**ФЕДЕРАЛЬНОЕ УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЪЕДИНЕНИЕ**

**В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ ПО УКРУПНЕННОЙ ГРУППЕ СПЕЦИАЛЬНОСТЕЙ И НАПРАВЛЕНИЙ ПОДГОТОВКИ**

**10.00.00 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

****

УТВЕРЖДАЮ

Председатель ФУМО ВО ИБ

А.Б. Пичкур

30 ноября 2021 г.

**Методические рекомендации**

**по разработке основной профессиональной образовательной программы   
высшего образования**

Специальность

**10.05.05 Безопасность информационных технологий**

**в правоохранительной сфере**

Уровень высшего образования

**Специалитет**

Москва, 2021 г.

СОДЕРЖАНИЕ

# Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение примерной основной образовательной программы

1.2. Нормативные документы

1.3. Перечень сокращений

# Раздел 2. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ

2.1. Общее описание профессиональной деятельности выпускников

2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО

2.3. Перечень основных задач профессиональной деятельности выпускников (по типам)

Раздел 3. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ, РЕАЛИЗУЕМЫХ В РАМКАХ НАПРАВЛЕНИЯ ПОДГОТОВКИ

3.1. Направленности (специализации) образовательных программ в рамках направления подготовки (специальности)

3.2. Квалификация, присваиваемая выпускникам образовательных программ

3.3. Объем программы

3.4. Формы обучения

3.5. Срок получения образования

Раздел 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1. Перечень обязательных компетенций выпускников

4.2. Перечень рекомендуемых профессиональных компетенции выпускников

4.3. Индикаторы достижения компетенций

Раздел 5. ПРИМЕРНАЯ СТРУКТУРА И СОДЕРЖАНИЕ ОПОП

5.1. Рекомендуемый объем обязательной части образовательной программы

5.2. Рекомендуемые типы практики

5.3. Примерный учебный план и примерный календарный учебный график

5.4. Примерная рабочая программа воспитания

5.5. Примерный календарный план воспитательной работы

5.6. Примерные программы дисциплин (модулей) и практик

5.7. Рекомендации по разработке фондов оценочных средств для промежуточной аттестации по дисциплине (модулю) или практике

5.8. Рекомендации по разработке программы государственной итоговой аттестации

Раздел 6. ПРИМЕРНЫЕ УСЛОВИЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПО ОПОП

Раздел 7. СПИСОК РАЗРАБОТЧИКОВ

Приложение 1. Перечень профессиональных стандартов, соответствующих профессиональной деятельности выпускников, освоивших программу специалитета по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

Приложение 2. Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программы специалитета по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

Приложение 3. Примерный учебный план программы специалитета по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

Приложение 4. Примерный календарный учебный график программы специалитета по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

# Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

**1.1. Назначение примерной основной образовательной программы**

Примерная основная образовательная программа (далее – ПООП) является комплексным методическим документом, рекомендованным организациям, осуществляющим образовательную деятельность по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

ПООП предназначена для разработки и реализации основных профессиональных образовательных программ высшего образования на основе федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденного приказом Минобрнауки России от 26 ноября 2020 года № 1461, зарегистрированного в Минюсте 22 декабря 2020 года, рег. номер 61703 (далее – ОПОП, образовательная программа) и с учётом профессиональных стандартов, сопряжённых с профессиональной деятельностью выпускников.

**1.2. Нормативные документы**

* Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»;
* Порядок разработки примерных основных образовательных программ, проведения их экспертизы и ведения реестра примерных основных образовательных программ, утвержденный приказом Минобрнауки России от 28 мая 2014 года № 594;
* Федеральный государственный образовательный стандарт высшего образования – специалитет по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», утвержденный приказом Минобрнауки России от 26 ноября 2020 года № 1461, зарегистрированный в Минюсте 22 декабря 2020 года, рег. номер 61703 (далее – ФГОС ВО);
* Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам магистратуры, программам специалитета, утвержденный приказом Минобрнауки России от 13 декабря 2013 года №1367 (далее – Порядок организации образовательной деятельности);
* Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утвержденный приказом Минобрнауки России от 29 июня 2015 г. № 636;
* Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования, утвержденное приказом Минобрнауки России от 27 ноября 2015 г. № 1383.

**1.3. Перечень сокращений, используемых в тексте ПООП**

|  |  |  |
| --- | --- | --- |
| з.е. | – | зачетная единица; |
| ОПК | – | общепрофессиональная компетенция; |
| ОПОП | – | основная профессиональная образовательная программа по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»; |
| Организация | – | организация, осуществляющая образовательную деятельность по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»; |
| ОТФ | – | обобщённая трудовая функция; |
| ПД | – | профессиональная деятельность; |
| ПК | – | профессиональная компетенция; |
| ПС | – | профессиональный стандарт; |
| ПООП | – | примерная основная образовательная программа по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»; |
| программа специалитета | – | основная образовательная программа высшего образования – программа специалитета 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»; |
| сетевая форма | – | сетевая форма реализации образовательных программ; |
| СПК | – | Совет по профессиональным квалификациям; |
| УК | – | универсальная компетенция; |
| ФГОС ВО | – | федеральный государственный образовательный стандарт высшего образования по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» |
| ФУМО |  | федеральное учебно-методическое объединение |
| ИД |  | индикатор достижения |

**Раздел 2. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ**

**2.1. Общее описание профессиональной деятельности выпускников**

Области профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие программу специализации, могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии (в сфере деятельности по обследованию и экспертизе компьютерных систем);

12 Обеспечение безопасности (в сфере защиты информации).

сфера обороны и безопасности;

сфера правоохранительной деятельности.

Выпускники могут осуществлять профессиональную деятельность в других областях профессиональной деятельности и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

***Типы задач профессиональной деятельности выпускников:***

проектно-технологический;

эксплуатационный;

аналитический;

организационно-управленческий;

экспертный.

При разработке и реализации программы специалитета организация ориентируется на все типы задач профессиональной деятельности, к которым готовится специалист.

***Перечень основных объектов (или областей знания) профессиональной деятельности выпускников:***

* информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности;
* технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта);
* объекты информатизации правоохранительных органов;
* организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере;
* судебно-экспертная деятельность в области компьютерной экспертизы;
* процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления.

**2.2. Перечень профессиональных стандартов, соотнесенных с ФГОС ВО**

Перечень профессиональных стандартов, соотнесенных с ФГОС ВО по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», приведен в Приложении 1.

Перечень обобщенных трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника программ специалитета по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», представлен в Приложении 2.

**2.3. Перечень основных задач профессиональной деятельности выпускников**

Выпускник, освоивший программу специалитета, готовится решать следующие основные задачи профессиональной деятельности в соответствии с видами профессиональной деятельности:

*проектно-технологическая деятельность:*

* сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
* проведение проектных расчётов элементов систем обеспечения информационной безопасности;
* разработка технологической и эксплуатационной документации;
* проведение предварительного технико-экономического обоснования проектных расчётов стандартных программных средств.

*эксплуатационная деятельность:*

* установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов технических систем обеспечения безопасности информации;
* участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации;
* администрирование подсистем обеспечения информационной безопасности на объекте;

*аналитическая деятельность:*

* получение и обработка поступающей информации;
* анализ и отбор данных и сведений для формирования информационных ресурсов;
* обработка акустических и видеозаписей, фотоматериалов с целью получения информации, необходимой для формирования ресурсов и оперативного реагирования;
* формирование автоматизированных, в том числе справочных, оперативно-розыскных, криминалистических учетов;
* осуществление информационного и оперативно-аналитического поиска;
* осуществление оперативно-розыскного анализа, идентификации, диагностики и прогнозирования, криминалистической диагностики;
* информационно-аналитическое обеспечение оперативно-розыскных мероприятий и следственных действий;

*организационно-управленческая деятельность:*

* организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;
* разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;
* организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач;

*экспертная деятельность:*

* производство компьютерно-технических экспертиз;
* выявление, классификация и последующий предметный анализ информационных объектов с признаками подготовки и/или совершения преступлений в сфере компьютерной информации.

Соотнесение областей, типов задач и конкретных трудовых функций (обобщённых трудовых функций) профильного и смежных профессиональных стандартов, имеющих отношение к профессиональной деятельности выпускника, приведены в таблице 1.

Таблица 1.

Соотнесение областей, типов задач и конкретных трудовых функций (обобщённых трудовых функций) профессиональных стандартов

|  |  |  |
| --- | --- | --- |
| Область  профессиональной деятельности  (по Реестру  Минтруда) | Типы задач  профессиональной  деятельности | Коды трудовых функций (задачи профессиональной деятельности) профильного профессионального стандарта |
| *06 Связь, информационные и коммуникационные технологии (в сфере деятельности по обследованию и экспертизе компьютерных систем)* | *аналитический* | 06.031 Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности:  A/01.7 - Автоматизированная информационно-аналитическая поддержка процессов принятия решений.  A/02.7 - Решение типовых задач обработки информации в ИАС государственных органов, обеспечивающих национальную безопасность.  A/03.7 - Решение типовых задач анализа информации в ИАС государственных органов, обеспечивающих национальную безопасность. |
| *организационно-управленческий* | 06.031 Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности:  D/01.7 - Управление работой коллектива информационно-аналитических работников и специалистов по созданию и эксплуатации ИАС.  D/02.7 - Разработка нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование ИАС.  D/03.7 - Организация работ по выполнению в ИАС требований защиты информации ограниченного доступа. |
| *12 Обеспечение безопасности (в сфере защиты информации)* | *проектно-технологический* | 06.033 Специалист по защите информации в автоматизированных системах:  D/02.7 - Разработка проектных решений по защите информации в автоматизированных системах.  40.178 Специалист в области проектирования автоматизированных систем управления технологическими процессами:  A/04.6 - Разработка простых узлов, блоков автоматизированных систем управления технологическими процессами.  В/01.6 - Предпроектное обследование технологического процесса (объекта управления), для которого разрабатывается проект автоматизированной системы управления.  B/02.6 - Разработка проектных решений отдельных частей автоматизированной системы управления технологическими процессами.  С/01.7 - Разработка концепции автоматизированной системы управления технологическими процессами. |
| *эксплуатационный* | 06.031 Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности:  C/01.7 - Настройка ИАС для решения задач в сфере профессиональной деятельности.  C/02.7 - Обеспечение функционирования ИАС.  C/03.7 - Обеспечение функционирования средств защиты информации в ИАС.  06.033 Специалист по защите информации в автоматизированных системах:  А/02.5 - Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем.  С/01.6 - Установка и настройка средств защиты информации в автоматизированных системах. |
| *экспертный* | Производство компьютерно-технических экспертиз |

**Раздел 3. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ, РЕАЛИЗУЕМЫХ В РАМКАХ НАПРАВЛЕНИЯ ПОДГОТОВКИ (СПЕЦИАЛЬНОСТИ)**

**3.1. Направленности (специализации) образовательных программ в рамках направления подготовки (специальности)**

При разработке программы специалитета Организация выбирает специализацию программы специалитета из следующего перечня:

специализация № 1 "Технологии защиты информации в правоохранительной сфере";

специализация № 2 "Информационно-аналитическое обеспечение правоохранительной деятельности";

специализация № 3 "Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации";

специализация № 4 "Компьютерная экспертиза";

специализация № 5 "Организация и технологии защиты информации (по отраслям)".

Программа специалитета, содержащая сведения, составляющие государственную тайну, разрабатывается и реализуется с соблюдением требований, предусмотренных законодательством Российской Федерации и иными нормативными правовыми актами в области защиты государственной тайны

**3.2. Квалификация, присваиваемая выпускникам образовательных программ**: специалист по защите информации.

**3.3. Объем программы**: 300 зачетных единиц (далее – з.е.).

**3.4. Формы обучения**: очная, очно-заочная.

**3.5. Срок получения образования**

Срок получения образования по программе специалитета (вне зависимости от применяемых образовательных технологий):

- в очной форме обучения, включая каникулы, предоставляемые после прохождения государственной итоговой аттестации, составляет 5 лет;

- в очно-заочной форме обучения увеличивается не менее чем на 6 месяцев и не более чем на 1 год по сравнению со сроком получения образования в очной форме обучения;

- при обучении по индивидуальному учебному плану инвалидов и лиц с ОВЗ может быть увеличен по их заявлению не более чем на 1 год по сравнению со сроком получения образования, установленным для соответствующей формы обучения.

**Раздел 4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

**4.1. Перечень компетенций выпускников**

Перечень универсальных компетенций:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

УК-2. Способен управлять проектом на всех этапах его жизненного цикла;

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;

УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия;

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия;

УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни;

УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;

УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов;

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности;

УК-10. Способен формировать нетерпимое отношение к коррупционному поведению.

Перечень общепрофессиональных компетенций:

ОПК-1. Способен на основе анализа основных этапов и закономерностей исторического развития Российского государства, его места и роли в контексте всеобщей истории формировать устойчивые внутренние мотивы профессионально-служебной деятельности, базирующиеся на гражданской позиции, патриотизме, ответственном отношении к выполнению профессионального долга.

ОПК-2. Способен анализировать мировоззренческие, социальные и личностно-значимые проблемы в целях формирования ценностных, этических основ профессионально-служебной деятельности.

ОПК-3. Способен использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач.

ОПК-4. Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации.

ОПК-5. Способен планировать проведение работ по комплексной защите информации на объекте информатизации.

ОПК-6. Способен применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач.

ОПК-7. Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач.

ОПК-8. Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.

ОПК-9. Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности.

ОПК-10. Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач.

ОПК-11. Способен использовать автоматизированные информационные системы в профессиональной деятельности.

Профессиональные компетенции определяются Организацией самостоятельно на основе профессиональных стандартов, соответствующих профессиональной деятельности выпускников (при наличии) (за исключением профессиональных компетенций, формируемых в рамках программ специалитета, указанных в пункте 1.5 ФГОС ВО).

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, перечень профессиональных компетенций, формируемых в рамках специализаций программы специалитета, указанных в пункте 1.14 ФГОС ВО, определяется на основе квалификационных требований к военно-профессиональной, специальной профессиональной подготовке выпускников, устанавливаемыми федеральным государственным органом, в ведении которого находятся соответствующие организации

При определении профессиональных компетенций на основе профессиональных стандартов Организация осуществляет выбор профессиональных стандартов, соответствующих профессиональной деятельности выпускников, из реестра профессиональных стандартов (перечня видов профессиональной деятельности), размещенного на специализированном сайте Министерства труда и социальной защиты Российской Федерации "Профессиональные стандарты" (http://profstandart.rosmintrud.ru) (при наличии соответствующих профессиональных стандартов).

Из каждого выбранного профессионального стандарта Организация выделяет одну или несколько обобщенных трудовых функций (далее - ОТФ), соответствующих профессиональной деятельности выпускников, на основе установленных профессиональным стандартом для ОТФ уровня квалификации и требований раздела "Требования к образованию и обучению". ОТФ может быть выделена полностью или частично.

При отсутствии профессиональных стандартов, соответствующих профессиональной деятельности выпускников, профессиональные компетенции определяются Организацией на основе анализа требований к профессиональным компетенциям, предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями, объединениями работодателей отрасли, в которой востребованы выпускники, иных источников.

Перечень рекомендуемых профессиональных компетенций по специализации **№ 4 «Компьютерная экспертиза»:**

ПК-Р4.1. Способен проводить исследования компьютерных инцидентов, правонарушений, преступлений.

ПК-Р4.2. Способен использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов.

ПК-Р4.3. Способен подготавливать экспертные заключения по результатам выполненных работ по экспертизе компьютерных систем.

Перечень рекомендуемых профессиональных компетенций по специализации **№ 5 «Организация и технология информационной безопасности»:**

ПК-Р5.1. Способен планировать и внедрять мероприятия защиты информации с учётом локальных нормативных актов и стандартов информационной безопасности.

ПК-Р5.2. Способен проводить аудит объектов информатизации в соответствии с нормативными документами.

ПК-Р5.3. Способен учитывать и использовать особенности информационных технологий, применяемых в правоохранительной сфере, при организации защиты обрабатываемой в них информации.

**4.2. Индикаторы достижения компетенций выпускников**

Перечень индикаторов достижения универсальных и общепрофессиональных компетенций выпускников, соотнесенных с компетенциями, приведен в таблицах 2, 3.

Организация вправе дополнить указанный перечень индикаторами, разработанными самостоятельно.

Индикаторы достижения профессиональных компетенций выпускников Организация разрабатывает самостоятельно.

Таблица 2

**Универсальные компетенции выпускников и индикаторы их достижения**

**специальность 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Код и наименование ОПК** | **Код индикатора** | **Индикаторы достижения компетенций** | **Наименование учебной, дисциплины (модуля), практики, НИР, ВКР, формирующие компетенцию по примерному учебному плану** | **Код ПС (код ОТФ, ТФ,) при наличии** |
| **Универсальные компетенции (УК)** | | | | |
| **УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;** | УК-1.1.1 | знает содержание и взаимосвязь основных принципов, законов, понятий и категорий философских наук, основные этапы развития философской мысли, основную проблематику и структуру философского знания | Философия;  Логика |  |
| УК-1.1.2 | знает понятие мировоззрения, исторические типы мировоззрения, соотношение философии и мировоззрения, соотношение философского мировоззрения и научной картины мира |
| УК-1.1.3 | знает основные источники информации о проблемных ситуациях в профессиональной деятельности и подходы к критическому анализу этой информации |
| УК-1.1.4 | знает порядок принятия решений при возникновении проблемных ситуаций в профессиональной деятельности |
| УК-1.2.1 | умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий в ходе решения профессиональных задач |
| **УК-2. Способен управлять проектом на всех этапах его жизненного цикла;** | УК-2.1.1 | знает основные модели жизненного цикла проекта, его этапы и фазы, их характеристики и особенности | Экономика |  |
| УК-2.2.1 | умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности |
| **УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;** | УК-3.1.1 | знает содержание организации и руководства деятельностью рабочего коллектива (группы) | Производственная (преддипломная) практика |  |
| УК-3.1.2 | знает социально-психологические характеристики рабочего коллектива (группы) |
| УК-3.1.3 | знает основы поддержания нравственных отношений в рабочем коллективе (группе) |
| УК-3.2.1 | умеет организовывать работу коллектива (группы) для решения поставленных задач в сфере профессиональной деятельности |
| **УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия;** | УК-4.1.1 | знает языковые нормы, правила составления и оформления различных служебных документов и научных текстов, а также формулы речевого этикета в профессиональном общении | Иностранный язык или  дисциплина (модуль) части, формируемой участниками образовательных отношений |  |
| УК-4.1.2 | знает основные фонетические особенности, лексический минимум, грамматический строй иностранного языка для устной и письменной коммуникации в сфере профессиональной деятельности | Иностранный язык |
| УК-4.2.1 | умеет составлять тексты различных типов в сфере профессиональной деятельности в соответствии с языковыми нормами, особенностями функциональных стилей речи и установленными стандартами |
| УК-4.2.2 | умеет вести диалогическую и монологическую речь в основных ситуациях профессионального общения на иностранном языке, читать и переводить (со словарем) тексты, извлекать и использовать в профессиональной деятельности полученную информацию |
| **УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия;** | УК-5.1.1 | знает особенности культуры народов России и основных мировых цивилизаций, особенности мировых и основных национальных религий, влияющие на взаимодействие в профессиональной деятельности | История (История России, Всеобщая история);  Политология |  |
| УК-5.2.1 | умеет учитывать национальные, этнокультурные и конфессиональные особенности при взаимодействии в профессиональной деятельности |
| **УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни;** | УК-6.1.1 | знает методы и средства самостоятельного решения задач в сфере профессиональной деятельности | Производственная (преддипломная) практика |  |
| УК-6.1.2 | знает основы деятельностного подхода |
| УК-6.2.1 | умеет определять приоритеты профессиональной деятельности и способы ее совершенствования на основе самооценки |
| УК-6.2.2 | умеет планировать самостоятельную деятельность в решении профессиональных задач |
| **УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности[[1]](#footnote-1);** | УК-7.1.1 | знает основы теории и методики физического воспитания | Физическая культура |  |
| УК-7.1.2 | знает основы организации и проведения самостоятельных занятий по физической подготовке |
| УК-7.2.1 | умеет переносить физическую нагрузку и психологическое напряжение, возникающее в связи с ней |
| **УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов1;** | УК-8.1.1 | знает опасные и вредные факторы системы «человек – среда обитания», факторы, угрожающие жизни человека в условиях чрезвычайных ситуаций и военных конфликтов | Безопасность жизнедеятельности[[2]](#footnote-2) |  |
| УК-8.1.2 | знает основные требования по охране окружающей среды, по охране труда и технике безопасности в профессиональной деятельности и в повседневной жизни, основные приемы оказания первой помощи |
| УК-8.2.2 | умеет использовать средства индивидуальной защиты, оказывать первую помощь при ранениях и травмах в повседневной деятельности, в условиях чрезвычайных ситуаций и военных конфликтов |
| **УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности** | УК-9.1.1 | знает основные виды доходов, финансовые инструменты, виды и источники возникновения экономических и финансовых рисков в экономике | Экономика |  |
| УК-9.1.2 | знает место, роль и функции государства в экономике, цели, задачи и инструменты бюджетно-налоговой, денежно-кредитной политики государства и их влияние на макроэкономические параметры и поведение индивидов |
| УК-9.1.3 | знает нормативные правовые акты, регламентирующие вопросы реализации бюджетно-налоговой и денежно-кредитной политики государства |
| УК-9.2.1 | умеет анализировать информацию, необходимую для принятия обоснованных экономических решений, уметь прогнозировать их последствия и применять полученные знания в сфере личного экономического и финансового планирования |
| УК-9.2.1 | умеет применять нормативные правовые акты при принятии экономических решений |
| **УК-10. Способен формировать нетерпимое отношение к коррупционному поведению** | УК-10.1.1 | знает содержание основных нормативных правовых актов в сфере противодействия коррупции | Правоохранительные органы |  |
| УК-10.2.2 | умеет соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей |

Таблица 3

**Общепрофессиональные компетенции выпускников и индикаторы их достижения**

**специальность 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»**

| **Код и наименование ОПК**  **специализации** | **Код**  **индикатора** | **Индикаторы достижения общепрофессиональных компетенций специализации** | **Наименование учебной дисциплины (модуля), практики, НИР, ВКР, формирующие ОПК по примерному учебному плану** | **Код ПС,**  **код ОТФ, ТФ,**  **(при наличии)** |
| --- | --- | --- | --- | --- |
| **Общепрофессиональные компетенции (ОПК)** | | | |  |
| **ОПК-1.** Способен на основе анализа основных этапов и закономерностей исторического развития Российского государства, его места и роли в контексте всеобщей истории формировать устойчивые внутренние мотивы профессионально-служебной деятельности, базирующиеся на гражданской позиции, патриотизме, ответственном отношении к выполнению профессионального долга. | ОПК-1.1 | Анализирует основные этапы и закономерности исторического развития России, осознает ее место и роль в контексте всеобщей истории | История (История России, Всеобщая история);  Политология;  Правоохранительные органы;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/03.7;  ОТФ D,  ТФ D/01.7. |
| ОПК-1.2 | Учитывает место и роль исторического развития России при формировании гражданской позиции и развитии патриотизма |
| **ОПК-2.** Способен анализировать мировоззренческие, социальные и личностно-значимые проблемы в целях формирования ценностных, этических основ профессионально-служебной деятельности. | ОПК-2.1 | Применяет основные категории философии к анализу мировоззренческой специфики различных культурных сообществ | Философия;  Правоохранительные органы;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/03.7;  ОТФ D,  ТФ D/01.7. |
| ОПК-2.2 | Анализирует социальные и личностно-значимые проблемы в целях формирования ценностных, этических основ профессионально-служебной деятельности |
| **ОПК-3.** Способен использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач. | ОПК-3.1 | Анализирует естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности | Математика;  Прикладная математика;  Математические основы обработки информации;  Дискретная математика;  Физика;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/02.7.  ПС 06.033 -  ОТФ D,  ТФ D/02.7. |
| ОПК-3.2 | Решает стандартные профессиональные задачи с применением междисциплинарных и общенаучных знаний, методов математического анализа и моделирования |
| ОПК-3.3 | Проводит теоретические и экспериментальные исследования объектов профессиональной деятельности |
| **ОПК-4.** Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации. | ОПК-4.1 | Выполняет технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности | Теория информационной безопасности и методология защиты информации;  Организационная защита информации;  Правовая защита информации;  Информационное право;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ D,  ТФ D/02.7;  ОТФ D,  ТФ D/03.7.  ПС 06.033 -  ОТФ A,  ТФ А/02.5;  ОТФ D,  ТФ D/02.7.  ПС 40.178 -  ОТФ A,  ТФ A/04.6;  ОТФ B,  ТФ В/01.6;  ОТФ B,  ТФ В/02.6;  ОТФ C,  ТФ С/01.7. |
| ОПК-4.2 | Разрабатывает рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации |
| **ОПК-5.** Способен планировать проведение работ по комплексной защите информации на объекте информатизации | ОПК-5.1 | Планирует проведение работ по комплексной защите информации на объекте информатизации в соответствии с действующими нормативными и методическими документами в области защиты информации | Теория информационной безопасности и методология защиты информации;  Организационная защита информации;  Технологии защищенного документооборота  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ C,  ТФ C/03.7;  ОТФ D,  ТФ D/02.7;  ОТФ D,  ТФ D/03.7.  ПС 06.033 -  ОТФ A,  ТФ А/02.5. |
| ОПК-5.2 | Подготавливает объект информатизации для прохождения аттестации на соответствие требованиям государственных и ведомственных нормативных документов |
| **ОПК-6.** Способен применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач. | ОПК-6.1 | Применяет положения теорий электрических цепей, радиотехнических сигналов, электрической связи, распространения радиоволн для решения профессиональных задач | Основы электротехники и радиоэлектроники  Основы электро-, радиоизмерений;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/02.7. |
| ОПК-6.2 | ОПК-6.2. Применяет положения теорий цифровой обработки сигналов, информации и кодирования для решения профессиональных задач |
| **ОПК-7.** Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач. | ОПК-7.1 | Применяет современные информационно-коммуникационные технологии, технические и программные средства при решении задач профессиональной деятельности | Средства вычислительной техники;  Программирование: языки, методы и технологии;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/01.7;  ОТФ А,  ТФ A/02.7;  ОТФ А,  ТФ A/03.7. |
| ОПК-7.2 | Применяет языки, методы и инструментальные средства программирования для решения профессиональных задач |
| **ОПК-8.** Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз. | ОПК-8.1 | Планирует и реализует комплекс мер по обеспечению безопасности информации | Техническая защита информации;  Программно-аппаратная защита информации;  Криптографическая защита информации;  Системы и сети передачи информации;  Технологии защищенного документооборота  Безопасность сетей ЭВМ;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ C,  ТФ C/01.7;  ОТФ C,  ТФ C/02.7;  ОТФ C,  ТФ C/03.7.  ПС 06.033 -  ОТФ C,  ТФ С/01.6. |
| ОПК-8.2 | ОПК-8.2. Обеспечивает комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз |
| **ОПК-9.** Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности. | ОПК-9.1 | Применяет технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности | Информатика и информационные технологии в правоохранительной деятельности;  Документоведение;  Специальные информационные технологии в правоохранительной деятельности;  Интеллектуальные технологии в задачах информационной безопасности;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/01.7;  ОТФ А,  ТФ A/02.7;  ОТФ А,  ТФ A/03.7. |
| **ОПК-10.** Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач. | ОПК-10.1 | Осуществляет аналитическую деятельность с последующим использованием данных при решении профессиональных задач | Информатика и информационные технологии в правоохранительной деятельности;  Специальные информационные технологии в правоохранительной деятельности;  Интеллектуальные технологии в задачах информационной безопасности;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/01.7;  ОТФ А,  ТФ A/02.7;  ОТФ А,  ТФ A/03.7. |
| **ОПК-11.** Способен использовать автоматизированные информационные системы в профессиональной деятельности. | ОПК-11.1 | Формирует и поддерживает в актуальном состоянии автоматизированные базы и банки данных | Информатика и информационные технологии в правоохранительной деятельности;  Документоведение;  Специальные информационные технологии в правоохранительной деятельности;  Интеллектуальные технологии в задачах информационной безопасности;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/01.7;  ОТФ А,  ТФ A/02.7;  ОТФ А,  ТФ A/03.7. |
| ОПК-11.2 | ОПК-11.2. Использует автоматизированные информационно-поисковые и логико-аналитические системы в профессиональной деятельности |

Таблица 4

**Рекомендуемые профессиональные компетенции выпускников и индикаторы их достижения**

**специальность 10.05.05 «Безопасность информационных технологий  
в правоохранительной сфере»**

**специализация № 4 «Компьютерная экспертиза»**

| **Код и наименование ПК** | **Код**  **индикатора**  **ПК** | **Индикаторы достижения рекомендуемых профессиональных компетенций** | **Наименование рекомендуемых учебной, дисциплины (модуля), практики, НИР, ВКР, формирующие ПК** | **Код ПС -**  **код ОТФ, ТФ** |
| --- | --- | --- | --- | --- |
| **Рекомендуемые профессиональные компетенции (ПК) Специализация № 4 «Компьютерная экспертиза»** | | | | |
| **ПК-Р4.1.** Способен проводить исследования компьютерных инцидентов, правонарушений, преступлений | ПК-Р4.1.1 | Проводит классификацию и общую характеристику методов и средств, применяемых при проведении экспертных исследований (экспертиз), и применяет имеющиеся знания при обнаружении, фиксации и исследовании объектов компьютерно-технической экспертизы | Компьютерная криминалистика;  Расследование компьютерных инцидентов;  Инструментальное обеспечение компьютерной экспертизы;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/01.7;  ОТФ А,  ТФ A/02.7;  ОТФ А,  ТФ A/03.7. |
| ПК-Р4.1.2 | Проводит компьютерно-технические экспертизы и исследования, направленные на решение идентификационных и диагностических задач при расследовании компьютерных инцидентов |
| ПК-Р4.1.3 | Применяет инструментальные средства и методы при производстве компьютерно-технических экспертиз и расследовании компьютерных инцидентов |
| **ПК-Р4.2.** Способен использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов | ПК-Р4.2.1 | Применяет приемы, средства и методы работы с цифровыми следами для получения розыскной и доказательственной информации | Расследование компьютерных инцидентов;  Методы хранения, восстановления и анализа данных;  Следообразование в компьютерных системах;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/01.7;  ОТФ А,  ТФ A/02.7;  ОТФ А,  ТФ A/03.7;  ОТФ C,  ТФ C/01.7;  ОТФ C,  ТФ C/02.7. |
| ПК-Р4.2.2 | Применяет методики поиска, обнаружения, фиксации, и исследования цифровых следов при различных типах воздействия (в том числе неправомерного) на автоматизированную (информационную) систему |
| ПК-Р4.2.3 | Осуществляет комплекс мероприятий, связанных с обнаружением, фиксацией, изъятием, хранением и исследованием цифровых доказательств совершения преступлений в целях дальнейшего производства компьютерных экспертиз |
| **ПК-Р4.3.** Способен подготавливать экспертные заключения по результатам выполненных работ по экспертизе компьютерных систем | ПК-Р4.3.1 | Составляет и оформляет заключения эксперта с применением правовых, теоретических, методических и организационных основ компьютерной экспертизы | Компьютерная криминалистика;  Правовые и организационные основы компьютерной экспертизы;  Производственная (преддипломная) практика. | ПС 06.031 -  ОТФ А,  ТФ A/03.7;  ОТФ D,  ТФ D/02.7. |
| ПК-Р4.3.2 | Интерпретирует результаты применения средств и методов для решения задач компьютерно-технической экспертизы |
| ПК-Р4.3.3 | Формулирует выводы по результатам экспертных исследований на основе поставленных перед экспертом вопросов |

Таблица 5

**Рекомендуемые профессиональные компетенции выпускников и индикаторы их достижения**

**специальность 10.05.05 «Безопасность информационных технологий   
в правоохранительной сфере»**

**специализация № 5 «Организация и технология информационной безопасности»**

| **Код и наименование ПК** | **Код**  **индикатора**  **ПК** | **Индикаторы достижения рекомендуемых профессиональных компетенций** | **Наименование рекомендуемых учебной, дисциплины (модуля), практики, НИР, ВКР, формирующие ПК** | **Код ПС -**  **код ОТФ, ТФ** |
| --- | --- | --- | --- | --- |
| **Рекомендуемые профессиональные компетенции (ПК) Специализация № 5 «Организация и технология информационной безопасности»** | | | | |
| **ПК-Р5.1.** Способен планировать и внедрять мероприятия защиты информации с учётом локальных нормативных актов и стандартов информационной безопасности | ПК-Р5.1.1 | Организовывает планирование разработки и внедрение защищенной автоматизированной системы с учетом требований информационной безопасности | Безопасность персональных данных; Технологии защищенного документооборота; Разработка и эксплуатация автоматизированных систем в защищенном исполнении. | ПС 06.031 -  ОТФ А,  ТФ A/01.7;  ОТФ А,  ТФ A/02.7;  ОТФ А,  ТФ A/03.7. |
| ПК-Р5.1.2 | Осуществляет проектную деятельность в области защиты информации в соответствии с требованиями нормативной правовой документации |
| ПК-Р5.1.3 | Проводит подготовку исходных данных для технико-экономического обоснования проектных решений при проектировании автоматизированных систем, обеспечивает и контролирует реализацию требований политики информационной безопасности |
| **ПК-Р5.2.** Способен проводить аудит объектов информатизации в соответствии с нормативными документами | ПК-Р5.2.1 | Проводит инструментальный анализ уязвимостей систем защиты информации автоматизированных систем | Аудит информационной безопасности; Безопасность операционных систем; Организационная защита информации. Правовая защита информации  Разработка и эксплуатация автоматизированных систем в защищенном исполнении | ПС 06.031 -  ОТФ А,  ТФ A/01.7;  ОТФ А,  ТФ A/02.7;  ОТФ А,  ТФ A/03.7;  ОТФ C,  ТФ C/01.7;  ОТФ C,  ТФ C/02.7. |
| ПК-Р5.2.2 | Применяет знания в области администрирования операционных систем при разработке и проведении исследований безопасности автоматизированных систем |
| ПК-Р5.2.3 | Организовывает комплексную защиту информации ограниченного доступа в соответствии с действующими нормативными и методическими документами в области защиты информации, с учетом решаемых задач и структуры объекта информатизации |
| **ПК-Р5.3.** Способен учитывать и использовать особенности информационных технологий, применяемых в правоохранительной сфере, при организации защиты обрабатываемой в них информации | ПК-Р5.3.1 | Обеспечивает выполнение требований информационной безопасности при внедрении и эксплуатации автоматизированной системы | Разработка и эксплуатация автоматизированных систем в защищенном исполнении; Интеллектуальные технологии в задачах информационной безопасности; Администрирование вычислительных сетей. | ПС 06.031 -  ОТФ А,  ТФ A/03.7;  ОТФ D,  ТФ D/02.7. |
| ПК-Р5.3.2 | Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности |
| ПК-Р5.3.3 | Контролирует функционирование средств вычислительной техник и систем обеспечения информационной безопасности |

**Раздел 5. ПРИМЕРНАЯ СТРУКТУРА И СОДЕРЖАНИЕ ОПОП**

**5.1. Рекомендуемый объем обязательной части образовательной программы**

Объем обязательной части программы специалитета без учета объема государственной итоговой аттестации должен составлять не менее 40 процентов общего объема программы специалитета.

Рекомендуемый объем обязательной части составляет не менее 120 з.е.

**5.2. Рекомендуемые типы практики**

Типы учебной практики:

ознакомительная практика;

оперативно-служебная (служебная) практика;

технологическая практика.

Типы производственной практики:

практика по профилю специализации;

оперативно-служебная (служебная) практика;

технологическая практика;

эксплуатационная практика;

экспертная практика;

преддипломная практика.

Организация:

выбирает один или несколько типов учебной практики и один или несколько типов производственной практики из указанного перечня;

вправе установить дополнительный тип (типы) учебной и (или) производственной практик;

устанавливает объемы практик каждого типа.

Общий объем практик должен составлять не менее 24 з.е.

**5.3. Примерный учебный план и примерный календарный учебный график**

Примерный учебный план и примерный календарный учебный график приведены в приложениях 3 и 4.

**5.4. Примерная рабочая программа воспитания**

Цели воспитательной работы:

- создание условий для активной жизнедеятельности обучающихся, их гражданского самоопределения, профессионального становления   
и индивидуально-личностной самореализации в созидательной деятельности для удовлетворения потребностей в нравственном, культурном, интеллектуальном, социальном и профессиональном развитии;

- подготовка творчески мыслящих и гармонично развитых специалистов, обладающих профессиональными навыками и высокими гражданскими качествами.

