МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра информационной безопасности и систем связи

Авторы-составители: **Батищева Светлана Эдуардовна**
Никитина Елена Юрьевна
Карпов Михаил Юрьевич

Кафедра математических и естественнонаучных дисциплин

Авторы-составители: **Абрамова Ирина Владимировна**

Рабочая программа дисциплины

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Код УМК 61257

Утверждено
Протокол №1
от «31» августа 2020 г.

Пермь, 2020

1. Наименование дисциплины

Основы информационной безопасности

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « Б.1 » образовательной программы по направлениям подготовки (специальностям):

Направление: **01.03.02** Прикладная математика и информатика

направленность Математическое моделирование и информационные технологии

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Основы информационной безопасности** у обучающегося должны быть сформированы следующие компетенции:

01.03.02 Прикладная математика и информатика (направленность : Математическое моделирование и информационные технологии)

ОПК.2 Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Индикаторы

ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности

4. Объем и содержание дисциплины

Направления подготовки	01.03.02 Прикладная математика и информатика (направленность: Математическое моделирование и информационные технологии)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	6
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	14
Проведение лабораторных работ, занятий по иностранному языку	0
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (3)
Формы промежуточной аттестации	Зачет (6 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Основы информационной безопасности

Курс «Основы информационной безопасности» позволяет познакомиться с основными понятиями информационной безопасности, национальной безопасности, угрозах безопасности, особенностях обеспечения информационной безопасности в системе национальной безопасности России.
Приобретение знаний и умений обеспечиваются в соответствии с ФГОС ВПО, СУОС специальностей «Компьютерная безопасность», «Информационная безопасность автоматизированных систем», направлений «Прикладная математика и информатика», «Бизнес-информатика», «Фундаментальная информатика и информационные технологии», содействует формированию профессионального воззрения и приобретения навыков системного подхода к решению сложных профессиональных задач с учетом современных требований безопасности.

Актуальность проблемы информационной безопасности

Интенсивное развитие информационных технологий (ИТ) создало предпосылки для глобального решения проблем информационной безопасности.
Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.
Изменения в сфере технологий обработки данных, возможность свободного выхода в глобальные информационно-вычислительные сети (например, Internet) с персонального компьютера, системы электронной коммерции, банковские системы, системы обеспечения деятельности органов власти - создают предпосылки для финансовых хищений, утечки информации конфиденциального характера или составляющей коммерческую тайну; распространение вредоносных программ – компьютерных вирусов, нарушающих целостность, сохранность, достоверность электронной информации; появление терминов «информационная война», «информационное оружие».

Основные термины и определения категории «безопасность», виды безопасности

Терминология категории «безопасность» вводится в соответствии с Российским законодательством.
Определяются понятия: безопасность, жизнено важные интересы, основные объекты безопасности, опасность, ущерб, угроза безопасности, вызов, обеспечение безопасности.
Рассматривается схема деятельности по обеспечению безопасности, основные принципы обеспечения безопасности, классификация видов безопасности.

Национальная безопасность Российской Федерации. Место информационной безопасности в системе Национальной безопасности Российской Федерации.

Развитие мира идет по пути глобализации всех сфер международной жизни. Между государствами обострились противоречия, связанные с неравномерностью развития в результате глобализационных процессов, углублением разрыва между уровнями благосостояния стран. Ценности и модели развития стали предметом глобальной конкуренции. Кроме того, усилится глобальное информационное противоборство.
Краткий анализ основных вызовов и угроз безопасности Российской Федерации в условиях современного глобального мира показывает, что существенную роль в их природе и содержании играет информационная сфера. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.
Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.
Рассматриваются положения основных концептуальных нормативных документов Российской

Федерации в этой сфере.

Понятие информационной безопасности. Эволюция подходов к защите информационной безопасности

Проблема защиты информации в информационных компьютерных системах оказалась в центре внимания специалистов практически с началом широкого использования средств электронной вычислительной техники для обработки информации.
Особая активность интересов к защите информации проявилась с конца 80-х гг. В 1989 г вводится понятие этапа развития по критерию используемых средств защиты и способов их применения. Несколько позже был принят методологический подход к защите информации. При этом выделены следующие периоды развития подходов к ЗИ: эмпирический; концептуально - эмпирический; теоретико – концептуальный. Рассматриваются обобщенные характеристики периодов развития подходов к защите информации.

