Приложение 4

к образовательной программе

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.04 Организационное и правовое обеспечение информационной безопасности
(индекс, наименование дисциплины в соответствии с учебным планом)

38.04.05 Бизнес-информатика
(код, наименование направления подготовки/специальности)

«Аналитическое обеспечение информационной безопасности»
направлению подготовки «бизнес-информатика»

очная форма обучения
(форма обучения)

Год набора 2026

Город
Санкт-Петербург, 2026 г.

**Автор(ы)-составитель(и) РПД:**

Сухостат Валентина Васильевна, кандидат техн. наук, кандидат пед. наук, доцент, доцент кафедры бизнес-информатика

**Заведующий кафедрой:**

Наумов Владимир Николаевич, доктор военных наук, кандидат технических наук, профессор, профессор кафедры бизнес-информатики

Рабочая программа дисциплины Б1.В.04 «Организационное и правовое обеспечение информационной безопасностью» одобрена на заседании кафедры бизнес-информатики факультета экономики и финансов Северо-Западного института управления РАНХиГС.

протокол № 6 от «_26_» _марта_2026 г.

**СОДЕРЖАНИЕ**

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина Б*1.В.04 «Организационное и правовое обеспечение информационной безопасностью»* обеспечивает формирование у обучающихся следующих универсальных, общепрофессиональных и профессиональных компетенций*:

| **ОТФ/ТФ и реквизиты ПС** (при наличии)** | **Код компетенции **** | **Наименование Компетенции **** | **Код индикатора достижения компетенций **** | **Наименование индикатора достижения компетенций **** | **Образовательный результат **** |
|---|---|---|---|---|---|
| **06**<br><br>СВЯЗЬ, ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ<br><br>**06.014**<br><br>МЕНЕДЖЕР ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ<br><br>**В**<br><br>Управление сервисами ИТ организации<br><br>**В/06.7**<br><br>Управление непрерывностью ИТ-сервисов | ПКс-4 | Способен управлять информационными сервисами, ресурсами ИТ и ИТ-инновациями. Управлять ИАС в защищенном исполнении, обслуживать системы защиты | ПКс-4.2 | Управляет ИАС в защищенном исполнении | ПКс -4.2 Зн 4<br>**Знать**<br>Методы непрерывного улучшения управления непрерывностью ИТ-сервисов<br><br>ПКс -4.2 У5<br>**Уметь**<br>Организовывать деятельность по непрерывному улучшению управления непрерывностью ИТ-сервисов |

** Дисциплина может формировать компетенцию полностью или частично.*
***Должно соответствовать Приложению 1 к образовательной программе*

## 2. Объем и место дисциплины в структуре образовательной программы

Общий объем дисциплины *Б1.В.04 «Организационное и правовое обеспечение информационной безопасностью»* - 3 зачетных единицы – 108 акад.час; объем академических часов, выделенных на контактную работу обучающихся с преподавателем - 31 акад часа, из них 8 акад. часов – лекции, 12 час – практические занятия, 9 часов – контактная работа на аттестацию в период экзаменационных сессий, и 59 акад. час. выделяется на самостоятельную работу обучающихся.

Место дисциплины в структуре образовательной программы.
Дисциплина изучается в 4-м семестре 2-го курса. Дисциплина Б1.В.04 «Организационное и правовое обеспечение информационной безопасности» относится к части дисциплин, формируемых участниками образовательных отношений учебного плана по направлению 38.04.05 Бизнес-информатика образовательной программы «Аналитическое обеспечение информационной безопасности». Преподавание дисциплины опирается на дисциплины программы магистратуры Б1.В.01 «Управление информационной безопасностью», Б1.В.05 «Методы бизнес-аналитики».
Дисциплина закладывает теоретический и методологический фундамент для овладения умениям и навыками в ходе овладения дисциплинами (модулями) по выбору 3 (ДВ.3), Б2.О.01(У) «Проектно-аналитическая практика» и Б2.О.02 (Н) «Научно-исследовательская работа».

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при подготовке магистерских диссертаций.