Задачи воспитательной работы:

- формирование уважительного отношения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности;

- воспитание внутренней потребности личности в здоровом образе жизни, ответственного отношения к природной и социокультурной среде;

- обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств необходимых для эффективной профессиональной деятельности;

- выявление и поддержка талантливой молодежи, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;

- создание и совершенствование условий для личностного   
и профессионального формирования обучающихся в соответствии с моделью личности выпускника;

- разработка системы воспитательной деятельности, которая позволит достигать высокого уровня характеристик, предполагаемых в модели личности выпускника.

Результаты реализации программы воспитания:

- формирование системы компетенций на основе использования ресурсов учебной, внеучебной и социально-ориентированной деятельности;

- формирование духовных, социальных и профессиональных ценностей;

- обогащение личностного и социального опыта обучающихся;

- профессионально-личностная самореализация обучающихся.

Направления воспитательной работы приведены в таблице 5.

Таблица 5

Направления воспитательной работы Организации

| №  п/п | Направления воспитательной работы | Воспитательные задачи |
| --- | --- | --- |
| 1 | Гражданско-правовое  и патриотическое воспитание, формирование патриотического сознания  и поведения обучающихся, уважения к закону | формирование патриотического сознания  и поведения обучающихся, уважения к закону  и правопорядку, готовности к достойному  служению обществу и государству, нетерпимого  отношения к коррупционному поведению |
| 2 | Нравственное воспитание, межнациональные отношения и толерантность | развитие духовно-нравственной культуры студента:  повышение степени освоения личностью социального опыта, ценностей культурно-регионального сообщества, культуры, приобщение студентов к нравственным ценностям, развитие нравственных чувств; становление нравственной воли; побуждение  к нравственному поведению;  развитие культуры межнационального общения  и формирование установок на равнозначность  и равноценность каждого члена общества,  социальная адаптация иностранных граждан,  социальная адаптация лиц с ограниченными  возможностями здоровья и инвалидов |
| 3 | Профессиональная ориентация | помощь в формировании критериев выбора индивидуальной траектории профессионального развития |
| 4 | Развитие добровольчества  и волонтерства | поддержка добровольческих и волонтерских инициатив по всем направлениям (в сфере гражданско-патриотического воспитания, охраны природы, спорта, донорства и т.д.) |
| 5 | Культурно-творческое воспитание | поддержка и развитие творческих способностей  и талантов обучающихся;  создание условий для развития эстетического вкуса, повышения уровня культуры, приобщение  к культурному наследию и традициям народов России |
| 6 | Физическое воспитание  и популяризация здорового образа жизни | формирование навыков здорового образа жизни, массового спорта и физической культуры, профилактика вредных привычек |
| 7 | Информационно-воспитательная работа | повышение культуры информационной безопасности в молодежной среде, противодействие распространению идеологии терроризма, экстремизма, национализма, ксенофобии |
| 8 | Развитие самоуправления обучающихся | поддержка инициативы обучающихся в вопросах организации учебной и внеучебной жизни |
| 9 | Воспитательная работа  в рамках учебной деятельности – научно-образовательное воспитание | содействие профессиональному самоопределению обучающихся, их профессиональному развитию;  формирование исследовательского и критического  мышления, мотивации к научно-исследовательской деятельности |

Управление воспитательной работой.

Основными функциями управления воспитательной работой выступают:

- планирование воспитательной работы на учебный год;

- организация воспитательной работы;

- анализ итогов воспитательной работы;

- контроль за исполнением управленческих решений   
по воспитательной работе;

- регулирование воспитательной работы.

Основным инструментом управления воспитательной работой Организации являются: Рабочая программа воспитательной работы, План воспитательной работы на учебный год, Концепция воспитательной деятельности (при наличии).

Реализация мероприятий воспитательной работы в Организации, мониторинг ее качества и анализ результатов реализуются поэтапно:

1 этап реализации программы воспитания обучающихся – формирование ценностно-смысловых основ профессиональной деятельности (1 курс):

- анализ портфолио (количество обучающихся, получивших почетные грамоты, благодарности, благодарственные письма за активную общественную работу, в сфере воспитательной деятельности);

- создание условий для формирования и исследования уровня удовлетворенности различными аспектами жизни обучающихся (анкетирование);

- создание условий для формирования студенческого самоуправления   
в студенческом коллективе и изучение динамики его развития (формирование старостата, анализ вовлеченности обучающихся в различные направления деятельности Студенческого совета, внеаудиторные мероприятия);

- изучение сформированности ценностных ориентиров, уровня ответственности, патриотических, гражданских качеств, толерантности   
в современных реалиях совместного сосуществования различных народов   
и национальностей в соответствии с общечеловеческими идеалами (анкетирование);

- популяризация здорового образа жизни, профилактика вредных привычек (анкетирование обучающихся).

2 этап реализации программы воспитания обучающихся –профессионализация (2-3 курс):

- анализ портфолио (количество обучающихся, получивших почетные грамоты, благодарности, сертификаты участников в мероприятиях профессиональной направленности, благодарственные письма за активную общественную работу, в сфере воспитательной деятельности);

- сформированность профессиональных ориентиров (анкетирование);

- оценка уровня правосознания, нетерпимости к коррупционному поведению, идеологии экстремизма, ксенофобии (анкетирование);

- оценка уровня понимания важности саморазвития, индивидуально- психологических свойств для себя и общества (анкетирование);

3 этап реализации программы воспитания обучающихся – формирование мотивации к профессиональной деятельности (4 курс):

- анализ портфолио (количество обучающихся, получивших почетные грамоты, благодарности, сертификаты участников в мероприятиях профессиональной направленности, благодарственные письма за активную общественную работу, в сфере воспитательной деятельности);

- исследование уровня готовности обучающихся к решению профессиональных задач (анкетирование преподавателей);

- анкетирование уровня оказания помощи в трудоустройстве;

- анализ карьерных устремлений выпускников;

- анализ уровня мотивации;

- выявление потребности в молодых специалистах (анкетирование работодателей).

Результаты анкетирования обобщаются отделом организации воспитательной работы, факультетами, обсуждаются коллегиальными органами управления Организации и являются основанием для совершенствования рабочей программы воспитания.

**5.5. Примерный календарный план воспитательной работы**

Календарный план воспитательной работы Организации включает перечень основных мероприятий по направлениям воспитательной работы.

Примерная форма плана представлена в таблице 6.

Таблица 6

Примерная форма календарного плана воспитательной работы Организации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Дата | Содержание и формы деятельности  *(наименование мероприятий, формы: например, учебная экскурсия (виртуальная экскурсия), дискуссия, проектная сессия, акция, концерт, деловая игра, студенческая конференция и т.д.*[[3]](#footnote-3) | Участники  *(курс, группа, члены кружка, секции, проектная команда и т.п.)* | Место проведения | Ответственные |
| 1 | 2 | 3 | 4 | 5 |
| СЕНТЯБРЬ | | | | |
| 1 | День знаний |  |  |  |
| 3 | День солидарности в борьбе с терроризмом |  |  |  |
|  | День города |  |  |  |
|  | Работа кураторов с первокурсниками |  |  |  |
| 13 | День программиста (256 день года) |  |  |  |
|  | Посвящение в студенты |  |  |  |
|  | Введение в профессию (специальность) |  |  |  |
|  | Посещение совета ветеранов ВОВ |  |  |  |
| 27 | Всемирный день туризма |  |  |  |
| 29 | День Интернета России |  |  |  |
| ОКТЯБРЬ | | | | |
| 1 | День пожилых людей |  |  |  |
| 16 | День отца |  |  |  |
| НОЯБРЬ | | | | |
| 4 | День народного единства |  |  |  |
| 7 | День проведения военного парада на Красной площади |  |  |  |
| 17 | Международный день студентов |  |  |  |
| 19 | День преподавателя высшей школы |  |  |  |
| 27 | День матери (последнее воскресенье месяца) |  |  |  |
| 1 | 2 | 3 | 4 | 5 |
| ДЕКАБРЬ | | | | |
| 3 | День неизвестного солдата |  |  |  |
| 4 | День информатики |  |  |  |
| 9 | День Героев Отечества |  |  |  |
| 12 | День Конституции Российской Федерации |  |  |  |
| ЯНВАРЬ | | | | |
| 1 | Новый год |  |  |  |
| 25 | «Татьянин день» (праздник студентов) |  |  |  |
| ФЕВРАЛЬ | | | | |
| 8 | День русской науки |  |  |  |
| 23 | День защитников Отечества |  |  |  |
|  | Мероприятия по направлению «Ценностные приоритеты современной молодежи» |  |  |  |
| МАРТ | | | | |
| 8 | Международный женский день |  |  |  |
| 14 | Международный день числа «ПИ» |  |  |  |
| 18 | День воссоединения Крыма с Россией |  |  |  |
|  | Мероприятия по пропаганде здорового  образа жизни |  |  |  |
| АПРЕЛЬ | | | | |
|  | Участие во всероссийской акции "День  единых действий" |  |  |  |
| 20 | День донора России |  |  |  |
|  | Донорская акция |  |  |  |
| 21 | День местного самоуправления |  |  |  |
| 29 | Всемирный день танцев |  |  |  |
| МАЙ | | | | |
| 1 | Праздник весны и труда |  |  |  |
| 7 | День Радио |  |  |  |
| 9 | День Победы |  |  |  |
|  | Всероссийская акция «Бессмертный полк» |  |  |  |
| 24 | День славянской письменности и культуры |  |  |  |
| 1 | 2 | 3 | 4 | 5 |
| 26 | День российского предпринимательства |  |  |  |
| 31 | День без табака |  |  |  |
| ИЮНЬ | | | | |
| 1 | Международный день защиты детей |  |  |  |
| 5 | День эколога |  |  |  |
| 6 | Пушкинский день России |  |  |  |
| 12 | День России |  |  |  |
| 22 | День памяти и скорби |  |  |  |
|  | Ежегодная церемония  награждения  «Студент года» и «Преподаватель года» |  |  |  |
| 27 | День молодежи России |  |  |  |
| ИЮЛЬ | | | | |
| 8 | День семьи, любви и верности |  |  |  |
| АВГУСТ | | | | |
| 22 | День Государственного Флага Российской Федерации |  |  |  |

**5.6. Примерные программы дисциплин (модулей) и практик**

**Б.1.О.1. Дисциплина «История (История России, Всеобщая история)»**

Коды формируемых компетенций:

В результате изучения дисциплины студент должен

знать:

- основные исторические этапы развития общества; основные тенденции отечественной истории в контексте мировой истории с древнейших времен по настоящее время.

уметь:

- учитывать ценности мировой и российской культуры для развития навыков межкультурного диалога;

- использовать знание и понимание проблем человека в современном мире.

владеть:

- навыками определения и аргументированного представления собственного отношения к дискуссионным проблемам истории, опираясь на знания мировой истории и социокультурных традиций мира.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Модуль 1. История древнего мира и средних веков**

Хронологические и географические рамки истории Древнего мира. Ранние цивилизации: Египет. Передняя Азия. Индия. Китай. Материальная культура и экономика ранних цивилизаций. Социальный строй. Политическая и военная организация. Античная цивилизация. Становление полисной цивилизации в Греции: географические и социальные предпосылки Древний Рим: этапы становления общества и государства. Экономика, общественный строй, государственный аппарат в республиканском и императорском Риме. Религии Древнего мира. Возникновение мировых религий. Асинхронность развития средневековых обществ, роль кочевников, хронологические рамки данного периода для разных стран. Великое переселение народов и его исторические результаты. Государства Европы VIII—XІ вв. Основные черты и этапы развития восточно-христианской цивилизации. Быт и хозяйство восточных славян. Общественные отношения. Верования. Славянский пантеон и языческие обряды. Племенные союзы восточных славян. Предпосылки образования государства у восточных славян. Основные направления внешней политики киевских князей в X-XII веках. Взаимоотношения Руси и Византии в XI–XII вв. Истоки русской культуры. Крещение Руси. Значение христианства в становлении национальной культуры. Политическая раздробленность и ее причины. Складывание средневековых классов и сословий. Аграрный характер средневековой цивилизации. Основные формы государственной власти. Сословно-представительные монархии. Церковь и общество. Социальные конфликты в Средние века. Крестовые походы. Процесс самоидентификации европейских государств в XIII - первая половина XVI в.в. Русь в эпоху феодальной раздробленности. Борьба Руси с иноземными завоевателями. Характер и особенности объединения Руси. Деятельность московских князей. Формирование органов центральной и местной власти. Тенденции развития государств в период позднего средневековья. Россия в царствование Ивана Грозного. Особенности социально-экономических отношений и сословно-представительных монархий в XVI- XVII вв.. «Смутное время» в истории российского государства.

**Модуль 2. История нового и новейшего времени**

Век просвещения» и «революций» в Европе: начало промышленного переворота и политических реформ. Особенности модернизационных процессов в европейских государствах в XVIII в. Становление российского абсолютизма. Реформы Петра I. Северная война и ее итоги. Эпоха дворцовых переворотов в российской истории. Особенности «просвещенного абсолютизма» в России. Екатерина II. Внешняя политика России во второй половине XVIII в. Россия и мир в XIX веке: политическое и социально-экономическое развитие, обострение геополитических проблем. Реформы начала царствования Александра I. Николай I. Смена политических приоритетов. Александр II и «великие реформы». Правление Александра III. Колониальные империи Великобритании и Франции. Возвышение Германии и США. Территориальная экспансия Японии. Россия в системе международных отношений. Основные направления и принципы внешней политики России в XIX в. Антифранцузские коалиции и Отечественная война 1812г. Борьба с Османской империей. Россия и христианские народы Балканского полуострова. Крымская война. Российская империя и народы Кавказа. Кавказская война. Россия и мир в к. XIX-н.ХХ в. в.: обострение геополитических проблем. Русско-японская война. I мировая война. Развитие науки и техники в XIX – нач.ХХ вв.. «Золотой» и «серебряный век» русской культуры. Роль ХХ столетия в мировой истории. Глобализация общественных процессов. Проблема экономического роста и модернизации. Социальная трансформация общества. Столкновение тенденций интернационализма и национализма, интеграции и сепаратизма, демократии и авторитаризма. Революционный процесс и изменение роли империй в мировой истории в к. XIX- нач. ХХ века. 1917 год в судьбе России. Первые мероприятия советской власти. Гражданская война в России – общенациональная трагедия. Образование СССР и его международное признание. Курс на строительство социализма в одной стране. Социально-экономические преобразования в СССР в 30-е гг.: модернизация на почве традиционализма. Мировой экономический кризис и Великая депрессия: истоки, развитие, последствия Формирование и развитие тоталитарных режимов. Сталинизм. II Мировая война. СССР в годы Великой Отечественной войны. Послевоенное развитие мира. Мировое сообщество в период «холодной войны». Распад колониальной системы. Попытки реформирования и обновления социалистической системы в СССР во второй половине1950-х начале 1960- гг. Советское государство в сер.1960-х-нач.1980-х гг. «Разрядка». Война в Афганистане. «Перестройка» в СССР и ее последствия для мирового сообщества. Окончание «холодной войны». Процессы европейской интеграции во второй половине XX в. «Бархатные революции» в Восточной Европе в 1989 г. РФ в 1990-е годы. Становление новой российской государственности. Россия и мир в нач. XXI в. Участие России в мировых интеграционных процессах и формировании современной международно-правовой системы. Проблемы современных международных отношений.

Рекомендуемый перечень основной литературы:

1. Семин, В.П. История: Россия и мир: учебное пособие по дисциплине "История" для студентов вузов неисторических факультетов / В. П. Семин - Москва: КНОРУС, 2013. - 544 с.

2. Рамбо А. История древней и новой России / А. Рамбо - Москва: Директ-Медиа, 2012. - 1224 с. http://biblioclub.ru/index.php?page=book&id=14492.

3. Соловьев С. М. История России с древнейших времен. - Москва: Директ-Медиа, 2016. – 444 с. - http://biblioclub.ru/index.php?page=book&id=442898.

4. История России (для студентов неисторических специальностей ЮФУ): учебник/ К.Г.Малыхин и др.; под общ. ред. К.Г.Малыхина; Южный федеральный университет. – Издание 2-е, переизд. и доп. – Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2020. – 460 с.

**Б.1.О.2. Дисциплина «Физическая культура»**

Коды формируемых компетенций: УК-7.

В результате изучения дисциплины студент должен

знать:

– основы теории и методики физического воспитания;

– основы организации и проведения самостоятельных занятий по физической подготовке;

уметь:

– переносить физическую нагрузку и психологическое напряжение, возникающее в связи с ней.

Примерное распределение часов: трудоемкость дисциплины 2 з.е., 72 час.

Форма контроля: зачет.

Содержание дисциплины:

Теоретические основы физической культуры. Планирование, организация, контроль и учет физической подготовки. Средства и методы физической подготовки. Формы проведения физической подготовки. Учебные занятия, утренняя физическая зарядка, спортивно-массовая работа. Физическая тренировка в процессе учебной деятельности. Самостоятельная тренировка. Основные разделы физической подготовки: гимнастика и атлетическая подготовка, ускоренное передвижение и лёгкая атлетика, спортивные и подвижные игры.

Рекомендуемый перечень основной литературы:

1. Муллер А.Б. Физическая культура. – М.: Издательство Юрайт, 2014;

2. Кошелев В.Ф., Малоземов О.Ю., Бердникова Ю.Г., Минаев А.В., Филимонова С.И. Физическое воспитание студентов в техническом вузе. – Екатеринбург: Изд-во АМБ, 2015.

**Б.1.О.3. Дисциплина «Иностранный язык»**

Коды формируемых компетенций: УК-4.

В результате изучения дисциплины студент должен

знать:

– основные фонетические особенности, лексический минимум, грамматический строй иностранного языка для устной и письменной коммуникации в сфере профессиональной деятельности;

уметь:

– вести диалогическую и монологическую речь в основных ситуациях профессионального общения на иностранном языке, читать и переводить (со словарем) тексты, извлекать и использовать в профессиональной деятельности полученную информацию.

Примерное распределение часов: трудоемкость дисциплины 9 з.е., 324 час.

Форма контроля: 3 зачета, экзамен.

Содержание дисциплины:

Язык как средство межкультурного общения. Фонетика. Лексика. Грамматический строй. Диалогическая и монологическая речь в основных ситуациях. Чтение и перевод текстов. Деловая переписка.

Рекомендуемый перечень основной литературы:

1. Орловская И.В., Самсонова Л.С., Скубриева А.И. Учебник английского языка для студентов технических университетов и вузов. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2006.

2. Карпова Т.А., Асламова Т.В., Закирова Е.С., Красавин П.А. Английский язык для технических вузов. – М.: КНОРУС, 2014.

**Б.1.О.4. Дисциплина «Философия»**

Коды формируемых компетенций: УК-1, ОПК-2.

В результате изучения дисциплины студент должен

знать:

– содержание и взаимосвязь основных принципов, законов, понятий и категорий философских наук, основные этапы развития философской мысли, основную проблематику и структуру философского знания;

– понятие мировоззрения, исторические типы мировоззрения, соотношение философии и мировоззрения, соотношение философского мировоззрения и научной картины мира.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

Философия как особый вид знания. Основные разделы, направления, методы и приемы философии. Философские учения, законы, категории, понятия. Структура и методология научного познания. Сущность, специфика, методология и методы научного исследования. Онтология и гносеология. Принципы, законы, категории диалектики и их применение в научном познании и практике. Философия человека и общества. Философские аспекты мировых религий.

Рекомендуемый перечень основной литературы:

1. Зотов А.Ф., Разин А.В., Миронов В.В. Философия. – М.: Проспект, 2020;

2. Чумаков А.Н. Философия. – М.: Проспект, 2021;

3. Алексеев П.В., Панин А.В. Философия. – М.: Проспект, 2021.

**Б.1.О.5. Дисциплина «Безопасность жизнедеятельности»**

Коды формируемых компетенций: УК-8

В результате изучения дисциплины студент должен

знать:

– опасные и вредные факторы системы «человек – среда обитания», факторы, угрожающие жизни человека в условиях чрезвычайных ситуаций и военных конфликтов;

– основные требования по охране окружающей среды, по охране труда и технике безопасности в профессиональной деятельности и в повседневной жизни, основные приемы оказания первой помощи;

уметь:

– использовать средства индивидуальной защиты, оказывать первую помощь при ранениях и травмах в повседневной деятельности, в условиях чрезвычайных ситуаций и военных конфликтов.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: зачет.

Содержание дисциплины:

**Комфортные и допустимые условия жизнедеятельности.** Введение в БЖД: цель, задачи и содержание дисциплины, ее место и роль среди других наук и в подготовке специалиста; проблема обеспечения безопасности человека в системе «человек - среда обитания»; концепция рисков. Микроклимат и воздушная среда рабочей зоны: влияние микроклимата на работоспособность человека; нормирование параметров микроклимата в конкретном производстве; тепловые излучения и влияние их на организм человека; нормирование тепловых излучений; адаптация и акклиматизация в условиях перегревания и переохлаждения; отопление, вентиляция и кондиционирование воздуха; естественная и механическая вентиляция. Действие вредных веществ на организм человека в конкретном производстве. Нормирование концентрации вредных веществ в воздушной среде рабочей зоны. Методы контроля состояния воздушной среды. Производственный шум: источники шума и шумовые характеристики в конкретном производстве; производственная вибрация; физические характеристики и измерение вибраций в конкретном производстве; характеристика и опасность совместного воздействия вибраций, шума, ультразвука и инфразвука. Производственное освещение: характеристика электрических источников света и осветительных приборов; естественное и совмещенное освещение в производственных цехах. Оптимизация параметров рабочих мест: виды и формы деятельности; энергетические затраты при различных формах деятельности; определение категории тяжести труда; способы оценки тяжести и напряженности трудовой деятельности; работоспособность и ее динамика; пути повышения эффективности трудовой деятельности; эргономические основы безопасности жизнедеятельности. Техногенные и природные чрезвычайные ситуации: прогнозирование параметров и оценка обстановки при ЧС; защитные мероприятия при ЧС; ликвидация последствий ЧС; защита от терроризма. **Электробезопасность при эксплуатации электрических устройств и оборудования.** Электробезопасность: действие электрического тока на организм человека; опасность поражения в различных электрических сетях; заземление и зануление; классификация помещений по электробезопасности; квалификационные группы персонала по электробезопасности; напряжение шага, прикосновения; защитные меры в электроустановках; защитные средства, применяемые в электроустановках; защитная изоляция: виды, роль в обеспечении электробезопасности, критические параметры; защита от статического электричества; организационные и технические мероприятия при эксплуатации электроустановок; средства индивидуальной защиты. Защита от электромагнитных полей высокой и сверхвысокой частоты: основные понятия и определения; физические характеристики электромагнитных полей (ЭМП); воздействие электромагнитных полей на организм человека; тепловой и функциональный эффект; органы человека с повышенной чувствительностью к ЭМП; организационные, технические и санитарно-гигиенические меры защиты от электромагнитных излучений в конкретном производстве; нормирование интенсивности ЭМП; расчет интенсивности ЭМП на рабочих местах в зависимости от параметров источника излучения и среды; определение границ опасной зоны. Защита от лазерных излучений: применение лазеров в технологических процессах; биологическое действие лазерного излучения: воздействие на глаза, кожу, внутренние органы и организм человека в целом; опасные и вредные производственные факторы, сопутствующие эксплуатации лазеров; основные способы и средства защиты от лазерного излучения: экранирование, блокировка, сигнализация, удаление рабочих мест из лазерно-опасной зоны; средства индивидуальной защиты. Радиационная безопасность: основные понятия, определения, единицы измерения в области радиационной безопасности; фоновое облучение человека; нормирование ионизирующих излучений; защита от воздействия ионизирующего излучения на производстве; средства индивидуальной защиты. Пожарная безопасность при эксплуатации электрических устройств: причины возникновения пожаров и взрывов в помещениях и в производственных процессах; опасные факторы при пожарах и взрывах; основные сведения из теории естественного окисления, теплового самовоспламенения и цепных реакций; самовоспламенение смеси газов, воспламенение жидкости, вспышка паров; оценка пожароопасности веществ и материалов; предупреждение взрывов и пожаров; ликвидация их последствий; показатели пожароопасности; классификация зданий и помещений по пожарной (взрывной) опасности; прогнозирование пожаров и взрывов; пожарная безопасность в технологических процессах конкретных производств; системы и средства пожаротушения, пожарной автоматики и сигнализации; средства индивидуальной защиты; правила эвакуации лиц, пострадавших на пожарах, в газоотравленных зонах, при отравлениях. Организация работы по охране труда, пожарной и электробезопасности: виды инструктажей и их периодичность; нормативные документы и инструкции, регламентирующие организацию деятельности по охране труда, пожарной и электробезопасности. Доврачебная помощь пострадавшему: способы и средства оказания доврачебной помощи на производстве и в быту; оказание первой помощи пострадавшим от электрического тока и при других несчастных случаях, возникающих при чрезвычайных ситуациях: ранение, ожоги, обморожения, переломы, вывихи, растяжения связок; условия успеха при оказании первой помощи: быстрота оказания помощи, обученность персонала методам оказания первой медицинской помощи.

Рекомендуемый перечень лабораторных работ:

1. Измерение освещенности.

2. Измерение уровня шума.

3. Оценка электробезопасности на рабочем месте.

Рекомендуемый перечень основной литературы:

1. Белов С.В. Безопасность жизнедеятельности и защита окружающей среды (техносферная безопасность). – М.: Юрайт, 2013;

2. Михайлов Л.А. Безопасность жизнедеятельности. – СПб.: Питер, 2013;

3. Каракиян В.И., Никулина И.М. Безопасность жизнедеятельности. – М.: Юрайт, 2015.

Перечень материально-технического обеспечения:

Для проведения лабораторных работ требуется учебная лаборатория, оборудованная стендами и установками Российского научно-производственного объединения «Росучприбор» или аналогичными:

– «Звукоизоляция и звукопоглощение БЖ2МП»;

– «Эффективность и качество освещения БЖ1МП»;

– «Электробезопасность трехфазных сетей переменного тока БЖ6/1»;

– «Защита от СВЧ излучения БЖ5МП»;

– «Максим 3». Тренажер оказания первой медицинской помощи с пультом управления и настенным табло.

**Б.1.О.6. Дисциплина «Политология»**

Коды формируемых компетенций: УК-5, ОПК-1.

В результате изучения дисциплины студент должен

знать:

- основные методологические подходы и направления современной политологии;

- основные политические институты, проблемы и процессы.

уметь:

- выявлять проблемы в политической сфере и устанавливать их связь с другими сферами жизни российского общества;

- анализировать политические проблемы и процессы, характерные для современности, определять их причины и следствия.

владеть:

- навыками анализа политических явлений и проблем современности;

- навыками обосновывать свою точку зрения по современной политической проблематике.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Политология как наука.** Политология как наука. Объект и предмет политологии как самостоятельной науки. Политическая жизнь общества и властные отношения. Понятие «политика». Особенности политики как самостоятельной сферы общественной жизни. Политология – учение о политике. Содержание и структура политологии: фундаментальный и прикладной уровни, теоретический и эмпирический уровни. Функции политологии. Место политологии в системе гуманитарного знания. Соотношение политологии права с юридическими науками. **История развития политических идей**. Зарождение политических знаний в античном мире (Др. Греция и Рим). Особенности развития политических знаний в эпоху Средневековья. Гражданско- правовых концепций Нового времени в Западной Европе. Специфика развития политической мысли России. Современные политические теории и школы. **Общество и политическая власть**. Природа власти. Механизмы осуществления политической власти. Субъект, объект, ресурсы власти. Понятия «власть», «политическая власть». Причины и условия проявления политической власти. Сущность политической власти, источники, методы функционирования, типы, свойства и функции. Понятие «легитимности» власти. Гражданское общество: понятие, структура, функции. Перспективы гражданского общества в России. Политические элиты и лидерство. Роль элит в осуществлении политической власти. **Политическая система**. Теория политических систем. Структура и функции политической системы. Политическая система общества как совокупность политических общностей, форм, норм и принципов взаимоотношений, в рамках которых реализуется политическая власть. Политические режимы. Типология политических режимов. Тоталитаризм как политический феномен ХХ в. Авторитарные политические режимы. Демократический режим: исторические формы и теоретические модели демократии. **Политические институты**. Государство: понятие, происхождение, органы и функции. Типология государственных систем. Формы государственного устройства и правления. Правовое социальное государство. Современное российское государство. Природа политической партии. Генезис и структура партий. Функции политической партии. Типология партий и партийных систем. Роль партий в системе власти. Российская партийная система. Общественно-политические организации и движения в политической жизни общества. Избирательные системы. Выборы как политический институт. Модификации основных избирательных моделей. **Политическая культура**. Политическая культура как субъективное измерение политики Психологические механизмы приобщения к политике: политическая социализация. Политическое участие и его формы. **Политическая идеология**. Политическое сознание: уровни, функции, формы. Место и роль идеологий в политике. Политические идеологии современности: либерализм, неоконсерватизм, марксистская традиция, современная международная социал-демократия. **Политические процессы и конфликты**. Понятие «политический процесс», его отличие от правового, экономического, идеологического процессов. Типы политических процессов, режимы существования и содержание и этапы. Реформы и революции в политическом развитии общества. Политическая модернизация. Универсальная теория политических процессов Д. Истона. Стадия «развития» политического процесса. Нестабильный «кризисный» политический процесс. Управленческие политические технологии и специфика их применения: «политический стиль». Понятие «политическое решение». Особенности политической модернизации современной России. **Международные отношения**. Особенности мирового политического процесса. Субъекты и формы международных отношений. Структура и система международных отношений. Основные теории международной политики. Современные тенденции международных отношений. Проблема глобализации. Политическая глобалистика: понятие и структура. Страны Запада и страны «третьего мира» в условиях глобализации. Россия и ее национально-государственные интересы в международной политике.

Рекомендуемый перечень основной литературы:

1. Зеленков, М. Ю. Политология : учебник / М. Ю. Зеленков. – 2-е изд., доп. и уточн. – Москва : Дашков и К°, 2020. – 340 с. – (Учебные издания для бакалавров). – URL: <https://biblioclub.ru/index.php?page=book&id=573147>.

2. Муштук, О. З. Политология : учебник : [16+] / О. З. Муштук. – 3-е изд., стер. – Москва : Университет Синергия, 2018. – 480 с. – (Университетская серия). – URL: <https://biblioclub.ru/index.php?page=book&id=571509>.

3. Батурин, В. К. Политология: учебник для бакалавров / В. К. Батурин, И. В. Батурина. – Москва : Юнити, 2016. – 391 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=446890>.

4. Политология : учебник / Н. Н. Гусев, А. И. Сацута, В. Ю. Бельский и др. ; ред. В. Ю. Бельский, А. И. Сацута. – Москва : Юнити, 2015. – 423 с. – (Cogito ergo sum). – URL: <https://biblioclub.ru/index.php?page=book&id=116625>.

**Б.1.О.7. Дисциплина «Логика»**

Коды формируемых компетенций: УК-1.

В результате изучения дисциплины студент должен

знать:

- основные особенности мышления как формы познания, общее понятие языка, его структуры и функций в познании, основные семантические категории языка, элементы языка логики;

- сущность понятия как формы мышления, содержание и объем понятия и их соотношение, основные виды понятий, отношения между понятиями по объему и содержанию;

- основные логические операции над понятиями (обобщение, ограничение, определение, деление объема);

- сущность высказывания (суждения), структуру и виды простых категорических суждений,

- распределенность терминов в простом атрибутивном суждении;

- основные виды сложных высказываний и их логический смысл, основные формы и правила дедуктивных выводов логики высказываний, основные формы и правила дедуктивных выводов логики предикатов;

- простой категорический силлогизм и его общие правила, основные виды вероятностных выводов;

- логическую структуру и виды аргументации, общие правила аргументации.

уметь:

- распознавать виды понятий, раскрывать содержание понятий (давать определение понятиям), обобщать и ограничивать понятия;

- устанавливать вид отношения между понятиями по объему и изображать их в виде круговых схем, определять правильность или неправильность деления объема понятия;

- распознавать виды простого категорического суждения, распознавать распределенность или нераспределенность термина в простом категорическом суждении;

- распознавать логический смысл заданного сложного высказывания и выражать символически его структуру;

- распознавать род и вид заданного умозаключения, устанавливать правильность или неправильность заданного простого категорического силлогизма;

- осуществлять и контролировать простейшие индуктивные обобщения, устанавливать правильность или неправильность заданной аргументации.

владеть:

- навыками анализа и толкования правовых актов;

- навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности;

- навыками анализа правоприменительной и правоохранительной практики разрешения правовых проблем и коллизий.

Примерное распределение часов: трудоемкость дисциплины 2 з.е., 72 час.

Форма контроля: зачет.

Содержание дисциплины:

**Логика и язык.** История возникновения логики как науки. Значение логики. Понятие языка. Семиотика. Синтаксический, семантический и прагматический аспекты анализа языка. Естественные и искусственные языки. Язык логики предикатов. Алфавит языка логики предикатов. Законы логики. Основные логические законы: закон тождества, закон противоречия, закон исключенного третьего, закон достаточного основания. **Понятия.** Понятие как форма мышления. Соотношение понятия и слова. Содержание и объем понятия. Закон обратного отношения между объемом и содержанием понятия. Виды понятий. Полная логическая характеристика понятия. Основные виды понятий. Отношения между понятиями. Сравнимые и несравнимые понятия. Совместимые и несовместимые понятия. Отношения совместимости и несовместимости понятий. Изображение отношений между понятиями с помощью круговых схем Эйлера. **Определение и классификация.** Обобщение и ограничение понятий. Обобщение понятий. Родовые категории. Ограничение понятий. Предел ограничения понятий. Отличие логических операций обобщения и ограничения понятий от мысленного перехода от части к целому и выделения части из целого. Определение понятий. Основные правила определения понятий. Деление и классификация понятий. **Суждение и норма.** Суждение как форма мышления. Общая характеристика суждения. Истинность и ложность суждений. Простые суждения. Виды и состав простых суждений. Распределенность терминов в суждениях. Сложные суждения. Логические отношения между суждениями. Сравнимые и несравнимые суждения. Совместимые и несовместимые суждения. Иллюстрация отношений между суждениями при помощи логического квадрата. Вывод новых суждений по логическому квадрату. Модальность суждений. **Вопросно-ответные ситуации.** Логика вопросов и ответов. Роль вопросно-ответной формы в процессе судопроизводства. Виды вопросов: по отношению к теме; по семантической характеристик, с точки зрения познавательной функции, по структуре. Виды ответов: по отношению к вопросу; по семантической характеристике, по области поиска ответов, по грамматической структуре, по объему информации, по степени точности. **Дедуктивные умозаключения.** Дедуктивные выводы из простых суждений. Непосредственные умозаключения. Простой категорический силлогизм. Умозаключения из суждений с отношениями. Дедуктивные выводы из сложных суждений. Представление умозаключений в виде схем. **Индукция и аналогия.** Индуктивные умозаключения. Схема индуктивного умозаключения. Полная и неполная индукция. Аналогия. Схемы рассуждений по аналогии. Виды аналогии. Условия состоятельности выводов по аналогии. **Логические основы аргументации.** Состав аргументации. Субъекты аргументации. Способы аргументации. Обоснование тезиса. Правила и ошибки в аргументации. Софизмы и паралогизмы.

Рекомендуемый перечень основной литературы:

1. Демидов, И. В. Логика : учебник : [16+] / И. В. Демидов ; под ред. Б. И. Каверина. – 9-е изд. – Москва : Дашков и К°, 2020. – 348 с. – (Учебные издания для бакалавров). – URL: <https://biblioclub.ru/index.php?page=book&id=573177>.

2. Яшин, Б. Л. Логика: учебник для учащихся высших и средних учебных заведений : [12+] / Б. Л. Яшин. – Изд. 2-е, стер. – Москва ; Берлин : Директ-Медиа, 2019. – 420 с. – URL: <https://biblioclub.ru/index.php?page=book&id=576772>.

3. Ельчанинова, Н. Б. Логика: учебное пособие. – Таганрог: ЮФУ, 2016. – 121 с. – URL: <https://biblioclub.ru/index.php?page=book&id=493040>.

4. Жоль, К. К. Логика : учебное пособие / К. К. Жоль. – Москва : Юнити, 2015. – 400 с. – URL: <https://biblioclub.ru/index.php?page=book&id=118262>.

5. Ивин, А. А. Логика : учебник / А. А. Ивин. – 3-е изд. – Москва: Директ-Медиа, 2015. – 452 с. – URL: <https://biblioclub.ru/index.php?page=book&id=278022>.

**Б.1.О.8. Дисциплина «Экономика»**

Коды формируемых компетенций: УК-2, УК-9.

