мобильных угроз	Лекция - презентация	Не предусмотрено	выполнение контрольной работы, устный опрос

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

6.2. Информационные технологии

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии*:*

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Цифровое обучение») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения (программного средства)	Назначение программного средства
Adobe Reader	Программа для просмотра электронных документов
Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Пакет офисных программ
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
KOMPAS-3D V13	Создание трехмерных ассоциативных моделей отдельных элементов и сборных конструкций из них
Blender	Средство создания трехмерной компьютерной графики
Cisco Packet Tracer	Инструмент моделирования компьютерных сетей
Google Chrome	Браузер
Far Manager	Файловый менеджер
Notepad++	Текстовый редактор
OpenOffice	Пакет офисных программ
Opera	Браузер

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «*Безопасность мобильных приложений*» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие изучаемых разделов, результатов обучения и оценочных средств

№ п/п	Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства

1.	Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	ПК-2	Лабораторная работа №1, устный опрос
2.	Тема 2. Построение системы защиты информации в организации	ПК-2	Тест, устный опрос
3.	Тема 3. Современные методики анализа и управления рисками информационной безопасности	ПК-2	Лабораторная работа №2, устный опрос
4.	Тема 4. Классификация и методы оценки угроз информационной безопасности от мобильных устройств	ПК-2	Контрольная работа №1, устный опрос
5.	Тема 5. Защита мобильных устройств	ПК-2	Лабораторная работа №3, устный опрос
6.	Тема 6. Внедрение систем MDM (Mobile Device Management), как составная часть стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств	ПК-2	Лабораторная работа №4, устный опрос
7.	Тема 7. Решение типовых проблем защиты мобильных устройств в корпоративной среде на примере использования Trend Micro Mobile Security	ПК-2	Лабораторная работа № 5, устный опрос
8.	Тема 8. Современные тенденции и направления развития методов и средств защиты от мобильных угроз	ПК-2	Контрольная работа №2, устный опрос

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

При решении комплексной ситуационной задачи можно использовать следующие критерии оценки:

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

В рабочей программе приведены фрагменты практических заданий. Полнотекстовые задания представлены на образовательном портале вуза, курс «*Безопасность мобильных приложений*».

Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ

Лабораторная работа 1

Под **несанкционированным доступом к информации** (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

- организационные;
- технологические;
- правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка

предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя, В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

- индивидуального объекта заданного типа;
- знаний некоторой известной только ему и проверяющей стороне информации;
- индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников.

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они изависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь"). Особым

подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя — некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя — некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя — совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под **парольной системой** будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей. Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности; база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем:

Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Задания.

1. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов.

Длина пароля символов k.

Скорость перебора s паролей в секунду.

После каждого из m неправильно введенных паролей идет пауза в v секунд

вариант	n	k	s	m	v
1	33	10	100	0	0
2	26	12	13	3	2
3	52	6	30	5	10
4	66	7	20	10	3
5	59	5	200	0	0
6	118	9	50	7	12
7	128	10	500	0	0
8	150	3	200	5	3
9	250	8	600	7	3
10	500	5	1000	10	10

Тема 2. Построение системы защиты информации в организации

Тест

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

1. По объекту воздействия угрозы бывают:

- воздействующие на информационную среду в целом
- воздействующие на отдельные элементы информационной среды
- активные
- пассивные

2. Выберите правильный вариант ответа. Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий (информационной безопасности), имеющих значительную вероятность компрометации бизнесоперации и создания угрозы

- инцидент
- нарушение
- сигнал

3. Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности называется

- событием (информационной безопасности)
- инцидентом (информационной безопасности) угрозой (информационной безопасности)

4. Первым шагом в управлении сетью является ее

- документирование
- ревизия
- оформление

5. Какова цель ревизии эффективности?

- Мониторинг и анализ работы сети.
- Определение того, работает ли сеть в соответствии со своим потенциалом.
- Идентификация типов оборудования и устройств, сети.
- Обеспечение информации о восстановлении после сбоя или катастрофического отказа.

Тема 3. Современные методики анализа и управления рисками информационной безопасности

Лабораторная работа 2

Архивирование с паролем

Необходимо создать текстовый файл, содержащий фамилию, имя, отчество студента

в объеме 50 записей. Провести архивирование файла. Любым редактором внести изменения согласно задания. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.

Провести архивацию файла с паролем. Внести искажения, попробовать разархивировать. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.