## 3. Содержание и структура дисциплины

3.1. Структура дисциплины

*Очная/очно-заочная/заочная форма обучения (оставить нужное)*

| № п/п | Наименование тем и (или) разделов | | Объем дисциплины, ак.час | | | | | | | | | | | | Форма текущего контроля успеваемости, промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ВСЕГО | Контактная работа обучающихся с преподавателем по видам учебных занятий | | | | | | | | | Самостоятельная работа | | | |
| | | | Период теоретического обучения | | | | | | Период промежуточной аттестации (сессия) | | | | | | |
| | | | Занятия лекционного типа | | Занятия семинарского типа | | ИК | КСР | КЭ | Кат тэк | Контроль | СРкр | СРэк | СР | |
| | | | Л | ВЛ | ЛР | ПЗ | | | | | | | | | |
| Тема 1 | Теоретические основы организационного и правового обеспечения информационной безопасности. | 34 | 2 | | | 4 | | | | 3 | | | 6 | 18 | Т |
| Тема 2 | Правовое обеспечение | 38 | 4 | | | 4 | | | | 3 | | | 6 | 20 | Т |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | информационной безопасности | | | | | | | | | | | | | |
| Тема 3 | Организационное обеспечение информационной безопасности | 36 | 2 | | | 4 | | | | 3 | | 6 | 21 | ПКЗ |
| Промежуточная аттестация | | | | | | | | | 2 | | | | | экзамен |
| **Итого** | 108 | | 8 | | | 12 | | | 2 | 9 | | 18 | 59 | |

*Используемые сокращения:*

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.

СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

3.2. Содержание дисциплины

## Тема 1. Теоретические основы организационного и правового обеспечения информационной безопасности

Основы обеспечения информационной безопасности. Основные сферы общественной жизни: экономическая сфера, социальная сфера, сфера духовной жизни, сфера государственного управления.

Понятие «информационная сфера». Информационная сфера. Субъектный сегмент. Общественный сегмент. Смешанный сегмент информационной инфраструктуры.

Обеспечение информационной безопасности. Обеспечение безопасности: базовые понятия. Обеспечение ИБ организации. Правовое обеспечение ИБ. Организационное обеспечение ИБ. Средства технического, кадрового, материального, финансового, информационного и научного обеспечения ИБ ВФ.

## Тема 2. Правовое обеспечение информационной безопасности

Понятие и содержание правового обеспечения ИБ. Место информационной безопасности в национальной безопасности РФ.

Информация как объект правоотношений в сфере обеспечения ИБ. Информационные технологии и защита информации.

Государственная тайна как особый вид защищаемой информации.

Правовое регулирование защиты сведений конфиденциального характера. Безопасность персональных данных. Служебная тайна как вид защищаемой информации. Коммерческая тайна и правовой режим обеспечения ее безопасности. Правовое регулирование защиты сведений профессиональной деятельности.

Правовое обеспечение информационной безопасности в сфере интеллектуальной собственности. Общие положения. Интеллектуальные права и правовое обеспечение безопасности их использования. Основы авторского и смежного права. Основы патентного права. Право промышленной собственности. Электронная подпись и правовое обеспечение безопасности переписки.

Правовое обеспечение защиты критической информационной инфраструктуры.

Обеспечение безопасности при использовании сетей связи и сети Интернет. Техническое регулирование и требования по безопасности информационных технологий.

Юридическая ответственность за правонарушения в области информации, информационных технологий и защиты информации. Понятие и виды юридической ответственности. Судебная защита прав и свобод человека и гражданина в информационной сфере. Уголовно-правовая ответственность в сфере компьютерной информации.

**Тема 3. Организационное обеспечение информационной безопасности**

Понятие, сущность и содержание организационного обеспечения ИБ. Организационная основа государственной системы обеспечения ИБ, полномочия органов государственной власти. Цель, принципы и приоритеты государственной политики в области технической защиты информации.

Государственная система лицензирования. Лицензирование в области обеспечения ИБ. Общие подходы и принципы организации безопасности предприятия и системы управления рисками.

Организация и порядок сертификации продукции в системе Федеральной службы по техническому контролю. Организация и порядок сертификации продукции в системе Федеральной службы безопасности.

Аттестация объектов информатизации по требованиям безопасности информации. Порядок проведения аттестации объектов информатизации. Требования к нормативным и методическим документам по аттестации объектов информатизации.

## 4. Типы оценочных материалов, показатели и критерии оценивания

4.1.Оценочныематериалыподисциплине(*наименование*)входятвсостав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам (модулям) образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

## 4.4. Типы заданий, сценарии выполнения, критерии оценивания

| ТИП ЗАДАНИЯ | ИНСТРУКЦИЯ | СЦЕНАРИИ ВЫПОЛНЕНИЯ | КРИТЕРИИ ОЦЕНИВАНИЯ |
|---|---|---|---|
| Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных | Прочитайте текст, выберите правильный ответ | 1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.<br>2. Внимательно прочитать предложенные вариант-ты ответа.<br>3. Выбрать один верный ответ.<br>4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В). | Ответ считается верным, если правильно указана цифра или буква |
| Задание закрытого типа на установление соответствия | Прочитайте текст и установите соответствие | 1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов.<br>2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.;<br>список 2 – утверждения, свойства объектов и т.д.<br>3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.<br>4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4). | Ответ считается верным, если правильно указаны цифры или буквы |
| Задание закрытого типа с выбором нескольких | Прочитайте текст, выберите правильные ответы | 1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. | Ответ считается верным, если правильно установлены все соответствия (позиции из |