Государственная система обеспечения информационной безопасности Российской Федерации

Рассматриваются основные элементы системы безопасности Российской Федерации на основании положений Российского законодательства. Определяются элементы системы информационной безопасности как подсистемы национальной безопасности. Рассматриваются основные правовые нормы деятельности субъектов системы информационной безопасности и их взаимосвязь.

Организационная основа информационной безопасности

Проводится классификация организационной основы системы информационной безопасности Российской Федерации. Рассматриваются основные организационные нормативные документы, регламентирующие деятельность в сфере информационной безопасности России.

Правовая основа информационной безопасности

Проводится классификация правовой основы системы информационной безопасности Российской Федерации. Рассматриваются основные правовые нормативные документы, регламентирующие деятельность в сфере информационной безопасности России.

Основные категории конфиденциальной информации: государственная тайна, персональные данные, коммерческая тайна

Вводятся основные категории защищаемой информации в соответствии с Российским законодательством. Разбираются основные подходы к обеспечению защиты конфиденциальной информации в соответствии с законодательством Российской Федерации. Выполняются практические работы, дающие первичные представления об основных подходах к защите таких категорий, как государственная тайна, персональные данные, коммерческая тайна.

Базовые основы защиты информации

Вводятся и рассматриваются исходные положения обеспечения информационной безопасности. Информационная безопасность базируется на законодательной основе. Информационная безопасность обеспечивается комплексом мер -организационных, программных, аппаратных. Средства защиты должны допускать оценку их эффективности. Средства защиты должны предусматривать контроль их эффективности. Средства защиты не должны снижать функциональные характеристики ИС.
Вводятся и рассматриваются принципы обеспечения ИБ: Системность, Комплексность, Непрерывность защиты, Разумная достаточность, Гибкость системы, Открытость алгоритмов защиты, Простота применения защиты.

Информация как объект защиты

На основе нормативной базы в области защиты информации вводятся основные определения, формируется понимание информации как объекта защиты, акцентируется внимание на правовых особенностях регулирования права интеллектуальной собственности. Рассматриваются виды представления информации.

Основные угрозы информационной безопасности. Классификация

Определяются источники информации, рассматриваются каналы доступа к информации, каналы получения. Вводится понятия и рассматриваются средства доступа к информации. Рассматривается классификация причин образования технических каналов утечки информации, классификация различного типа каналов несанкционированного доступа к информации, т.к. открытый канал порождает утечку информации, возникают проблемы с сохранностью информационных ресурсов, с обеспечением целостности, доступности и конфиденциальности информационных активов.
Проводится классификация угроз информационной безопасности.

Организационно-технические документы в сфере защиты информации. Понятие безопасности и их взаимосвязь

Рассматривается база организационно-технических документов, регламентирующих основные базовые понятия, их взаимосвязь, взаимодействие. Базовые основы по ЗИ представлены в организационно – технических документах: ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности. Критерии оценки; ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью; и др.
В соответствии с положениями ГОСТ Р ИСО/МЭК 15408-2002 вводится к рассмотрению схема взаимодействия основных понятий информационной безопасности, разбирается взаимосвязью

Методы и средства защиты информации

Вводится и разбирается классификация методов и средств защиты информационных ресурсов. Дается характеристика каждой группе. Разбираются положительные и отрицательные стороны средств защиты информационных ресурсов.
Рассматриваются основные механизмы обеспечения безопасности.

Политика безопасности организации

Безопасность информационных активов связана с защитой активов от угроз, где угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами. Во внимание следует принимать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека, злонамеренными или иными.
Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения.
Положения ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью.» должны расцениваться как отправная точка для разработки руководства по обеспечению ИБ под конкретные нужды организации. Разработка политики безопасности организации позволяет определить требования к информационной безопасности с учетом следующих факторов: оценка рисков организации, юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг, специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации. Рассматриваются мероприятия по управлению информационной безопасностью.