В результате изучения дисциплины студент должен

знать:

– основные виды доходов, финансовые инструменты, виды и источники возникновения экономических и финансовых рисков в экономике;

– место, роль и функции государства в экономике, цели, задачи и инструменты бюджетно-налоговой, денежно-кредитной политики государства и их влияние на макроэкономические параметры и поведение индивидов;

– нормативные правовые акты, регламентирующие вопросы реализации бюджетно-налоговой и денежно-кредитной политики государства;

уметь:

– анализировать информацию, необходимую для принятия обоснованных экономических решений, уметь прогнозировать их последствия и применять полученные знания в сфере личного экономического и финансового планирования;

– применять нормативные правовые акты при принятии экономических решений.

Примерное распределение часов: трудоемкость дисциплины 2 з.е., 72 час.

Форма контроля: зачет.

Содержание дисциплины:

Место, роль и функции государства в экономике. Цели, задачи и инструменты бюджетно-налоговой, денежно-кредитной политики государства. Основные виды доходов. Финансовые инструменты. Виды и источники возникновения экономических и финансовых рисков в экономике. Нормативные правовые акты, регламентирующие вопросы реализации бюджетно-налоговой и денежно-кредитной политики. Требования антикоррупционного законодательства.

Рекомендуемый перечень основной литературы:

1. Лобачева Е.Н. Экономическая теория. – М.: Издательство Юрайт, 2019;

2. Салов А.И. Экономика. – М.: Литера, 2017;

3. Гребенников П.И. Экономика. – СПб.: Питер, 2019.

**Б.1.О.9. Дисциплина «Математика»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- основы линейной алгебры и геометрии, математического анализа, теории функции комплексного переменного, дифференциального и интегрального исчисления, элементы комбинаторного анализа, теории вероятностей и математической статистики;

- математические методы описания объектов.

уметь:

- применять инструменты дифференциального и интегрального исчисления для решения задач, применять математический аппарат для решения инженерных задач;

- моделировать процессы профессиональной деятельности.

владеть:

- базовым инструментарием математики для решения прикладных задач;

- вычислительными навыками и инструментами математического аппарата.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: 2 экзамена.

Содержание дисциплины:

Комплексные числа. Элементы линейной алгебры. Матрицы, действия над ними. Некоторые методы решения СЛАУ. Векторная алгебра. Элементы аналитической геометрии. Введение в математический анализ. Дифференциальное исчисление функции одной переменной. Интегральное исчисление функции одной переменной. Функции нескольких переменных. Кратные, криволинейные и поверхностные интегралы. Элементы теории поля. Числовые и функциональные ряды. Обыкновенные дифференциальные уравнения. Теория функций комплексной переменной. Случайные величины, закон больших чисел. Случайные функции. Математическая статистика.

Рекомендуемый перечень основной литературы:

1. Курош А. Г. Лекции по общей алгебре / А.Г. Курош - Москва: Гос. изд-во физико-математической лит., 1962. - 399 с. - http://biblioclub.ru/index.php?page=book&id=220855.

2. Бермант А. Ф. Курс математического анализа. 1 / А.Ф. Бермант - Изд. 12-е, стереотип. - Москва: Гос. изд-во физ.-мат. лит., 1959. - 465 с. - http://biblioclub.ru/index.php?page=book&id=256386.

3. Сапунцов Н.Е., Гамолина И.Э., Куповых Г.В. Конспект лекций по курсу теория вероятностей и математическая статистика. Изд-во ЮФУ, 2019. - https://hub.lib.sfedu.ru/storage/1/756959/3abb3530-163b-47eb-8091-92425b2aca1b/.

4. Гмурман В. Е. Руководство к решению задач по теории вероятностей и математической статистике: учеб. пособие - 11-е изд., перераб. - М.: Высшее образование, 2008. - 404 с.

**Б.1.О.10. Дисциплина «Прикладная математика»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- методы математического исследования;

- методы математического моделирования для решения задач прикладного характера;

уметь:

- анализировать естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и составлять математическую модель прикладной задачи;

- проводить теоретические и экспериментальные исследования объектов профессиональной деятельности и обрабатывать эмпирические и экспериментальные данные;

- решать стандартные профессиональные задачи с применением междисциплинарных и общенаучных знаний;

владеть:

- навыками применения современного математического инструментария для решения инженерных задач, самостоятельно расширять и углублять математические знания.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: 2 экзамена.

Содержание дисциплины:

**Теория погрешностей. Вычислительные алгоритмы**. Основные источники погрешностей. Абсолютная и относительная погрешности. Определение количества верных значащих цифр результата вычислений. Погрешности суммы, разности, произведения, частного, степени и корня. Общая формула для погрешности. Правила округления. Понятие о вероятностной оценке погрешности. Понятие вычислительного алгоритма. Требования к вычислительному алгоритму. Устойчивость и сложность алгоритма. **Численное решение нелинейных уравнений**. Графический метод решения. Отделение корней уравнения. Метод хорд. Метод касательных (Ньютона). Комбинированный метод хорд и касательных. Оценка погрешности. Метод итераций. Условия сходимости методов и оценка погрешностей. Условия сходимости методов и оценка погрешностей. **Численное решение систем уравнений.** Системы линейных уравнений. Метод Гаусса. Вычисление определителей и обращение матрицы методом Гаусса. Метод итераций, условия сходимости и оценка погрешностей. Приведение системы линейных уравнений к виду, удобному для итераций. Метод Зейделя. Оценка числа итераций. Системы нелинейных уравнений. Метод Ньютона. Метод итераций. Метод градиента. Условия сходимости методов и оценка погрешностей. **Интерполирование и приближение функций**. Аппроксимация функций. Постановка задачи. Теорема существования и единственности обобщенного интерполяционного многочлена. Приближение таблично заданных функций. Линейная интерполяция. Интерполяция кубическими сплайнами. Интерполяционные формулы Лагранжа и Ньютона. Интерполяция многочленами n - степени. Оценка погрешности интерполирования. Среднеквадратическое приближение функций при помощи тригонометрических многочленов. Равномерное и наилучшее равномерное приближение функций. **Решение разностных уравнений**. Конечные разности различных порядков и их свойства. Задача Коши и краевые задачи для разностных уравнений. Разностные уравнения первого порядка. Однородные разностные уравнения второго порядка с постоянными коэффициентами. Неоднородные разностные уравнения второго порядка с постоянными коэффициентами. **Численное дифференцирование интегрирование функций**. Численное дифференцирование. Регуляризация дифференцирования. Вычисление определенных интегралов по формуле прямоугольников. Оценка погрешности вычислений. Формула трапеций. Оценка погрешности. Формула Симпсона (парабол.). Оценка погрешности. **Численные методы решения обыкновенных дифференциальных уравнений**. Интегрирование обыкновенных дифференциальных уравнений с помощью рядов. Метод Эйлера. Метод Эйлера с уравниванием. Метод Рунге-Кутта. Оценка погрешностей и выбор шага. Метод Рунге-Кутта для системы дифференциальных уравнений первого порядка. Решение системы дифференциальных уравнений операционным методом. **Численные методы решения уравнений с частными производными**. Постановка задачи. Задача Коши и краевая задача. Точные методы решения. Сетка и шаблон. Методы составления разностных схем. Понятие об устойчивости и неустойчивости разностной схемы. **Статистическое моделирование и обработка экспериментальных данных**. Случайные числа и их получение. Метод Монте-Карло. Вычисление кратных интегралов методом Монте-Карло. Доверительный интервал. Моделирование нормальной случайной величины. Сравнение величин. Нахождение стохастической зависимости. Метод наименьших квадратов. Подбор эмпирических формул. **Пакеты прикладных программ по вычислительной математике**. Математическое обеспечение ЭВМ, типы пакетов прикладных программ, структура пакетов, программирование на ЭВМ. Интегрированный пакет Mathcad. Состав и функциональные возможности пакетов. Основы работы с пакетами. Вывод графической информации. Редактирование текстовой информации. Задание переменных величин и функций. Вычисление значений элементарных функций. Векторные и матричные операции. Операторы математического анализа. Функции интерполирования и регрессии. Решение алгебраических уравнений и систем. Решение обыкновенных дифференциальных уравнений. Преобразования Лапласа, Фурье и др. Подбор эмпирических формул. Функции математической статистики.

Рекомендуемый перечень основной литературы:

1. Системный анализ и математическое моделирование сложных экологических и экономических систем. Теоретические основы и приложения: монография / отв. ред. Ф. А. Сурков, В. В. Селютин; Южный федеральный университет. – Ростов-на-дону: Издательство Южного федерального университета, 2015. – 162 с.

2. Модели управления устойчивым развитием активных систем и их приложения: монография / под ред. Г. А. Угольницкого; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2019. – 255 с.

3. Методы численного интегрирования обыкновенных дифференциальных уравнений: учебное пособие / Ляпунова И. А., Куповых Г.В., Бажанов Н.Н.; Южный федеральный университет. – Ростов-на-Дону; Таганрог, 2019. – 49 с.

4. Моделирование связанных задач: математические постановки и конечно-элементные технологии : учебное пособие / А. В. Наседкин, А. А. Наседкина; Южный Федеральный университет. – Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2019. – 176 с.

**Б.1.О.11. Дисциплина «Математические основы обработки информации»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- математические средства представления информации;

- математические модели как средство работы с информацией;

- статические методы обработки информации;

уметь:

- анализировать естественнонаучную сущность проблем, возникающих в ходе обработки информации и составлять по ним математическую модель прикладной задачи;

- проводить теоретические и экспериментальные исследования объектов профессиональной деятельности и обрабатывать эмпирические и экспериментальные данные на основе обработанной ранее информации;

владеть:

- современными навыками математической обработки информации для решения инженерных задач.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: зачет.

Содержание дисциплины:

**Тема 1**. Роль математики в обработке информации. Математические средства представления информации. Формулы. Таблицы. Графики. Диаграммы. Использование элементов теории множеств для работы с информацией. Основные (ключевые) понятия: информация, способы обработки информации. Информация и ее виды; способы обработки информации; характеристика направлений развития информатики. Математические средства представления информации. Формулы. Таблицы. Графики. Диаграммы. Основные (ключевые) понятия: таблица, график, диаграмма, формула. Систематизация информации и построение таблиц; чтение графиков и диаграмм; построение графиков и диаграмм на основе анализа информации. Использование элементов теории множеств для работы с информацией Основные (ключевые) понятия: множество, объединение, пересечение, дополнение множеств, декартово произведение множеств. Способы задания множеств; операции над множествами. **Тема 2.** Математические модели в науке как средство работы с информацией. Использование логических законов при работе с информацией. Методы решения комбинаторных задач как средство обработки и интерпретации информации. Математические модели в науке как средство работы с информацией Основные (ключевые) понятия: процессы и явления; функции и графики; уравнения и неравенства. Процессы и явления, описываемые с помощью функций; график функции как модель процесса или явления; интерпретация результатов исследования функции в соответствии с условиями задачи; уравнения и неравенства как математические модели; интерпретация результатов решения уравнений и неравенств. Использование логических законов при работе с информацией. Основные (ключевые) понятия: высказывания и предикаты, конъюнкция, дизъюнкция, импликация, эквиваленция, отрицание высказываний, кванторы. Логические операции; связь между логическими операциями и операциями над множествами; интерпретация информации на основе использования законов логики. Методы решения комбинаторных задач как средство обработки и интерпретации информации Основные (ключевые) понятия: комбинаторная задача, размещения, перестановки, сочетания. Понятие комбинаторной задачи; основные формулы комбинаторики; решение комбинаторных задач, соответствующих специфике профессиональной деятельности. **Тема 3**. Элементы математической статистики. Статистическое распределение выборки. Методы статистической обработки исследовательских данных Элементы математической статистики. Статистическое распределение выборки. Основные (ключевые) понятия: случайная величина, значение случайной величины, интервальный ряд, объем выборки, выборочная средняя, полигон частот, математическое ожидание, дисперсия. Первичная обработка опытных данных при изучении случайной величины; составление вариационного ряда выборки, определение размаха выборки, составление статистического ряда; гистограмма как способ представления информации. Методы статистической обработки исследовательских данных. Основные (ключевые) понятия: выборочный ряд и его характеристики; выборочный метод.

Рекомендуемый перечень основной литературы:

1. Мишуров Ю.Н. Статистические методы обработки информации (конспект лекций): учебно-методическое пособие / Ю.Н.Мишуров. – Ростов-на-Дону, 2015. - 31 с.

2. Математические основы защиты информации: учебник / В. С. Пилиди; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2019. – 308 с.

3. Методы математической обработки экспериментальных данных: Учебно-методическое пособие / Гребенникова И.В., - 2-е изд., стер. - М.:Флинта, Изд-во Урал. ун-та, 2017. - 124 с. - Режим доступа: http://znanium.com/catalog/product/947245.

4. Математические методы анализа: Учебное пособие / Трофимова Е.А., Плотников С.В., Гилёв Д.В., - 2-е изд., мтер. - М.:Флинта, 2017. - 272 с.: Режим доступа: http://znanium.com/catalog/product/959371.

**Б.1.О.12. Дисциплина «Дискретная математика»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- основы теории множеств, математической логики, теории графов и комбинаторики для понимания естественнонаучной сущности проблем, возникающих в ходе профессиональной деятельности.

уметь:

- применять методы базовый инструментарий теории множеств, математической логики, теории графов, булевой алгебры, элементов комбинаторики для проведения анализа естественнонаучных проблем, возникающих в ходе профессиональной деятельности.

владеть:

- навыками проведения анализа естественнонаучных проблем, возникающих в ходе профессиональной деятельности с помощью базового инструментария теории множеств, математической логики, теории графов и комбинаторики.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Специальные разделы теории множеств. Основы алгебры множеств.** Алгебра множеств: Понятие множества. Способы задания множеств. Включение и семейство множеств. Теоретико-множественные операции над множествами. Доказательства равенств множеств. Прямое произведение множеств. Проектирование и инверсия множеств. Композиция множеств. Соответствия, функции, отношения: Понятие соответствия. Операции над соответствиями. Образ и прообраз множества при данном соответствии. Сужение и продолжение соответствия. Свойства соответствий. Функции. Морфизмы. Понятие отношения. Операции над отношениями. Свойства отношений. Нечеткие множества: Нечеткие множества. Нечеткое включение и равенство нечетких множеств. Нечеткие соответствия и отношения. Интуиционистское нечеткое множество. **Основы математической и нечеткой логики.** Элементы логики: Логические высказывания. Логические операции. Доказательства равенств логических высказываний. Построение таблиц истинности. Аксиомы и законы алгебры логики. Бинарная логика. Булевы функции: Элементы теории булевых функций. Классы булевых функций. Теорема о функциональной полноте булевых функций. Нормальные формы булевых функций. Минимизация булевых функций в классическом базисе: методы карт Карно, неопределенных коэффициентов, Квайна-Мак-Класски. Минимизация булевых функций в других базисах. Логические выводы: Понятие формальной системы. Исчисление высказываний. Формулы и аксиомы исчисления высказываний. Логический вывод на основе принципа резолюции. Логика предикатов. Вывод на основе дедукции, индукции и аналогии. Многозначная логика. Нечеткая логика. **Элементы теории графов. Основы комбинаторики.** Элементы теории графов: Понятие графа. Способы задания графов. Связность графа, Цепи и циклы. Плоский граф. Метрика графа. Эйлеров и Гамильтонов графы. Операции над графами. Задача коммивояжера. Основы комбинаторики: Правило суммы и правило произведения. Понятие r-выборки. R-перестановки и сочетания с повторениями и без повторений. Подстановки. Размещение и заполнение. Рекуррентные соотношения.

Рекомендуемый перечень основной литературы:

1. Гладков Л.А., Курейчик В.В., Курейчик В.М. Дискретная математика. Учебник. Под редакцией В.М. Курейчика, допущено УМО ВУЗов по университетскому политехническому образованию в качестве учебника для студентов высших учебных заведений, обучающихся по направлениям информатика и вычислительная техника и информационные системы – Москва: Изд-во Физмат лит, 2014. – 496 с.

2. Гладков Л.А., Курейчик В.В., Курейчик В.М. Основы дискретной математики. Учебник. – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 312с.

http://ntb.tgn.sfedu.ru/UML/UML\_1525084.pdf

3. Гладков Л.А., Курейчик В.В., Курейчик В.М. Дискретная математика. Теория графов: учебное пособие. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 162с.

http://ntb.tgn.sfedu.ru/UML/UML\_4576.pdf

4. Редькин Н.П. Дискретная математика: учебник // Москва: Физматлит, 2009, 263 c. - http://biblioclub.ru/index.php?page=book\_red&id=75709.

5. Берштейн Л.С., Боженюк А.В. Основы дискретной математики.- Учебное пособие. - Таганрог: Изд-во ТТИ ЮФУ, 2012. – 127 с.

http://ntb.tgn.sfedu.ru/UML/UML\_4937.pdf

**Б.1.О.13. Дисциплина «Физика»**

Коды формируемых компетенций: ОПК-3.

В результате изучения дисциплины студент должен

знать:

- основные законы механики;

- основные законы термодинамики и молекулярной физики;

- основные законы электричества и магнетизма;

- основы теории колебаний и волн, оптики;

- основы квантовой физики и физики твёрдого тела;

уметь:

- использовать математические модели физических явлений и процессов.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: 2 экзамена.

Содержание дисциплины:

**Механика материальной точки.** Кинематика материальной точки и абсолютно твердого тела: элементы векторной алгебры; система отсчета; декартова система координат; радиус-вектор; перемещение; скорость; компоненты скорости по декартовым координатным осям; вычисление пройденного пути; ускорение; компоненты ускорения по декартовым координатным осям; тангенциальное, нормальное и полное ускорения (для плоского движения материальной точки); кинематика вращательного движения абсолютно твердого тела; угловая скорость и угловое ускорение; связь между угловыми и линейными скоростями и ускорениями; кинематика плоского движения абсолютно твердого тела; мгновенная ось вращения. Динамика материальной точки: инерциальная система отсчета; законы ньютона; границы применимости классической механики; основная задача механики; задача Коши; преобразования Галилея; принцип относительности Галилея. Законы сохранения: сохраняющиеся величины; аддитивные интегралы движения; связь законов сохранения со свойствами пространства и времени; работа и мощность; работа центральных сил и сил однородного силового поля; потенциальная энергия частицы во внешнем (центральном и однородном) поле сил; связь между потенциальной энергией и силой; градиент; свойства градиента; кинетическая энергия материальной точки и системы материальных точек; связь кинетической энергии материальной точки с работой всех сил, действующих на материальную точку; закон сохранения полной механической энергии для частицы, движущейся в консервативном поле сил; импульс материальной точки и системы материальных точек; закон сохранения импульса системы взаимодействующих материальных точек; центр масс; движение центра масс системы материальных точек; система центра масс; момент импульса материальной точки (системы материальных точек) относительно точки и относительно оси; момент силы относительно точки и относительно оси; закон сохранения момента импульса системы взаимодействующих материальных точек. **Механика твердого тела.** Механика твердого тела: законы динамики твердого тела; момент импульса твердого тела, вращающегося вокруг неподвижной оси; момент инерции; теорема Гюйгенса-Штейнера; вычисление моментов инерции; кинетическая энергия тела, вращающегося вокруг неподвижной оси; работа, совершаемая внешними силами при вращении твердого тела относительно неподвижной оси; кинетическая энергия тела при плоском движении; гироскоп; прецессия гороскопа. Механические колебания: гармонические колебания; энергия гармонического колебания; собственные механические колебания; затухающие колебания; логарифмический декремент затухания; добротность колебательной системы. Элементы специальной теории относительности: принцип относительности Эйнштейна; принцип постоянства скорости света; преобразования Лоренца (без вывода); следствия из преобразований Лоренца (длина тела в разных инерциальных системах отсчета; собственная длина тела; относительность временного интервала; собственное время; относительность понятия одновременности; абсолютный характер причинно-следственных связей); интервал; его инвариантность относительно преобразований Лоренца; мировая точка; мировая линия; релятивистское преобразование скоростей; релятивистское выражение для импульса; релятивистское выражение для энергии; релятивистское преобразование энергии-импульса. **Статистическая термодинамика.** Молекулярная физика и термодинамика: термодинамический и статистический методы исследования системы многих тел; уравнение состояния идеального газа; состояние термодинамической системы; процесс; основные законы (начала) термодинамики; первое начало термодинамики; внутренняя энергия идеального газа; работа, совершаемая идеальным газом; частные случаи (изобарический, изохорический, изотермический процессы); теплоемкость идеального газа при постоянном объеме и при постоянном давлении; соотношение Майера; адиабатический процесс; уравнение адиабаты идеального газа; работа, совершаемая идеальным газом при адиабатическом процессе; политропический процесс; уравнение политропы идеального газа; показатель политропы; теплоемкость идеального газа при политропическом процессе, ее связь с Ср и Сv; работа, совершаемая идеальным газом при политропическом процессе; энтропия идеального газа (термодинамический вывод); второе начало термодинамики; КПД циклов; цикл Карно. **Электричество.** Электрическое поле в вакууме: электрический заряд; закон сохранения электрического заряда; закон Кулона; электрическое поле; вектор напряженности электрического поля Е; принцип суперпозиции электрических полей; основная задача электростатики; работа сил электростатического поля; потенциал; связь между потенциалом и вектором напряженности электрического поля; энергия взаимодействия системы зарядов; поле системы зарядов на больших расстояниях; дипольный электрический момент системы зарядов; электрический диполь; электрический момент диполя; поле диполя; электрический диполь во внешнем электрическом поле; элементы векторного анализа; векторные поля; поток вектора; дивергенция вектора; теорема Гаусса-Остроградского; теорема гаусса для электростатического поля; циркуляция вектора; теорема о циркуляции вектора напряженности электростатического поля; применение теорема Гаусса при решении основной задачи электростатики. Электрическое поле в диэлектриках: поляризация диэлектриков; электрическое поле в диэлектриках; объемные и поверхностные связанные заряды; вектор поляризованности диэлектрика Р и его свойства; вектор электрического смещения D; диэлектрическая проницаемость среды; теорема Гаусса для поля вектора D; условия на границе двух диэлектриков; примеры на вычисление полей в диэлектриках. Проводники в электрическом поле: электростатика проводников; условие равновесия зарядов на проводнике; проводник во внешнем электрическом поле; электроемкость уединенного проводника; конденсаторы; емкость конденсатора; соединения конденсаторов; расчет емкости конденсаторов различных конфигураций. Энергия электрического поля: Энергия электрического поля; плотность энергии электрического поля. Постоянный электрический ток: электрический ток; уравнение непрерывности; электродвижущая сила; электрическое поле проводника с током; закон ома для однородного и неоднородного участка цепи; разветвленные цепи постоянного тока; правила Кирхгофа; переходные процессы в цепи с конденсатором; работа и мощность тока; закон Джоуля-Ленца. **Магнетизм.** Магнитное поле в вакууме: магнитное поле; вектор магнитной индукции; закон Био-Савара-Лапласа; принцип суперпозиции магнитных полей; силовые линии магнитного поля; основная задача магнитостатики; магнитное поле движущегося заряда; сила Лоренца; движение заряженных частиц в магнитном поле; сила ампера; сила взаимодействия параллельных токов; поток и циркуляция вектора магнитной индукции; контур с током в магнитном поле; дипольный магнитный момент контура с током; магнитное поле контура с током; работа, совершаемая при перемещении тока в магнитном поле; элементы векторного анализа; дивергенция и ротор магнитного поля; теорема Стокса; теорема о циркуляции вектора магнитной индукции. Электромагнитная индукция: явление электромагнитной индукции; закон электромагнитной индукции Фарадея; правило Ленца; электродвижущая сила индукции; токи Фуко; скин-эффект; явление самоиндукции; индуктивность; взаимная индукция; ток при замыкании и размыкании цепи с индуктивностью; энергия магнитного поля. Уравнения Максвелла: вихревое электрическое поле; ток смещения; уравнения Максвелла. Электрические колебания. Переменный ток: квазистационарные токи; свободные гармонические колебания в колебательном контуре без активного сопротивления; свободные затухающие колебания в контуре; вынужденные колебания в контуре; резонанс. **Волны.** Упругие волны: распространение волн в упругой среде; волновое уравнение; уравнение волны; энергия упругой волны; вектор Умова. Электромагнитные волны: волновое уравнение электромагнитного поля; плоская электромагнитная волна; энергия и импульс электромагнитного поля; вектор Пойнтинга; излучение диполя; эффект Доплера для электромагнитных волн. Фотометрия: световой поток; фотометрические величины и единицы. **Оптика.** Интерференция света: интерференция световых волн; когерентность; способы наблюдения интерференции света. Дифракция света: дифракция света; принцип Гюйгенса-Френеля; зоны Френеля; дифракция Френеля от простейших преград; волновой параметр; дифракция Фраунгофера на щели; дифракционная решетка; угловая дисперсия и разрешающая сила спектрального прибора; критерий Рэлея. Поляризация света: естественный и поляризованный свет; поляризация света при отражении и преломлении; закон Брюстера; формулы Френеля; поляризация при двойном лучепреломлении; интерференция поляризованных волн; прохождение плоскополяризованного света через кристаллическую пластинку; кристаллическая пластинка между двумя поляризаторами; искусственное двойное лучепреломление; вращение плоскости поляризации. Дисперсия света: дисперсия света; групповая скорость; элементарная теория дисперсии; поглощение света; закон Бугера; рассеяние света. **Квантовая оптика.** Тепловое излучение: тепловое излучение; закон Кирхгофа; формула Рэлея-Джинса; формула Планка; закон Стефана-Больцмана; закон смещения Вина. Фотоны: Тормозное рентгеновское излучение; внешний фотоэффект; фотоны; эффект Комптона. **Квантовая механика.** Боровская теория атома: закономерности в атомных спектрах; обобщенная формула Бальмера; опыты по рассеянию α- частиц; ядерная модель атома Резерфорда; атом Резерфорда-Бора; постулаты Бора; элементарная теория водородного атома; условие квантования Бора Зоммерфельда; опыт Франка и Герца. Элементы квантовой механики: гипотеза де Бройля; волновые свойства вещества; дифракция электронов; принцип неопределенностей; состояние частицы в квантовой теории; принцип суперпозиции состояний; основные постулаты квантовой механики; смысл ψ- функции; свойства ψ- функции; плотность вероятности; нормировка; уравнение Шредингера; квантование энергии; задача на определение собственных функций и собственных значений энергии частицы в бесконечно высокой одномерной потенциальной яме.

Рекомендуемый перечень лабораторных работ:

1. Изучение динамики поступательного движения твердых тел с помощью машины Атвуда.

2. Определение ускорения свободного падения тел с помощью оборотного маятника.

3. Изучение динамики плоского движения твердых тел с помощью маятника Максвелла.

4. Экспериментальное подтверждение закона Дюлонга и Пти.

5. Исследование собственных колебаний в простом колебательном контуре.

6. Определение диэлектрической проницаемости твердых тел.

7. Изучение переходных процессов в цепи электрического тока.

8. Изучение вихревого электрического поля.

9. Изучение интерференции с помощью бипризмы Френеля.

10. Методы получения и исследования дифракционной картины.

11. Изучение прозрачной дифракционной решетки с помощью гониометра.

12. Экспериментальное подтверждение закона Стефана – Больцмана.

Рекомендуемый перечень основной литературы:

1. Савельев И.В. Курс общей физики. В 5 тт. Т.1. Механика. СПб.: Лань, 2011. -448 с.

2. Савельев И.В. Курс общей физики. В 5 тт. Т.2. Электричество и магнетизм. СПб.: Лань, 2011. -348 с.

3. Савельев И.В. Курс общей физики. В 5 тт. Т.3. Молекулярная физика и термодинамика. СПб.: Лань, 2011. -224 с.

4. Савельев И.В. Курс общей физики. В 5 тт. Т.4. Волны. Оптика. СПб.: Лань, 2011. -256 с.

5. Савельев И.В. Курс общей физики. В 5 тт. Т.5. Квантовая оптика. Атомная физика. Физика твердого тела. Физика атомного ядра и элементарных частиц. СПб.: Лань, 2011. -384 с.

Перечень материально-технического обеспечения:

учебная лаборатория механики, МКТ и термодинамики; лаборатория электростатики, электромагнетизма, колебательных и волновых процессов; лаборатория волновой оптики и квантовой физики, оснащенные лабораторными стендами и демонстрационными установками по изучаемым темам.

**Б.1.О.14. Дисциплина «Основы электротехники и радиоэлектроники»**

Коды формируемых компетенций: ОПК-6.

В результате изучения дисциплины студент должен

знать:

− основные понятия и законы теории сигналов и электрических цепей;

− принципы построения аналоговых и цифровых электронных схем;

– основы теории кодирования и теории цифровой обработки сигналов;

– особенности излучения и распространения радиоволн различных диапазонов в различных средах;

уметь:

– проводить анализ процессов, происходящих в радиоэлектронных цепях;

владеть:

– навыками исследования электрических цепей, радиотехнических сигналов, распространения радиоволн различных диапазонов в различных средах.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

Электрические цепи. Линейные элементы электрических цепей и их радиоэлектронные аналоги. Расчет электрических цепей. Делители напряжения и резонансные цепи. Электрические фильтры. Электрические цепи с распределёнными параметрами. Диоды и диодные схемы. Транзисторы и транзисторные схемы. Операционные усилители. Цифро-аналоговые и аналого-цифровые преобразователи. Цифровые комбинационные устройства. Цифровые устройства с памятью. Понятие и классификация электрических сигналов. Спектральное представление сигналов. Технические системы связи; линии и каналы связи. Методы представления информации в каналах связи. Основы систем электросвязи.

Рекомендуемый перечень лабораторных работ:

1. Законы Ома и Кирхгофа.

2. Частотные характеристики простых цепей

3. Временные характеристики цепей первого и второго порядков

4. Выпрямитель.

5. Усилители на биполярном и/или полевом транзисторе.

6. Функциональные устройства на операционном усилителе.

7. Цифро-аналоговые и аналого-цифровые преобразователи.

8. Цифровые комбинационные устройства

9. Трансформация спектров электрических сигналов

10. Длинные линии

Рекомендуемый перечень основной литературы:

1. Штыков, В. В.  Введение в радиоэлектронику : учебник и практикум для вузов / В. В. Штыков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 228 с. — (Высшее образование). — ISBN 978-5-534-08405-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/471059> (дата обращения: 19.11.2021).

2. Новожилов, О. П. Электротехника (теория электрических цепей) в 2 ч. Часть 1. : учебник для вузов / О. П. Новожилов. — Москва : Издательство Юрайт, 2020. — 403 с. — (Высшее образование). — ISBN 978-5-534-04038-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/451960> (дата обращения: 19.11.2021).

3. Бобровников, Л. З. Электроника в 2 ч. Часть 1 : учебник для вузов / Л. З. Бобровников. — 6-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 288 с. — (Высшее образование). — ISBN 978-5-534-00109-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/472264> (дата обращения: 19.11.2021).

4. Бобровников, Л. З. Электроника в 2 ч. Часть 2 : учебник для вузов / Л. З. Бобровников. — 6-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 275 с. — (Высшее образование). — ISBN 978-5-534-00112-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/472289> (дата обращения: 19.11.2021).

5. Берикашвили, В. Ш.  Радиотехнические системы: основы теории : учебное пособие для вузов / В. Ш. Берикашвили. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 105 с. — (Высшее образование). — ISBN 978-5-534-09917-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/473181> (дата обращения: 19.11.2021).

Перечень материально-технического обеспечения:

учебная лаборатория в области электроники и схемотехники, оснащенная учебно-лабораторными стендами, средствами для измерения и визуализации частотных и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов, цифровой обработки сигналов логическими интегральными схемами.

**Б.1.О.13. Дисциплина «Основы электро-, радиоизмерений»**

Коды формируемых компетенций: ОПК-6.

В результате изучения дисциплины студент должен

знать:

- основные виды метрологической деятельности и основы обеспечения единства измерений в Российской Федерации;

- основы теории измерений и теории погрешностей;

- методы электро- и радиоизмерений, способы измерений напряжений, токов, мощности, частоты, способы анализа формы и параметров сигналов;

- принципы построения электро- и радиоизмерительной техники, типовой технический состав и функциональное назначение электро- и радиоизмерительной аппаратуры, её характеристики;

уметь:

- применять современную электро- и радиоизмерительную аппаратуру, её технические и программные средства в профессиональной деятельности;

- проводить измерительные эксперименты и обработку результатов измерений;

владеть:

- навыками использования современной электро- и радиоизмерительной аппаратуры при проведении измерений;

- навыками постановки измерительного эксперимента в соответствии с программой экспериментальных исследований;

- навыками обработки результатов электро- и радиоизмерений.

Примерное распределение часов: трудоёмкость дисциплины 3 з. е., 108 час.

Форма контроля: экзамен.

Содержание дисциплины:

Основные понятия в области метрологии. Национальная система обеспечения единства измерений в Российской Федерации. Виды и методы измерений. Средства измерений. Погрешности измерений. Погрешности и метрологические характеристики средств измерений. Обработка результатов измерений.

Основные элементы электро- и радиоизмерительных приборов. Преобразователи электрических величин. Измерение напряжения и тока. Измерение электрической мощности. Измерение шумовых параметров радиоэлектронных устройств. Исследование формы электрических сигналов. Типы осциллографов и их классификация. Измерение частоты. Анализ спектра сигнала. Классификация и основные характеристики частотомеров и анализаторов спектра радиосигналов. Измерение фазового сдвига цифрового сигнала. Измерение дрожания фазы цифрового сигнала. Прочие виде электро- и радиоизмерений. Автоматизация измерений, компьютерно-измерительные системы, виртуальные приборы.

Рекомендуемый перечень лабораторных работ:

1. Обработка результатов измерения напряжения и силы тока.

2. Измерение электрической мощности.

3. Исследование формы и параметров электрических сигналов с помощью осциллографов.

4. Измерение частоты и анализ спектра электрических сигналов.

Рекомендуемый перечень основной литературы:

1. Данилин, А. А. Измерения в радиоэлектронике : учебное пособие для вузов / А. А. Данилин, Н. С. Лавренко ; под ред. А. А. Данилина. – 2-е изд., стер. – Санкт-Петербург : Издательство «Лань», 2021. – 408 с. : ил. – Режим доступа по подписке. – URL: <https://e.lanbook.com/book/171427> (дата обращения: 19.11.2021). – ISBN 978-5-8114-8068-5. – Текст : электронный.

2. Шишмарёв, В. Ю. Электрорадиоизмерения : учебник для вузов / В. Ю. Шишмарёв, В. И. Шанин. – 3-е изд., испр. и доп. – Москва : Издательство Юрайт, 2021. – 345 с. – Режим доступа по подписке. – URL: https://urait.ru/bcode/472738 (дата обращения: 19.11.2021). – ISBN 978-5-534-11645-8. – Текст : электронный.

3. Шишмарёв, В. Ю. Электрорадиоизмерения. Практикум : практическое пособие для вузов / В. Ю. Шишмарёв. – 3-е изд., испр. и доп. – Москва : Издательство Юрайт, 2021. – 234 с. – Режим доступа по подписке. – URL: https://urait.ru/bcode/473176 (дата обращения: 19.11.2021). – ISBN 978-5-534-08587-7. – Текст : электронный.

4. Метрология и радиоизмерения : учебник / И. В. Лютиков, А. Н. Фомин, В. А. Леусенко и др. ; под общ. ред. Д. С. Викторова ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2016. – 508 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=497346 (дата обращения: 19.11.2021). – ISBN 978-5-7638-3477-2. – Текст : электронный.

Перечень материально-технического обеспечения:

учебная лаборатория в области электро-, радиоизмерений, оснащённая приборами электроизмерительными комбинированными (мультиметрами), вольтметрами универсальными, измерителями мощности ВЧ- и СВЧ-диапазона, осциллографами цифровыми многоканальными (не менее двух каналов), частотомерами, анализаторами спектра, генераторами НЧ-, ВЧ- и СВЧ-сигналов, программируемыми генераторами импульсов.

**Б.1.О.16. Дисциплина «Информатика и информационные технологии в правоохранительной деятельности»**

Коды формируемых компетенций: ОПК-9, ОПК-10, ОПК-11.

В результате изучения дисциплины студент должен

знать:

- основные методы поиска, хранения, обработки, систематизации, обобщения и анализа информации из различных источников;

- современные информационно-коммуникационные технологии, применяемые для решения задач профессиональной деятельности;

- способы представления, передачи, преобразования, хранения и защиты различных видов информации;

- современные тенденции развития информатики и вычислительной техники, компьютерных технологий;

- способы представления различных видов информации в компьютере, измерение информации, технологии передачи информации.