| | | | |
|---|---|---|---|
| правильных ответов из нескольких вариантов предложенных | | 2. Внимательно прочитать предложенные вариант-ты ответа.<br>3. Выбрать несколько правильных ответов.<br>4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г). | одного столбца верно сопоставлены с позициями другого) |
| Задание закрытого типа на установление последовательности | Прочитайте текст и установите последовательность | 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.<br>2. Внимательно прочитать предложенные варианты ответа.<br>3. Построить верную последовательность из предложенных элементов.<br>4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135). | Ответ считается верным, если правильно указана вся последовательность цифр |
| Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора | Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа | 1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.<br>2. Внимательно прочитать предложенные варианты ответа.<br>3. Выбрать один верный ответ.<br>4. Записать только номер (или букву) выбранного варианта ответа. | Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа |

| | | | |
|---|---|---|---|
| | | 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования). | |
| Задание открытого типа с развернутым ответом | Прочитайте текст и запишите развернутый обоснованный ответ | 1. Внимательно прочитать текст задания и понять суть вопроса.<br>2.Продумать логику и полноту ответа.<br>3.Записать ответ, используя четкие компактные формулировки.<br>4.В случае расчетной задачи, записать решение и ответ | Ответ считается верным:<br>1. Отсутствие фактических ошибок.<br>2. Раскрытие объема используемых понятий (полнота ответа).<br>3.Обоснованность ответа (наличие аргументов).<br>4. Логическая последовательность излагаемого материала. |

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

| **Итоговая балльная оценка** | **Традиционная система** | **Бинарная система** | **ECTS** | |
|---|---|---|---|---|
| | | | **Для традиционной системы** | **Для бинарной системы** |
| 95-100 | Отлично | Зачтено | A | P/ Passed |
| 85-94 | | | B | P/ Passed |
| 75-84 | Хорошо | | C | P/ Passed |
| 65-74 | | | D | P/ Passed |
| 55-64 | Удовлетворительно | | E | P/ Passed |
| 0-54 | Неудовлетворительно | Не зачтено | F | F/Failed |

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

| Максимальная сумма баллов за текущий контроль успеваемости | Максимальная сумма баллов за промежуточную аттестацию | Максимальная итоговая балльная оценка | Максимальная сумма баллов за повторную промежуточную аттестацию |
|---|---|---|---|
| 60 баллов | 40 баллов | 100 баллов | 100 баллов |

## 5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

*тестирование, реферат, эссе, упражнения, опрос, контрольная работа, кейс и т.д. (должны совпадать с теми, что отражены в п. 3.1.)*

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

### Тема 1. Теоретические основы организационного и правового обеспечения информационной безопасности ПКс-4.2

*Тестовые задания с инструкцией по выполнению:*

*Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных.*

*Сценарий выполнения*

1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько верных ответов.

4. Записать только номера (или буквы) выбранного варианта ответа (например, 3 или В).

*Пример*

*Задание 1.* Выберите правильный ответ, чтобы закончить фразу:

Основными составляющими правового обеспечения информационной безопасности являются:

1) планирование использования и управления применением материальных, людских, финансовых и др. ресурсов, выделяемых для противодействия угрозам, связанных с информацией и информационной инфраструктурой;
2) совокупность норм права;
3) правоприменительная практика.

*Задание закрытого типа с выбором только одного правильного ответа из нескольких вариантов предложенных.*

1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные вариант-ты ответа.

3. Выбрать тот ответ, который считаете верными.

4. Запишите только один номер (или букву) выбранных вариантов ответа (например, 3 или В).

Пример

*Задание 2*. Выберите правильный ответ, чтобы продолжить

Международная организация по стандартизации (ISO) под словом «система» в системе менеджмента информационной безопасности понимает:

1) действующее устройство;
2) приложение;
3) процесс, программу действий или методологию.

Задание закрытого типа на установление соответствия

1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов.

2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.;

список 2 – утверждения, свойства объектов и т.д.

3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.

4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).

Задание 3. Установите соответствие между термином и его определением.

| Термин | Определение |
|---|---|
| 1 Управление доступом | А Систематический, независимый и задокументированный процесс, предназначенный для получения свидетельств и объективной оценки. |
| 2 Атака | В Попытка уничтожения раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования. |
| 3 Аудит | С Обеспечение санкционированного доступа к активам в соответствии с бизнес-требованиями и требованиями безопасности. |

*Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора*

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.
2. Внимательно прочитать предложенные варианты ответа.
3. Выбрать один верный ответ.
4. Записать только номер (или букву) выбранного варианта ответа.
5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).