Провести архивацию файла с паролем, состоящим из 3-х цифр. Провести попытку подбора пароля с использованием программного обеспечения. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения, время подбора.

Варианты:

архиватор zip. Искажение двух байт.
архиватор arj. Искажение трех байт.
архиватор rar. Искажение трех байт.
архиватор zip. Удаление двух байт.
архиватор arj. Удаление трех байт.
архиватор rar. Удаление трех байт.
архиватор arj. Добавление трех байт.
архиватор rar. Добавление трех байт.
архиватор zip. Добавление двух байт.
архиватор zip. Удаление двух байт.

Тема 4. Классификация и методы оценки угроз информационной безопасности от мобильных устройств

Контрольная работа №1

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений»
2. Категорирование информации
3. Задание требований к информационной безопасности организации
4. Понятие угрозы информационной безопасности. Классификация угроз ИБ
5. Состав средств и мер защиты информации. Классификация средств и мер защиты информации
6. Объект и субъект защиты информации
7. Каналы утечки информации. Классификация каналов утечки информации
8. Модель нарушителя информационной безопасности
9. Классификация нарушителей информационной безопасности
10. Компьютеные «Вирусы». Их виды
11. Способы борьбы с компьютерными вирусами

Тема 5. Защита мобильных устройств

Лабораторная работа №3

Составьте алгоритмическое и программное обеспечение:

1. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.
2. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и текстового файла. Учтите регистр вводимого текста.
3. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.
4. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и текстового файла. Учтите регистр вводимого текста.
5. Постройте программно таблицу Вижинера и выведите в файл.

Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

Тема 6. Внедрение систем MDM (Mobile Device Management), как составная часть стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств

Лабораторная работа №4

Составьте программное обеспечение, реализующее алгоритм обмена ключами. Ключи должны автоматически формироваться в файлы. Должна быть обеспечена наглядность выполнения алгоритма. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

Тема 7. Решение типовых проблем защиты мобильных устройств в корпоративной среде на примере использования Trend Micro Mobile Security

Лабораторная работа №5

Составьте программное обеспечение, реализующее алгоритм RSA. Исходные данные должны передаваться через файлы: файл с открытым ключом, закрытым ключом

и шифруемая информация. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

Тема 8. Современные тенденции и направления развития методов и средств защиты от мобильных угроз

Контрольная работа №2

1. Определение понятия «Система информационной безопасности»
2. Элементы системы информационной безопасности
3. Определение понятия «Государственная тайна»
4. Регулирование правовых отношений в области защиты государственной тайны
5. Модели безопасности их применение
6. Место ИБ экономических систем в национальной безопасности страны
7. Основы конфиденциального документооборота
8. Особенности работы с персоналом, владеющим конфиденциальной информацией
9. Принципы построения защищенных компьютерных систем
10. Элементы операционной системы
11. Управление доступом пользователей в опреационных системах
12. Парольная политика популярных операционных систем
13. Состав локально-вычислительных сетей
14. Коммутаторы, концентраторы, маршрутизаторы
15. Организация доступа в локальных сетях
16. Контроль сетевых подключений
17. Управление сетевой маршрутизацией
18. Управление доступом к компьютерам
19. Система управления паролями
20. Управление доступом к приложениям
21. Управление доступом к библиотекам исходных текстов программ

Примерный перечень вопросов к зачету

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений»
2. Категорирование информации
3. Задание требований к информационной безопасности организации
4. Виды возможных нарушений информационной системы. Общая классификация информационных угроз.
5. Угрозы ресурсам компьютерной безопасности. Угрозы, реализуемые на уровне локальной компьютерной системы. Человеческий фактор.
6. Угрозы компьютерной информации, реализуемые на аппаратном уровне.
7. Удаленные атаки на компьютерные системы. Причины уязвимостей компьютерных сетей.
8. Состав средств и мер защиты информации. Классификация средств и мер защиты информации
9. Объект и субъект защиты информации
10. Каналы утечки информации. Классификация каналов утечки информации
11. Модель нарушителя информационной безопасности 12. Классификация нарушителей информационной безопасности
13. Компьютерные вирусы. История. Определение по УК РФ.