уметь:

- осуществлять поиск, выбор, систематизацию, обобщение и критический анализ информации;

- применять информационно-коммуникационные технологии для решения задач профессиональной деятельности;

- применять информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности;

- использовать различные системы счисления для представления числовой информации, выполнять операции над числовыми данными, представленными в различных формах.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

Понятие информатики, история развития информатики, место информатики в ряду других фундаментальных наук. Информатизация общества. Понятие информации. Сообщения и сигналы. Меры информации. Количество и качество информации. Классификация информации. Информационные процессы. Информационные системы и технологии. Современные проблемы информационных технологий. Представление информации. Кодирование различных видов информации. Сжатие информации. История компьютеров. Классификация компьютеров. Тенденции развития компьютеров. Структура компьютера. Внутренние устройства системного блока. Основная и внешняя память. Внешние устройства ПК. Понятие вычислительной системы. Понятие и виды систем счисления. Двоичная, восьмеричная и шестнадцатеричная системы счисления. Преобразование чисел из одной системы счисления в другие. Представление чисел с фиксированной и плавающей запятой в ЭВМ. Прямой, обратный и дополнительный коды. Модифицированный код. Сложение и вычитание целых чисел с фиксированной запятой. Сложение и вычитание чисел с плавающей запятой. Умножение и деление чисел с фиксированной запятой в прямом и дополнительном кодах. Особенности выполнения операций умножения и деления для формата с плавающей запятой. Компьютерные сети. Классификация сетей. Топология сетей. Физическая среда передачи данных. Модели и протоколы сетей. Интернет. История. Структура. Сервисы. Алгоритм. Программа. Данные. Классификация программного обеспечения. Системное программное обеспечение. Файловая система. Прикладное программное обеспечение. Технологии программирования. Информационная безопасность. Угрозы информационной безопасности. Методы и средства защиты.

Рекомендуемый перечень лабораторных работ:

1. Вычисления, функции и уравнения в Scilab.

2. Решение СЛАУ, численное дифференцирование и интегрирование в Scilab.

3. Основы символьных вычислений в Maple.

4. Построение графиков в MAPLE 11. Решение уравнений. Элементы математического анализа и линейной алгебры.

5. Исследование системных ресурсов персонального компьютера средствами операционной системы Windows 10.

6. Использование сетевых инструментов совместной работы.

Рекомендуемый перечень основной литературы:

1. Грошев А. С. Информатика [Электронный ресурс] / А.С. Грошев. - М., Берлин: Директ-Медиа, 2015. - 484 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=428591.

2. Информатика: учебное пособие [Электронный ресурс] / Е.Н. Гусева, И.Ю. Ефимова, Р.И. Коробков и др. - 3-е изд., стереотип. - М.: Флинта, 2011. - 260 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=83542.

3. Информатика [Текст]: общий курс: учебник / под общ. ред. акад. РАН, д-ра техн. наук, проф. В. И. Колесникова. - 4-е изд. – М.: Дашков и К°, 2014. - 400 с.

4. Информатика [Текст]: базовый курс: учеб. пособие / под ред. С. В. Симоновича. - 2-е изд. - СПб.: Питер, 2010. - 640 с.

Перечень материально-технического обеспечения:

для проведения лабораторных занятий используются учебные аудитории, оснащенные средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами, проекционным оборудованием и/или интерактивной электронной доской Smart Board и ПК с подключением к сети Интернет.

**Б.1.О.17. Дисциплина «Средства вычислительной техники»**

Коды формируемых компетенций: ОПК-7

В результате изучения дисциплины студент должен

знать:

- Современные инфокоммуникационные технологии в профессиональной деятельности;

- Современные технические и программные средства для решения различных задач профессиональной деятельности;

- Современные среды и языки программирования.

уметь:

- Применять технические и программные средства для решения задач профессиональной деятельности;

- Строить архитектуру программного обеспечения;

- Применять методы и средства проектирования программного обеспечения;

- Применять методы и средства проектирования баз данных;

- Применять методы и средства проектирования программных интерфейсов.

владеть:

- Инфокоммуникационными технологиями в профессиональной деятельности.

- Современными средами программирования и использования программных библиотек для разработки программного обеспечения для решения профессиональных задач;

- Существующими типовыми решениями и шаблонами проектирования программного обеспечения;

- Методами и средствами проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Модуль 1. Современные информационно-коммуникационные технологии**. Основные понятия и определения информационно-коммуникационных технологий. Технологии, направленные на обработку, передачу и преобразование информации. Программное и аппаратное обеспечение информационно-коммуникационных технологий. Этапы разработки и внедрения информационно-коммуникационных технологий. **Модуль 2. Аппаратное обеспечение информационно-коммуникационных технологий**. Основные понятия и определения структуры ЭВМ. Архитектуры ЭВМ разных поколений. Механизмы обработки информации при помощи аппаратных средств ВТ. Системные и периферийные устройства современной вычислительной техники. **Модуль 3. Программное обеспечение информационно-коммуникационных технологий**. Понятие языка программирования. Низкоуровневое и высокоуровневое программирование. Объектно-ориентированное программирование. Современные среды программирования, программные библиотеки для разработки программного обеспечения для решения профессиональных задач. Общие понятия языка программирования C/C++. Структура программы на языке C/C++. Знакомство с платформой .NET. Особенности машинно-ориентированных языков программирования. Машинно-ориентированные языки программирования. Система команд языка Ассемблера для МП Intel 8086. Особенности программирования на языке Ассемблера для МП Intel 8086.

Рекомендуемый перечень лабораторных работ:

1. Механизмы обработки информации при помощи аппаратных средств ВТ. Системные регистры ВС, работа с основными вычислительными операциями АЛУ.

2. Стековая память, организация стеков и очередей ВС.

3. Работа с программируемым таймером ВС.

4. Работа с контроллером прерываний ВС.

5. Основы С# и технологии .NET. Элементарные конструкции программирования. Сложные конструкции программирования.

6. Основы объектно-ориентированного программирования.

7. Разработка приложения с графическим интерфейсом.

Рекомендуемый перечень основной литературы:

1. Авдеев В.А. Периферийные устройства: интерфейсы, схемотехника, программирование. Учеб. Пособие. – М.: ДМК Пресс, 2016. - 848 с.

2. Рихтер Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C#. 4-е изд. — СПб.: Питер, 2013. — 896 с.: ил. — (Серия «Мастер-класс»). ISBN 978-5-496-00433-62.

3. Сафонов В. О. Возможности Visual Studio 2013 и их использование для облачных вычислений / В.О. Сафонов - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 380 с. http://biblioclub.ru/index.php?page=book&id=429144.

4. Албахари, Джозеф, Албахари, Бен. C# 7.0. Карманный справочник.: Пер. с англ. - СпБ.:ООО "Альфа-книга", 2017. - 224 с.: ил. - Прал.тит.англ. ISBN 978-5-9909446-1-9 (рус.)

5. Язык С#. Решение задач: учеб. пособие/ В.В.Подбельский. - М.:Финансы и статистика, 2014. - 296с.:ил. ISBN 978-5-279-03553-3.

Перечень материально-технического обеспечения:

для проведения лабораторных занятий используются учебные аудитории, оснащенные средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами, проекционным оборудованием и/или интерактивной электронной доской Smart Board и ПК с подключением к сети Интернет.

**Б.1.О.18. Дисциплина «Программирование: языки, методы и технологии»**

Коды формируемых компетенций: ОПК-7.

В результате изучения дисциплины студент должен

знать:

- типовые алгоритмы и структуры данных;

- зависимость сложности программной реализации алгоритмов от сложности структуры данных;

- способы представления и кодирования различных видов информации;

- принципы создания программной реализации алгоритма, синтаксис и семантику языков программирования С/С++;

- способы отладки и тестирования программ.

уметь:

- применять типовые алгоритмы и структуры данных для решения поставленной задачи;

- представлять числовые данные в различных кодах, выполнять над ними операции;

- создавать программный код, реализовывать отдельные фрагменты сложных программ для решения профессиональных задач;

- использовать принципы структурного и объектного подхода для создания программ.

владеть навыками:

- разработки алгоритмов решения задач профессиональной деятельности, оценки сложности алгоритма;

- использования современной среды программирования и использования программных библиотек для разработки программ;

- использования современной среды разработки для отладки программного кода.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

**Модуль 1. Основы представления и обработки информации в ПК. Алгоритмизация. Основные структуры данных и алгоритмы обработки данных. Оформление алгоритмов**

Системы счисления. Представления знаковых целых чисел и основные операции над ними. Способы быстрой реализации операций умножения и деления. Представление чисел в формате с плавающей точкой и основные операции над ними. Понятие алгоритма, основные алгоритмические конструкции, формы записи алгоритмов. Основные свойства и требования к алгоритмам. Представление алгоритмов в виде блок-схем, псевдокода, структурограмм. Методы и этапы трансляции программы. Способы компиляции программы (компиляция, интерпретация, JIT-компиляция). Типовой набор средств разработки. Интегрированная среда разработки MS Visual Studio.

**Модуль 2. Программирование на C/C++**

Понятие языка программирования. Общие понятия языка программирования C/C++. Структура программы на языке C/C++. Понятие блока (составного оператора). Понятие препроцессора. Элементы препроцессинга (подключение заголовочных файлов, описание констант). Базовые типы данных в C/C++, переменные и константы. Идентификаторы, разделители, специальные символы. Комментарии. Преобразование типов (явное и неявное). Понятие оператора и операции в языке C/C++. Виды операций (унарные, бинарные, тернарные) и их примеры. Понятие префиксной и постфиксной формы записи унарных операций. Бинарные операции (отношения, арифметические, условные логические, побитовые логические, арифметического сдвига). Тернарная операция. Операция присваивания и ее особенности в языке C/C++. Понятие о "ленивых вычислениях". Приоритет и порядок выполнения операций. Форматированный ввод/вывод данных. Модификаторы и спецификаторы форматов для целых, вещественных чисел, символов и строковых значений. Базовые управляющие операторы. Операторы ветвлений. Операторы циклов. Основные операции переходов. Массивы. Описание массива и доступ к элементам массива. Одномерные и многомерные массивы. Организация хранения элементов массива в памяти. Инициализация массива. Массивы символов (строки). Библиотечные средства ввода/вывода и обработки символьной информации. Файлы. Понятие потока и файла. Прямой и последовательный доступ. Отличия текстового и бинарного файла. Работа с файлами: файловая переменная, открытие и закрытие файла, проверка достижения конца файла. Форматный ввод/вывод из файла. Ввод/вывод в бинарном режиме. Перенаправление потоков ввода/вывода. Указатели. Понятие адреса и значения. Операции с указателем. Связь между указателями и массивами. Функции. Объявление и определение функции в языке C/C++. Механизм вызова и возврата из подпрограммы. Использование стека. Понятие о формальных и фактических параметрах. Способы передачи параметров в подпрограммы. Передача параметров по адресу и по значению. Способы возврата значений из подпрограммы. Локальные переменные функции. Понятие о рекурсивных функциях. Математические функции. Составные типы данных: структуры, доступ к компонентам структур, объединения, битовые поля. Классы и модели управления памятью. Область видимости и время жизни имен (переменных, функций). Динамическое управление памятью. Препроцессор. Директивы условной компиляции. Построение многомодульных программ. Понятие единицы трансляции. Заголовочные файлы. Классы и модели управления памятью. Область видимости и время жизни имен (переменных, функций). Препроцессор. Макроопределения и макроподстановки. Директивы условной компиляции и их использование для повышения эффективности отладки программ. Цели и задачи стандартизации языка программирования. Эволюция языка программирования на примере языка С. Традиционные уязвимости языка C. Организации, занимающиеся стандартизацией языков программирования. Подходы к автодокументированию программного кода. Инструментарий Doxygen. Примеры рекомендаций для различных составляющих Coding Style.

**Модуль 3. Структуры данных и алгоритмы обработки данных**

Оценка сложности работы алгоритмов. Алгоритмы сортировки, основанные на сравнении (сортировка слиянием, быстрая сортировка, нижняя оценка на время работы алгоритмов сортировки). Алгоритмы сортировки с линейным временем выполнения (сортировка подсчетом). Элементарные структуры данных (стек, очередь, связанные списки). Введение в алгоритмы поиска (двоичный поиск в отсортированном массиве, двоичное дерево поиска). Деревья. Хеширование. Обработка строк.

**Модуль 4. Объектно-ориентированное программирование на языке С++**

Основные элементы языка С++. Операторы ввода-вывода на языке С++. Работа с файлами. Объектно-ориентированный подход к программированию. Основные понятия ООП. Инкапсуляция. Наследование. Полиморфизм. Пользовательские типы. Члены класса. Конструкторы и деструкторы класса. Порядок вызова. Конструкторы копирования. Атрибуты доступа к членам класса. Стили оформления определения класса. Создание объектов в стеке и в свободной памяти. Состояние и поведение объектов. Интерфейс класса. Методы класса и их вызов. Дружественные и статические методы. Операции класса. Перегрузка операций. Шаблонные/обобщённые функции. Шаблонные/обобщённые классы. Перегрузка функций. Базовый и производный классы. Доступ к наследуемым компонентам. Создание и разрушение объектов производного класса. Иерархия классов и ее интерфейс. Множественное наследование. Полиморфизм и виртуальные функции. Вызов виртуальных функций. Виртуальный деструктор. Динамический выбор объектов. Область видимости. Пространства имен. Обработка исключительных ситуаций. Влияние способа обработки ошибок и исключений на безопасность программ. Стандартная библиотека С++. Контейнеры, итераторы и алгоритмы. Представления объектных моделей в документах. Язык UML. Диаграммы классов, состояний, последовательностей. Приемы и паттерны объектного проектирования. Паттерны Наблюдатель, Декоратор, Синглтон, MVC. Библиотека .Net. Управляемый С++.

Рекомендуемый перечень лабораторных работ:

1. Знакомство со средой разработки. Структура программы. Алгоритмы с ветвлением.

2. Одномерные массивы. Циклы.

3. Символы. Символьные массивы. Строки, поиск в массиве.

4. Текстовые файлы. Чтение и запись в файл.

5. Работа со списком структур.

6. Алгоритмы сортировки.

7. Реализация стека.

8. Реализация связанного списка.

9. Разработка приложения на С++ в объектном стиле.

10. Разработка приложения с графическим интерфейсом.

11. Разработка приложения для работы с данными.

Рекомендуемый перечень основной литературы:

1. Новожилов, О. П.  Информатика в 2 ч. Часть 1 : учебник для вузов / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 320 с. — (Высшее образование). — ISBN 978-5-534-09964-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455239.

2. Царев Р. Ю. Программирование на языке Си / Р.Ю. Царев - Красноярск: Сибирский федеральный университет, 2014. - 108 с. [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=364601.

3. Огнева, М. В.  Программирование на языке С++: практический курс : учебное пособие для вузов / М. В. Огнева, Е. В. Кудрина. — Москва : Издательство Юрайт, 2020. — 335 с. — (Высшее образование). — ISBN 978-5-534-05123-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454165.

4. Керниган Б. В. Язык программирования C / Б.В. Керниган; Д.М. Ричи - Москва: Интернет-Университет Информационных Технологий, 2006. - 272 с. [Электронный ресурс] . - URL: http://biblioclub.ru/index.php?page=book&id=234039.

Перечень материально-технического обеспечения:

для проведения лабораторных занятий используются учебные аудитории, оснащенные средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами, проекционным оборудованием и/или интерактивной электронной доской Smart Board и ПК с подключением к сети Интернет.

**Б.1.О.19. Дисциплина «Системы и сети передачи информации»**

Коды формируемых компетенций: ОПК-8.

В результате изучения дисциплины студент должен

знать:

- принципы построения и функционирования современных компьютерных сетей;

- функции вычислительных сетей;

- критерии оценки эффективности и надежности средств защиты ВС;

- современные информационно-коммуникационные технологии, технические и программные средства для построения, настройки, мониторинга состояния вычислительной сети;

- документационное обеспечение проектирования, настройки вычислительной сети;

- основные типы и способы защиты информации в вычислительной сети;

уметь:

- решать задачи анализа и выбора современного информационно-коммуникационного оборудования для создания и настройки вычислительной сети;

- использовать средства ВС для обеспечения эффективного и безопасного функционирования автоматизированных систем;

- оценивать эффективность и надежность защиты ВС;

- решать задачи обеспечения работоспособности вычислительной сети и настройки прикладных сервисов в ней;

- проводить проверку работоспособности вычислительной сети, ее защищенности;

владеть:

- навыками планирования, развертывания и работы с ВС;

- навыками работы с ВС на различных уровнях сетевой модели OSI;

- навыками установки и настройки ВС различных классов с учетом требований по обеспечению информационной безопасности;

- навыками обеспечения настройки вычислительной сети, а также установки и настройки прикладных сервисов в вычислительной сети;

- навыками настройки сервисов, обеспечивающих безопасность данных в вычислительной сети.

Примерное распределение часов: трудоемкость дисциплины 9 з.е., 324 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

Пользователи, файлы и процессы ОС Linux. Средства администрирования и мониторинга серверов и рабочих станций, работающих под управлением ОС Linux. Основы администрирования в Linux. Системное администрирование с помощью сетевых инструментов Linux Настройка DNS для ОС Linux. Настройка LDAP сервера для OC Linux Настройка Rsyslog для OC Linux. Резервное копирование данных и дисковые массивы. Управление сетевым подключением с помощью протокола DHCP. Организация сетей, управляемых ОС Windows. Администрирование сетей ОС Windows. Администрирование web-сервера Apache. Протоколы передачи гипертекста. Протоколы передачи файлов. Администрирование сервера FTP. Протоколы передачи сообщений электронной почты. Администрирование почтового сервера. Система усиленной защиты SELinux и её администрирование. Настройка сервиса OpenSSL.

Рекомендуемый перечень лабораторных работ:

1. Пользователи, файлы и процессы ОС Linux.

2. Средства диспетчеризации ОС Linux.

3. Системное администрирование с помощью сетевых инструментов Linux.

4. Настройка DNS для ОС Linux.

5. Обеспечение целостности и доступности данных в ОС Linux. RAID.

6. Настройка LDAP сервера для OC Linux.

7. Настройка Rsyslog для OC Linux.

8. Настройка шаблона безопаности в ОС Windows.

9. Установка и настройка web-сервера Apache.

10. Установка и настройка почтового сервера.

Рекомендуемый перечень основной литературы:

1. Проскуряков, А. В. Компьютерные сети. Основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков. — Ростов-на-Дону : ЮФУ, 2018. — 201 с. — ISBN 978-5-9275-2792-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125052 (дата обращения: 14.05.2021).

2. Кузьмич, Р. И. Вычислительные системы, сети и телекоммуникации : учебное пособие / Р. И. Кузьмич, А. Н. Пупков, Л. Н. Корпачева. — Красноярск : СФУ, 2018. — 120 с. — ISBN 978-5-7638-3943-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/117794 (дата обращения: 14.05.2021).

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/471908 (дата обращения: 14.05.2021).

4. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/471236 (дата обращения: 14.05.2021).

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

**Б.1.О.20. Дисциплина «Теория информационной безопасности и методология защиты информации»**

Коды формируемых компетенций: ОПК-4, ОПК-5.

В результате изучения дисциплины студент должен

знать:

- информационное законодательство, основы закономерностей создания и функционирования информационно-правовых процессов в мире;

- основы понятий в области информационного права;

- методы и средства поиска, систематизации правовой информации;

- основы правовых ресурсов сети Интернет;

- основы современных средств идентификации и установления подлинности технических средств, средства обеспечения защиты файлов, средства защиты операционной системы и программ пользователей, системы обнаружения атак, инструментальные средства выявления уязвимостей, системы анализа защищённости, основные типы уязвимостей и информационных атак на ресурсы информационных систем;

- особенности государственной политики в области защиты информации, правовые и организационные основы защиты информации в России;

- принципы и методы обеспечения информационной безопасности;

- понятия государственной тайны и иных охраняемых законом тайн, сведений, составляющих государственную тайну, и сведений конфиденциального характера;

- организационные и правовые основы лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием и сертификацией средств защиты информации, а также оказанием услуг по защите государственной тайны;

уметь:

- применять законодательство в информационных правоотношениях;

- пользоваться правовыми базами;

- осуществлять поиск правовой информации;

- классифицировать уязвимости, информационные атаки и их возможные последствия, выявлять технологические и эксплуатационные уязвимости программно-аппаратного обеспечения информационных систем, проводить анализ существующих моделей информационных атак;

- применять нормы информационного права в профессиональной деятельности;

- использовать нормативные правовые акты и методические документы в области защиты информации и обеспечения информационной безопасности;

- определять состав информации ограниченного доступа применительно к видам тайн;

владеть:

- навыками анализа, сбора и обработки правовой информации, имеющей значение для реализации в соответствующих сферах профессиональной деятельности, правового моделирования в информационных правоотношениях;

- навыками настройки и эксплуатации программно-аппаратных средств межсетевого экранирования, систем обнаружения атак и вторжений, средств разграничения доступа;

- навыками работы с документами ограниченного доступа и обеспечения их защиты; использования справочных правовых систем в профессиональной деятельности.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

Основные понятия, термины и определения. Основы государственной политики в области информационной безопасности. Угрозы информационной безопасности. Меры обеспечения безопасности информации. Стандарты в области информационной безопасности и защиты информации. Обеспечение безопасности компьютерных систем. Техническая защита информации.

Рекомендуемый перечень основной литературы:

1. Нестеров С. А. Основы информационной безопасности / С.А. Нестеров - Санкт-Петербург: Издательство Политехнического университета, 2014. - 322 с.

http://biblioclub.ru/index.php?page=book&id=363040

2. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов - М.|Берлин: Директ-Медиа, 2015. – 105 с.

http://biblioclub.ru/index.php?page=book&id=362895

3. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов - М.|Берлин: Директ-Медиа, 2015. - 253 с.

http://biblioclub.ru/index.php?page=book&id=276557

**Б.1.О.21. Дисциплина «Информационное право»**

Коды формируемых компетенций: ОПК-4.

В результате изучения дисциплины студент должен

знать:

- информационное законодательство, основные закономерности создания и функционирования информационно-правовых процессов в мире;

- основные понятия в области информационного права;

- методы и средства поиска, систематизации правовой информации, основы правовых ресурсов сети Интернет;

- особенности государственной политики в области защиты информации, правовых и организационных основ защиты информации в России;

- понятия государственной тайны и иных охраняемых законом тайн, сведения, составляющие государственную тайну, и сведения конфиденциального характера;

- организационные и правовые основы лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием и сертификацией средств защиты информации, а также оказанием услуг по защите государственной тайны;

- нормативные правовые основы деятельности подразделений по защите информации;

- содержания институтов правовой защиты государственной, служебной, коммерческой, банковской и профессиональной тайн, а также правовой защиты персональных данных;

- номенклатуру защищаемой информации, правовой ответственности за утечку защищаемой информации и утрату ее носителей;

- правовые основы обеспечения национальной безопасности Российской Федерации, общих закономерностей правомерного поведения, правонарушения и юридической ответственности;

уметь:

- применять нормы информационного права в профессиональной деятельности, использовать нормативные правовые акты и методические документы в области обеспечения информационной безопасности;

- определять состав информации ограниченного доступа применительно к различным видам тайн;

- осуществлять поиск правовой информации и пользоваться правовыми базами;

- использовать методы выявления, предотвращения, пресечения и раскрытия преступлений и иных правонарушений в информационной сфере;

- разрабатывать меры и мероприятия по предупреждению нарушения безопасности защищаемой информации;

- планировать и осуществлять деятельность по предупреждению и профилактике преступлений и иных правонарушений в информационной сфере;

владеть:

- навыками анализа, сбора и обработки правовой информации, имеющей значение для реализации в соответствующих сферах профессиональной деятельности, правового моделирования в информационных правоотношениях;

- навыками работы с документами ограниченного доступа и обеспечения их защиты;

- навыками работы с законодательными и иными нормативными актами, регламентирующими организацию и деятельность по защите информации;

- навыками использования справочных правовых систем в профессиональной деятельности.

Примерное распределение часов: трудоемкость дисциплины 2 з.е., 72 час.

Форма контроля: зачет.

Содержание дисциплины:

Понятие, предмет, методы и система информационного права. Информационно-правовые нормы и информационные правоотношения. Право на поиск, получение и использование информации. Правовое обеспечение информационных технологий и средств связи. Правовой режим электронной подписи. Институт массовой информации. Правовое регулирование рекламной деятельности. Информационные аспекты интеллектуальной собственности. Правовые режимы информации с ограниченным доступом. Правовое регулирование информационных отношений в области государственной тайны. Неприкосновенность частной жизни. Персональные данные. Правовой режим охраны коммерческой тайны. Правовой режим охраны банковской тайны. Правовой режим охраны профессиональной тайны. Правовой режим охраны служебной тайны. Правовое регулирование отношений в сети Интернет. Преступления в сфере компьютерной информации.

Рекомендуемый перечень основной литературы:

1.  Лапина, М.А. Информационное право: учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин ; ред. И.Ш. Килясханова. - Москва: Юнити-Дана, 2015. - 336 с. - (Высшее профессиональное образование: Юриспруденция). - Библиогр. в кн. - ISBN 5-238-00798-1 ; То же [Электронный ресурс].

- URL: http://biblioclub.ru/index.php?page=book&id=118624.

2. Ефимова, Л.Л. Информационное право: учебно-методический комплекс / Л.Л. Ефимова. - Москва: Евразийский открытый институт, 2011. - 336 с. - ISBN 978-5-374-00547-9 ; То же [Электронный ресурс].

- URL: <http://biblioclub.ru/index.php?page=book&id=90541>.

3. Ельчанинова Н. Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие. – Таганрог: – Изд-во ЮФУ, 2017. – 76 с. То же [Электронный ресурс]. – URL: https://hub.lib.sfedu.ru/repository/material/800754734/

**Б.1.О.22. Дисциплина «Правовая защита информации»**

Коды формируемых компетенций: ОПК-4.

В результате изучения дисциплины студент должен

знать:

- основы отечественных и зарубежных стандартов в области управления информационной безопасностью;

- правовые нормы, стандарты в области управления информационной безопасностью;

- основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации, в том числе информации ограниченного доступа;

- способы формализации, расчета и управления рисками и инцидентами информационной безопасности;

- методы организации работы служб информационной безопасности;

уметь:

- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации с учетом структуры объекта информатизации и внешних воздействий и вероятных угроз;

- применять действующую законодательную базу в области обеспечения информационной безопасности;

- применять методики анализа и расчета рисков информационной безопасности в соответствие с отечественными и мировыми практиками, управления инцидентами информационной безопасности, анализа эффективности систем защиты информации СОИБ;

- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем;

- применять методы формирования политик информационной безопасности организации на различных уровнях;

владеть:

- навыками формирования требований по защите информации объекта информатизации;

- навыками работы с нормативными правовыми актами в соответствии с уровнями секретности;

- навыками формирования требований по защите информации, обеспечивающих соблюдение режима секретности;

- навыками составления политик безопасности верхнего, среднего и нижнего уровней;

- навыками организации, обеспечения и управления информационной безопасностью на предприятии.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

Структура информационного законодательства РФ. Правовые основы пользования информационными ресурсами. Правовое обеспечение защиты государственной тайны. Правовое обеспечение защиты конфиденциальной информации. Основы использования организационных и технических методов защиты информации. Лицензирование и сертификация в области защиты информации. Система юридической ответственности за нарушение норм защиты информации.

Рекомендуемый перечень основной литературы:

1. Струков В.И. Учебно-методическое пособие по курсу «Правовое обеспечение защиты информации», часть 1. - Таганрог: ТТИ ЮФУ, 2008г. - 45 с. (№4196).

2. Струков В.И. Учебно-методическое пособие по курсу «Правовое обеспечение защиты информации», часть 2. - Таганрог: ТТИ ЮФУ, 2009г. - 48 с. (№4196-2)

3. Правовое обеспечение информационной безопасности: учеб. пособие / под ред. С. Я. Казанцева - 2-е изд., испр. и доп. - М.: Академия, 2007. - 240 с. http://biblioclub.ru/index.php?page=book&id=235577

4. Ельчанинова Н. Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие. – Таганрог: – Изд-во ЮФУ, 2017. – 76 с. То же [Электронный ресурс]. – URL: https://hub.lib.sfedu.ru/repository/material/800754734/

**Б.1.О.23. Дисциплина «Организационная защита информации»**

Коды формируемых компетенций: ОПК-4, ОПК-5.

В результате изучения дисциплины студент должен

знать:

- основы отечественных и зарубежных стандартов в области управления информационной безопасностью;

- правовые нормы, стандарты в области управления информационной безопасностью;

- основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации, в том числе информации ограниченного доступа;

- способы формализации, расчета и управления рисками и инцидентами информационной безопасности;

- методы организации работы служб информационной безопасности;

уметь:

- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации с учетом структуры объекта информатизации и внешних воздействий и вероятных угроз;

- применять действующую законодательную базу в области обеспечения информационной безопасности;

- применять методики анализа и расчета рисков информационной безопасности в соответствие с отечественными и мировыми практиками, управления инцидентами информационной безопасности, анализа эффективности систем защиты информации СОИБ;

- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем;

- применять методы формирования политик информационной безопасности организации на различных уровнях;

владеть:

- навыками формирования требований по защите информации объекта информатизации;

- навыками работы с нормативными правовыми актами в соответствии с уровнями секретности;

- навыками формирования требований по защите информации, обеспечивающих соблюдение режима секретности;

- навыками составления политик безопасности верхнего, среднего и нижнего уровней;

- навыками организации, обеспечения и управления информационной безопасностью на предприятии.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

Основные элементы управления рисками ИБ. Методическое и нормативное обеспечение процесса управления рисками ИБ. Роль стандартов, требований, технологий защиты. Системный подход к управлению рисками. Оценка рисков информационной безопасности: активы, требования безопасности. Оценка рисков информационной безопасности: идентификация требований, анализ угроз и уязвимостей, методика CVSS. Обработка рисков ИБ: определение приоритетов аварийного восстановления, непрерывности бизнеса. Инвестиции в ИБ. Инструментальные средства для управления рисками. Экономическое обоснование. Основы управления информационной безопасностью. Система управления информационной безопасностью. Угрозы информационной безопасности в информационных системах. Индикаторы. Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью: ISO/IEC 17799; ISO/IEC 27001:2013; Сертификация СУИБ на соответствие ISO 27001. Методики оценки рисков и Управления рисками информационной безопасности. Проектирование систем обеспечения информационной безопасности на предприятии. Этапы разработки и внедрения системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ. Управление инцидентами информационной безопасности. Ситуационные центры SOC.

Рекомендуемый перечень основной литературы:

1. А.А. Астахов Искусство управления рисками . –М.: ДМК Пресс, 2010. – 312с. ISBN 978-5-94074-574-7. Электронная книга, доступ: http://анализ-риска.рф

2. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. вузов / под ред. А. А. Стрельцова - М.: Academia, 2008 - 249 с. <http://biblioclub.ru/index.php?page=book&id=115167>

3. Бачило И. Л. Информационное право [Текст] : учебник для студ. вузов / под ред. Б. Н. Топорина. - 2-е изд., с изм. и доп. - М. : Юридический центр Пресс, 2005. - 723 с. - (Учебники и учебные пособия). - Библиогр. в конце глав. - ISBN 5-94201-433-7 : 357.00.

**Б.1.О.24. Дисциплина «Документоведение»**

Коды формируемых компетенций: ОПК-9, ОПК-11.

В результате изучения дисциплины студент должен

знать:

- виды организационных и распорядительных документов, регламентирующих работу по защите информации;

- порядок разработки документов в области защиты информации, нормативные требования к созданию и оформлению документов;

- понятие государственной тайны и иных охраняемых законом тайн, сведений, составляющих государственную тайну и сведений конфиденциального характера;

- понятие и правовую основу режима секретности, секретного и несекретного делопроизводства;

уметь:

- применять нормы законодательства в области делопроизводства, защиты государственной и иной охраняемой законом тайны;

- самостоятельно составлять и правильно и полно отражать результаты профессиональной деятельности в рабочей документации в точном соответствии с законом;

владеть:

- навыками работы с нормативными документами, регламентирующими требования к оформлению документов и установлению режима секретности;

- навыками обеспечения защиты государственной тайны и соблюдения режима секретности в процессе служебной деятельности.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: зачет.

Содержание дисциплины:

Документ и его классификация. Способы и средства документирования. Документ, как объект нападения и защиты. Способы и средства документирования. Системы документации, составление и оформление документов. Структура документа, его составление и оформление. Классификация документов и систем документации. Классификация документов и систем документации. Унифицированные системы документации. Организация делопроизводства и режима секретности. Режим секретности как одно из направлений обеспечения безопасности личности, общества и государства. Методика регламентации состава конфиденциальных документов. Методика регламентации состава конфиденциальных документов.

Рекомендуемый перечень основной литературы:

1. Семко, И. А. Основы делопроизводства : учебное пособие / И. А. Семко, Л. А. Алтухова. – Ставрополь : СтГАУ, 2018. – 119 с. // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/141613‒ Режим доступа: для авториз. пользователей.

2. Мишенин, С. Е. Организация и технология документационного обеспечения управления: электронное учебное пособие : учебное пособие / С. Е. Мишенин. – Кемерово : КемГУ, 2017. – 477 с. – ISBN 978-5-8353-2149-0 // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/99438 (дата обращения: 28.12.2020). ‒ Режим доступа: для авториз. пользователей.

3. Лапкова, А. Г. Документационное обеспечение управления персоналом : практикум / А. Г. Лапкова ; ОмГТУ. – Электрон. текстовые дан. (1,33 Мб). – Омск : Изд-во ОмГТУ, 2020. – 1 CD-ROM. URL: http://lib.omgtu.ru/?id=ShowFT&o=sc&b=80674a995e562dbbde870c747e1f2dd5

4. Анацкая, А. Г. Защита электронного документооборота : учебное пособие / А. Г. Анацкая. — Омск : СибАДИ, 2019. — 87 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/149493 (дата обращения: 28.12.2020). — Режим доступа: для авториз. пользователей.

**Б.1.О.25. Дисциплина «Технологии защищенного документооборота»**

Коды формируемых компетенций: ОПК-5, ОПК-8.

В результате изучения дисциплины студент должен

знать:

- требования нормативно-методических документов в области информационной безопасности при разработке защищенных автоматизированных систем;

- теоретические и методические основы построения электронного документооборота в различных организационных структурах;

- понятие документирования и документооборота, виды и формы документов, требования к их оформлению;

- методы и приемы защиты электронной документированной информации и носителей данной информации от несанкционированного доступа в процессе выполнения каждой процедуры и операции;

- правовые основы электронного документооборота;

- принципы обеспечения информационной безопасности автоматизированных систем;

- понятие государственной тайны и иных охраняемых законом тайн, сведений, составляющих государственную тайну;

уметь:

- применять нормативно-методические документы при разработке защищенных автоматизированных систем;

- обоснованно выбирать системы электронного документооборота в организационных структурах;

- составлять и правильно оформлять деловую и служебную документацию;

- описывать основные функциональные подсистемы СЭД и их взаимодействие в рамках комплексной системы;

- использовать нормативно-правовую базу в решении профессиональных задач при использовании систем электронного документооборота;

- обоснованно выбирать средства защиты информационно-технологических ресурсов автоматизированной системы;

- определять сведения, относящиеся к государственной тайне, засекречивать и рассекречивать носители, составляющие государственную тайну, определять порядок допуска к государственной тайне;

владеть:

- навыками организации разработки защищенной автоматизированной системы с учетом требований информационной безопасности;

- навыками работы с документами ограниченного доступа и обеспечения их защиты;

- навыками организации делопроизводства и документооборота в различных организационных структурах;

- навыками применения методов и средств анализа и совершенствования систем документооборота;

- навыками практического применения знаний нормативно-правовых основ в сфере электронного документооборота;

- навыками восстановления работоспособности средств защиты информационно-технологических ресурсов автоматизированной системы при возникновении нештатных ситуаций;

- навыками работы с документами ограниченного доступа и обеспечения их защиты.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

Технологии защищенного документооборота. Традиционный печатный документооборот (бумажные носители). Требования к подготовке, передаче и хранению документов. Криптография с симметричными и открытыми ключами. Доверие к открытому ключу и цифровые сертификаты. Особенности юридического определения электронной подписи. Закон РФ "Об электронной подписи". Электронный документооборот. Требования к подготовке, передаче и хранению электронных документов. Системы автоматизации документооборота. Нормативно-методическое и правовое обеспечение стандартизации и автоматизации документооборота. Системы автоматизации документооборота. Защита информации в системах электронного документооборота. Обзор особенностей внедрения систем электронного документооборота.

Рекомендуемый перечень лабораторных работ:

1. Защита персональных данных.

2. Защита компьютерной информации на уроне доступа в систему.

3. Защита от компьютерных вирусов.

4. Защита от атак по локальным и глобальным сетям.