Пример

*Задание 4.*

«Информационное измерение» государства определяется

1) ролью и местом информации и информационной инфраструктуры в деятельности государственных органов и организаций по выполнению функций государства;
2) деятельностью его органов по стимулированию развития информационной инфраструктуры и активной информационной деятельности граждан по защите их прав и свобод в этой области

*Задание открытого типа с развернутым ответом*

1. Внимательно прочитать текст задания и понять суть вопроса.
2. Продумать логику и полноту ответа.
3. Записать ответ, используя четкие компактные формулировки.
4. В случае расчетной задачи, записать решение и ответ

*Задание 5.*

Раскройте понятия «информационная безопасность» и «обеспечение информационной безопасности».

*Задание закрытого типа на установление последовательности действий*

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.
2. Внимательно прочитать предложенные варианты ответа.
3. Построить верную последовательность из предложенных элементов.
4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).

*Задание 6.* Укажите уровни общей структуры нормативно-методических документов компании в области информационной безопасности в порядке возрастания:

1) политика информационной безопасности;
2) процедуры, инструкции, стандарты конфигурации, журналы, записи;
3) частные политики, стандарты.

**Тема 2. Правовое обеспечение информационной безопасности**

**ПКс- 4.2**

*Задание открытого типа с развернутым ответом*

*Вопрос 1* Раскрыть содержание предметной сферы законодательства в области информации, информационных технологий и защиты информации.

*Вопрос 2*

Сравните риск-ориентированный и процессный подходы к управлению информационной безопасности.

*Задание закрытого типа на установление последовательности*

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.

2. Внимательно прочитать предложенные варианты ответа.

3. Построить верную последовательность из предложенных элементов.

4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).

*Задание 1.* Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему (последовательность номеров через запятую):

1) морально-этический;
2) организационно-технический;
3) нормативно-правовой;
4) программно-аппаратный;
5) духовно-нравственный.

*Задание закрытого типа с выбором одного правильного ответа из нескольких предложенных вариантов*

1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать один верный ответ.

4. Записать только номер выбранного варианта ответа.

*Задание 2.* Что (кто) НЕ является элементом системы обеспечения информационной безопасности РФ (номер по порядку)?

1) Палаты Федерального собрания;
2) Президент РФ;
3) Органы местного самоуправления;
4) Общественная Палата;
5) Органы исполнительной власти;
6) Совет безопасности.

*Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных.*

1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько ответов из предложенных вариантов.

2. Внимательно прочитать предложенные варианты ответа.

3. Выбрать несколько верных ответов.

4. Записать только номера (или буквы) выбранного варианта ответа (например, 3 или В).

*Задание 3.* Выберите, что включает в себя система менеджмента:
1) организационную структуру;
2) политики;
3) планирование;
4) оценку информационных рисков, планирование мер по обработке рисков;
5) должностные обязанности;
6) ресурсы.

*Задание закрытого типа на установление соответствия*

1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов.
2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.;
список 2 – утверждения, свойства объектов и т.д.
3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.
4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).

*Задание 4.* Соотнесите термин из левого столбца с его правильным определением из правого столбца. Каждому термину соответствует одно определение.

| **Термин** | **Определение** |
|---|---|
| 1. Обеспечение непрерывности информационной безопасности | А. Процессы и процедуры, гарантирующие непрерывность операций по обеспечению информационной безопасности |
| 2. Событие информационной безопасности | В. Выявленное состояние системы, услуги или сети, указывающее на возможное нарушение политики обеспечения информационной безопасности |

| Термин | Определение |
|---|---|
| 3. Инцидент информационной безопасности | С Одно или несколько нежелательных или неожиданных событий информационной безопасности, которые с высокой степенью вероятности могут привести к компрометации в бизнес- процессах и создают угрозы для информационной безопасности |

*Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора*

1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.Внимательно прочитать предложенные варианты ответа.
2. Выбрать один верный ответ.
3. Записать только номер (или букву) выбранного варианта ответа.
4. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).

*Задание 5.* Кто НЕ наделен полномочиями по отнесению сведений к государственной тайне?

1) Министр сельского хозяйства;
2) Председатель Банка РФ;
3) Руководитель Росгидромета;
4) Руководитель Федеральной таможенной службы

**Тема 3. Организационное обеспечение информационной безопасности**

**ПКс – 4.2**

*Практческие контрольные задания*

**Задание 1.** «Нормативно-правовое обеспечение ИБ. Построение концептуальной модели ИБ».

1. Составить логическую схему знаний по содержанию блока.
2. Составить терминологический словарь согласно нормативно-правовым документам и стандартам (https://fstec.ru/).
3. Провести анализ содержания основных законодательных и нормативно-правовых документов, регулирующих вопросы обеспечения ИБ на федеральном, региональном и ведомственного уровнях, используя справочно-правовую систему «Консультант Плюс».
4. Раскрыть содержание определения средств (методов) защиты информации в ФЗ.