14. Определение понятия «Система информационной безопасности»
15. Элементы системы информационной безопасности
16. Определение понятия «Государственная тайна»
17. Регулирование правовых отношений в области защиты государственной тайны
18. Модели безопасности их применение
19. Место ИБ экономических систем в национальной безопасности страны
20. Основы конфиденциального документооборота
21. Особенности работы с персоналом, владеющим конфиденциальной информацией
22. Принципы построения защищенных компьютерных систем
23. Элементы операционной системы
24. Управление доступом пользователей в операционных системах
25. Парольная политика популярных операционных систем
26. Состав локально-вычислительных сетей
27. Коммутаторы, концентраторы, маршрутизаторы
28. Организация доступа в локальных сетях
29. Контроль сетевых подключений
30. Управление сетевой маршрутизацией
31. Управление доступом к компьютерам
32. Система управления паролями
33. Управление доступом к приложениям
34. Управление доступом к библиотекам исходных текстов программ
35. Правовое урегулирование защиты информации. Стандарты ИБ
36. Защита данных криптографическими методами. Методы шифрования.
37. Защита данных криптографическими методами. Алгоритмы шифрования.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ПК-2. Способен разрабатывать, вводить в действие и обслуживать базы данных; дополнять, модифицировать и совершенствовать базы данных и другие хранилища информации				
1.	Задание закрытого типа	Мобильная ОС – это (специально разработанное) программное обеспечение, которое позволяет смартфонам, планшетам и другим (беспроводным) устройствам выполнять приложения и программы 1. Мобильная ОС 2. Портативное (мобильное) вычислительное устройство 3. Средство вычислительной техники. 4. Персональный компьютер	1	2
2.		Концепция применения мобильных технологий, подразумевающая, что организация приобретает и обслуживает вычислительные устройства (в т.ч. мобильные), используемые и управляемые работниками, обычно с разрешением на использование этого устройства также и в личных целях 1. Корпоративное устройство, управляемое пользователем (COPE) 2. Устройство BYOD 3. Корпоративное устройство (EMM)	1	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		4. Мобильная ОС		
3.		Концепция применения мобильных технологий, при которой любое устройство, находящееся в собственности пользователя, может использоваться где угодно, как в личных, так и в служебных целях 1. Корпоративное устройство, управляемое пользователем (COPE) 2. Устройство BYOD 3. Корпоративное устройство (EMM) 4. Мобильная ОС	2	3
4.		Ресурс, находящийся вне организации, доступ или использование которого обеспечивается через Интернет, другую публичную или частную сеть 1. Облачный сервис 2. Устройство BYOD 3. Корпоративное устройство (EMM) 4. Мобильная ОС	1	3
5.		Метод разработки и/или размещения и управления мобильными приложениями, который ограничивает среду выполнения определенного кода. 1. «Песочница» или контейнер приложений 2. «Двойной профиль» 3. «Кодовый контейнер» 4. «Упаковка приложений»	1	3
6.	Задание открытого типа	Что такое «Мобильные технологии»?	«Мобильные технологии» – это совокупность: • технических средств (включая средства управления, контроля и обеспечения без-опасности); • организационно-распорядительных мероприятий и документов; • персонала обеспечения; • комплекса стандартов, протоколов, способов и методов, обеспечивающих передачу голоса и данных по беспроводным каналам связи от абонента до абонента или от абонента до (корпоративной, ведомственной, публичной и др.) информационной и/или вычислительной системы, а также межмашинное взаимодействие	5
7.		Что включают технические составляющие, обеспечивающие функционирование корпоративных мобильных технологий?	Технические составляющие, обеспечивающие функционирование корпоративных мобильных технологий, включают: 1. Одно или более мобильных устройств, управляемых пользователями (абонентами) – работниками организации. 2. Беспроводная среда передачи данных: Wi-Fi, сотовая (GSM/ GPRS/ EDGE/ 3G/ LTE и аналогичные), спутниковая и др., обеспечиваемая одним или несколькими операторами связи – от абонента до приемного устройства оператора связи. 3. Канал передачи данных от сети	6