Рекомендуемый перечень основной литературы:

1. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М. : Флинта, 2016. – 186 с. http://biblioclub.ru/index.php?page=book&id=93356.

2. Петренко В. И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко - Ставрополь: СКФУ, 2016. - 201 с. http://biblioclub.ru/index.php?page=book&id=459205

3. Правовое регулирование информационных отношений в области государственной и коммерческой тайны, персональных данных / О.В. Ахрамеева - Ставрополь: Ставропольский государственный аграрный университет, 2015. - 59 с. http://biblioclub.ru/index.php?page=book&id=438603

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

**Б.1.О.26. Дисциплина «Техническая защита информации»**

Коды формируемых компетенций: ОПК-8.

В результате изучения дисциплины студент должен

знать:

- технические каналы утечки информации;

- возможности технических средств перехвата информации;

- организацию защиты информации от утечки по техническим каналам на объектах информатизации;

- основы физической защиты объектов информатизации;

уметь:

- пользоваться нормативными документами в области технической защиты информации.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Нормативно-правовые документы в области технической защиты информации (ТЗИ).** Концепция, организация и методология технической защиты информации. Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации. **Основные понятия и определения.** Цели и задачи ТЗИ. Определение технического канала утечки информации. Структурная схема технического канала утечки информации. Классификация и характеристики технических каналов утечки информации. **Физическая защита объектов информатизации.** Общие положения концепции защиты объектов. Назначение, виды и основные характеристики систем охраны, используемых на объектах информатизации. **Методы и средства ТЗИ.** Содержание работ, организационно-распорядительные документы, аттестация, сертификация. Средства защиты. Организационные и технические средства и системы защиты. Взаимодействие средств защиты. Основные и вспомогательные средства защиты. Принципы построения средств защиты. Техническая защита помещений и технических средств обработки информации. Методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее. Типовые нарушения в организации и осуществлении ТЗИ. **Методы и средства контроля эффективности ТЗИ.** Показатели эффективности защиты информации, обрабатываемой техническими средствами. Методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий на нее. Методы контроля эффективности защиты информации от утечки по техническим каналам. Средства контроля эффективности защиты информации от утечки по техническим каналам. Методы и методики проведения измерений, оценки и обработки их результатов.

Рекомендуемый перечень лабораторных работ:

1. Побочные электромагнитные излучения средств вычислительной техники.

2. Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях.

3. Защита от побочных электромагнитных излучений средств вычислительной техники пространственным зашумлением.

Рекомендуемый перечень основной литературы:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Солдатов А.А. «Технические средства и методы защиты информации», учебное пособие для вузов, 4-е изд., испр. и доп., 2012 г.

2. Меньшаков Ю.К. «Основы защиты от технических разведок», учебное пособие, 2011 г.

3. Бузов Г.А. «Защита информации ограниченного доступа от утечки по техническим каналам», справочное издание, 2017 г.

Перечень материально-технического обеспечения:

учебная лаборатория в области технической защиты информации, оснащенная специальным оборудованием. Анализатор спектра полоса частот 9КГц-3ГГц (например, Agilent Technologies E4403B). Интерфейс сопряжения анализатора спектра с компьютером (GPIB, USB). Набор антенн электрических и магнитных (полоса частот 9КГц-3ГГц). Эквивалент сети. Генераторы пространственного и линейного зашумления. Фильтры питания ФСП или аналогичные. Специализированное программное обеспечение для проведения специальных исследований средств вычислительной техники.

**Б.1.О.27. Дисциплина «Программно-аппаратная защита информации»**

Коды формируемых компетенций: ОПК-8.

В результате изучения дисциплины студент должен

знать:

- методы обнаружения каналов, через которые идет утечка информации по техническим каналам и знание существующих технических и программно-аппаратных средств и технологий для обработки и защиты информации;

- принципы работы устройств технических систем защиты информации; выбора компонентов устройств обеспечивающих требуемые характеристики безопасности информации с последующим контролем работоспособности примененной аппаратуры.

уметь:

- использовать необходимые методы выявления утечек информации по техническим каналам, применять технические и аппаратно-программные средства и технологии для обработки и защиты информации от утечек информации;

- устанавливать,настраивать и обслуживать технические системы защиты информации с последующей поддержкой работоспособности установленной аппаратуры.

владеть:

- навыками применения технических и программно-аппаратных средств и технологий, навыки расчета оценки утечки информации из выделенного помещения расчетно-экспериментальными методами по техническим каналам;

- навыками установки, настройки и эксплуатации технических систем защиты информации с последующей поддержкой их в работоспособном состоянии.

Примерное распределение часов: трудоемкость дисциплины 4 з.е., 144 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Основные понятия и содержание дисциплины "Программно-аппаратные средства защиты информации".** Предмет, задачи и содержание курса. Место курса среди других дисциплин. Структура курса. Методика аудиторной и самостоятельной работы студентов по изучению курса. Содержание курсовых проектов и требования по их подготовке, оформлению и сдаче. Научная и учебная литература. Периодические издания. **Защита программ с помощью электронных ключей, интеллектуальных карт и брелоков.** Защита программ с помощью электронных ключей на примере HASP 4 М4. Принципы защиты программ от копирования с помощью электронных ключей. Пристыковочный механизм и механизм использования API. Основные типы интеллектуальных карт. Характеристики интеллектуальных карт в соответствии с международными стандартами ISO 7816-3, ISO 7816-4. Защита интеллектуальных карт. Принципы программирования интеллектуальных карт. Виды ключей и их использование для защиты файлов и приложений в интеллектуальных картах на примере ASE, e-Token PRO. Особенности применения брелоков для защиты информации. **Программно-аппаратные средства шифрования.** Программно-аппаратные средства реализации блочных и поточных симметричных шифров. Особенности реализации асимметричных систем шифрования, защита файлов от изменения с помощью электронной цифровой подписи, имитовставки. Контроль целостности сообщений путем шифрования, использования хэш-функций, кодов аутентификации сообщений. Реализация алгоритмов ГОСТ 28147-89, ГОСТ 34.10-94, ГОСТ 34.11-94, 34.11-2012, ГОСТ 34.10-2001, 34.10-2012. Характеристики программно-аппаратных средств шифрования ведущих мировых и отечественных производителей. Средства криптографической защиты данных фирмы АНКАД, Инфотекс, Крипто Про. **Системы аутентификации.** Идентификация и аутентификация пользователя. Простейшие системы аутентификации с использованием пароля. Механизмы взаимной аутентификации «запрос – ответ», «временной штемпель». Схема «рукопожатия». Протоколы аутентификации. Схема аутентификации в стандарте CCITT Recommendation X 509. Системы биометрической аутентификации. Схемы аутентификации с применением одноразовых паролей. **Системы управления криптографическими ключами.** Генерация ключей. Схема генерации случайного сеансового ключа в соответствии со стандартом ANSI X 9.17. Хранение ключей согласно стандарту ISO 8532. Протокол централизованного распределения сеансовых ключей для симметричных криптосистем. Система KERBEROS. Протокол централизованного распределения открытых ключей. Инфраструктура открытых ключей. Сертификаты открытых ключей. Иерархия удостоверяющих центров. Прямой обмен ключами по схеме Диффи-Хеллмана. Пересылка ключа по технологии электронного цифрового конверта. **Основные подходы к разграничению доступа.** Дискреционная модель разграничения доступа. Механизмы битов защиты, списков прав доступа. Полномочное разграничение доступа. Уровни безопасности, категории. Примеры реализации. Разграничение доступа с помощью программно-аппаратного комплекса «Аккорд». **Аудит.** Четыре группы функций, реализующих средства регистрации и учета событий безопасности. Типовой набор событий, подлежащих регистрации. **Защита программ от изучения.** Защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям, защита программ от изменения и разрушающего воздействия; понятие изолированной программной среды. **Защита от разрушающих программных воздействий (РПВ).** Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки, компьютерные вирусы как особый класс РПВ. Администрирование подсистем программно-аппаратной защиты.

Рекомендуемый перечень лабораторных работ:

1. Программная реализация защиты программ с помощью электронных ключей типа “HASP HL”.

2. Программная реализация методов аутентификации с помощью смарт-карт “e-Token PRO”.

3. Изучение способов защиты данных с помощью криптографических средств на примере ViPNet SafeDisk.

4. Изучение способов формирования электронной цифровой подписи (ЭЦП) на примере КриптоАРМ (КриптоПро CSP).

5. Реализация методов построения инфраструктуры открытых ключей на примере УЦ «Крипто Про».

6. Реализация методов разграничения доступа к ресурсам компьютера “Аккорд”.

Рекомендуемый перечень основной литературы:

1. Бабенко Л.К., Маро Е.А. Методы защиты приложений от несанкционированного использования с помощью аппаратных ключей HАSР HL. Учебное пособие. Изд-во ЮФУ, 2015. 87 стр. Электронный ресурс, ссылка: http://hub.sfedu.ru/allocator/files/d652ba29-ba89-4179-b82a-0a8a317a331f/predisplay/

2. Бабенко Л.К., Ищукова Е.А. Криптографические методы и средства обеспечения информационной безопасности, 2011. – Электронный ресурс, ссылка: <http://ntb.tgn.sfedu.ru/UML/UML_4789.pdf>

3. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б. Современные интеллектуальные пластиковые карты. – М.: Гелиос АРВ, 2015. – 416 с.,ил. Электронный ресурс, ссылка: http://hub.sfedu.ru/allocator/files/264ccffe-2c58-4d6d-a6b2-d04d78b871d5/predisplay/

4. Долозов Н. Л. Программные средства защиты информации / Н.Л. Долозов; Т.А. Гультяева - Новосибирск: НГТУ, 2015. - 63 с. Электронный ресурс, ссылка: http://biblioclub.ru/index.php?page= book&id=438307

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

**Б.1.О.28. Дисциплина «Криптографическая защита информации»**

Коды формируемых компетенций: ОПК-8.

В результате изучения дисциплины студент должен

знать:

- основные технические и программные средства, используемые в области современной криптографии;

- основные информационные технологии, используемые в автоматизированных системах;

- основные требования к шифрам и основные характеристики шифров, модели шифров и математические методы их исследования;

- принципы построения и функционирования, примеров реализаций современных криптографических систем;

уметь:

- эффективно применять технические и программные средства и технологии в криптографии; оценивать криптографическую стойкость используемых шифров в составе автоматизированных систем;

- проектировать, разрабатывать и тестировать программно-аппаратные средства защиты информации компьютерных систем, сетей, систем управления информационной безопасности;

- оценивать криптографическую стойкость используемых шифров в составе автоматизированных систем;

- проводить выбор средств обеспечения криптографической безопасности для использования их в составе информационной системы с целью обеспечения требуемого уровня защищенности;

владеть:

- навыками работы с новыми программными средствами для решения поставленных задач в области криптографии и криптоанализа;

- навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;

- навыками организации и обеспечения режима секретности;

- криптографической терминологией;

- навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках.

Примерное распределение часов: трудоемкость дисциплины 3 з.е., 108 час.

Форма контроля: экзамен.

Содержание дисциплины:

Основы современной криптографии. Математические основы криптографии. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Функции хэширования. Программно-аппаратные средства защиты. Защита программ с помощью электронных ключей, интеллектуальных карт и брелоков. Системы аутентификации. Модели разграничения доступа и аудит событий. Системы управления криптографическими ключами. Защита программ от изучения и разрушающих программных воздействий.

Рекомендуемый перечень лабораторных работ:

1. Программная реализация защиты программ с помощью электронных ключей типа “HASP HL”.

2. Программная реализация методов аутентификации с помощью смарт-карт “e-Token PRO”.

3. Реализация методов построения инфраструктуры открытых ключей на примере УЦ «Крипто Про». Реализация методов разграничения доступа к ресурсам компьютера “Аккорд”.

Рекомендуемый перечень основной литературы:

1. Учебно-методическое пособие "Оценка стойкости блочных шифров с помощью метода слайдовой атаки" по курсу "Криптографические методы защиты информации" [Текст] / ЮФУ, ИТА, ИКТИБ, Каф. БИТ ; сост.: Л. К. Бабенко, Е. А. Ищукова. - Таганрог : Изд-во ЮФУ, 2015. - 34 с. http://ntb.tgn.sfedu.ru/UML/UML\_5440.pdf

2. Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование: учебное пособие // Таганрог: Изд-во ЮФУ, 2015. – 219 с. <http://ntb.tgn.sfedu.ru/UML/UML_5441.pdf>.

3. Лапонина О. Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина - 2-е изд., исправ. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. [Электронный доступ] <http://biblioclub.ru/index.php?page=book&id=429094>

4. Бабенко Л.К., Маро Е.А. Методы защиты приложений от несанкционированного использования с помощью аппаратных ключей HАSР HL. Учебное пособие. Изд-во ЮФУ, 2015. 87 стр. Электронный ресурс, ссылка: http://hub.sfedu.ru/allocator/files/d652ba29-ba89-4179-b82a-0a8a317a331f/predisplay/

5. Бабенко Л.К., Беспалов Д.А., Макаревич О.Б. Современные интеллектуальные пластиковые карты. – М.: Гелиос АРВ, 2015. – 416 с.,ил. Электронный ресурс, ссылка: http://hub.sfedu.ru/allocator/files/264ccffe-2c58-4d6d-a6b2-d04d78b871d5/predisplay/

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

**Б.1.О.29. Дисциплина «Специальные информационные технологии в правоохранительной деятельности»**

Коды формируемых компетенций: ОПК-9, ОПК-10, ОПК-11.

В результате изучения дисциплины студент должен

знать:

- возможности применения информационных технологий в профессиональной деятельности;

- основные виды программных средств, в том числе отечественного производства, применяемых для решения задач профессиональной деятельности;

- методы представления информации в аналоговых и цифровых каналах связи;

- основные понятия, сущность информации, формы ее представления;

- основные принципы и методы представления информации;

- основы работы с современными источниками информации;

- процедуры применения современных методов обработки результатов;

- основные классы современных информационно-коммуникационных технологий;

- основы Интернет-технологий;

- современные технологии и средства технической разведки, тенденции их развития;

- технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации;

- назначение, состав, функции и возможности автоматизированных справочных систем, информационно-поисковых систем, банков и баз данных, систем оперативной идентификации, логико-аналитических и экспертных систем, их характеристики и порядок использования в правоохранительных органах;

- теоретические основы автоматизированных баз данных, структуру автоматизированных баз данных, системы управления базами данных для информационных систем различного назначения;

- состав, функции и возможности автоматизированных справочных информационных, информационно-поисковых и логико-аналитических систем, технологии их построения;

- технологии автоматизированного ввода, обработки хранения, поиска, передачи и получения информации в подразделениях правоохранительных органов (по профилю подготовки);

уметь:

- выбирать современные информационные технологии для решения различных задач профессиональной деятельности;

- вести библиографическую работу с использованием современных информационных технологий;

- представлять результаты профессиональной деятельности с использованием современных информационно-коммуникационных технологий;

- работать с операционными системами, офисными программами, приложениями, информационно-правовыми системами;

- осуществлять ввод, обработку, хранение, поиск, передачу и получение информации, работать с использованием автоматизированных справочных информационно-поисковых систем;

- составлять запросы, собирать оперативно значимую информацию, проводить экспресс анализ информации, определять актуальность и значимость поступающей информации;

- работать с системами управления базами данных;

- работать с базами данных справочных систем, систем оперативной идентификации и логико-аналитических систем;

владеть:

- навыками применения программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности;

- навыками сбора, анализа обработки и передачи информации методами кодирования и декодирования информации;

- навыками работы с автоматизированными информационно-справочными и информационно-поисковыми системами;

- навыками работы с базами данных;

- навыками выбора рациональных способов и программно-аппаратных средств защиты информации;

- навыками осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач;

- навыками работы в системах управления базами данных,

- навыками использования информационно-поисковых и логико-аналитических систем.

Примерное распределение часов: трудоемкость дисциплины 6 з.е., 216 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

Технологии логико-аналитической деятельности. Справочные правовые системы в правоохранительной деятельности. КонсультантПлюс. Справочные правовые системы в правоохранительной деятельности. ГАРАНТ. Методы разведки по открытым источникам (OSINT). Применение технологий распознавания образов в правоохранительной деятельности. Применение глобальных навигационных систем в правоохранительных целях. Восстановление удаленных данных в целях обнаружения доказательств совершения преступлений. Технологии криминалистической деятельности. Основы цифрового следообразования. Методы криминалистического исследования изображений в целях выявления подделок. Методы криминалистического исследования аудио файлов в целях выявления подделок. Методы криминалистического исследования видео файлов в целях выявления подделок. Государственная автоматизированная система «Правосудие». Обзор систем криминалистических и оперативно-розыскных учетов в правоохранительных органах. Практические рекомендации по организации защиты конфиденциальной информации.

Рекомендуемый перечень лабораторных работ:

1. Справочная правовая система КонсультантПлюс.

2. Справочная правовая система ГАРАНТ.

3. Розыск физических лиц и составление на них досье на основе технологии разведки по открытым источникам (OSINT).

4. Анализ фреймворков по распознаванию лиц.

5. Основы восстановления удаленных данных в целях обнаружения доказательств совершения преступлений.

6. Методы криминалистического исследования изображений в целях выявления подделок.

7. Методы криминалистического исследования аудио файлов в целях выявления подделок.

8. Методы криминалистического исследования видео файлов в целях выявления подделок.

9. Государственная автоматизированная система «Правосудие».

Рекомендуемый перечень основной литературы:

1. Ельчанинова Н. Б. Информационные технологии в юридической деятельности: учебное пособие. – Таганрог: – Изд-во ЮФУ, 2016. – 128 с. То же [Электронный ресурс]. – URL: https://hub.lib.sfedu.ru/repository/material/800757440/

2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. http://biblioclub.ru/index.php?page=book&id=276557

3. Гранкина, А.Б. Документационное обеспечение управления в органах Следственного комитета Российской Федерации : учебное пособие / А.Б. Гранкина, А.Ж. Саркисян. - Москва: Юнити-Дана, 2015. - 167 с. http://biblioclub.ru/index.php?page=book&id=426576

4. Противодействие преступлениям террористической и экстремистской направленности: Вопросы теории и практики оперативно-розыскной деятельности : учебно-методическое пособие / В.В. Волченков, А.Б. Богданов, И.И. Ильинский и др. ; ред. В.В. Волченкова, Б.П. Михайлова. - Москва :Юнити-Дана, 2015. - 432 с. http://biblioclub.ru/index.php?page=book&id=119518.

Перечень материально-технического обеспечения:

учебная лаборатория в области компьютерной криминалистики, оснащенная средствами исследования и восстановления поврежденных носителей данных, устройством для копирования информации с компьютерных носителей с возможностью блокирования операций записи, **системами анализа и восстановления данных,** комплексом для криминалистического исследования фонограмм.

**Б.1.О.30. Дисциплина «Правоохранительные органы»**

Коды формируемых компетенций: УК-10, ОПК-1, ОПК-2.

В результате изучения дисциплины студент должен

знать:

- основные и производные понятия системы правоохранительных органов Российской Федерации;

- федеральные законы и подзаконные нормативные акты, регламентирующие деятельность правоохранительных органов.

уметь:

- логично, последовательно, аргументировано отвечать на вопросы в объеме тематического содержания курса;

- работать с правовыми актами, регламентирующими правоохранительную деятельность.

владеть:

- навыками установления юридически правильной квалификации отношений, регулируемых законодательством о государственной службе;

- навыками оптимального использования политических знаний при исполнении государственной службы.

Примерное распределение часов: трудоемкость дисциплины 2 з.е., 72 час.

Форма контроля: зачет.

Содержание дисциплины:

**Понятие правоохранительной деятельности.** Правоохранительная деятельность, ее признаки и основные направления, понятие и задачи. Цели правоохранительной деятельности. Предмет и система курса «Правоохранительные органы», его соотношение с другими юридическими дисциплинами. Нормативная база изучения курса. Общая характеристика правовых актов о деятельности правоохранительных органов. Классификация правовых актов о правоохранительных органах. **Судебная власть и судебная система в РФ.** Понятие судебной власти и правосудия; система органов, ее осуществляющая. Понятие и основные признаки судебной власти. Место судебной власти в системе государственной власти РФ. Развитие законодательства о судебной системе России. Судебная система современной России. Понятия звена судебной системы и судебной инстанции. Предметный, территориальный и персональный признаки подсудности. **Суды общей юрисдикции.** Верховный суд РФ - высший судебный орган судов общей юрисдикции. Порядок формирования Верховного суда РФ, его состав, структура, судебные полномочия и организация работы в Верховном суде РФ. Суды среднего звена системы судов общей юрисдикции, их полномочия, состав, структура, организация работы и место в системе судов общей юрисдикции. Основное звено системы судов общей юрисдикции. Районный суд - основное звено общих судов. Полномочия районного суда, организация работы в районном суде. Мировые суды РФ. Военные и иные специализированные суды. Основы организации, подведомственности и подсудности военных судов. **Арбитражные суды и иные арбитражные органы.** История арбитража в России, государственный и ведомственный арбитраж. Федеральные арбитражные суды округов: порядок образования, структура и полномочия. Арбитражные апелляционные суды, как самостоятельное звено в подсистеме арбитражных судов. Арбитражные суды субъектов РФ. Иные арбитражные органы: МАК, МКАС и проч. Третейский суд. **Конституционный Суд Российской Федерации и конституционные (уставные) суды субъектов РФ**. Понятие и история конституционного контроля, его сущность и виды. Сущность конституционного судопроизводства и правовые основы организации и деятельности Конституционного суда. Компетенция Конституционного суда Российской Федерации. Статус судьи Конституционного суда Российской Федерации. Принципы и общие правила конституционного судопроизводства. Компетенция и порядок формирования конституционных (уставных) судов субъектов Российской Федерации. **Правовой статус судей, присяжных и арбитражных заседателей.** Правовой статус судей и его обеспечение. Независимость судей и ее гарантии. Порядок наделения судей полномочиями. Требования, предъявляемые к кандидатам на должности судей. Срок полномочий судьи. Общая характеристика и порядок формирования судейского сообщества. Органы судейского сообщества. Полномочия квалификационных коллегий судей и правовое регулирование производства в них. Статус присяжных и арбитражных заседателей. **Органы обеспечения деятельности судов**. Правоохранительные органы исполнительной власти в РФ: судебный департамент и органы юстиции. Правовое регулирование организационного обеспечения деятельности судов. Судебный департамент – особенности правового положения. Система службы судебных приставов Министерства юстиции РФ. Уголовно-исполнительная система. Требования, предъявляемые к лицу, назначаемому на должность судебного пристава. Организация и полномочия судебных приставов. **Прокуратура Российской Федерации.** Основные этапы развития и становления прокуратуры. Основные функции (виды деятельности) прокуратуры. Прокурорский надзор, его основные виды и направления прокурорской деятельности. Средства прокурорского надзора. Система, структура и полномочия органов прокуратуры. Основные правовые акты прокурорского надзора. Правовой статус кадров, органов и учреждений прокуратуры. Требования, предъявляемые к лицам, назначаемым на должность прокуроров и следователей прокуратуры. Военная прокуратура, особенности статуса, система органов. **Органы, осуществляющие организацию выявления и расследования преступлений**. История развития органов, осуществляющих выявление и расследование преступлений. Органы, осуществляющие оперативно-розыскную деятельность. Органы и должностные лица, осуществляющие дознание, и их компетенция. Органы, осуществляющие предварительное следствие, и их компетенция. Государственные органы, обеспечивающие охрану порядка и безопасности. Органы обеспечения безопасности: Совет Безопасности РФ, органы Федеральной службы безопасности. Органы внутренних дел. Органы внешней разведки РФ, Федеральная пограничная служба РФ. Федеральные органы государственной охраны. Налоговые органы. Таможенные органы. **Юридическая помощь и ее организация в Российской Федерации. Нотариат. Адвокатура.** Понятие и сущность юридической помощи в РФ. Понятие задачи и основы организации нотариата. Порядок назначения на должность нотариуса, права и обязанности нотариуса. Основные правила нотариальных действий. Принципы организации и задачи адвокатуры. Правовой статус адвоката. Организация адвокатской деятельности и адвокатуры.

Рекомендуемый перечень основной литературы:

1. Правоохранительные органы : учебник / ред. И. И. Сыдорук, А. В. Ендольцева, Р. С. Тамаев. – 8-е изд., перераб. и доп. – Москва : Юнити, 2012. – 471 с. – URL: <https://biblioclub.ru/index.php?page=book&id=495462>.

2. Правоохранительные органы : учебное пособие / А. В. Ендольцева, Н. Д. Эриашвили, В. Н. Галузо и др. ; ред. А. В. Ендольцева. – Москва : Юнити, 2015. – 231 с. – URL: <https://biblioclub.ru/index.php?page=book&id=436810>.

3. Марфицин, П. Г. Правоохранительные органы: учебно-методическое пособие / П. Г. Марфицин, Л. Б. Обидина, И. С. Тарасов. — 2-е изд. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2019. — 80 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/144831.

4. Сидорова, Н. В. Правоохранительные органы: практикум / Н. В. Сидорова, Е. В. Смахтин, Е. А. Хабарова ; отв. ред. В. В. Петров ; Тюменский государственный университет. – Тюмень : Тюменский государственный университет, 2017. – 79 с. – URL: <https://biblioclub.ru/index.php?page=book&id=573970>.

**Дисциплины специализации №4 «Компьютерная экспертиза»**

**Б.1.С.4.1. Дисциплина «Компьютерная криминалистика»**

Коды формируемых компетенций: ПК-Р4.1, ПК-Р4.3.

В результате изучения дисциплины студент должен

знать:

1. - порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;
2. - виды и составы преступлений в сфере компьютерной информации;
3. - основные требования, предъявляемые к составу и оформлению научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем;
4. - методику проведения работ по информационно-аналитической и технической экспертизе компьютерных систем;

уметь:

1. - подготавливать научно-технические экспертные заключения, по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем;
2. - обобщать и анализировать данные, получаемые в ходе проведения работ по информационно-аналитической и технической экспертизе компьютерных систем; фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов;
3. - фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов.

владеть:

- навыками производства компьютерно-технических экспертиз;

1. - навыками подготовки и оформления заключений эксперта в соответствии с требованиями законодательства.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

**Роль компьютерной криминалистики** в обеспечении информационной безопасности. **Компьютерные преступления. Криминалистическая характеристика. Несанкционированный доступ. Разработка вредоносных программ. Нарушение правил эксплуатации ЭВМ. Безопасность критической информационной инфраструктуры. Онлайн-мошенничество. Нарушение авторских прав. Фишинг. Киберсквоттинг. Кардерство. Расследование инцидентов информационной безопасности**. Цели расследования инцидентов информационной безопасности. Основные субъекты таких расследований. Неотложные действия после инцидента информационной безопасности. Последовательность действий при расследовании. **Работа с лог-файлами.** Анализ лог-файлов сетевого трафика. Что такое сервис whois. Утилита tracert. Какую информацию может дать провайдерская компания. **Правовые основы производства экспертиз**. Правовая регламентация производства экспертиз по гражданским и уголовным делам. Процессуальный статус эксперта и соблюдение норм законодательства. Требования к заключению эксперта. Участие эксперта в судебном заседании. **Производство компьютерно-технической экспертизы**. Основное оборудование и программные средства, необходимые для производства экспертизы. Блокираторы записи и дубликаторы. Экспертные системы – EnCase, Paraben Commander, Forensic Toolkit. Возможные виды проводимых исследований. Планирование экспертизы в зависимости от вопросов, сформулированных следователем. **Поиск доказательственной информации на компьютерах**. Основные принципы изъятия компьютерной техники и носителей информации. В каких объектах содержится доказательственная информация. Методы сокрытия таких данных от обнаружения. **Артефакты ОС Windows.** Исследование реестра ОС. Системы сбора и анализа журналов ОС. Корреляция событий. Создание и исследование Timeline. **Исследование дампов оперативной памяти**. Утилиты volatility, redline и др. **Работа с системами анализа и восстановления данных**. Поиск, анализ, извлечение и восстановление информации с помощью систем EnCase, Paraben Commander, Forensic Toolkit, Belkasoft и др. **Поиск сообщений электронной почты и мессенджеров**. Основные почтовые программы и места, где они сохраняют данные. Чтение почты с помощью Paraben Commander. Структура почтового сообщения. Анализ служебной информации. Методы анализа и восстановления переписки в мессенджерах. **Работа с криптографией**. Основные средства криптографической защиты. AES, EFS, PGP, архиваторы с шифрованием, офисные пакеты, базы данных. Основы поиска зашифрованных данных. Вскрытие защищённых данных. Программное обеспечение Passware Forensic Kit и Elcom Soft Password Recovery Bundle. Взлом хешей MD5, SHA-1, SHA-256, LM, NTLM и т.д. Извлечение паролей из браузеров, программ для мгновенного обмена сообщениями и других программ.

Рекомендуемый перечень лабораторных работ:

1. **Поиск доказательственной информации на компьютерах.**

2. **Артефакты ОС Windows**.

3. **Исследование дампов оперативной памяти.**

4. **Работа с системами анализа и восстановления данных.**

5. **Поиск сообщений электронной почты и мессенджеров.**

6. **Работа с криптографией.**

Рекомендуемый перечень основной литературы:

1. Степанов-Егиянц, В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография / В.Г. Степанов-Егиянц. – Москва : Статут, 2016. – 190 с. http://biblioclub.ru/index.php?page=book&id=452481.

2. Моисеева, Т.Ф. Основы судебно-экспертной деятельности: конспект лекций / Т.Ф. Моисеева. – Москва: Российский государственный университет правосудия (РГУП), 2016. – 191 с. http://biblioclub.ru/index.php?page=book&id=439610.

3. Пелешенко В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие / В.С. Пелешенко; С.В. Говорова; М.А. Лапина - Ставрополь: СКФУ, 2017. - 86 с. http://biblioclub.ru/index.php?page=book&id=467139.

4. Бегларян, М.Е. Судебная компьютерно-техническая экспертиза: научно-практическое пособие / М.Е. Бегларян. – Москва: Юнити, 2015. – 71 с. http://biblioclub.ru/index.php?page=book&id=446544.

5. Компьютерная криминалистика: лабораторный практикум: специальность 10.05.03 (090303.65) Информационная безопасность автоматизированных систем. Специализация "Защищенные автоматизированные системы управления" / сост.: И.А. Калмыков, В.С. Пелешенко; Сев.-Кав. федер. ун-т. - Ставрополь: СКФУ, 2017. - 84 с.

Перечень материально-технического обеспечения:

учебная лаборатория в области компьютерной криминалистики, оснащенная средствами исследования и восстановления поврежденных носителей данных, устройством для копирования информации с компьютерных носителей с возможностью блокирования операций записи, **системами анализа и восстановления данных,** комплексом для криминалистического исследования фонограмм.

**Б.1.С.4.2. Дисциплина «Расследование компьютерных инцидентов»**

Коды формируемых компетенций: ПК-Р4.1, ПК-Р4.2.

В результате изучения дисциплины студент должен

знать:

- виды оперативно-розыскных мероприятий и возможные формы участия в них специалистов в области информационных технологий;

- основы расследования преступлений, совершаемых с использованием компьютерной техники и средств телекоммуникаций;

- понятийный аппарат в сфере обработки компьютерной информации;

- стандарты по тематике управления инцидентами;

- классификации и виды компьютерных инцидентов (КИ).

уметь:

- использовать средства операционных систем для поиска и фиксации следов КИ;

- выполнять типовые действия, выполняемые в рамках процесса управления инцидентами;

- использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов;

- организовывать безопасное хранение и восстановление данных автоматизированных систем.

владеть:

- профессиональной терминологией;

- видами отдельных следственных действий и возможные формы участия в них специалистов в области информационных технологий;

- навыками восстановления операционных систем после сбоев, вызванных КИ;

- навыками администрирования операционными системами семейств Windows и Unix;

- навыками обнаружения атак и распознавания вторжений;

- методами локализация ущерба, причиненного произошедшим инцидентом.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**1. Определение компьютерного инцидента. Понятие и виды компьютерных преступлений.** Субъекты информационных отношений. Интересы субъектов информационных отношений в информационной сфере. Юридическое понятие компьютерной информации. Понятие и виды компьютерных преступлений. Общие положения состояния преступности в сфере компьютерной информации, а также правоохранительной деятельности по раскрытию и расследованию этих преступлений. Основные стадии компьютерного преступления (подготовка, развитие, скрытие следов). Определение компьютерного инцидента. Проблема. Кодификатор Международной уголовной полиции генерального секретариата ИНТЕРПОЛА. Краткая характеристика некоторых видов компьютерных преступлений по кодификатору ИНТЕРПОЛА. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Уголовно-правовая характеристика нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети.

**2. Типы и причины компьютерных инцидентов.** Известная ошибка. Язык инцидентов и проблем. Модель ITIL Service Support как руководство ИТ-организациями при разработке подходов к управлению обслуживанием. Компьютерный инцидент как следствие невозможности создания абсолютной защиты. Инциденты, причиной которых являются намеренно осуществляемые нападения на информационные ресурсы предприятия. Примеры инцидентов.

**3. Стандарты по тематике управления инцидентами. Команда реагирования на компьютерные чрезвычайные события (Computer Emergency Response Team, CERT).** Стандарты по тематике управления инцидентами. ISO/IEC. Стандарты ITU-T E.409. Набор документов CERT/СС, NIST SP 800-61. Общие требования к построению системы управления ИБ (СУИБ), относящиеся, в том числе и к процессам управления инцидентами в стандарте ISO/IEC 27001-2005. Инфраструктура управления инцидентами ИБ в стандарте ISO/IEC TR 18044. Описание методологии планирования, внедрения, оценки и улучшения процессов управления инцидентами в документе CMU/SEI-2004-TR-015. Практики по построению процессов управления инцидентами и реагирования на них в рекомендациях NIST SP 800-61. Команда реагирования на компьютерные чрезвычайные события (Computer Emergency Response Team, CERT).

**4. Процесс управления инцидентами.** Типовые действия, выполняемые в рамках процесса управления инцидентами. Идентификация инцидента. Реагирование на инцидент ИБ. Восстановление после инцидента ИБ. Организация реагирования на инциденты. Построение централизованной системы реагирования на инциденты. Состав технической и организационной документации, необходимой для восстановления информационных систем и данных после инцидентов. Порядок хранения архивных (резервных) копий данных и программных приложений обработки данных в местах, защищенных от механических воздействий, краж, наводнений, пожаров и т.п. (в т.ч., возможно, в местах, территориально удаленных от основных мест хранения и обработки информации). Соглашения с поставщиками программных и аппаратных средств, входящих в информационную инфраструктуру предприятия, о срочной поставке компонент, вышедших из строя и требующих замены в случае чрезвычайной ситуации.

**5. Процесс реагирования на инциденты.** Процесс реагирования на инциденты, причиной которых являются намеренно осуществляемые нападения на информационные ресурсы предприятия. Обнаружение атак и распознавание вторжений. Определение характера нарушений. Локализация и устранение последствий. Определение конкретных параметров нарушения (нападения), его характера (конкретных сегментов сети, серверов, групп рабочих станций, приложений, затронутых нападением). Блокирование (полное или частичное) работы информационной системы (сервера, базы данных, сегмента сети и т.п.) с целью недопущения дальнейших разрушительных действий, распространения вредоносных программ или утечки конфиденциальной информации.

**6. Качественный анализ инцидента.** Идентификация нападающего. Анализ технических аспектов нападения. Качественный анализ процесса нападения в контексте функционирования атакуемой системы защиты информации. Организация взаимодействия со сторонними организациями, которые могут содействовать в идентификации нападающего. Анализ целей и мотивов нападавших.

**7. Анализ фундаментальных причин и последствий инцидента.** Анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным (если оно было успешным). Анализ последствий (в том числе и долгосрочных) нападения для всей деятельности предприятия.

**8. Оценка затрат на восстановление после инцидента.** Затраты на замену скомпрометированных паролей, кодов и ключей. Определение стоимости поврежденного оборудования. Штрафные санкции за разглашение конфиденциальной информации. Оценка упущенной выгоды. Оценка падения рыночной стоимости предприятия.

**9. Нематериальный ущерб от инцидентов.** Моральный ущерб и последствия от разглашения информации личного характера.

**10. Восстановление после инцидента.** Смена скомпрометированных паролей отдельных пользователей. Переустановка поврежденных операционных систем, а также поврежденного программного обеспечения. Восстановление нарушенной конфигурации (настроек) программного обеспечения и операционных систем. Восстановление поврежденной информации (баз данных, файлов). Организация информационной работы о произошедших инцидентах.