5. Дать характеристику содержания понятия «информационная безопасность РФ» согласно Стратегии национальной безопасности.
6. Дать характеристику российских стандартов в области обеспечения информационной безопасности и перечислить их основные функции (составить таблицу).
7. Описать перечень средств защиты информации, указанных в Законе РФ «О государственной тайне».
8. Определить перечень средств защиты информации, закрепленных ФЗ-149 «Об информации, информационных технологиях и защите информации».
9. Построить концептуальную модель ИБ.
10. Предоставить отчет в виде документа и презентации.

**Задание 2.** «Разработка политики безопасности кафедры бизнес-информатики».

1. Изучить шаблоны документов, описывающих политику информационной безопасности организации, представленные в разделе " Политика безопасности " сайта SecurityPolicy.ru (основная цель проекта SecurityPolicy.ru - создание сообществом специалистов комплектов типовых документов по информационной безопасности для различных организаций, которыми могут воспользоваться все желающие без ограничений, а также подборка шаблонов документов по информационной безопасности, законодательных и нормативных актов)
2. Изучить устав и стратегические цели СЗИУ (факультета ЭиФ/ кафедры БИ).
3. Подобрать наиболее подходящий шаблон документа для описания политики безопасности ВУЗа (подразделения), при необходимости модифицировав его структуру
4. Разработать политику безопасности ВУЗа (подразделения) с учетом специфики его деятельности и планов развития.

Предоставить отчет в виде документа и презентации.

5.3. Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает 2 КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

*Расчет по контрольным точкам дисциплины*

| Наименование | Максимальное | Коэффициент веса | Результат контрольной |
|---|---|---|---|

| контрольной точки | количество баллов за работу в рамках КТ, которое может набрать студент | контрольной точки | точки, участвующий в формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО) |
|---|---|---|---|
| КТ 1 | 100 | 0,2 | 20 |
| КТ 2 | 100 | 0,2 | 20 |
| КТ 3 | 100 | 0,2 | 20 |
| Итого: | х | 0,6 | 60 |

Формула расчета результата контрольной точки:
Результат контрольной точки = Количество баллов за работу в рамках КТ х Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

**КТ – 1.**
***Тема 1***
*Тестовые задания по теме 1*
**КТ – 1**

***Тема 2,***
*Тестовые задания по теме 2.*
**КТ – 2**

***Тема 3***
*Практическое контрольное задание (ПКЗ)*
**КТ – 3**

*1.* Для каждой формы текущего контроля успеваемости обучающихся в рамках КТ определены критерии оценивания результатов выполнения задания. *Критерии оценивания тестирования*

| Критерии оценки | Диапазон баллов | Описание критерия |
|---|---|---|
| *Количество правильных ответов* | *0* | *Количество правильных ответов менее 55%* |
| | 25 | *Количество правильных ответов от 55% до 64%* |
| | 50 | *Количество правильных ответов от* |

| | | |
|---|---|---|
| | | *65% до 74%* |
| | 75 | *Количество правильных ответов от 75% до 84%* |
| | 100 | *Количество правильных ответов от 85% до 100%* |
| Итого максимально: | 100 | |

*НАПРИМЕР: из 20 вопросов правильных ответов составляет 75% - значит это значит, что за тест студент получит 75% от максимального балла, то есть 15 баллов вместо максимальных 20.*

1. *Критерии оценивания Практического контрольного задания:*

| Критерии оценки | Диапазон баллов | Описание критерия |
|---|---|---|
| *Правильность выполнения задачи и содержание комментариев, наличие иллюстративных объектов – сриншотов* | *50-60* | *Правильные решения и последовательность выполнения и. Задание выполнено полностью, сделаны выводы* |
| | *40-49* | *Допущены незначительные недочеты, отсутствуют выводы* |
| | *30-40* | *Допущены некоторые ошибки. Отсутствуют скриншоты.* |
| *Возможность демонстрировать работу системы* | | *Или задание выполнено не полностью* |
| | | *Задание выложено с опозданием* |
| | *5-29* | *Не выполнена и половина задания, результаты не получены, много ошибок. Но выложено во-время* |
| *Грамотность изложения и оформления работы* | ***10*** | *Соблюдены все правила грамматики, орфографии, форматирования и представления визуальной части. Баллы не снижаются* |
| | *6-10* | *Не все правила оформления соблюдены* |
| | *0-5* | *Многочисленные ошибки, нечитаемые или непонятные скриншоты, затрудняющие восприятие текста. Или отсутствие в содержании демонстрационной части* |
| *Идентификация объектов* | ***15*** | *Существование идентификации объектов* |
| | *0* | *Нет идентификации* |
| *Защита работы* | ***10- 15*** | *Четкое изложение хода выполнения* |

| | | |
|---|---|---|
| | | *задания* |
| | | *Способность пояснить, что будет если какие-то параметры будут изменены или рассказать, как можно другой ответ получить* |
| | *5-10* | *Изложение – неуверенное и затруднения ответов при правильном решении.* |
| | *0-5* | *Неспособность пояснить как получены результаты, для чего выполнялись задания* |
| Итого максимально: | 100 | |

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для решения заданий (ПКЗ) студенту разрешается использование разных средств; программ для работы с электронными таблицами для обработки, анализа и визуализации данных, онлайновых инструментов.