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			оператора связи до объекта доступа (ресурс в корпоративной, ведомственной, общедоступной или другой сети). 4. Корпоративная информационная система, включая приложения и данные. 5. Сторонние информационные системы, доступ пользователя (работника организации) к которым осуществляется посредством мобильных устройств (публичные, ведомственные и др., исключая корпоративные) – если это разрешено политикой организации.	
8.		Набор базовых характеристик любого мобильного устройства	Набор базовых характеристик любого мобильного устройства: 1. Малые геометрические размеры и вес. 2. Наличие, как минимум, одного беспроводного интерфейса сетевого доступа (для передачи голоса и данных): интерфейс Wi-Fi, сотовой связи или другой для подключения устройства к сетевой инфраструктуре оператора связи с возможностью подключения к сети Интернет или к другой сети передачи данных. 3. Специализированная мобильная операционная система (ОС). 4. Наличие встроенных в мобильную ОС функций для синхронизации данных (со стационарным компьютером или ноутбуком, с серверами организации, поставщиками услуг или третьими сторонами и т.п.).	6
9.		Основные модели управления мобильными услугами	Основные модели управления мобильными услугами: 1. Самостоятельное (или внутреннее) управление (on-premise): – управление мобильной инфраструктурой, находящейся внутри организации, силами работников самой организации; – внешнее управление мобильной инфраструктурой, находящейся внутри организации, силами сторонней сервисной компании (outsourcing). 2. Облачное (cloud) управление.	8
10.		На какие области может быть разделено обеспечение мобильной безопасности?	Обеспечение мобильной безопасности может быть разделено на несколько перечисленных ниже областей. • Доступ к данным. Должен быть обеспечен только авторизованный доступ работников – пользователей мобильных устройств к корпоративным данным. • Передача данных. Должен быть обеспечен защищенный канал передачи данных. • Хранение данных. Должна быть	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			обеспечена защита хранящихся на мобильном устройстве данных. • Защита устройства. Должна быть обеспечена защита собственно мобильного устройства от несанкционированного использования • Безопасность использования. Обеспечение безопасности при конфигурировании, инициализации, внедрении, управлении и контроле мобильных решений. Ниже перечислены наиболее часто применяющиеся меры обеспечения безопасности мобильных вычислений..	

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Оценка качества освоения дисциплины в ходе текущей и промежуточной аттестации обучающихся осуществляется в соответствии с «Положением о балльно-рейтинговой системе оценки учебных достижений студентов» (приказ от 13.01.2014 № 08-01-01/08).

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	5/10	50	По расписанию
2.	*Выполнение контрольной работы*	2/10	20	
3.	*Устный опрос*	6/2	12	
4.	*Тест*	1/8	8	
Всего			**90**	-
Блок бонусов				
5.	*Посещение занятий без пропусков*	1	3	
6.	*Своевременное выполнение всех заданий*	1	3	
7.	*Активность студента на занятии*	1	4	
Всего			**10**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ

8.1. Основная литература

1. Шаньгин В.Ф., Информационная безопасность и защита информации/ Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0 -URL: http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).
2. Защита информации: учебное пособие / Ю.М. Краковский - Ростов н/Д : Феникс, 2016. - (Высшее образование). - URL: http://www.studentlibrary.ru/book/ISBN9785222269114.html (ЭБС «Консультант студента»).
3. Комплексные (интегрированные) системы обеспечения безопасности [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 7. - М. : Горячая линия - Телеком, 2013. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202381.html (ЭБС «Консультант студента»).
4. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М. : Горячая линия - Телеком, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература

1. Основы информационной безопасности : Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М. : Горячая линия - Телеком, 2011. -URL: http://www.studentlibrary.ru/book/ISBN5935172925.html (ЭБС «Консультант студента»).
2. Информационная безопасность: защита и нападение / Бирюков А.А. - М. :ДМК Пресс, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785940746478.html (ЭБС «Консультант студента»).
3. Галатенко, В. А. Основы информационной безопасности: курс лекций: учеб.пособие / В. А. Галатенко ; под ред. В. Б. Бетелина.- 2-е изд., испр. - М. :Интернет-Ун-т Информ. Технологий, 2004. - 264 с.
4. Девянин П.Н. Модели безопасности компьютерных систем.-М.: Академия, 2005. 144 с.
5. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия; уч. пособие. -2 изд. – М.: Издат.-торговая корпорация «Дашков и К», 2005, – 336 ч.
6. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : уч.пособие. – М.: Издат центр «Академия», 2005, – 256 с. 7. Мельников,В.П. Информационная безопасность и защита информации : доп. УМО по ун-тскому политех. образованию в качестве учеб. пособия для студентов вузов,обучающихся по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова. - 4-изд. ; стер. - М. : Академия, 2009. - 336 с. -

(Высшее профессиональное образование). - ISBN 978-5-7695-6150-4 : 306-46.

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента». Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет кучебной литературе и дополнительным материалам, приобретенным на основании прямыхдоговоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием: проектор и экран проектора. Лабораторные работы проводятся в дисплейных классах, оснащенных программным обеспечением, указанным в пункте 6.3 и доступом в Интернет. Для самостоятельной работы в распоряжении студента имеются читальный зал и дисплейные классы, обеспечивающие свободный доступ в Интернет.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).