**11. Аудит и сертификация по требованиям информационной безопасности ОС.** Цели аудита. Установление степени защищенности информационных ресурсов предприятия. Выявление недостатков и определение направлений дальнейшего развития системы защиты информации. Основные этапы проведения аудита. Инициирование проведения аудита. Сбор информации и проведение обследования аудиторами. Анализ имеющейся политики информационной безопасности и другой организационной документации. Анализ собранных данных и выработка рекомендаций. Сертификация на соответствие общепризнанным нормам и требованиям в сфере информационной безопасности (в частности, на соответствие национальным и международным стандартам).

Рекомендуемый перечень лабораторных работ:

1. Выявление предпосылок и обстоятельств, приведших к возникновению компьютерного инцидента.

2. Описание методологии планирования, внедрения, оценки и улучшения процессов управления инцидентами.

3. Анализ причин инцидента, проведение расследования, предоставление отчета об инциденте.

4. Расчет прямого ущерба на основе трудоемкости работ по восстановлению информации и данных о средней стоимости рабочего времени соответствующих специалистов.

5. Локализация ущерба, причиненного произошедшим инцидентом.

6. Подготовка аудиторского отчета и аттестационного заключения.

Рекомендуемый перечень основной литературы:

1. Пелешенко В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие / В.С. Пелешенко; С.В. Говорова; М.А. Лапина - Ставрополь: СКФУ, 2017. - 86 с. http://biblioclub.ru/index.php?page=book&id=467139.

2. Федеральная служба безопасности Российской Федерации. Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения», Москва, 12 ноября 2018 г. No 33 [Электронный ресурс]. URL: http://www.fsb.ru/files/fsbdoc/normakt/standart\_sto\_2018.doc (дата об- ращения 25.05.2021).

3. Network Forensics Investigative Methodology (OSCAR) [Электронный ресурс]. URL: http://comp.org.uk/network-forensics-investigative-metho- dology-oscar.html (дата обращения 25.05.2021).

4. Инструментальный контроль и защита информации: учебное пособие / Н. А. Свинарев, О. В. Ланкин, А. П. Данилкин, С. В. Потехецкий. — Воронеж : ВГУИТ, 2013. — 192 с. — ISBN 978-5-00032-018-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/72884 (дата обращения: 26.05.2021).

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

**Б.1.С.4.3. Дисциплина «Инструментальное обеспечение компьютерной экспертизы»**

Коды формируемых компетенций: ПК-Р4.1.

В результате изучения дисциплины студент должен

знать:

- виды служебной информации в компьютерной системе;

- возможные места расположения системной информации в ОС;

- значимость файлов регистрации событий (log-файлы) для определения следовой информационной картины совершенного противоправного деяния;

- программные продукты для преодоления парольных защит, принцип их работы;

- программные средства для просмотра и сравнения файлов.

уметь:

- применять методики судебных экспертных исследований в профессиональной деятельности;

- применять программные средства для просмотра и редактирования реестра;

- использовать справочно-информационных и справочно-поисковых систем, предназначенных для обеспечения различных видов экспертной деятельности;

- использовать технологии виртуальных машин.

владеть:

- основами анализа экспертной практики, условиями, способствовавшими совершению преступлений, и разрабатывать предложения направленные на их устранения;

- способами обнаружения и нейтрализации программно-аппаратных средств защиты, используемых для ограничения доступа к информации;

- неразрушающими методами исследования информации.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: зачет с оценкой.

Содержание дисциплины:

Тема 1. Научные и правовые основы применения криминалистической техники. Естественные, технические науки – основной источник развития криминалистической техники. Применение криминалистической техники следователем, специалистом, оперативным работником, экспертом и судьей. Тенденции и перспективы развития криминалистической техники. Роль криминалистической техники в разработке методов предупреждения преступлений. Экспертные инструменты и авторское право.

Тема 2. Классификация технико-криминалистических средств. Основные технико-криминалистические средства, применяемые для обнаружения, фиксации, изъятия и предварительного исследования средств, их классификация. Комплекты технико-криминалистических средств. Передвижные криминалистические лаборатории. Научно-технические средства и методы, используемые при лабораторном исследовании. Измерительная, микроскопическая, аналитическая, вычислительная техника. Основные задачи ее применения.

Тема 3. Система анализа и учета уголовных дел САУД-М. Гипертекстовая система ИНТЕЛТЕКСТ. АРМС для расследования конкретных видов преступлений. Специальная информационная система (СИС), предназначенная для автоматизации следственных действий, анализа работы следователей и следственных отделов, управления их работой. Следственные экспертные системы. Справочные правовые системы (СПС). Автоматизированное рабочее место следователя (АРМ СЛЕДОВАТЕЛЯ).

Тема 4. Клонирование цифровых объектов для исследования. Создание судебных загрузочных дисков EnCase. Этапы использования начальной загрузки DOS. Клонирование с диска на диск в DOS. Клонирование данных по сети. Подготовка сетевого загрузочного диска EnCase. Этапы клонирования по сети. Основные понятия программы EnCase. Формат файла исследуемых данных EnCase. Компоненты и назначение файла исследуемых данных. Верификация файла исследуемых данных. Хэширование дисков и томов Файлы дела для программы EnCase.Резервный файл (.cbak). программы EnCase. Папка записи КЭШа EnCase.. Программная среда EnCase. Структура программы EnCase. Создание дела. Навигация панели древовидного представления объектов. Навигация в панели табличного представления объектов. Регулировка панели. Общие режимы просмотра. Опции EnCase.

Тема 5. Расширенные возможности EnCase. Поиск и монтирование разделов. Монтирование файлов. Системный реестр. История системного реестра. Методы исследования реестра. Содержимое вкладки «EnScript» и пути к скриптам. Редактирование, копирование, перемещение и удаление скриптов.

Тема 6. Инструментальные средства TASK и TASKAutopsy. TASKAutopsy CookieView. Анализ файлов Cookies. Инструмент исследования Windows-машин в поисках улик, касающихся Web – активности NetAnalysis.

Тема 7. Состав, назначение, технические характеристики, функциональные возможности аппаратно-программного комплекса для криминалистического исследования компьютерных носителей информации. Варианты комплектации комплекса: для лабораторных исследований компьютерной информации; для копирования компьютерной информации из средств вычислительной техники при работе специалиста на месте происшествия.

Тема 8. Подготовка оборудования, настройка программного обеспечения, особенности применения в лабораторных и выездных условиях.

Тема 9. Способы представления полученных результатов исследования (различные режимы просмотра, табличная форма представления исследуемой информации, сортировка по атрибутам, визуализация графических файлов распространения форматов). Технология создания и редактирования пометок, комментариев экспертов. Автоматизация процесса подготовки отчетов по проведенным исследованиям; режимы прямой печати отчета и преобразование отчета в текстовый формат.

Тема 10. Средства (артефакты) Windows, полезные при производстве КЭТ. Системные директории Cookies, sendTo,Favorites History и другие. Файлы с расширением .spl bkb.shd, Start Menu OC Windows и 2/2 директория Recept.Файл NTUSER.DAT.

Тема 11. Программный инструментарий эксперта компьютерной экспертизы при работе в программной среде Linux.. Виды используемого программного обеспечения, цели, особенности, условия применения (по материал экспертной практики).

Тема 12. Программно-техническая экспертиза iPhone. Open-source утилиты. Бэкапы iOS. Бэкапы iCloud. Облачное хранилище iCloud. Бэкапы iTunes.

Тема 13. Программно-техническая экспертиза Android. Open-source утилиты. Бэкапы. Кэш приложений.

Тема 14. Использование программно-технического обеспечения для криминалистического исследования документов.

Тема 15. Принципы технико-криминалистического исследования документов автоматизированными системами, осуществляемого на персональном компьютере. Развитие программно-аппаратных комплексов. Состав оборудования, используемого экспертами.

Тема 16. Выявление программно-техническими способами распространение способов подделки документов: подчистка, травление, смывание, дописка, исправление и иные изменения теста документов.

Тема 17. Способы защиты документов от подделок. Декодирование способов защиты документов от подделок и их экспертное исследование. Компьютерная экспертиза подделки подписи.

Тема 18. Основные и специальные программы применяемые для проведения исследования письма. Введение в персональный компьютер процессуально значимой информации. Корректировка полученного изображения относительно общих и частных признаков почерка. Проблемы автоматического анализа письма.

Рекомендуемый перечень лабораторных работ:

1. Автоматизированное рабочее место следователя.

2. Работа с EnCaseForensics.

3. Получение следственных образов.

4. Методы исследования реестра. Автоматизация процесса подготовки отчетов по проведенным исследованиям.

5. Анализ системного сектора.

6. Журналы регистраций событий.

7. Способы анализа мобильного устройства без модификации его прошивки.

8. Проведение почерковедческой̆ экспертизы.

Рекомендуемый перечень основной литературы:

1. Инструментальный контроль и защита информации : учебное пособие / Н. А. Свинарев, О. В. Ланкин, А. П. Данилкин, С. В. Потехецкий. — Воронеж : ВГУИТ, 2016. — 192 с. — ISBN 978-5-00032-018-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/72884 (дата обращения: 26.05.2021).

2. Россинская, Е. Р. Теория судебной экспертизы: Учебник / Е.Р. Россинская, Е.И. Галяшина, А.М. Зинин; Под ред. Е.Р. Россинской. - Москва : Норма: НИЦ Инфра-М, 2016. - 384 с. ISBN 978-5-91768-344-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/369688 (дата обращения: 26.05.2021).

3. Федеральная служба безопасности Российской Федерации. Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения», Москва, 12 ноября 2018 г. No 33 [Электронный ресурс]. URL: http://www.fsb.ru/files/fsbdoc/normakt/standart\_sto\_2018.doc (дата об- ращения 25.07.2019).

4. Россинская Е. Р. Научно-техническое обеспечение учебных экспертно-криминалистических лабораторий: Научно-практическое пособие/ Е.Р. Россинская, Е.И. Галяшина и др. - М.: Юр.Норма, НИЦ ИНФРА-М, 2015. - 160 с. ЭБС Znanium.com

Перечень материально-технического обеспечения:

учебная лаборатория в области компьютерной криминалистики, оснащенная средствами исследования и восстановления поврежденных носителей данных, устройством для копирования информации с компьютерных носителей с возможностью блокирования операций записи, **системами анализа и восстановления данных**.

**Б.1.С.4.4. Дисциплина «Методы хранения, восстановления и анализа данных»**

Коды формируемых компетенций: ПК-Р4.2.

В результате изучения дисциплины студент должен

знать:

- множество программных решений, используемых для восстановления данных;

- рациональное использование носителей и резервное копирование.

уметь:

- восстанавливать данные с извлечением удаленных или поврежденных данных;

- восстанавливать данные с основных типов носителей: винчестеров, полупроводниковых накопителей и лазерных дисков.

владеть:

- навыками обнаружения атак и распознавания вторжений;

- методами локализация ущерба, причиненного произошедшим инцидентом;

- навыками анализа причин инцидента, проведения расследования, предоставления отчета об инциденте.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: экзамен.

Содержание дисциплины:

Логическая организация файловой системы: одноуровневая; иерархическая (дерево); иерархическая (сеть). Физическая организация файла: непрерывное размещение; связанный список блоков; связанный список индексов; перечень номеров блоков. Функции физического уровня файловой системы. Хранение файла на жестком диске. Смежное размещение. Связный список. Таблица отображения файлов. Индексные узлы. Жесткая ссылка. Журналируемые ФС. Отображаемые в память файлы. Виды файловых систем. Файловая система FAT. Ошибки файловой системы FAT. Файловая система NTFS. Сравнительная характеристика FAT 32 и NTFS. Достоинства и недостатки. Файловые системы VFAT, FAT32, HPFS (High Performance File System), EXT2FS (Second Extended File System) и EXT3FS, BeFS, FFS (Fast File System) AMIGA, FFS BSD, NFS (Networked File System). Сетевые файловые системы: принципы построения; модель сетевой файловой системы, интерфейс сетевой файловой системы, протоколы SMB/CIFS, NCP, NFS. Файловая система UNIX. Особенности файловой системы. Индексная файловая система UNIX. Специальный файл устройства. Именованный канал. Символьная ссылка. Виртуальная файловая система. Дерево каталогов. Стандартные каталоги в файловой системе UNIX. Файловая система Linux. Базовая архитектура файловой системы. Процесс связывания файловой системы с устройством в Linux - монтирование (mounting). Архитектурное представление компонентов файловой системы Linux. Уровень виртуальной файловой системы. Узлы inode и dentry. Структура inode и связанные с ней операции. Буферный кэш. Файловые системы MINIX, MS-DOS и ext2. Нежурналируемые файловые системы. Файловые системы с журналированием (ext3, JFS и ReiserFS). Файловые системы с шифрованием. Файловая система Filesystem in Userspace. Архитектура и технологии резервирования и защиты данных. Архитектура резервного копирования. Операции резервного копирования и восстановления. Дедупликация. Введение в репликацию данных. Типы репликации. Архивирование данных. Миграция данных. Защита больших данных и данных мобильных устройств. Архитектура центра обработки данных. Программно-определяемый центр обработки данных. Обзор облачных технологий хранения данных. Защита данных в облаках. Резервное копирование как услуга. Защита больших данных и данных мобильных устройств. Характеристики больших данных. Аналитика большая данных. Файловая система Hadoop (HDFS).

Рекомендуемый перечень лабораторных работ:

1. Поиск и восстановление данных собственными средствами прикладного ПО Windows.

2. Восстановление данных с жестких дисков.

3. Восстановление данных с flash-накопителей.

4. Восстановление данных из поврежденных и разрушенных RAID-массивов.

Рекомендуемый перечень основной литературы:

1. Бережной, А.Н. Сохранение данных: теория и практика [Электронный ресурс] - Электрон. дан. - Москва : ДМК Пресс, 2016. — 317 с. - Режим доступа: https://e.lanbook.com/book/82823.

2. Иванов, Н.А. Средства резервного копирования и восстановления данных в операционных системах Windows и Linux: методические указания к проведению практических занятий по направлению подготовки 09.03.01 «Информатика и вычислительная техника» [Электронный ресурс] : метод. указ. — Электрон. дан. — Москва : МИСИ – МГСУ, 2016. — 40 с. — Режим доступа: https://e.lanbook.com/book/73946.

3. Shanmuganathan Kumaravel, Libor Miklas Introduction to Storage Area Networks: Электрон. дан. — Redbooks ibm.com/redbooks, Режим доступа - http://www.redbooks.ibm.com/redbooks/pdfs/sg245470.pdf.

4. Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments 2nd Edition, Edited by Somasundaram Gnanasundaram and Alok Shrivastava, Published by John Wiley & Sons.

Перечень материально-технического обеспечения:

учебная лаборатория в области компьютерной криминалистики, оснащенная средствами исследования и восстановления поврежденных носителей данных, устройством для копирования информации с компьютерных носителей с возможностью блокирования операций записи, **системами анализа и восстановления данных**.

**Б.1.С.4.5. Дисциплина «Следообразование в компьютерных системах»**

Коды формируемых компетенций: ПК-Р4.2.

В результате изучения дисциплины студент должен

знать:

- стандарты по тематике управления инцидентами;

- классификации и виды компьютерных инцидентов (КИ).

уметь:

- использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов;

- организовывать безопасное хранение и восстановление данных автоматизированных систем.

владеть:

- навыками администрирования операционными системами семейств Windows и Unix;

- навыками обнаружения атак и распознавания вторжений;

- методами локализация ущерба, причиненного произошедшим инцидентом.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: экзамен.

Содержание дисциплины:

О природе следов в информационной среде компьютерных систем. Отличие информационной среды от физической. Понятие информационного объекта (объекта информационной среды). Следообразующий и следовоспринимающие объекты компьютерных систем. Криминалистически значимые свойства информации. Свойства и признаки информационных объектов. Закономерности формирования служебной информации как основа объективности криминалистического исследования информационных систем. Классификация следов в компьютерных системах. След в информационной среде и его связь с признаком. Предварительная классификация следов в компьютерных системах. Возможности криминалистического исследования компьютерных систем. Проблемы идентификационных исследований. Функциональный подход к классификации следов в компьютерных системах. Форматы некоторых распространенных типов файлов. Форматы файлов с текстовым описанием. Форматы баз данных. Классические DBF-файлы. Файловая организация данных в некоторых системах управления базами данных. Следы установки и работы системы управления базами данных в файлах операционной системы и иной файловой структуре носителя информации. Следы подготовки и обработки документов в базах данных. Сложные форматы бинарных файлов. Контейнерная организация файлов (на примере PE-EXE и OLE2 файлов). Блочная структура файлов (на примере PE-EXE и MP3 файлов). Формат PE-EXE (Portable Executable) и особенности исследования файлов этого формата. Формат OLE2 и особенности исследования файлов этого формата.

Рекомендуемый перечень лабораторных работ:

1. Классификация следов в компьютерных системах.

2. Исследование СУБД.

3. Исследование Portable Executable файлов.

4. Исследование OLE2 файлов.

Рекомендуемый перечень основной литературы:

1. Инструментальный контроль и защита информации : учебное пособие / Н. А. Свинарев, О. В. Ланкин, А. П. Данилкин, С. В. Потехецкий. — Воронеж : ВГУИТ, 2013. — 192 с. — ISBN 978-5-00032-018-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/72884 (дата обращения: 26.05.2021).

2. Россинская, Е. Р. Теория судебной экспертизы: Учебник / Е.Р. Россинская, Е.И. Галяшина, А.М. Зинин; Под ред. Е.Р. Россинской. - Москва : Норма: НИЦ Инфра-М, 2013. - 384 с. ISBN 978-5-91768-344-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/369688 (дата обращения: 26.05.2021).

3. ГОСТ Р ИСО/МЭК 27037‒2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифро- вой форме. – М.: Стандартинформ, 2014. – 48 с.

4. ГОСТ Р ИСО/МЭК 30121‒2017 Информационные технологии (ИТ). Концепция управления рисками, связанными с проведением судебной экспертизы свидетельств, представленных в цифровой форме. – М.: Стандартинформ, 2017. – 12 с.

Перечень материально-технического обеспечения:

учебная лаборатория в области компьютерной криминалистики, оснащенная средствами исследования и восстановления поврежденных носителей данных, устройством для копирования информации с компьютерных носителей с возможностью блокирования операций записи, **системами анализа и восстановления данных**.

**Б.1.С.4.6. Дисциплина «Правовые и организационные основы компьютерной экспертизы»**

Коды формируемых компетенций: ПК-Р4.3.

В результате изучения дисциплины студент должен

знать:

- понятийный аппарат компьютерной экспертизы, правовые, теоретические, методические и организационные основы компьютерной экспертизы;

- систему методов и средств судебно-экспертных исследований;

- основы правового статуса эксперта и специалиста, их права, обязанности, ответственность, порядок участия в судебном процессе.

уметь:

- составлять и оформлять заключения эксперта и специалиста, справки о предварительном исследовании с соблюдением требований действующего законодательства;

- интерпретировать результаты применения средств и методов для решения задач компьютерно-технической экспертизы.

владеть:

- логическими формами при построении выводов по результатам экспертных исследований;

- навыками оформления в соответствии с требованиями законодательства заключений эксперта по результатам проведения компьютерно-технической экспертизы.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: зачет с оценкой.

Содержание дисциплины:

Система законодательства о государственной судебно-экспертной деятельности. Процессуальные, методические, организационные основы компьютерной экспертизы. Обязанности и права эксперта. Производство компьютерно-технической экспертизы. Финансовое, организационное, методическое и информационное обеспечение экспертной деятельности. Правовой статус эксперта в уголовном, гражданском и административном процессе. Типичные ошибки при производстве компьютерных экспертиз. Ошибки, допускаемые на подготовительной стадии экспертного исследования. Ошибки юридического характера, связанные с производством экспертного исследования. Ошибки методического характера, связанные с производством экспертного исследования. Ошибки, связанные с оформлением экспертного заключения. Рекомендации по оформлению экспертных заключений. Подготовка и участие эксперта в судебных заседаниях.

Рекомендуемый перечень лабораторных работ:

1. Процессуальные и организационно-методические основы компьютерной экспертизы.

2. Порядок изъятия, фиксации, документирования цифровых доказательств.

3. Порядок назначения компьютерно-технической экспертизы.

4. Производство компьютерно-технической экспертизы.

5. Составление и оформление заключения эксперта.

6. Подготовка и участие эксперта в судебных заседаниях.

Рекомендуемый перечень основной литературы:

1. Моисеева, Т.Ф. Основы судебно-экспертной деятельности: конспект лекций / Т.Ф. Моисеева. – Москва: Российский государственный университет правосудия (РГУП), 2016. – 191 с. http://biblioclub.ru/index.php?page=book&id=439610.

2. Бегларян, М.Е. Судебная компьютерно-техническая экспертиза: научно-практическое пособие / М.Е. Бегларян. – Москва: Юнити, 2015. – 71 с. http://biblioclub.ru/index.php?page=book&id=446544.

3. Майлис, Н.П. Теория и практика судебной экспертизы в доказывании: учебное пособие / Н.П. Майлис. – Москва: Юнити-Дана : Закон и право, 2015. – 263 с. http://biblioclub.ru/index.php?page=book&id=446415.

4. Майлис, Н.П. Введение в судебную экспертизу: учебное пособие / Н.П. Майлис. – 2-е изд., перераб. и доп. – Москва: Юнити, 2015. – 159 с. http://biblioclub.ru/index.php?page=book&id=114758.

Перечень материально-технического обеспечения:

учебная лаборатория в области компьютерной криминалистики, оснащенная средствами исследования и восстановления поврежденных носителей данных, устройством для копирования информации с компьютерных носителей с возможностью блокирования операций записи, **системами анализа и восстановления данных,** комплексом для криминалистического исследования фонограмм.

**Б.1.С.4.7. Дисциплина «Безопасность сетей ЭВМ»**

Коды формируемых компетенций: ОПК-8.

В результате изучения дисциплины студент должен

знать:

- основные типы и способы применения межсетевых экранов, обобщённую концепцию выбора межсетевых экранов;

- основные программные средства антивирусной защиты;

- принципы разработки политики безопасности.

уметь:

- проводить проверку прохождения пакетов через настроенный межсетевой экран;

- проводить проверку способности персонального межсетевого экрана оказывать противодействие атакам злоумышленника;

- использовать инструментальные средства выявления уязвимостей - системы анализа защищённости;

- минимизировать риски использования сетевого оборудования непредназначенного для защиты сети (коммутаторы и маршрутизаторы).

владеть:

- навыками установки и настройки программно-аппаратных средств защиты информации согласно требованиям безопасности;

- навыками проведения тестирования программно-аппаратных средств защиты информации, разработки набора тестов и методики проведения тестирования и проверки работоспособности системы защиты;

- навыками настройки сетевого оборудования в соответствии с разработанной политикой безопасности.

Примерное распределение часов: трудоемкость дисциплины 10 з.е., 360 час.

Форма контроля: зачет с оценкой, экзамен.

Содержание дисциплины:

Модуль 1. Противодействие угрозам, уязвимостям атакам в компьютерной сети

Основные понятия информационной безопасности. Необходимость обеспечения сетевой безопасности. Взаимосвязь основных понятий безопасности информационных систем. Потеря данных. Триада безопасной ИТ-инфраструктуры – Конфиденциальность, Целостность, Доступность. Обзор сетевых топологий. Сети центров обработки данных. Облачные и виртуальные сети. Вектор атаки злоумышленника. Потенциал нарушителя по ФСТЭК. Типы нарушителей ФСТЭК. Классификация злоумышленников компании CISCO. Проблемы защиты информации в компьютерных сетях. Угрозы сетевой безопасности (связанные с пассивными действиями) ФСТЭК. Угрозы облачной инфраструктуры. Угрозы виртуальной инфраструктуры. Классификация сетевых атак. Разработка системы защиты. Политика информационной безопасности. Структура ПБ. Необходимость создания ПБ. Российская специфика разработки политик безопасности. Основные цели и задачи ПБ. Модель построения корпоративной системы защиты информации. Лучшие практики создания политик безопасности. Структура руководящих документов безопасности. Подход IBM к разработке документов безопасности. Пример стандарта безопасности для ОС семейства UNIX. Сетевой доступ удалённый доступ. Целостность системы. «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014). Классы защищенности. Выбор мер защиты информации. Подход компании Cisco Systems. Политика сетевого подключения. Политика межсетевого экрана. Угрозы кибербезопасности, уязвимости и атаки. Типовые угрозы для конечных пользователей. Типы персональных данных. Угрозы Интернет-сервисам. Внутренние и внешние угрозы. Типы вредоносного ПО. Защита от вредоносных программ Уязвимости мобильных устройств. Вирусы, интернет-черви и «троянские кони». Принципы работы сканера безопасности. Средства сканирования сети на наличие уязвимостей. Сканер уязвимостей Zenmap. Сканер уязвимостей Nessus. Определение уязвимостей узла сети. Системы классификации уязвимостей. Классификация уязвимостей программных систем. Классификация уязвимостей. Классификация троянских вирусов. Атаки в компьютерных сетях. Классификация сетевых атак. Классификация сетевых атак компании CISCO. Жизненный цикл типовой атаки. Определение цели сканирования. Определение топологии сети. Анализ АС. Анализ возможных атак на АС. Основные стадии многоэтапной атаки. Эволюция инструментов безопасности. Разведывательные атаки. Угроза получения предварительной информации об объекте защиты. Угроза обнаружения хостов. Угроза получения предварительной информации об объекте защиты. Краткая информация об инструментах проведения атак. Проблемы безопасности сети. Анализ сетевого трафика. Сетевая карта интерфейса (Network Interface Card (NIC). Обработка сетевого пакета внутри ядра ОС. Кадр. Создание сети. Перехват пакетов. Как включить «неразборчивый режим». Аirmon-ng. BPF: пакетный фильтр BSD . Перехват пакетов – Sniffing. Принципы работы пакетных снифферов. Ограничения использования снифферов. Инструменты анализа сетевого трафика. Анализатор пакетов Wireshark. Пример пакета. Wireshark. Архитектура инструмента Wireshark. Сканирование сети. Сканирование. Методы предварительного сканирования. Сканирование TCP портов. Методы сканирования: сетевое сканирование — определение находящихся в сети узлов. ЭХО-запрос и ЭХО-ответ. Cканирование портов — выявление открытых портов и функционирующих сервисов. История создания. Сетевые порты. Определение состояния порта. Определение цели сканирования. Реализация ICMP – сканирования. Стадия рекогносцировки. Используем программу снифер для анализа трафика. Различные типы UDP сканирования. Проведение сканирования. TCP NULL, FIN и Xmas сканирования. Сканирование TCP-портов флагом FIN. -sO (Сканирование IP протокола). Результаты сканирования. Определение типа ОС. Сканирование узлов сети на наличие уязвимостей. Сетевые атаки – стадия вторжения и атакующее воздействие. Типы уязвимостей. Политики безопасности. Сценарии атаки на систему безопасности. Атаки на переполнение буфера. Технологическая уязвимость типа «переполнение буфера». Активные атаки. Подбор пароля. Атаки типа «отказ в обслуживании». Атака фрагментированными пакетами со смещением (Teardrop Attack). Атака Land. Ping смерти (Ping Of Death). Атака широковещательными ICMP ECHO пакетами (Smurf Attack). Атаки на протоколы стека ТСР/IP. SYN-flood. SYN-flood стенд. Инструментарий. Реализация атаки. Трафик перехваченный на узле-жертве. Воздействие на систему. Противодействие атаке. TCP Reset Attack. Атака, направленная на разрыв соединения. порядковые номера и подтверждения tcp. Управление потоком TCP. Размер окна и подтверждения. TCP Reset Attack на Telnet соединение. Проведение атаки – установление соединения telnet. Проведение атаки – формирования пакета RST. Посылаемый пакет. Результат атаки. Перехват TCP-сессии. Запуск атаки TCP Session Hijacking. Подготовка к атаке. Выполнение атаки. Результаты атаки. Анализ процесса. Атаки на подмену сообщений. Атаки доступа. Атака Человек посередине. Реализация атаки «Man in the Middle». DNS Domain Name System «система доменных имён» Структура DNS Служба DNS: домены и зоны Формирование DNS запросов Угрозы DNS-атак. Типы. Подмена DNS-ответа; внедрение ложного DNS-сервера Схема реализации атаки в случае, если доступа к трафику жертвы нет: Атака на кеш DNS-сервера / подмена вышестоящего DNS-сервера (атака Каминского). Формат DNS ответа Реализация атаки local DNS poisoning.

**Модуль 2.** **Разработка и настройка систем защиты информации в компьютерных сетях**

Безопасность сетевых устройств. Безопасность коммутаторов и маршрутизаторов. Безопасный локальный и удаленный доступ. Предварительная настройка. Повышение безопасности доступа. Алгоритмы защиты пароля. Обеспечение доступа к линии. Расширенная Настройка функций входа в систему. Расширенная Настройка функций входа в систему. Баннерные сообщения. Активация подключения по SSH. Изменение конфигурации SSH. Подключение по SSH. Ограничение доступности команд. Ограничения уровней привилегий. Функция отказоустойчивости Cisco. Маршрутизаторы в качестве целей. Безопасность обновлений маршрутов. Аутентификация MD5. Настройка аутентификации OSPF MD5. Атака с двойным тегированием. Сеть PVLAN периметра. Защита неиспользуемых портов. DHCP Spoofing Attack. Отслеживание DHCP-сообщений. ARP Spoofing and ARP Poisoning Attack. Угрозы безопасности коммутатора. Безопасность граничного маршрутизатора. Мониторинг устройств и управление ими . Использование системного журнала (Syslog) для защиты сети .Основные сведения о системном журнале. Серверы Syslog. Клиенты Syslog. Syslog-сообщение. Основные сведения о протоколе SNMP. База информации управления (Management Information Base, MIB) Уязвимости SNMPНастройка защиты SNMPv3 .Пример настройки защиты SNMPv3. Протокол сетевого времени. Сервер NTP. Аутентификация NTP. Протоколы обнаружения: CDP и LLDP. Настройки для протоколов и сервисов. Уязвимости плоскостей управления и менеджмента. Разграничение доступа на маршрутизаторе. Представления команд на основе ролей. Конфигурирование представлений команд на основе ролей. Конфигурирование суперпредставлений команд CLI на основе ролей. Проверка представлений команд CLI на основе ролей. Ограничения уровней привилегий. Конфигурирование и присвоение уровней привилегий. Модель ААА. Введение. Система управления доступом к сети . Аутентификация без ААА. Компоненты ААА. AAA для аутентификации в системе Cisco Secure Access Control System (ACS). Методы аутентификации. Локальная модель ААА. Локальная аутентификация AAA. Настройка локальной аутентификации AAA с помощью CLI 3.2.1.1 Аутентификация административного доступа. Стандартный и именованный методы. Точная настройка конфигурации аутентификации. Варианты отладки. Отладка аутентификации AAA. Серверная аутентификация ААА. Серверное решение ААА. Характеристики серверного решения AAA . Сравнение локальной и серверной аутентификации ААА. Знакомство с системой управления защищенным доступом Cisco (Access Control System, ACS). Режимы аутентификации. Авторизация. Учет. Знакомство с протоколами TACACS+ и RADIUS. Аутентификация TACACS+. Аутентификация RADIUS. Интеграция TACACS+ и ACS. Интеграция ААА с Active Directory. Интеграция AAA и Identity Service Engine. Процедура настройки серверной аутентификации ААА. Настройка серверов TACACS+. Настройка серверов RADIUS. Конфигурирование аутентификации с использованием сервера ААА. Знакомство с серверной авторизацией ААА. Обеспечение безопасности с использованием аутентификации 802.1X на основе портов. Защита от атак на протокол STP. Обеспечение безопасности локальной сети (LAN). Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне. Протокол связующего дерева. Введение в протокол связующего дерева . Различные реализации протокола STP. Роли портов STP. Корневой мост STP. Стоимость пути STP. Формат кадра BPDU 802.1D. Распространение и обработка BPDU-сообщений. Расширенный ИД системы. Выбор корневого моста. Защита от атак на DHCP. Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне . Нейтрализация атак DHCP. Спуфинг DHCP. Истощение DHCP. Нейтрализация атак DHCP. Конфигурирование DHCP Snooping. Пример конфигурирования DHCP Snooping. Нейтрализация атак ARP 6.2.6.1 Спуфинг ARP и ARP Poisoning. Нейтрализация атак ARP. Конфигурирование динамического инспектирования ARP. Пример конфигурирования динамического инспектирования ARP. Обеспечение безопасности VLAN. Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне. Нейтрализация атак на сеть VLAN. Атаки перехода (Hopping) VLAN. Спуфинг сообщений DTP. Ввод подставного коммутатора. Атака с двойным тегированием (Double-Tagging) VLAN. Нейтрализация атак перехода VLAN. Функция границы частной сети VLAN (PVLAN Edge). Граница PVLAN. Частные сети VLAN. Преимущества частных сетей VLAN. Примеры реализации частных сетей VLAN. Типы портов частной сети VLAN. Конфигурирование частных сетей VLAN на многоуровневом коммутаторе 3560. Использование команды switchport protected в коммутаторе 2960. Обеспечение безопасности порта. Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне. Атаки на таблицу CAM. Базовый режим работы коммутатора Компрометация межсетевых экранов/ Пример работы таблицы CAM Инструменты атаки на таблицу САМ 3 Нейтрализация атак на таблицы CAM 6.2.3.1 Противодействие атакам на таблицы CAM Включение опций защиты портов Нарушения защиты портов Устаревание данных защиты порта Работа защиты портов совместно с IP-телефонам SNMP-уведомление об изменениях MAC-адресов. Защита межфилиальной связи, VPN. Современные угрозы сетевой безопасности. Сети VPN. Компоненты сети IPsec VPN и их функционирование. Реализация сетей IPsec VPN между двумя пунктами с помощью CLI. Обзор сети VPN. Топологии сетей VPN. Знакомство с сетями VPN. Сети IPsec VPN 3-го уровня. Внедрение виртуальных частных сетей (VPN). Сети VPN. Обзор сети VPN. Знакомство с сетями VPN. Технологии IPsec. Конфиденциальность. Целостность. Аутентификация. Безопасный обмен ключами. Authentication Header (AH). ESP. ESP выполняет шифрование и аутентификацию. Транспортный и туннельный режимы. Протокол Internet Key Exchange (IKE). Согласование ключей на фазе 1 и 2. Фаза 2. Согласование ассоциаций SA. Настройка сети IPsec VPN между двумя пунктами. Установление IPsec-соединения. Топология сети IPsec VPN между двумя пунктами. Задачи по настройке сети IPsec VPN. Существующие конфигурации списка ACL. Преобразование адресов, NAT. Технология NAT. NAT позволяет скрыть адреса внутренней сети. Зачем нужен NAT. Базовый NAT. NAPT. Двойной NAT. Ограничения NAT.

**Модуль 3. Разработка системы защиты с помощью межсетевого экрана**

Межсетевые экраны, классификация, основы работы. Определение межсетевого экрана. Принципы создания системы защиты. Особенности применения МЭ. Принципы создания системы защиты с помощью МЭ. Стек протоколов. Типы межсетевых экранов. Фильтрование пакетов. Достоинства и недостатки пакетных фильтров. Межсетевой экран Cisco ASA. ASA Firewall Models. Advanced ASA Firewall Feature. Review of Firewalls in Network Design. ASA Firewall Modes of Operation. ASA Licensing Requirements. Overview of ASA 5505. Уровни безопасности ASA. ASA 5505 Deployment Scenarios. Basic ASA Settings. ASA Default Configuration. Configuring Basic Settings. Configuring Dynamic PAT. Configuring Static NAT. Introduction to Objects and Object Groups. Configuring Network Objects. Configuring Service Objects. Object Groups. ASA ACLs. Configuring ACLs. Applying ACLs. ACLs and Object Groups. Межсетевой экран Dlink. Особенности применения межсетевых экранов и маршрутизаторов D-Link. Интернет-маршрутизаторы серии Unified Services. Маршрутизаторы ADSL. Обзор межсетевых экранов NetDefend D-Link. Межсетевой экран DFL-860E. Архитектура NetDefendOS. Прохождение пакета через межсетевой экран D-Link. Управление межсетевыми экранами D-Link NetDefend. Персональные межсетевые экраны. Исследование архитектуры и функционирования МЭ на примере предложенного ПО/ Исследование механизмов взаимодействия средств сетевой безопасности с операционной системой. Подходы к организации фильтрования трафика в ОС Windows. Outpost Personal Firewall PRO. Norton Personal Firewall. Тестирование персональных межсетевых экранов. Принципы создания системы защиты с помощью межсетевого экрана. Основной режим работы пакетного фильтра. Проверка на сетевом уровне. Проверка на транспортном уровне. Таблица необходимых правил фильтра. Пример использования пакетного фильтра. Stateful Firewalls – МЭ Состояний. Состояния ТСР-соединения. Разработка конфигурации межсетевого экрана. Что такое ACL-список. Принцип работы ACL-списков. Типы ACL-списков Cisco для IPv4. Присваивание номеров и имён ACL-спискам. Где следует размещать ACL-списки. Размещение стандартного ACL-списка. Задание порядка записей ACL-списка. Настройка межсетевого экрана Iptables. Работа классического брандмауэра. Сетевое сканирование защищенного сервера. Демилитаризованная зона (DMZ). Межсетевые экраны прикладного уровня. Прокси-шлюзы прикладного уровня. Компрометация межсетевых экранов. Основные способы развертывания межсетевых экранов в корпоративных сетях. Межсетевой экран, представленный как фильтрующий маршрутизатор. Межсетевой экран на основе двухпортового шлюза. Межсетевой экран на основе экранированного шлюза. Межсетевой экран с экранированной подсетью. Недостатки применения межсетевых экранов. Организация комплексной защиты корпоративной сети. Защита корпоративной сети от несанкционированного доступа из Интернет. Организация внутренней политики безопасности корпоративной сети. Реализации межсетевых экранов. Способы обхода межсетевых экранов.