## 6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация проводится в форме *экзамена.*
*Вопросы для подготовки к экзамену:*

1) Понятие «информационная сфера». Субъектный сегмент. Общественный сегмент.
2) Смешанный сегмент информационной инфраструктуры.
3) Информация как объект правоотношений в сфере обеспечения ИБ.
4) Информационные технологии и защита информации.
5) Правовое обеспечение информационной безопасности в сфере интеллектуальной собственности. Общие положения
6) Государственное регулирование в сфере информационной безопасности.
7) Обеспечение безопасности: базовые понятия.
8) Защищенная электронная подпись. Цифровые сертификаты.
9) Интеллектуальные права и правовое обеспечение безопасности их использования
10) Основы авторского и смежного права.
11) Право промышленной собственности.
12) Обеспечение безопасности при использовании сетей связи и сети Интернет.

13) Правовое обеспечение защиты критической информационной инфраструктуры.

14) Техническое регулирование и требования по безопасности информационных технологий

15) Понятие и виды юридической ответственности.

16) Компьютерные преступления. Уголовно-правовая ответственность в сфере компьютерной информации.

17) Судебная защита прав и свобод человека и гражданина в информационной сфере.

18) Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

19) Обеспечение информационной безопасности на государственном уровне.

20) Обеспечение информационной безопасности на уровне предприятия.

21) Коммерческая тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

22) Государственная тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

23) Персональные данные: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

24) Банковская тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

25) Тайна страхования: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

26) Налоговая тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

27) Врачебная тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

28) Тайна переписки: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

29) Служебная тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

30) Профессиональная тайна: определение, угрозы, защитные меры и ответственность за разглашение согласно нормативно-правовым документам.

31) Правовые основания отнесения сведений к категории ограниченного доступа.

32) Понятие, сущность и содержание организационного обеспечения ИБ.

33) Организационная основа государственной системы обеспечения ИБ, полномочия органов государственной власти.

34) Цель, принципы и приоритеты государственной политики в области технической защиты информации.

35) Государственная система лицензирования в области обеспечения ИБ..

36) Общие подходы и принципы организации безопасности предприятия и системы управления рисками.

37) Национальные стандарты в области информационной безопасности и защиты информации.

38) Международные стандарты в области информационной безопасности и защиты информации.

39) Организация и порядок сертификации продукции в системе Федеральной службы по техническому контролю.

40) Организация и порядок сертификации продукции в системе Федеральной службы безопасности.

41) Аттестация объектов информатизации по требованиям безопасности информации

6.2. Типовые оценочные материалы промежуточной аттестации.

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

| ТИП ЗАДАНИЯ | СЦЕНАРИИ ВЫПОЛНЕНИЯ | ТИПОВЫЕ ЗАДАНИЯ |
|---|---|---|
| Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных | 1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.<br>2. Внимательно прочитать предложенные варианты ответа.<br>3. Выбрать один верный ответ.<br>4. Записать только номер (или букву) выбранного | К органам защиты государственной тайны относятся:<br>1) Федеральная служба безопасности;<br>2) Служба внешней разведки;<br>3) Министерство внутренних дел;<br>4) Федеральная служба по техническому и экспортному контролю;<br>5) Министерство обороны (неверное зачеркнуть). |
| | | По виду защищаемой информации различаются угрозы НСД к:<br>1) речевой информации;<br>2) видовой информации;<br>3) сигнальной информации; |

| | | |
|---|---|---|
| | варианта ответа (например, 3 или В). | 4) логической информации;<br>5) тестовой информации |
| Задание закрытого типа на установление последовательности | 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.<br><br>2. Внимательно прочитать предложенные варианты ответа.<br><br>3. Построить верную последовательность из предложенных элементов.<br><br>4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135). | 1. Укажите последовательность методов аутентификации по обеспечиваемому уровню защищенности (от наименее безопасного к наиболее защищенному)<br>1) аппаратная аутентификация<br>2) биометрическая аутентификация<br>3) парольная аутентификация<br><br>2. Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему (последовательность номеров через запятую):<br><br>1) морально-этический;<br>2) организационно-технический;<br>3) нормативно-правовой;<br>4) программно-аппаратный;<br>5) духовно-нравственный. |
| Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов предложенных | 1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.<br><br>2. Внимательно прочитать предложенные варианты ответа.<br><br>3. Выбрать несколько правильных ответов.<br><br>4. Записать только номера (или буквы) выбранного варианта ответа (например, 1 4 или А Г). | При отсутствии трудовых договоров охрана КТ должна включать в себя:<br><br>1) определение перечня сведений;<br>2) ограничение доступа;<br>3) учет лиц, получивших доступ;<br>4) регулирование отношений с контрагентами;<br>5) нанесение грифа «Коммерческая тайна» (неверное зачеркнуть). |
| Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием | 1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.<br><br>2. Внимательно прочитать предложенные варианты ответа. | Выбрать верный ответ и обосновать свой выбор.<br>Коммерческая тайна – это:<br>1) общее понятие для тайн профессиональной, личной, семейной;<br>2) то же самое, что и интеллектуальная собственность;<br>3) то же самое, что и профессиональная тайна;<br>4) то же самое, что и банковская тайна; |