Информационные воздействия, информационное оружие, информационная война

Дается определение информационной войны и основных понятий, относящихся к этой категории. Вводятся понятия: Информационная операция, информационная война, информационное оружие, Средства массовой коммуникации. Рассматриваются аспекты тайного принуждения личности как специфический способ управления. Обозначается значение контроля за информационными потоками для социального управления. Информационная война тесно связана/переплетена с психологической войной. Рассматриваются методы информационной войны.

Рассматривается использование тайного принуждения личности в различных сферах социального взаимодействия. Проводятся анализ, систематизация и уточнение основных понятий, отображающих проявления тайного принуждения личности.

Итоговое контрольное мероприятие

Итоговая отчетность проводится в форме защиты творческой работы на выбранную студентом из рассмотренных на занятиях тему.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

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

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/87995.html

2. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 c. — ISBN 978-5-906-17271-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/33857

3. Голиков, А. М. Основы информационной безопасности : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2007. — 288 c. — ISBN 978-5-868889-467-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/13957

Дополнительная:

1. Морозов, А. В. Информационное право и информационная безопасность. Часть 2 : учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. — Москва, Саратов : Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 604 c. — ISBN 978-5-00094-297-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/66771.html

2. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 c. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/77317.html

3. Морозов, А. В. Информационное право и информационная безопасность. Часть 1 : учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. — Москва, Саратов : Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. — 436 c. — ISBN 978-5-00094-296-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/72395.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Основы информационной безопасности** предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
ОС Microsoft Windows 7 Pro OEM (Предустановленная версия); Microsoft Office Professional/ Standard 2007(Open License: 42030513 от 11.04.2007); Kaspersky Endpoint Security for Business; Справочно-правовая система «КонсультантПлюс»; Яндекс.Браузер (свободно распространяемое ПО) и/или Google Chrome (свободно распространяемое ПО).
При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:
система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).
система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

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

Учебная аудитория для проведения занятий лекционного типа.
Основное оборудование: специализированная мебель, меловая доска, переносной проектор, переносной экран.
Учебная аудитория для проведения занятий семинарского (практического) типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – Компьютерный класс № 302 (корп.2).
Основное оборудование: специализированная мебель, персональные компьютеры, проектор, экран.
Учебно-наглядные пособия и демонстрационное оборудование.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения библиотеки СГПИ филиал ПГНИУ.

Помещение библиотеки СГПИ филиал ПГНИУ, оснащенное компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ПГНИУ; ауд. 317 (корп.2).
Основное оборудование: специализированная мебель, меловая доска, проектор, экран, ноутбуки, телевизор.
ПО: ОС Microsoft Windows (предустановленная версия - OEM или версия согласно лицензионным соглашениям); пакет офисных приложений Microsoft Office (версия согласно лицензионным соглашениям); Kaspersky Endpoint Security for Business; Справочно-правовая система «КонсультантПлюс»; Яндекс.Браузер (свободно распространяемое ПО) и/или Google Chrome (свободно распространяемое ПО); ОС «Альт Образование».

Фонды оценочных средств для аттестации по дисциплине
Основы информационной безопасности

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.2

Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Знать основные положения и концепции в области программирования, Знать архитектуру языков программирования, основную терминологию и базовые алгоритмы, Знать основные требования информационной безопасности. Уметь применять основные положения и концепции в области программирования при решении профессиональных задач. Владеть навыками реализации базовых алгоритмов при решении профессиональных задач.	**Неудовлетворител** Знает менее 50% основных положений и концепций в области программирования, Знает менее 50% архитектуры языков программирования, основную терминологию и базовые алгоритмы, Знает основные требования информационной безопасности **Удовлетворительн** Знает не менее 50% основных положений и концепций в области программирования, Знает не менее 50% архитектуры языков программирования, основную терминологию и базовые алгоритмы, Знает основные требования информационной безопасности **Хорошо** Знает не менее 70% основных положений и концепций в области программирования, Знает не менее 70% архитектуры языков программирования, основную терминологию и базовые алгоритмы, Хорошо знает основные требования информационной безопасности **Отлично** Знает основные положения и концепции в области программирования, Знает не менее 80% архитектуры языков программирования, основную терминологию и базовые алгоритмы, Отлично знает основные требования информационной безопасности