**Модуль 4. Технологии обеспечения сетевой безопасности**

Куб кибербезопасности. Принципы информационной безопасности. Состояния данных. Меры кибербезопасности. Принцип конфиденциальности. Защита конфиденциальных данных. Контроль доступа. Законы и ответственность. Принцип целостности данных. Требования к целостности данных. Проверки целостности. Принцип доступности. Обеспечение доступности. Варианты хранения данных. Задачи защиты хранящихся данных. Методы передачи данных. Задачи защиты передаваемых данных. Виды обработки данных. Задачи защиты обрабатываемых данных. Защита уровней обеспечения кибербезопасности. Безопасность операционной системы. Защита от вредоносных программ. Управление исправлениями. Межсетевые экраны (брандмауэры) и системы обнаружения вторжений на основе хоста. Защита коммуникаций. WPA/WPA2. Взаимная аутентификация. Разграничение доступа к файлам. Шифрование файлов. Резервное копирование данных и систем. Фильтрация и блокирование содержимого. Клонирование жесткого диска и утилита Deep Freeze. Защитные кабели и замки. Блокировка компьютера после бездействия. Управление удаленным доступом. Защита портов и сервисов. Привилегированные учетные записи. Групповые политики. Включение журналов и оповещений. Контроль аппаратных средств. Разграничение физического доступа. Технологии реагирования на инциденты. Подготовка. Обнаружение и анализ. Изоляция, ликвидация и восстановление. Подведение итогов по инцидентам информационной безопасности. Сетевой модуль Cisco NAC. Системы обнаружения вторжений. Система предотвращения вторжений. NetFlow и IPFIX. Продвинутые средства анализа угроз. Виды аварий. Аварийное восстановление. План аварийного восстановления. Внедрение мер аварийного восстановления. Необходимость в непрерывности бизнес-процессов. Аспекты непрерывности бизнес-процессов. Лучшие практики обеспечения непрерывности бизнес-процессов. Разработка и реализация политики безопасности. Уровни обеспечения кибербезопасности. Контрольные цели. Средства управления. Политики. Стандарты. Рекомендации. Процедуры. Обзор модели. Уровни обеспечения кибербезопасности. Контрольные цели. Средства управления. Использование модели кибербезопасности ISO и состояния данных. Модель кибербезопасности ISO и меры защиты. Методы обнаружения атак. Основные понятия и определения. Определение среды функционирования СОА. Основные значимые компоненты СОА. Типовая архитектура СОА. Анализ существующих подходов к построению СОА. Методы обнаружения атак. Методы обнаружения злоупотреблений. Методы обнаружения аномалий. Результаты сравнительного анализа. «Простые» сигнатуры. Идентификация компонентов «сложной» сигнатуры. Создание оптимальной «сложной» сигнатуры. Рекомендации по использованию элементов заголовка для создания сигнатур. Сигнатуры систем анализа протокола. Выполнение анализа протокола на FTP трафике. Структура сигнатуры. Структура сигнатуры сетевого события. Перечень событий, обнаруживаемых СОА. Обнаружение аномалий в трафике сети. Обнаружение опасных данных в сетевом пакете. Обнаружение аномалий в заголовках сетевого пакета (протокола). Описание некоторых систем обнаружения атак. 1.Вrо. 2.OSSEC. 3 STAT. 4. Prelude. 5. Snort. 6. RealSecure компании ISS. Классические системы обнаружения атак. Между маршрутизатором и межсетевым экраном. В демилитаризованной зоне. За межсетевым экраном. В ключевых сегментах внутренней сети. У сервера удаленного доступа. Технология антивирусной защиты информации. История компьютерных вирусов. Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы Файлово-загрузочные вирусы. Стелс-вирусы. Шифрующиеся вирусы. Полиморфные шифрующиеся вирусы. Макрокомандные шифрующиеся вирусы. Почтовые вирусы. Вирусы в пакетных файлах ОС. Вирусы в драйверах ОС. Бестелесные вирусы. Вирусы для пиринговых сетей. Комбинированные вирусы. Коллекционные вирусы. Черви. Логические бомбы. Троянские объекты. Троянские программы. Троянские Web-сайты. Троянские сообщения E-Mail. Программы Backdoor. Основные методы защиты от компьютерного вируса. Разработчики продуктов для борьбы с компьютерными вирусами. Мониторинг сети. Введение в Syslog. Принцип работы Syslog. Формат сообщений syslog. Служба меток времени. Сервер Syslog. Ведение журналов по умолчанию. Команды маршрутизатора и коммутатора для клиентов syslog. Проверка syslog. Знакомство с SNMP. Принцип работы SNMP. Ловушки агента SNMP. Идентификатор объекта информационной базы управления (MIB). Этапы настройки SNMP. Проверка настройки SNMP. Практические рекомендации по обеспечению безопасности. Краткое описание протокола NetFlow. Общие сведения о NetFlow. Потоки в сети. Настройка NetFlow. Анализ NetFlow с помощью сборщика данных NetFlow. Отладка сети. Документирование сети. Диаграммы топологии сети. Формирование базовых показателей сети. Измерение данных. Общие процедуры поиска и устранения неполадок. Сбор данных о симптомах. Опрос конечных пользователей. Использование многоуровневых моделей для поиска устранения неполадок. Методы поиска и устранения неполадок. Указания по выбору метода поиска и устранения неполадок. Программные средства поиска и устранения неполадок. Средства поиска и устранения неполадок аппаратного обеспечения. Применение сервера Syslog для устранения неполадок. Поиск и устранение неполадок на физическом уровне. Поиск и устранение неполадок канального уровня. Поиск и устранение неполадок сетевого уровня. Поиск и устранение неполадок на транспортном уровне — ACL-списки. Поиск и устранение неисправностей на уровне приложений. Инструментарий для анализа защищённости. Сканеры уязвимостей. Тестирование на возможность проникновения. Анализаторы пакетов. Инструментальные средства безопасности. Определение ролей специалистов по кибербезопасности. Общие угрозы и уязвимости, связанные с пользователями. Управление угрозами, связанными с пользователями. Распространенные угрозы для устройств. Управление угрозами, связанными с устройствами. Распространенные угрозы для локальной сети. Распространенные угрозы для частного облака. Управление угрозами для частного облака. Распространенные угрозы для общедоступного облака. Управление угрозами для общедоступного облака. Распространенные угрозы для физических средств. Управление угрозами для физических средств. Распространенные угрозы для приложений. Способы устранения уязвимостей. Управление угрозами для приложений. Этические ценности специалиста по обеспечению кибербезопасности. Институт компьютерной этики. Гражданское и уголовное законодательство и нормативные требования информационного и телекоммуникационного права. Законы об уведомлении в случае нарушения безопасности.

Рекомендуемый перечень лабораторных работ:

1. Изучение сетевых атак, а также инструментов для аудита безопасности и проведения атак.

2. Мониторинг состояния элементов сети с использованием анализаторов сетевого трафика Wireshark.

3. Обнаружение уязвимостей сетевого узла с помощью сканеров безопасности.

4. Атаки на TCP/IP.

5. Защита маршрутизатора для административного доступа.

6. Защита административного доступа с помощью AAA и RADIUS.

7. Защита коммутаторов 2-го уровня.

8. Настройка сети Site-to-Site VPN с помощью Cisco IOS.

9. Настройка преобразования адреса и номера порта (PAT).

10. Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI).

11. Конфигурация межсетевого экрана Dlink Базовая настройка и настройка межсетевого экрана.

12. Настройка программного межсетевого экрана ОС LINUX.

13. Тестирование персонального экрана.

14. Исследование механизмов осуществления и обнаружения сетевых атак.

15. Обнаружение уязвимостей сетевого узла с помощью сканеров портов.

Рекомендуемый перечень основной литературы:

1. Мэйволд Э. Безопасность сетей / Э. Мэйволд - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с. http://biblioclub.ru/index.php?page=book&id=429035.

2. Пелешенко В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие / В.С. Пелешенко; С.В. Говорова; М.А. Лапина - Ставрополь: СКФУ, 2017. - 86 с. http://biblioclub.ru/index.php?page=book&id=467139.

3. Лапонина О. Р. Межсетевые экраны / О.Р. Лапонина - 2-е изд., исправ. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 466 с. http://biblioclub.ru/index.php?page=book&id=429093.

4. Кияев В. Безопасность информационных систем / В. Кияев; О. Граничин - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. http://biblioclub.ru/index.php?page=book&id=429032.

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации, средствами контроля защищенности информации, системами обнаружения и предотвращения атак и доступом к Сетевой академии CISCO: Networking Academy https://www.netacad.com.

**Б.1.С.4.8. Дисциплина «Интеллектуальные технологии в задачах информационной безопасности»**

Коды формируемых компетенций: ОПК-9, ОПК-10, ОПК-11.

В результате изучения дисциплины студент должен

знать:

- основные требования информационной безопасности при решении стандартных задачи профессиональной деятельности.

уметь:

- применять основные требования информационной безопасности при решении стандартных задачи профессиональной деятельности.

владеть:

- навыками применения основных требований информационной безопасности при решении стандартных задачи профессиональной деятельности.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Модуль 1. Интеллектуальные технологии**

**Введение. Исторические аспекты появления и развития интеллектуальных систем.** Гносеологическая проблемы познания мозга. Тест Тьюринга и интуитивный подход. Гипотеза Ньюэлла-Саймона. Работы У. Мак-Каллока, У. Питса, Ф. Розенблатта, Д. Хебба, М. Минского, С. Пайперта, Д. Хопфилда, Д. Холланда, А. Ньюэлла, Г. Саймона, М.Г. Гаазе-Рапопорта, Д.А.Поспелова, П. Розенблума, К. Гёделя, Р. Пенроуза и др. **Структура и процедура систем продукций.** Структура систем продукций. Процедура систем продукций. **Стратегии управления систем продукций.** Стратегии управления систем продукцийс возвращением. Алгоритм рекурсивной процедуры BACKTRACK. Процедура BACKTRACK с оптимизацией выбора. **Стратегии поиска на графе.** Язык графов в системах продукций. Неинформированные процедуры поиска на графе. Эвристические процедуры поиска на графе. Применение оценочных функций. **Специализированные системы продукций.** Коммутативные системы продукций. Разложимые системы продукций. Язык И/ИЛИ графов. Обратные и двусторонние системы продукций. **Оценка эффективности систем продукций. Поиск на игровых деревьях.** Минимаксная процедура. Альфа-бета процедура. Эффективность поиска с помощью альфа-бета процедуры. **Введение. Естественная иммунная система.** Сопоставление нервной и иммунной систем. **Моделирование иммунной системы.** Общие принципы моделирования иммунной системы. Модель иммунной сети. Модель отрицательного отбора. Формальное описание модели отрицательного отбора. Реализация модели отрицательного отбора. Модель клональной селекции. Формальное описание модели клональной селекции. Модель гиперклетки. **Виды детекторов.** Строковые детекторы. Числовые детекторы. V-детекторы. Алгоритм формирования V-детекторов. **Применение ИИС в компьютерной безопасности.** Мониторинг информационных процессов в КС средствами ИИС. Обнаружение аномалий процессов в КС средствами ИИС. Обнаружение атак на КС средствами ИИС. Динамические биометрические системы идентификации личности реализуемые средствами ИИС.

**Модуль 2. Безопасность систем баз данных**

**Основные понятия и определения**. Угрозы безопасности в КС. Методы оценивания угроз. Разработка СБД. **Методы и средства персонализации и аутентификации в СБД.** Парольная аутентификация. Одноразовые пароли. Функциональные методы аутентификации. Аутентификация при удаленном доступе в сетях. Протокол аутентификации РАР. Протокол аутентификации CHAP. Протокол аутентификации S/Key. Протокол аутентификации Kerberos. Персональные средства аутентификации. Биометрические средства аутентификации. Аутентификация по информации, ассоциированной с субъектом. Аутентификация объектов. Аутентификация процессов. Особенности процедур идентификации, аутентификации в СБД. **Методы и средства авторизации в СБД.** Субъектно-объектная модель доступа. Монитор безопасности. Политики и модели безопасности. Дискреционные модели. Мандатные модели. Ролевые модели. **Управление доступом в СБД.** Основные понятия. Основные категории пользователей СБД. Виды привилегий в СУБД. Группы. Роли. Представления. Особенности привилегий доступа к реляционным таблицам БД. Использование представлений для фильтрации привилегий. Агрегатные функции. Особенности привилегий доступа к процедурам. Права доступа к БД. Иерархия прав доступа. Получение информации о привилегиях. Соотношение прав доступа СУБД и ОС. Мандатная защита в СУБД. **Обеспечение конфиденциальности данных в СБД.** Основные понятия. Скрытые каналы на основе анализа параметров протекания процессов. Решение проблем скрытых каналов. Нейтрализация скрытых каналов утечки информации на основе технологий представлений. Нейтрализация скрытых каналов утечки информации на основе техники разрешенных процедур. Скрытые каналы утечки информации, специфичные для реляционных СУБД. Особенности хранения и обработки данных в БД. **Обеспечение целостности данных.** Основные понятия. Модели обеспечения целостности. Обеспечение целостности данных в реляционных СБД. Доменная целостность. Сущностная целостность. Ссылочная целостность. Декларативные способы обеспечения целостности. Процедурные способы обеспечения целостности. Применение декларативных и процедурных средств поддержания целостности. **Обеспечение высокой доступности СБД.** Сохранность данных в СБД. Организация дисковых массивов (RAID). Отказоустойчивые кластеры и системы. Кластеры высокой доступности (готовности). Технологии постоянного дублирования. Зеркальное отображение баз данных. Тиражирование данных. Технологии архивирования. Резервное копирование БД. Восстановление баз данных. Репликация баз данных.

Рекомендуемый перечень лабораторных работ:

1. Разработка персональной СБД.

2. Разработка защиты персональной СБД.

3. Обеспечение защиты данных с помощью представлений.

4. Обеспечение целостности данных в полях реляционных таблиц.

5. Обеспечение ссылочной целостности данных.

Рекомендуемый перечень основной литературы:

1. Герасименко Е.М. Методы машинного обучения в научных исследованиях. – Ростов-на-Дону-Таганрог: Издательство Южного федерального университета, 2020.

2. Данилова Н.В., Белявский Г.И. Анализ данных. Машинное обучение. – Ростов-на-Дону-Таганрог: Издательство Южного федерального университета, 2020.

3. Искусственный интеллект. Современный подход / С. Расел, П. Норвиг: Пер. с англ. – М.: Издательский дом «Вильямс», 2007. – 1407 с.

4. Искусственные иммунные системы и их применение [Текст], под ред. Д. Дасгупты; пер. с англ. А. А. Романюхи. – Москва: Физматлит, 2006. – 344 с.

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

**Дисциплины специализации №5 «Организация и технология информационной безопасности»**

**Б.1.С.5.1. Дисциплина «Администрирование вычислительных сетей»**

Коды формируемых компетенций: ПК-Р5.3.

В результате изучения дисциплины студент должен

Знать:

- основы функционирования средств электронно-вычислительной техники и сетевого оборудования, принципов работы сетевых протоколов и постронеия локальных вычислительных сетей

Уметь

- обеспечивать работоспособность компьютерной техники и переферийного оборудования

Владеть:

- навыками администрирования, восстановления и разграничения доступа в операционных системах семейств Windows и Unix

Примерное распределение часов: трудоемкость дисциплины 10 з.е., 360 час.

Форма контроля: зачет, экзамен.

Содержание дисциплины:

Системное администрирование ОС Linux. Пользователи, файлы и процессы ОС Linux. Средства администрирования и мониторинга серверов и рабочих станций, работающих под управлением ОС Linux. Основы администрирования в Linux. Системное администрирование с помощью сетевых инструментов Linux. Настройка DNS для ОС. Linux. Администрирование сервисов ОС Linux. Настройка LDAP сервера для OC Linux. Настройка Rsyslog для OC Linux. Резервное копирование данных и дисковые массивы. Управление сетевым подключением с помощью протокола DHCP. Администрирование сети под управление OC Windows. Организация сетей, управляемых ОС Windows. Администрирование сетей ОС Windows. Администрирование прикладных сервисов. Администрирование web-сервера Apache. Протоколы передачи гипертекста. Протоколы передачи файлов. Администрирование сервера FTP. Протоколы передачи сообщений электронной почты. Администрирование почтового сервера. Система усиленной защиты SELinux и её администрирование. Настройка сервиса OpenSSL.

Рекомендуемый перечень лабораторных работ:

1. **Пользователи, файлы и процессы ОС Linux.**

**2. Средства диспетчеризации ОС Linux.**

**3. Системное администрирование с помощью сетевых инструментов Linux.**

**4. Настройка DNS для ОС Linux.**

5. Обеспечение целостности и доступности данных в ОС Linux. RAID.

6. Настройка LDAP сервера для OC Linux.

7. Настройка Rsyslog для OC Linux.

**8. Настройка шаблона безопасности в ОС Windows.**

9. **Установка и настройка web-сервера Apache.**

**10. Установка и настройка почтового сервера.**

Рекомендуемый перечень основной литературы:

1. Элсенпитер Р. Администрирование сетей Microsoft Windows XP Professional / Р. Элсенпитер; Велт - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 650 с. – URL: http://biblioclub.ru/index.php?page=book&id=428821.

2. Учебный курс "Основы администрирования ОС Linux" / Составитель С. Гончарук, 2016. – URL: https://www.opennet.ru/docs/RUS/linuxadmin/.

3. Гимбицкая Л. А. Администрирование в информационных системах / Л.А. Гимбицкая; З.М. Альбекова - Ставрополь: СКФУ, 2014. - 66 с. – URL: http://biblioclub.ru/index.php?page=book&id=457276.

Перечень материально-технического обеспечения:

учебная аудитория лекционного типа, оснащенная интерактивной доской и компьютером преподавателя, а также лаборатория безопасности ОС, оснащенная интерактивной доской и компьютерами для преподавателя и учащихся с виртуальными машинами.

**Б.1.С.5.2. Дисциплина «Безопасность персональных данных»**

Коды формируемых компетенций: ПК-Р5.1.

В результате изучения дисциплины студент должен

Знать:

- современные технологии обеспечения информационной безопасности

Уметь:

- применять средства обеспечения информационной безопасности

Владеть:

- навыками использования нормативно-методических документов в области информационной безопасности для обоснования проектных решений при проектировании автоматизированных систем, контроля реализации требований политик информационной безопасности

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: зачет с оценкой.

Содержание дисциплины:

Основные понятия, термины и определения. Классификация информации конфиденциального характера и выделение категории персональных данных. Обзор и анализ нормативно-методических документов Российской Федерации в области защиты персональных данных. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Модель угроз для информационных систем персональных данных. Организация и обеспечение режимов защиты персональных данных. Оценка эффективности системы защиты информационных систем персональных данных. Нормативно-методическое и правовое обеспечение стандартизации и автоматизации документооборота. Системы автоматизации документооборота. Защита информации в системах электронного документооборота. Обзор особенностей внедрения систем электронного документооборота. Основные понятия, термины и определения. Классификация информации конфиденциального характера и выделение категории персональных и фискальных данных. Обзор и анализ нормативно-методическеских документов Российской Федерации в области защиты персональных и фискальных данных. Обзор и анализ требований законодательства к оператору персональных данных. Основные принципы обработки персональных и фискальных данных. Обзор и анализ результатов прохождение проверок организаций государственными регуляторами в области защиты информации. Организация режима обработки ПДн и фискальных данных, соответствующая разработка организационно-распорядительной документации по защите информации. Классификация систем обработки персональных и фискальных данных. Определение уровня защищенности. Разработка модели вероятного нарушителя и модели актуальных угроз безопасности. Определение требований к системе защиты информации. Выбор технических средств защиты информации при проектировании системы защиты информации персональных и фискальных данных. Вопросы настройки средств защиты информации и разработки сопутствующей необходимой документации. Составление технического задания на выполнение работ по созданию системы защиты информации в информационной системе персональных и фискальных данных. Особенности проведения торгов. Проведение оценки эффективности принятых мер по защите информации в ИСПДн, аттестация информационной системы.

Рекомендуемый перечень лабораторных работ:

1. Защита персональных данных.

2. Защита компьютерной информации на уроне доступа в систему.

3. Защита от компьютерных вирусов.

4. Защита от атак по локальным и глобальным сетям.

Рекомендуемый перечень основной литературы:

1. Нестеров С. А. Основы информационной безопасности / С.А. Нестеров - Санкт-Петербург: Издательство Политехнического университета, 2014. - 322 с.

http://biblioclub.ru/index.php?page=book&id=363040.

2. Загинайлов Ю. Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов - М.|Берлин: Директ-Медиа, 2015. – 105 с.

http://biblioclub.ru/index.php?page=book&id=362895.

3. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов - М.|Берлин: Директ-Медиа, 2015. - 253 с.

http://biblioclub.ru/index.php?page=book&id=276557.

Перечень материально-технического обеспечения:

учебная аудитория лекционного типа, оснащенная интерактивной доской и компьютером преподавателя.

**Б.1.С.5.3. Дисциплина «Разработка и эксплуатация автоматизированных систем в защищенном исполнении»**

Коды формируемых компетенций: ПК-Р5.1, ПК-Р5.2, ПК-Р5.3.

В результате изучения дисциплины студент должен

Знать:

- методологию и методики проведения мероприятий по защите информации вс учётом специфики правоохранительной сферы

- принципы обеспечения информационной безопасности автоматизированных систем

Уметь:

- проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности

- выстраивать антивирусную защиту локальной сети и отдельных компьютеров

- обосновывать выбор средств защиты информационно-технологических ресурсов автоматизированной системы

Владеть:

- навыками участия в разработке системы обеспечения информационной безопасности объекта

- навыками формирования требований по защите информации объекта информатизации.

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: экзамен.

Содержание дисциплины:

Защищенные автоматизированные системы. Основные понятия и классификация. Классификация автоматизированных систем (АС). Информационные технологии, используемые в АС. Жизненный цикл АС. Основные угрозы безопасности информации в автоматизированных системах. Отказоустойчивость АС. Основы организации разработки защищенных АС. Последовательность и содержание этапов разработки АС. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС. Общие принципы проектирования защищенных АС. Проектирование защищенных АС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АС. Организация хранения информации в защищенных АС. Основы эксплуатации защищенных АС. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС. Порядок обеспечения защиты информации при эксплуатации АС. Организация технического обслуживания защищенных АС. Средства диагностирования защищенных АС. Аппаратно-программные средства диагностики АС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков. Основы администрирования АС. Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования АС. Настройка сетевой подсистемы защищенной АС. Принципы функционирования информационных сервисов АС. Установка и настройка работы информационных сервисов АС. Удаленное администрирование компонентов АС. Управление дисковой подсистемой АС.

Рекомендуемый перечень лабораторных работ:

1. Технология создания отказоустойчивых АС.

2. Настройка сетевой подсистемы защищенной АС.

3. Настройка программных средств администрирования АС.

4. Управление дисковой подсистемой АС.

Рекомендуемый перечень основной литературы:

1. Проскуряков, А. В. Компьютерные сети. Основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков. — Ростов-на-Дону : ЮФУ, 2018. — 201 с. — ISBN 978-5-9275-2792-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125052 (дата обращения: 14.05.2021).

2. Кузьмич, Р. И. Вычислительные системы, сети и телекоммуникации : учебное пособие / Р. И. Кузьмич, А. Н. Пупков, Л. Н. Корпачева. — Красноярск : СФУ, 2018. — 120 с. — ISBN 978-5-7638-3943-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/117794 (дата обращения: 14.05.2021).

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/471908 (дата обращения: 14.05.2021).

4. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/471236 (дата обращения: 14.05.2021).

Перечень материально-технического обеспечения:

учебная аудитория лекционного типа, оснащенная интерактивной доской и компьютером преподавателя.

**Б.1.С.5.4. Дисциплина «Аудит информационной безопасности»**

Коды формируемых компетенций: ПК-Р5.2.

В результате изучения дисциплины студент должен

Знать:

- методы поиска уязвимостей и анализа способов их эксплуатации

Уметь:

- проводить поиск, анализ и документирование уязвимостей

Владеть:

- навыками классификации автоматизированной системы, определения архитектуры и топологиы сети, определения актуальных угроз, типа возможного нарушителя, разрабатывать модель угроз, работать с нормативно-правовой документацией

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: экзамен.

Содержание дисциплины:

Основы менеджмента риска в организации. Менеджмент риска. Термины и определения. Классификация методов оценки риска. Экспертные методы оценки риска. Методы оценки риска, основанные на причинно-следственном анализе. Аналитические методы оценки риска. Методология анализа риска информационной безопасности предприятия. Международная нормативная база обеспечения информационной безопасности на основ риск-анализа. Стандарт Банка России СТО БР ИББС-2.2-2009. Методика ФСТЭК РФ определения угроз безопасности информации в информационных системах. Программные средства анализа риска и управления безопасностью предприятия. Методы проведения аудита информационной безопасности. Концепция аудита ИБ систем ИТ и организаций в РФ. Организация мероприятий по аудиту ИБ объекта информатизации. Комплексный аудит информационной безопасности АС. Аудит безопасности информационных технологий. Аудит автоматизированных банковский систем (АБС). Организационные, этические и правовые аспекты аудита информационных технологий и систем обеспечения ИБ. Уязвимости и средства их выявления. Инструментальные средства аудита ИБ).

Рекомендуемый перечень лабораторных работ:

1. Обратная социальная инженерия. Сбор информации из открытых источников.
2. Движение информации в DLP-системе. Виды перехвата. Платформа NetworkSniffer.
3. Рабочие инструменты аналитика DLP-системы.
4. Создание политик в AlertCenter.
5. Создание отчётов в ReportCenter

Рекомендуемый перечень основной литературы:

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] – Саратов: Профобразование, 2018. – 702 c. – Режим доступа: <http://www.iprbookshop.ru/63594.html>.
2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]. – Саратов: Профобразование, 2018. – 544 c. – Режим доступа: <http://www.iprbookshop.ru/63592.html>.

Перечень материально-технического обеспечения:

учебная аудитория для проведения лекционных занятий, практических занятий, текущего контроля и промежуточной аттестации, оснащенная необходимым для этого оборудованием.

**Б.1.С.5.5. Дисциплина «Безопасность операционных систем»**

Коды формируемых компетенций: ПК-Р5.2.

В результате изучения дисциплины студент должен

Знать:

- методы организации защиты информации в современных ОС

Уметь:

- использовать средства операционных систем для обеспечения информационной безопасности автоматизированных систем

Владеть:

- навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности

Примерное распределение часов: трудоемкость дисциплины 7 з.е., 252 час.

Форма контроля: экзамен.

Содержание дисциплины:

Основы защиты информации в современных ОС. Вопросы безопасности ОС семейства Microsoft Windows. Требования к защите ОС. Основные подсистемы безопасности ОС семейства Microsoft Windows. Аутентификация в ОС семейства Microsoft Windows. Разграничение доступа в ОС семейства Microsoft Windows Службы сертификации в ОС семейства Microsoft Windows. Защита сетевого взаимодействия. Протокол IPSec. Обеспечение целостности в ОС семейства Microsoft Windows. Инструменты администрирования ОС семейства Microsoft Windows. Вопросы безопасности Unix-подобных ОС. Идентификация и аутентификация в Unix-подобных ОС. Разграничение доступа в Unix-подобных ОС Подсистемы аудита в Unix-подобных ОС.

Рекомендуемый перечень лабораторных работ:

1. Работа с учетными записями пользователей в клиентских ОС семейства Microsoft Windows.

2. Настройка параметров безопасности в клиентских ОС семейства Microsoft Windows.

3. Обеспечение безопасности ресурсов с помощью разрешений NTFS в клиентских ОС семейства Microsoft Windows.

4. Управление хранением данных в клиентских ОС семейства Microsoft Windows.

5. Архивация и восстановление данных в клиентских ОС семейства Microsoft Windows.

6. Аудит ресурсов и событий в клиентских ОС семейства Microsoft Windows.

7. Управление загрузкой ОС Microsoft Windows Server.

8. Управление объектами Active Directory в ОС Microsoft Windows Server.

9. Механизм групповых политик в ОС Microsoft Windows Server.

10. Базовые навыки администрирования в ОС Ubunta.

Рекомендуемый перечень основной литературы:

1. Пескова О.Ю., Половко И.Ю. Администрирование операционных систем Часть 1 Администрирование одноранговых сетей и рабочих групп под управлением клиентских ОС семейства Microsoft Windows Учебное пособие / Ростов-на-Дону - Таганрог, 2017-145 с.

2. Пескова О.Ю., Половко И.Ю. Администрирование операционных систем Часть 2 Администрирование доменов под управлением серверных ОС семейства Microsoft Windows Учебное пособие / Ростов-на-Дону - Таганрог, 2017. -73 с.

3. Пескова О.Ю., Половко И.Ю. Безопасность операционных систем Часть 1 Подсистемы безопасности операционных систем семейства Microsoft Windows учебное пособие / Министерство образования и науки Российской федерации, Федеральное государственное автономное образовательное учреждение высшего образования "Южный федеральный университет". Таганрог, 2016.-130 с.

4. Котельников Е. Введение во внутреннее устройство Windows, 2-е изд., исправ. Москва: Национальный Открытый Университет «ИНТУИТ», 2016.- 261 стр.. – (http://biblioclub.ru/index.php?page=book\_red&id=429084&sr=1).

Перечень материально-технического обеспечения:

учебная лаборатория в области безопасности ОС, оснащенная интерактивной доской и компьютерами для преподавателя и учащихся с виртуальными машинами.

**Б.1.С.5.6 Дисциплина «Безопасность сетей ЭВМ»**

Коды формируемых компетенций: ОПК-8.

В результате изучения дисциплины студент должен

знать:

- основные типы и способы применения межсетевых экранов, обобщённую концепцию выбора межсетевых экранов;

- основные программные средства антивирусной защиты;

- принципы разработки политики безопасности.

уметь:

- проводить проверку прохождения пакетов через настроенный межсетевой экран;

- проводить проверку способности персонального межсетевого экрана оказывать противодействие атакам злоумышленника;

- использовать инструментальные средства выявления уязвимостей - системы анализа защищённости;

- минимизировать риски использования сетевого оборудования непредназначенного для защиты сети (коммутаторы и маршрутизаторы).

владеть:

- навыками установки и настройки программно-аппаратных средств защиты информации согласно требованиям безопасности;

- навыками проведения тестирования программно-аппаратных средств защиты информации, разработки набора тестов и методики проведения тестирования и проверки работоспособности системы защиты;

- навыками настройки сетевого оборудования в соответствии с разработанной политикой безопасности.

Примерное распределение часов: трудоемкость дисциплины 10 з.е., 360 час.

Форма контроля: зачет с оценкой, экзамен.

Содержание дисциплины:

Модуль 1. Противодействие угрозам, уязвимостям атакам в компьютерной сети

Основные понятия информационной безопасности. Необходимость обеспечения сетевой безопасности. Взаимосвязь основных понятий безопасности информационных систем. Потеря данных. Триада безопасной ИТ-инфраструктуры – Конфиденциальность, Целостность, Доступность. Обзор сетевых топологий. Сети центров обработки данных. Облачные и виртуальные сети. Вектор атаки злоумышленника. Потенциал нарушителя по ФСТЭК. Типы нарушителей ФСТЭК. Классификация злоумышленников компании CISCO. Проблемы защиты информации в компьютерных сетях. Угрозы сетевой безопасности (связанные с пассивными действиями) ФСТЭК. Угрозы облачной инфраструктуры. Угрозы виртуальной инфраструктуры. Классификация сетевых атак. Разработка системы защиты. Политика информационной безопасности. Структура ПБ. Необходимость создания ПБ. Российская специфика разработки политик безопасности. Основные цели и задачи ПБ. Модель построения корпоративной системы защиты информации. Лучшие практики создания политик безопасности. Структура руководящих документов безопасности. Подход IBM к разработке документов безопасности. Пример стандарта безопасности для ОС семейства UNIX. Сетевой доступ удалённый доступ. Целостность системы. «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014). Классы защищенности. Выбор мер защиты информации. Подход компании Cisco Systems. Политика сетевого подключения. Политика межсетевого экрана. Угрозы кибербезопасности, уязвимости и атаки. Типовые угрозы для конечных пользователей. Типы персональных данных. Угрозы Интернет-сервисам. Внутренние и внешние угрозы. Типы вредоносного ПО. Защита от вредоносных программ Уязвимости мобильных устройств. Вирусы, интернет-черви и «троянские кони». Принципы работы сканера безопасности. Средства сканирования сети на наличие уязвимостей. Сканер уязвимостей Zenmap. Сканер уязвимостей Nessus. Определение уязвимостей узла сети. Системы классификации уязвимостей. Классификация уязвимостей программных систем. Классификация уязвимостей. Классификация троянских вирусов. Атаки в компьютерных сетях. Классификация сетевых атак. Классификация сетевых атак компании CISCO. Жизненный цикл типовой атаки. Определение цели сканирования. Определение топологии сети. Анализ АС. Анализ возможных атак на АС. Основные стадии многоэтапной атаки. Эволюция инструментов безопасности. Разведывательные атаки. Угроза получения предварительной информации об объекте защиты. Угроза обнаружения хостов. Угроза получения предварительной информации об объекте защиты. Краткая информация об инструментах проведения атак. Проблемы безопасности сети. Анализ сетевого трафика. Сетевая карта интерфейса (Network Interface Card (NIC). Обработка сетевого пакета внутри ядра ОС. Кадр. Создание сети. Перехват пакетов. Как включить «неразборчивый режим». Аirmon-ng. BPF: пакетный фильтр BSD . Перехват пакетов – Sniffing. Принципы работы пакетных снифферов. Ограничения использования снифферов. Инструменты анализа сетевого трафика. Анализатор пакетов Wireshark. Пример пакета. Wireshark. Архитектура инструмента Wireshark. Сканирование сети. Сканирование. Методы предварительного сканирования. Сканирование TCP портов. Методы сканирования: сетевое сканирование — определение находящихся в сети узлов. ЭХО-запрос и ЭХО-ответ. Cканирование портов — выявление открытых портов и функционирующих сервисов. История создания. Сетевые порты. Определение состояния порта. Определение цели сканирования. Реализация ICMP – сканирования. Стадия рекогносцировки. Используем программу снифер для анализа трафика. Различные типы UDP сканирования. Проведение сканирования. TCP NULL, FIN и Xmas сканирования. Сканирование TCP-портов флагом FIN. -sO (Сканирование IP протокола). Результаты сканирования. Определение типа ОС. Сканирование узлов сети на наличие уязвимостей. Сетевые атаки – стадия вторжения и атакующее воздействие. Типы уязвимостей. Политики безопасности. Сценарии атаки на систему безопасности. Атаки на переполнение буфера. Технологическая уязвимость типа «переполнение буфера». Активные атаки. Подбор пароля. Атаки типа «отказ в обслуживании». Атака фрагментированными пакетами со смещением (Teardrop Attack). Атака Land. Ping смерти (Ping Of Death). Атака широковещательными ICMP ECHO пакетами (Smurf Attack). Атаки на протоколы стека ТСР/IP. SYN-flood. SYN-flood стенд. Инструментарий. Реализация атаки. Трафик перехваченный на узле-жертве. Воздействие на систему. Противодействие атаке. TCP Reset Attack. Атака, направленная на разрыв соединения. порядковые номера и подтверждения tcp. Управление потоком TCP. Размер окна и подтверждения. TCP Reset Attack на Telnet соединение. Проведение атаки – установление соединения telnet. Проведение атаки – формирования пакета RST. Посылаемый пакет. Результат атаки. Перехват TCP-сессии. Запуск атаки TCP Session Hijacking. Подготовка к атаке. Выполнение атаки. Результаты атаки. Анализ процесса. Атаки на подмену сообщений. Атаки доступа. Атака Человек посередине. Реализация атаки «Man in the Middle». DNS Domain Name System «система доменных имён» Структура DNS Служба DNS: домены и зоны Формирование DNS запросов Угрозы DNS-атак. Типы. Подмена DNS-ответа; внедрение ложного DNS-сервера Схема реализации атаки в случае, если доступа к трафику жертвы нет: Атака на кеш DNS-сервера / подмена вышестоящего DNS-сервера (атака Каминского). Формат DNS ответа Реализация атаки local DNS poisoning.