| | | |
|---|---|---|
| выбора | 3. Выбрать один верный ответ.<br>4. Записать только номер (или букву) выбранного варианта ответа.<br>5. Записать аргументы, обосновывающие выбор ответа (например, 1 текст обоснования) | 5) частный случай государственной тайны;<br>6) частный случай конфиденциальной информации. |
| | | Выбрать верный ответ и обосновать свой выбор.<br>Захват всех ресурсов компьютера одним приложением или процессом в многозадачной операционной системе является угрозой<br>1) нарушения конфиденциальности;<br>2) нарушения целостности;<br>3) отказа служб. |
| Задание открытого типа с развернутым ответом | 1. Внимательно прочитать текст задания и понять суть вопроса.<br>2.Продумать логику и полноту ответа.<br>3.Записать ответ, используя четкие компактные формулировки. | Прочитайте вопрос и запишите развернутый обоснованный ответ<br>Зачем нужна фильтрация по прокси-серверам? |
| | | Прочитайте вопрос и запишите развернутый обоснованный ответ<br>Зачем нужна фильтрация по почтовым серверам? |
| Задание закрытого типа на установление соответствия | 1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов.<br>2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.;<br>список 2 – утверждения, свойства объектов и т.д.<br>3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.<br>4. Записать попарно буквы и цифры (в зависимости от задания) | Ответ считается верным, если правильно указаны цифры или буквы<br>А)… – федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры;<br>Б)… – федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства РФ в области персональных данных;<br>В)… – государственный орган, на который возложены функции по лицензированию и сертификации в сфере криптографической защиты и защиты государственной тайны.<br>1) ФСБ; |

| | | |
|---|---|---|
| | вариантов ответа (например, А1 или Б4). | 2) ФСТЭК;<br>3) Роскомнадзор. |

6.3. Критерии и шкала оценивания на основе БРС.

Критерии и балльная шкала определяются преподавателем

*Критерии и балльная шкала определяются преподавателем*

| КРИТЕРИИ ОЦЕНИВАНИЯ | РЕЗУЛЬТАТ В БАЛЛАХ |
|---|---|
| Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок | 40 |
| Дан развернутый ответ на поставленный вопрос, где обучающийся демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями. | 30-39 |
| Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий. | 20-29 |
| Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено, т.е. обучающийся не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя. | 0-19 |

6.4. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для выполнения тестовых заданий требуется кабинет с компьютерами и электронная образовательная система вуза ЭОС Moodle. Если необходимо, студент может использовать калькулятор, бумагу, ручку. В исключительных случаях допустимо проведение экзамена в СДО, для чего необходима система электронного взаимодействия, например, МТС-Link Yandex.telemost,

## 7. Методические материалы по освоению дисциплины (модуля)

Для изучения основных вопросов дисциплины необходимо конспектировать материалы лекций, работать с рекомендованной преподавателем литературой, а также ресурсами информационно-телекоммуникационной сети «Интернет». Для приобретения навыков активного использования знаний полезно обсуждать плановые и возникающие вопросы, а также решаемые задачи на практических занятиях. Чтобы легче и прочнее усвоить материал следует постоянно использовать конкретные примеры, сравнения из уже полученных областей наук.

Методические материалы по дисциплине находятся в электронной образовательной системе Moodle. Структура курса представлена отдельными темами, в которых можно найти Лекционные материалы, практические задания и методические рекомендации по их выполнению, а также тестовые вопросы по каждой теме и список вопросов для подготовки к опросам и тестированию.

Важной составной частью учебного процесса в вузе являются практические занятия, которые закрепляют теоретические знания, полученные на лекциях и изученные в дополнительной литературе. Практические занятия помогают глубже усвоить учебный материал, приобрести умения применять принципы решения разнообразных проблем, определять и оценивать ресурсы и существующие ограничения разного рода проектов.

При подготовке к практическим занятиям необходимо проанализировать конспект лекции, ознакомиться с рекомендованной литературой по соответствующей теме, осуществить подготовку по рекомендованным в рабочей программе вопросам для обсуждения темы, выполнить домашнее задание (при необходимости).

Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. Особое внимание, работая самостоятельно, необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы нужно стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в

изложении и разъяснении полученных знаний, развивается речь, также благоприятно действует на результаты. При необходимости следует обращаться за консультацией к преподавателю (в том числе по электронной почте). Для самостоятельной работы имеют значение записи. Они помогают понять построение изучаемого материала, выделить основные положения, проследить их логику. Ведение записей способствует активизации и мобилизации мышления наряду со зрительной, и моторную память. Полезно записывать идеи.

После изучения базовых тем курса проводится текущий контроль знаний студентов в виде опроса или письменного тестирования. Типовые тесты и задания по темам дисциплины приведены в специальном разделе данной рабочей программы.

Подготовка к текущему и промежуточному контролю предполагает изучение представленных вопросов к зачету, работу над тестами, представленными в данной рабочей программе, выполнение семестровой проектной работы по применению системного подхода и методов системного анализа к выбранной системе.

## 8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации: учебник / сост. И.Г. Дровникова, А. В. Калач, И.И. Лившиц, Е.А. Рогозин, А.В. Скрипников.; ФКОУ ВО Воронежский институт ФСИН России – Воронеж, ИПЦ «Научная книга», 2022. – 304 с. – Текст: электронный // ЭБС Znanium [сайт]. — URL:https://znanium.com/catalog/document?id=426504.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/469235.

3. Основы управления информационной безопасностью : учебное пособие : Допущено УМО ... / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва: Горячая линия-Телеком, 2016.- 244 с. - (Вопросы управления информационной безопасностью. Вып. 1). - Библиогр.: с. 234-239. - ISBN 978-5-9912-0361-6.

4. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2021. — 111 с. — (Высшее образование). —

ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait-ru.idp.nwipa.ru/bcode/476798.

Все источники основной литературы взаимозаменяемы

8.2 Дополнительная литература

1. Дронов В.Ю. Международные и отечественные стандарты по информационной Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст: электронный. - URL: https://znanium.com/catalog/product/1021744
2. Веселов Г.Е. Менеджмент риска информационной безопасности: учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. — Электрон. дан. - Таганрог:Южный федеральный университет, 2016. - 107 с.
3. Основы управления информационной безопасностью : учебное пособие : Допущено УМО ... / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва : Горячая линия-Телеком, 2016. - 244 с. - (Вопросы управления информационной безопасностью. Вып. 1). - Библиогр.: с. 234-239. - ISBN 978-5-9912-0361-6.

**8.3.Нормативные правовые документы и иная правовая информация**

Не используются

**8.4. Интернет-ресурсы**

Обучающимся обеспечен доступ к материалам курса в СДО Академии http://lms.ranepa.ru, а так же через сайт научной библиотеки к следующим подписным электронным ресурсам:

***Русскоязычные ресурсы***

1. Электронные учебники электронно-библиотечной системы (ЭБС) *«Айбукс»*
2. Электронные учебники электронно-библиотечной системы (ЭБС) *«Юрайт»*
3. Электронные учебники электронно-библиотечной системы (ЭБС) *«Лань»*
4. Электронные учебники электронно-библиотечной системы (ЭБС) «*ZNANIUM.COM*»
5. Электронные учебники электронно-библиотечной системы (ЭБС) «BOOK.RU»

6. Оценка качества информационной инфраструктуры организации. http://www.dir-consulting.ru/ocenka-kachestva-informacionnoj-infrastruktury-organizacii.html
7. Управление инцидентами и проблемами – понятия и принципы / ИнфраМенеджер, Электронный ресурс URL: [https://www.inframanager.ru/library/about-methodology/upravlenie-incidentami/]
8. Колесов А. HP ITSM и эффективность обслуживания информационных систем предприятий / http://www.bytemag.ru/?ID=602758
9. Управление ИТ-услугами / http://www.itexpert.ru/rus/articles/200406222006/200406222044

## 9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

| № п/п | Наименование |
|---|---|
| 1. | Специализированные залы для проведения лекций, оснащенные персональным компьютером/ноутбуком и мультимедийным проектором |
| 2. | Аудитории и компьютерные классы, оборудованные посадочными местами и персональными компьютерами с выходом в Интернет для проведения практических занятий |
| 3. | «МТС Линк» — российская платформа для онлайн-коммуникаций и совместной работы команд ; «Яндекс Телемост» — сервис для видеоконференций от Яндекса; Я-мессенджер |
| 4. | Технические средства обучения: персональные компьютеры; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV; программы для работы с электронными таблицами для обработки, анализа и визуализации данных; соответствующие онлайн-инструменты для построения интеллект-карты и моделей в различных нотациях |
| 5. | Научная библиотека (в т.ч. электронные информационные ресурсы научной библиотеки) |
| 6. | СДО Академии https://lms.ranepa.ru/ |