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 44 до 60
«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Правовая основа информационной безопасности **Письменное контрольное мероприятие**	Письменная работа, включающая в себя тестовые задания закрытого и открытого типа, имеющие целью определить знание нормативной базы, закрепляющей основные понятия категории «национальная безопасность», понимание категории национальной безопасности, классификацию и перечень угроз национальной безопасности, особенности обеспечения информационной безопасности в системе национальной безопасности Российской федерации; знание структуры правового обеспечения информационной безопасности.
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Основные категории конфиденциальной информации: государственная тайна, персональные данные, коммерческая тайна **Письменное контрольное мероприятие**	Письменная работа, включающая в себя тестовые задания закрытого и открытого типа, имеющие целью определить знание нормативной базы, закрепляющей понятие информации как объекта защиты, ограничения доступа к информации, отнесенной к категории защищенной; знание подходов к защите Государственной тайны, коммерческой тайны и персональных данных

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Политика безопасности организации **Письменное контрольное мероприятие**	Письменная работа, включающая в себя тестовые задания закрытого и открытого типа, имеющие целью определить знание организационно – технических документов по обеспечению информационной безопасности, классификацию методов и средств защиты информации, виды угроз информационной безопасности; определить понимание критериев защищенности систем, представление о проблемах и направлениях развития аппаратных и программных средств защиты информации, представление о каналах утечки и искажения информации
ОПК.2.1 Применяет знания основных положений и концепций в области программирования, архитектуру языков программирования, основную терминологию и базовые алгоритмы, основные требования информационной безопасности	Итоговое контрольное мероприятие **Итоговое контрольное мероприятие**	Письменная работа, включающая в себя тестовые задания закрытого и открытого типа, имеющие целью определить знание системы национальной безопасности России, вызовов и угроз национальной безопасности; правовой основы обеспечения информационной безопасности Российской Федерации; категорий конфиденциальной информации и принципов её защиты; классификацию методов и средств защиты информации; видов угроз информационной безопасности; определить представление о каналах утечки и искажения информации; о критериях защищенности систем; о проблемах и направлениях развития аппаратных и программных средств защиты информации

Спецификация мероприятий текущего контроля

Правовая основа информационной безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знать нормативную базу, основные определения категории национальной безопасности, классификацию и перечень угроз национальной безопасности	10
Знать структуру правового обеспечения информационной безопасности	10
Знать особенности обеспечения информационной безопасности в системе национальной безопасности Российской Федерации	10

Основные категории конфиденциальной информации: государственная тайна, персональные данные, коммерческая тайна

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знать понятие информации как объекта защиты, юридические аспекты оборота информации	10
Знать особенности подходов к защите государственной тайны, коммерческой тайны и персональных данных	10
Знать правовую основу ограничения доступа к информации, отнесенной к категории защищенной	10

Политика безопасности организации

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Понимать критерии защищенности систем, иметь представление о проблемах и направлениях развития аппаратных и программных средств защиты информации	15
Знать организационно – технические документы по обеспечению информационной безопасности, классификацию методов и средств защиты информации, виды угроз информационной безопасности	10
Иметь представление о каналах утечки и искажения информации	5

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **1.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **5**

Показатели оценивания	Баллы
Знать классификацию методов и средств защиты информации	2

Знать правовую основу обеспечения информационной безопасности РоссийскойФедерации	2
Знать категории конфиденциальной информации и принципов её защиты	1
Способность определить наличие каналов утечки и искажения информации	1
Знать классификацию видов угроз информационной безопасности	1
Иметь представление о проблемах и направлениях развития аппаратных и программных средств защиты информации	1
Иметь представление о критериях защищенности систем	1
Знать структуру системы национальной безопасности России, вызовов и угроз национальной безопасности	1