**Модуль 2.** **Разработка и настройка систем защиты информации в компьютерных сетях**

Безопасность сетевых устройств. Безопасность коммутаторов и маршрутизаторов. Безопасный локальный и удаленный доступ. Предварительная настройка. Повышение безопасности доступа. Алгоритмы защиты пароля. Обеспечение доступа к линии. Расширенная Настройка функций входа в систему. Расширенная Настройка функций входа в систему. Баннерные сообщения. Активация подключения по SSH. Изменение конфигурации SSH. Подключение по SSH. Ограничение доступности команд. Ограничения уровней привилегий. Функция отказоустойчивости Cisco. Маршрутизаторы в качестве целей. Безопасность обновлений маршрутов. Аутентификация MD5. Настройка аутентификации OSPF MD5. Атака с двойным тегированием. Сеть PVLAN периметра. Защита неиспользуемых портов. DHCP Spoofing Attack. Отслеживание DHCP-сообщений. ARP Spoofing and ARP Poisoning Attack. Угрозы безопасности коммутатора. Безопасность граничного маршрутизатора. Мониторинг устройств и управление ими . Использование системного журнала (Syslog) для защиты сети .Основные сведения о системном журнале. Серверы Syslog. Клиенты Syslog. Syslog-сообщение. Основные сведения о протоколе SNMP. База информации управления (Management Information Base, MIB) Уязвимости SNMPНастройка защиты SNMPv3 .Пример настройки защиты SNMPv3. Протокол сетевого времени. Сервер NTP. Аутентификация NTP. Протоколы обнаружения: CDP и LLDP. Настройки для протоколов и сервисов. Уязвимости плоскостей управления и менеджмента. Разграничение доступа на маршрутизаторе. Представления команд на основе ролей. Конфигурирование представлений команд на основе ролей. Конфигурирование суперпредставлений команд CLI на основе ролей. Проверка представлений команд CLI на основе ролей. Ограничения уровней привилегий. Конфигурирование и присвоение уровней привилегий. Модель ААА. Введение. Система управления доступом к сети . Аутентификация без ААА. Компоненты ААА. AAA для аутентификации в системе Cisco Secure Access Control System (ACS). Методы аутентификации. Локальная модель ААА. Локальная аутентификация AAA. Настройка локальной аутентификации AAA с помощью CLI 3.2.1.1 Аутентификация административного доступа. Стандартный и именованный методы. Точная настройка конфигурации аутентификации. Варианты отладки. Отладка аутентификации AAA. Серверная аутентификация ААА. Серверное решение ААА. Характеристики серверного решения AAA . Сравнение локальной и серверной аутентификации ААА. Знакомство с системой управления защищенным доступом Cisco (Access Control System, ACS). Режимы аутентификации. Авторизация. Учет. Знакомство с протоколами TACACS+ и RADIUS. Аутентификация TACACS+. Аутентификация RADIUS. Интеграция TACACS+ и ACS. Интеграция ААА с Active Directory. Интеграция AAA и Identity Service Engine. Процедура настройки серверной аутентификации ААА. Настройка серверов TACACS+. Настройка серверов RADIUS. Конфигурирование аутентификации с использованием сервера ААА. Знакомство с серверной авторизацией ААА. Обеспечение безопасности с использованием аутентификации 802.1X на основе портов. Защита от атак на протокол STP. Обеспечение безопасности локальной сети (LAN). Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне. Протокол связующего дерева. Введение в протокол связующего дерева . Различные реализации протокола STP. Роли портов STP. Корневой мост STP. Стоимость пути STP. Формат кадра BPDU 802.1D. Распространение и обработка BPDU-сообщений. Расширенный ИД системы. Выбор корневого моста. Защита от атак на DHCP. Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне . Нейтрализация атак DHCP. Спуфинг DHCP. Истощение DHCP. Нейтрализация атак DHCP. Конфигурирование DHCP Snooping. Пример конфигурирования DHCP Snooping. Нейтрализация атак ARP 6.2.6.1 Спуфинг ARP и ARP Poisoning. Нейтрализация атак ARP. Конфигурирование динамического инспектирования ARP. Пример конфигурирования динамического инспектирования ARP. Обеспечение безопасности VLAN. Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне. Нейтрализация атак на сеть VLAN. Атаки перехода (Hopping) VLAN. Спуфинг сообщений DTP. Ввод подставного коммутатора. Атака с двойным тегированием (Double-Tagging) VLAN. Нейтрализация атак перехода VLAN. Функция границы частной сети VLAN (PVLAN Edge). Граница PVLAN. Частные сети VLAN. Преимущества частных сетей VLAN. Примеры реализации частных сетей VLAN. Типы портов частной сети VLAN. Конфигурирование частных сетей VLAN на многоуровневом коммутаторе 3560. Использование команды switchport protected в коммутаторе 2960. Обеспечение безопасности порта. Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне. Атаки на таблицу CAM. Базовый режим работы коммутатора Компрометация межсетевых экранов/ Пример работы таблицы CAM Инструменты атаки на таблицу САМ 3 Нейтрализация атак на таблицы CAM 6.2.3.1 Противодействие атакам на таблицы CAM Включение опций защиты портов Нарушения защиты портов Устаревание данных защиты порта Работа защиты портов совместно с IP-телефонам SNMP-уведомление об изменениях MAC-адресов. Защита межфилиальной связи, VPN. Современные угрозы сетевой безопасности. Сети VPN. Компоненты сети IPsec VPN и их функционирование. Реализация сетей IPsec VPN между двумя пунктами с помощью CLI. Обзор сети VPN. Топологии сетей VPN. Знакомство с сетями VPN. Сети IPsec VPN 3-го уровня. Внедрение виртуальных частных сетей (VPN). Сети VPN. Обзор сети VPN. Знакомство с сетями VPN. Технологии IPsec. Конфиденциальность. Целостность. Аутентификация. Безопасный обмен ключами. Authentication Header (AH). ESP. ESP выполняет шифрование и аутентификацию. Транспортный и туннельный режимы. Протокол Internet Key Exchange (IKE). Согласование ключей на фазе 1 и 2. Фаза 2. Согласование ассоциаций SA. Настройка сети IPsec VPN между двумя пунктами. Установление IPsec-соединения. Топология сети IPsec VPN между двумя пунктами. Задачи по настройке сети IPsec VPN. Существующие конфигурации списка ACL. Преобразование адресов, NAT. Технология NAT. NAT позволяет скрыть адреса внутренней сети. Зачем нужен NAT. Базовый NAT. NAPT. Двойной NAT. Ограничения NAT.

**Модуль 3. Разработка системы защиты с помощью межсетевого экрана**

Межсетевые экраны, классификация, основы работы. Определение межсетевого экрана. Принципы создания системы защиты. Особенности применения МЭ. Принципы создания системы защиты с помощью МЭ. Стек протоколов. Типы межсетевых экранов. Фильтрование пакетов. Достоинства и недостатки пакетных фильтров. Межсетевой экран Cisco ASA. ASA Firewall Models. Advanced ASA Firewall Feature. Review of Firewalls in Network Design. ASA Firewall Modes of Operation. ASA Licensing Requirements. Overview of ASA 5505. Уровни безопасности ASA. ASA 5505 Deployment Scenarios. Basic ASA Settings. ASA Default Configuration. Configuring Basic Settings. Configuring Dynamic PAT. Configuring Static NAT. Introduction to Objects and Object Groups. Configuring Network Objects. Configuring Service Objects. Object Groups. ASA ACLs. Configuring ACLs. Applying ACLs. ACLs and Object Groups. Межсетевой экран Dlink. Особенности применения межсетевых экранов и маршрутизаторов D-Link. Интернет-маршрутизаторы серии Unified Services. Маршрутизаторы ADSL. Обзор межсетевых экранов NetDefend D-Link. Межсетевой экран DFL-860E. Архитектура NetDefendOS. Прохождение пакета через межсетевой экран D-Link. Управление межсетевыми экранами D-Link NetDefend. Персональные межсетевые экраны. Исследование архитектуры и функционирования МЭ на примере предложенного ПО/ Исследование механизмов взаимодействия средств сетевой безопасности с операционной системой. Подходы к организации фильтрования трафика в ОС Windows. Outpost Personal Firewall PRO. Norton Personal Firewall. Тестирование персональных межсетевых экранов. Принципы создания системы защиты с помощью межсетевого экрана. Основной режим работы пакетного фильтра. Проверка на сетевом уровне. Проверка на транспортном уровне. Таблица необходимых правил фильтра. Пример использования пакетного фильтра. Stateful Firewalls – МЭ Состояний. Состояния ТСР-соединения. Разработка конфигурации межсетевого экрана. Что такое ACL-список. Принцип работы ACL-списков. Типы ACL-списков Cisco для IPv4. Присваивание номеров и имён ACL-спискам. Где следует размещать ACL-списки. Размещение стандартного ACL-списка. Задание порядка записей ACL-списка. Настройка межсетевого экрана Iptables. Работа классического брандмауэра. Сетевое сканирование защищенного сервера. Демилитаризованная зона (DMZ). Межсетевые экраны прикладного уровня. Прокси-шлюзы прикладного уровня. Компрометация межсетевых экранов. Основные способы развертывания межсетевых экранов в корпоративных сетях. Межсетевой экран, представленный как фильтрующий маршрутизатор. Межсетевой экран на основе двухпортового шлюза. Межсетевой экран на основе экранированного шлюза. Межсетевой экран с экранированной подсетью. Недостатки применения межсетевых экранов. Организация комплексной защиты корпоративной сети. Защита корпоративной сети от несанкционированного доступа из Интернет. Организация внутренней политики безопасности корпоративной сети. Реализации межсетевых экранов. Способы обхода межсетевых экранов.

**Модуль 4. Технологии обеспечения сетевой безопасности**

Куб кибербезопасности. Принципы информационной безопасности. Состояния данных. Меры кибербезопасности. Принцип конфиденциальности. Защита конфиденциальных данных. Контроль доступа. Законы и ответственность. Принцип целостности данных. Требования к целостности данных. Проверки целостности. Принцип доступности. Обеспечение доступности. Варианты хранения данных. Задачи защиты хранящихся данных. Методы передачи данных. Задачи защиты передаваемых данных. Виды обработки данных. Задачи защиты обрабатываемых данных. Защита уровней обеспечения кибербезопасности. Безопасность операционной системы. Защита от вредоносных программ. Управление исправлениями. Межсетевые экраны (брандмауэры) и системы обнаружения вторжений на основе хоста. Защита коммуникаций. WPA/WPA2. Взаимная аутентификация. Разграничение доступа к файлам. Шифрование файлов. Резервное копирование данных и систем. Фильтрация и блокирование содержимого. Клонирование жесткого диска и утилита Deep Freeze. Защитные кабели и замки. Блокировка компьютера после бездействия. Управление удаленным доступом. Защита портов и сервисов. Привилегированные учетные записи. Групповые политики. Включение журналов и оповещений. Контроль аппаратных средств. Разграничение физического доступа. Технологии реагирования на инциденты. Подготовка. Обнаружение и анализ. Изоляция, ликвидация и восстановление. Подведение итогов по инцидентам информационной безопасности. Сетевой модуль Cisco NAC. Системы обнаружения вторжений. Система предотвращения вторжений. NetFlow и IPFIX. Продвинутые средства анализа угроз. Виды аварий. Аварийное восстановление. План аварийного восстановления. Внедрение мер аварийного восстановления. Необходимость в непрерывности бизнес-процессов. Аспекты непрерывности бизнес-процессов. Лучшие практики обеспечения непрерывности бизнес-процессов. Разработка и реализация политики безопасности. Уровни обеспечения кибербезопасности. Контрольные цели. Средства управления. Политики. Стандарты. Рекомендации. Процедуры. Обзор модели. Уровни обеспечения кибербезопасности. Контрольные цели. Средства управления. Использование модели кибербезопасности ISO и состояния данных. Модель кибербезопасности ISO и меры защиты. Методы обнаружения атак. Основные понятия и определения. Определение среды функционирования СОА. Основные значимые компоненты СОА. Типовая архитектура СОА. Анализ существующих подходов к построению СОА. Методы обнаружения атак. Методы обнаружения злоупотреблений. Методы обнаружения аномалий. Результаты сравнительного анализа. «Простые» сигнатуры. Идентификация компонентов «сложной» сигнатуры. Создание оптимальной «сложной» сигнатуры. Рекомендации по использованию элементов заголовка для создания сигнатур. Сигнатуры систем анализа протокола. Выполнение анализа протокола на FTP трафике. Структура сигнатуры. Структура сигнатуры сетевого события. Перечень событий, обнаруживаемых СОА. Обнаружение аномалий в трафике сети. Обнаружение опасных данных в сетевом пакете. Обнаружение аномалий в заголовках сетевого пакета (протокола). Описание некоторых систем обнаружения атак. 1.Вrо. 2.OSSEC. 3 STAT. 4. Prelude. 5. Snort. 6. RealSecure компании ISS. Классические системы обнаружения атак. Между маршрутизатором и межсетевым экраном. В демилитаризованной зоне. За межсетевым экраном. В ключевых сегментах внутренней сети. У сервера удаленного доступа. Технология антивирусной защиты информации. История компьютерных вирусов. Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы Файлово-загрузочные вирусы. Стелс-вирусы. Шифрующиеся вирусы. Полиморфные шифрующиеся вирусы. Макрокомандные шифрующиеся вирусы. Почтовые вирусы. Вирусы в пакетных файлах ОС. Вирусы в драйверах ОС. Бестелесные вирусы. Вирусы для пиринговых сетей. Комбинированные вирусы. Коллекционные вирусы. Черви. Логические бомбы. Троянские объекты. Троянские программы. Троянские Web-сайты. Троянские сообщения E-Mail. Программы Backdoor. Основные методы защиты от компьютерного вируса. Разработчики продуктов для борьбы с компьютерными вирусами. Мониторинг сети. Введение в Syslog. Принцип работы Syslog. Формат сообщений syslog. Служба меток времени. Сервер Syslog. Ведение журналов по умолчанию. Команды маршрутизатора и коммутатора для клиентов syslog. Проверка syslog. Знакомство с SNMP. Принцип работы SNMP. Ловушки агента SNMP. Идентификатор объекта информационной базы управления (MIB). Этапы настройки SNMP. Проверка настройки SNMP. Практические рекомендации по обеспечению безопасности. Краткое описание протокола NetFlow. Общие сведения о NetFlow. Потоки в сети. Настройка NetFlow. Анализ NetFlow с помощью сборщика данных NetFlow. Отладка сети. Документирование сети. Диаграммы топологии сети. Формирование базовых показателей сети. Измерение данных. Общие процедуры поиска и устранения неполадок. Сбор данных о симптомах. Опрос конечных пользователей. Использование многоуровневых моделей для поиска устранения неполадок. Методы поиска и устранения неполадок. Указания по выбору метода поиска и устранения неполадок. Программные средства поиска и устранения неполадок. Средства поиска и устранения неполадок аппаратного обеспечения. Применение сервера Syslog для устранения неполадок. Поиск и устранение неполадок на физическом уровне. Поиск и устранение неполадок канального уровня. Поиск и устранение неполадок сетевого уровня. Поиск и устранение неполадок на транспортном уровне — ACL-списки. Поиск и устранение неисправностей на уровне приложений. Инструментарий для анализа защищённости. Сканеры уязвимостей. Тестирование на возможность проникновения. Анализаторы пакетов. Инструментальные средства безопасности. Определение ролей специалистов по кибербезопасности. Общие угрозы и уязвимости, связанные с пользователями. Управление угрозами, связанными с пользователями. Распространенные угрозы для устройств. Управление угрозами, связанными с устройствами. Распространенные угрозы для локальной сети. Распространенные угрозы для частного облака. Управление угрозами для частного облака. Распространенные угрозы для общедоступного облака. Управление угрозами для общедоступного облака. Распространенные угрозы для физических средств. Управление угрозами для физических средств. Распространенные угрозы для приложений. Способы устранения уязвимостей. Управление угрозами для приложений. Этические ценности специалиста по обеспечению кибербезопасности. Институт компьютерной этики. Гражданское и уголовное законодательство и нормативные требования информационного и телекоммуникационного права. Законы об уведомлении в случае нарушения безопасности.

Рекомендуемый перечень лабораторных работ:

1. Изучение сетевых атак, а также инструментов для аудита безопасности и проведения атак.

2. Мониторинг состояния элементов сети с использованием анализаторов сетевого трафика Wireshark.

3. Обнаружение уязвимостей сетевого узла с помощью сканеров безопасности.

4. Атаки на TCP/IP.

5. Защита маршрутизатора для административного доступа.

6. Защита административного доступа с помощью AAA и RADIUS.

7. Защита коммутаторов 2-го уровня.

8. Настройка сети Site-to-Site VPN с помощью Cisco IOS.

9. Настройка преобразования адреса и номера порта (PAT).

10. Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI).

11. Конфигурация межсетевого экрана Dlink Базовая настройка и настройка межсетевого экрана.

12. Настройка программного межсетевого экрана ОС LINUX.

13. Тестирование персонального экрана.

14. Исследование механизмов осуществления и обнаружения сетевых атак.

15. Обнаружение уязвимостей сетевого узла с помощью сканеров портов.

Рекомендуемый перечень основной литературы:

1. Мэйволд Э. Безопасность сетей / Э. Мэйволд - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с. http://biblioclub.ru/index.php?page=book&id=429035.

2. Пелешенко В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие / В.С. Пелешенко; С.В. Говорова; М.А. Лапина - Ставрополь: СКФУ, 2017. - 86 с. http://biblioclub.ru/index.php?page=book&id=467139.

3. Лапонина О. Р. Межсетевые экраны / О.Р. Лапонина - 2-е изд., исправ. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 466 с. http://biblioclub.ru/index.php?page=book&id=429093.

4. Кияев В. Безопасность информационных систем / В. Кияев; О. Граничин - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. http://biblioclub.ru/index.php?page=book&id=429032.

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации, средствами контроля защищенности информации, системами обнаружения и предотвращения атак и доступом к Сетевой академии CISCO: Networking Academy https://www.netacad.com.

**Б.1.С.5.7. Дисциплина «Интеллектуальные технологии в задачах информационной безопасности»**

Коды формируемых компетенций: ОПК-9, ОПК-10, ОПК-11, ПК-Р5.3.

В результате изучения дисциплины студент должен

знать:

- основные требования информационной безопасности при решении стандартных задачи профессиональной деятельности.

уметь:

- применять основные требования информационной безопасности при решении стандартных задачи профессиональной деятельности.

владеть:

- навыками применения основных требований информационной безопасности при решении стандартных задачи профессиональной деятельности.

Примерное распределение часов: трудоемкость дисциплины 5 з.е., 180 час.

Форма контроля: экзамен.

Содержание дисциплины:

**Модуль 1. Интеллектуальные технологии**

**Введение. Исторические аспекты появления и развития интеллектуальных систем.** Гносеологическая проблемы познания мозга. Тест Тьюринга и интуитивный подход. Гипотеза Ньюэлла-Саймона. Работы У. Мак-Каллока, У. Питса, Ф. Розенблатта, Д. Хебба, М. Минского, С. Пайперта, Д. Хопфилда, Д. Холланда, А. Ньюэлла, Г. Саймона, М.Г. Гаазе-Рапопорта, Д.А.Поспелова, П. Розенблума, К. Гёделя, Р. Пенроуза и др. **Структура и процедура систем продукций.** Структура систем продукций. Процедура систем продукций. **Стратегии управления систем продукций.** Стратегии управления систем продукцийс возвращением. Алгоритм рекурсивной процедуры BACKTRACK. Процедура BACKTRACK с оптимизацией выбора. **Стратегии поиска на графе.** Язык графов в системах продукций. Неинформированные процедуры поиска на графе. Эвристические процедуры поиска на графе. Применение оценочных функций. **Специализированные системы продукций.** Коммутативные системы продукций. Разложимые системы продукций. Язык И/ИЛИ графов. Обратные и двусторонние системы продукций. **Оценка эффективности систем продукций. Поиск на игровых деревьях.** Минимаксная процедура. Альфа-бета процедура. Эффективность поиска с помощью альфа-бета процедуры. **Введение. Естественная иммунная система.** Сопоставление нервной и иммунной систем. **Моделирование иммунной системы.** Общие принципы моделирования иммунной системы. Модель иммунной сети. Модель отрицательного отбора. Формальное описание модели отрицательного отбора. Реализация модели отрицательного отбора. Модель клональной селекции. Формальное описание модели клональной селекции. Модель гиперклетки. **Виды детекторов.** Строковые детекторы. Числовые детекторы. V-детекторы. Алгоритм формирования V-детекторов. **Применение ИИС в компьютерной безопасности.** Мониторинг информационных процессов в КС средствами ИИС. Обнаружение аномалий процессов в КС средствами ИИС. Обнаружение атак на КС средствами ИИС. Динамические биометрические системы идентификации личности реализуемые средствами ИИС.

**Модуль 2. Безопасность систем баз данных**

**Основные понятия и определения**. Угрозы безопасности в КС. Методы оценивания угроз. Разработка СБД. **Методы и средства персонализации и аутентификации в СБД.** Парольная аутентификация. Одноразовые пароли. Функциональные методы аутентификации. Аутентификация при удаленном доступе в сетях. Протокол аутентификации РАР. Протокол аутентификации CHAP. Протокол аутентификации S/Key. Протокол аутентификации Kerberos. Персональные средства аутентификации. Биометрические средства аутентификации. Аутентификация по информации, ассоциированной с субъектом. Аутентификация объектов. Аутентификация процессов. Особенности процедур идентификации, аутентификации в СБД. **Методы и средства авторизации в СБД.** Субъектно-объектная модель доступа. Монитор безопасности. Политики и модели безопасности. Дискреционные модели. Мандатные модели. Ролевые модели. **Управление доступом в СБД.** Основные понятия. Основные категории пользователей СБД. Виды привилегий в СУБД. Группы. Роли. Представления. Особенности привилегий доступа к реляционным таблицам БД. Использование представлений для фильтрации привилегий. Агрегатные функции. Особенности привилегий доступа к процедурам. Права доступа к БД. Иерархия прав доступа. Получение информации о привилегиях. Соотношение прав доступа СУБД и ОС. Мандатная защита в СУБД. **Обеспечение конфиденциальности данных в СБД.** Основные понятия. Скрытые каналы на основе анализа параметров протекания процессов. Решение проблем скрытых каналов. Нейтрализация скрытых каналов утечки информации на основе технологий представлений. Нейтрализация скрытых каналов утечки информации на основе техники разрешенных процедур. Скрытые каналы утечки информации, специфичные для реляционных СУБД. Особенности хранения и обработки данных в БД. **Обеспечение целостности данных.** Основные понятия. Модели обеспечения целостности. Обеспечение целостности данных в реляционных СБД. Доменная целостность. Сущностная целостность. Ссылочная целостность. Декларативные способы обеспечения целостности. Процедурные способы обеспечения целостности. Применение декларативных и процедурных средств поддержания целостности. **Обеспечение высокой доступности СБД.** Сохранность данных в СБД. Организация дисковых массивов (RAID). Отказоустойчивые кластеры и системы. Кластеры высокой доступности (готовности). Технологии постоянного дублирования. Зеркальное отображение баз данных. Тиражирование данных. Технологии архивирования. Резервное копирование БД. Восстановление баз данных. Репликация баз данных.

Рекомендуемый перечень лабораторных работ:

1. Разработка персональной СБД.

2. Разработка защиты персональной СБД.

3. Обеспечение защиты данных с помощью представлений.

4. Обеспечение целостности данных в полях реляционных таблиц.

5. Обеспечение ссылочной целостности данных.

Рекомендуемый перечень основной литературы:

1. Герасименко Е.М. Методы машинного обучения в научных исследованиях. – Ростов-на-Дону-Таганрог: Издательство Южного федерального университета, 2020.

2. Данилова Н.В., Белявский Г.И. Анализ данных. Машинное обучение. – Ростов-на-Дону-Таганрог: Издательство Южного федерального университета, 2020.

3. Искусственный интеллект. Современный подход / С. Расел, П. Норвиг: Пер. с англ. – М.: Издательский дом «Вильямс», 2007. – 1407 с.

4. Искусственные иммунные системы и их применение [Текст], под ред. Д. Дасгупты; пер. с англ. А. А. Романюхи. – Москва: Физматлит, 2006. – 344 с.

Перечень материально-технического обеспечения:

учебная лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

**Примерные программы практик**

**Б.2.О.1. Производственная (преддипломная) практика**

Цель: преддипломная практика обеспечивает подготовку выпускной квалификационной работы, а также имеет целью закрепление профессиональных знаний и практических навыков ведения самостоятельной научно-исследовательской, производственно-технологической и организационно-управленческой работы, полученных студентами в процессе обучения.

Задачи:

- осуществление сбора, обработки, анализа и систематизации научно-технической информации по теме выпускной квалификационной работы;

- выбор методик и средств решения поставленной задачи, разработка плана и графика подготовки выпускной квалификационной работы;

- проектирование защищенных информационных систем, разработка и исследование технологий защиты информации, проведение экспериментальных исследований в соответствии с планом подготовки выпускной квалификационной работы;

- оформление пояснительной записки к выпускной квалификационной работе, подготовка доклада и презентации.

Формируемые компетенции: УК-3, УК-6, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-6, ОПК-7, ОПК-8, ОПК-9, ОПК-10, ОПК-11, ПК-Р4.1, ПК-Р4.2, ПК-Р4.3.

**Б.2.О.2. Производственная практика (тип – научно-исследовательская работа)**

Цель: систематизация, закрепление и расширение теоретических знаний и практических навыков по образовательной программе, применение этих знаний при самостоятельном решении конкретных задач по соответствующим видам профессиональной деятельности, получение практических навыков ведения самостоятельной научно-исследовательской работы, подготовка информационной и опытной базы для написания выпускной квалификационной работы.

Задачи:

- осуществление сбора, обработки, анализа и систематизации научно-технической информации по теме исследования;

- выбор методик и средств решения поставленной задачи, разработка плана и программы проведения научных исследований и технических разработок;

- проведение экспериментальных исследований в процессе проектирования защищенных информационных систем и технологий защиты информации с применением современных математических методов, технических и программных средств;

- оформление научно-технические отчетов, обзоров, подготовка публикаций по результатам выполненных исследований, научных докладов.

Формируемые компетенции: УК-4, ОПК-3, ОПК-7, ОПК-9, ОПК-10, ОПК-11.

**Б.2.О.3. Учебная практика (тип – ознакомительная)**

Цель: получение первичных профессиональных умений и навыков по образовательной программе, углубление и расширение знаний, полученных студентами при теоретическом обучении, подготовка их к изучению последующих дисциплин и прохождению производственной практики.

Задачи:

- закрепление и углубление результатов теоретической подготовки и приобретение первичных навыков и компетенций в сфере профессиональной деятельности;

- формирование умений самостоятельно работать с научной и технической литературой;

- углубление навыков самостоятельного решения практических задач;

- формирование навыков работы в научном коллективе.

Формируемые компетенции: УК-2, ОПК-4, ОПК-7, ОПК-9, ОПК-10, ОПК-11.

**5.7. Рекомендации по разработке фондов оценочных средств для промежуточной аттестации**

Для каждой учебной дисциплины (модуля) Организация разрабатывает фонды оценочных средств (далее – ФОС).

ФОС может быть представлен в виде части рабочей программы учебной дисциплины (модуля), практики, в виде отдельного единого документа или комплекта документов.

ФОС должен включать в себя:

1. Перечень компетенций по учебной дисциплине (модулю), практике с указанием (при необходимости) этапов их формирования в процессе освоения образовательной программы.

2. Перечень индикаторов достижения соответствующих компетенций, включающий в себя индикаторы, предусмотренные ПООП, и индикаторы, определенные организацией самостоятельно (при необходимости).

3. Перечень форм и средств текущей и промежуточной аттестаций, используемых для оценивания индикаторов достижения компетенций. К ним могут относиться тесты, экзаменационные вопросы и вопросы для зачета, задачи, задания, кейсы, отчеты о лабораторных работах и прочие средства.

4. Описание шкал и процедур оценивания индикаторов достижения и соответствующих им компетенций.

Конкретная структура, состав и содержание ФОС разрабатываются и устанавливаются Организацией самостоятельно.

**5.8. Рекомендации по разработке программы государственной итоговой аттестации**

Программа ГИА включает в себя критерии оценивания ВКР и программу государственного экзамена (если Организация включила государственный экзамен в состав ГИА).

Программа ГИА может быть представлена в виде в виде единого документа или комплекта документов.

Конкретная структура, состав и содержание программы ГИА разрабатываются и устанавливаются Организацией самостоятельно.

Программа ГИА должна включать в себя:

1. Перечень компетенций, выносимых на ГИА.

2. Перечень индикаторов достижения компетенций, выносимых на ГИА, включающий в себя индикаторы, предусмотренные ПООП, и индикаторы, определенные организацией самостоятельно (при необходимости).

3. Описание шкал и процедур оценивания индикаторов достижения и соответствующих им компетенций.

Программа государственного экзамена должна включать в себя вопросы и (или) задания, необходимые для оценивания индикаторов достижения компетенций, выносимых на государственный экзамен.

Для оценивания ВКР в программу ГИА рекомендуется включать следующие критерии:

1) Профессиональная группа критериев: степень актуальности тематики работы; степень раскрытия темы ВКР; корректность постановки задачи исследования и разработки; оригинальность и новизна полученных результатов, научных, конструкторских и технологических решений.

2) Справочно-информационная группа критериев: степень комплексности работы, использование в ней знаний дисциплин (модулей); использование информационных ресурсов Интернет; использование современных пакетов компьютерных программ и технологий.

3) Оформительская группа критериев: объем и качество выполнения графического материала.

4) Показатели защиты: качество защиты; уровень ответов.

5) Отзывы руководителя и рецензента: оценка руководителя; оценка рецензента.

**Раздел 6. ПРИМЕРНЫЕ УСЛОВИЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПО ОПОП**

Требования к условиям реализации программы специалитета включают в себя общесистемные требования, требования к материально-техническому и учебно-методическому обеспечению, требования к кадровым и финансовым условиям реализации программы специалитета, а также требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по программе специалитета.

## 6.1. Общесистемные требования к реализации программы специалитета

Организация должна располагать на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы специалитета по [Блоку 1](#Par105) "Дисциплины (модули)" и [Блоку 3](#Par111) "Государственная итоговая аттестация" в соответствии с учебным планом.

Каждый обучающийся в течение всего периода обучения должен быть обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде Организации из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), как на территории Организации, так и вне ее. Условия для функционирования электронной информационно-образовательной среды могут быть созданы с использованием ресурсов иных организаций.

Электронная информационно-образовательная среда Организации должна обеспечивать:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации программы специалитета с применением электронного обучения, дистанционных образовательных технологий электронная информационно-образовательная среда Организации должна дополнительно обеспечивать:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы специалитета;

проведение всех видов учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды должно соответствовать законодательству Российской Федерации.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, формирование, использование и эксплуатация электронной информационно-образовательной среды, доступ обучающихся к электронной информационно-образовательной среде, а также к современным профессиональным базам данных и информационным справочным системам, к компьютерной технике, подключенной к локальным сетям и (или) сети "Интернет", организуются федеральным государственным органом, в ведении которого находятся соответствующие Организации.

При реализации программы специалитета в сетевой форме требования к реализации программы специалитета должны обеспечиваться совокупностью ресурсов материально-технического и учебно-методического обеспечения, предоставляемого организациями, участвующими в реализации программы специалитета в сетевой форме.

## 6.2. Требования к материально-техническому и учебно-методическому обеспечению программы специалитета

Помещения должны представлять собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения, а также криминалистической и специальной техникой, табельным оружием, специальными средствами при реализации программ специалитета в рамках специализаций "Технологии защиты информации в правоохранительной сфере", "Информационно-аналитическое обеспечение правоохранительной деятельности", "Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации", состав которых определяется в рабочих программах дисциплин (модулей).

Минимально необходимый для реализации программы специалитета перечень материально-технического обеспечения включает в себя специально оборудованные помещения для проведения учебных занятий, в том числе:

лаборатории и полигоны:

- лаборатория электротехники, электро-, радиоизмерений;

- лаборатория информатики и программирования;

- лаборатория программно-аппаратных средств обеспечения информационной безопасности;

- лаборатория проектирования систем информационной безопасности;

- лаборатория систем и сетей передачи данных;

- лаборатория физики (исследования физических процессов);

- полигон технической защиты информации;

- спортивный зал;

- библиотека;

- специальная библиотека (библиотека литературы ограниченного доступа) - при реализации программы специалитета, содержащей сведения ограниченного доступа;

для специализаций "Технологии защиты информации в правоохранительной сфере", "Информационно-аналитическое обеспечение правоохранительной деятельности", "Оперативно-техническое обеспечение раскрытия и расследования преступлений в сфере компьютерной информации" также:

тир (для стрельбы из табельного оружия);

кабинеты:

- специальной техники и технических систем безопасности;

- огневой подготовки;

- тактико-специальной (военно-профессиональной или специальной профессиональной) подготовки;

- выделенное помещение (класс, аудитория) для проведения учебных занятий, в ходе которых до обучающихся доводятся сведения, составляющие государственную тайну.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Организации.

Допускается частичная замена оборудования его виртуальными аналогами.

Организация должна быть обеспечена необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

При использовании в образовательном процессе печатных изданий библиотечный фонд должен быть укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), программах практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

Обучающимся должен быть обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и подлежит обновлению (при необходимости).

Доступ обучающихся к профессиональным базам данных и информационным справочным системам в федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, организуется федеральным государственным органом, в ведении которого находятся соответствующие организации.

Обучающиеся из числа инвалидов и лиц с ОВЗ должны быть обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

## 6.3. Требования к кадровым условиям реализации программы специалитета

Реализация программы специалитета обеспечивается педагогическими работниками Организации, а также лицами, привлекаемыми Организацией к реализации программы специалитета на иных условиях.

Квалификация педагогических работников Организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах (при наличии).

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, квалификационные характеристики должностей руководителей и педагогических работников высшего образования и дополнительного профессионального образования определяются в соответствии с законодательством Российской Федерации.

Не менее 70 процентов численности педагогических работников Организации, участвующих в реализации программы специалитета, и лиц, привлекаемых Организацией к реализации программы специалитета на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны вести научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля).

Не менее 5 процентов численности педагогических работников Организации, участвующих в реализации программы специалитета, и лиц, привлекаемых Организацией к реализации программы специалитета на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны являться руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (иметь стаж работы в данной профессиональной сфере не менее 3 лет).

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, доля указанных педагогических работников должна составлять не менее 1 процента их общей численности.

Не менее 50 процентов численности педагогических работников Организации, участвующих в реализации основных образовательных программ высшего образования, и лиц, привлекаемых к образовательной деятельности Организации на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), должны иметь ученую степень (в том числе ученую степень, полученную в иностранном государстве и признаваемую в Российской Федерации) и (или) ученое звание (в том числе ученое звание, полученное в иностранном государстве и признаваемое в Российской Федерации).

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, к педагогическим работникам с учеными степенями и (или) учеными званиями приравниваются преподаватели военно-профессиональных и специальных профессиональных дисциплин (модулей) без ученых степеней и (или) ученых званий, имеющие профильное высшее образование, опыт военной службы (службы в правоохранительных органах) в области и с объектами профессиональной деятельности, соответствующими программе специалитета, не менее 10 лет, воинское (специальное) звание не ниже "майор" ("майор полиции", "майор внутренней службы", "майор юстиции", "капитан 3 ранга", а также имеющие боевой опыт, или государственные (ведомственные) награды, или государственные (отраслевые) почетные звания, или государственные премии.

В числе педагогических работников с ученой степенью доктора наук и (или) ученым званием профессора могут учитываться преподаватели военно-профессиональных дисциплин (модулей), специальных профессиональных дисциплин (модулей) с ученой степенью кандидата наук, имеющие или государственные (ведомственные) награды, или государственные (отраслевые) почетные звания, или государственные премии.

## 6.4. Требования к финансовым условиям реализации программы специалитета

Финансовое обеспечение реализации программы специалитета должно осуществляться в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования - программ специалитета и значений корректирующих коэффициентов к базовым нормативам затрат, определяемых Министерством науки и высшего образования Российской Федерации.

В Организации, в которой законодательством Российской Федерации предусмотрена военная или иная приравненная к ней служба, служба в правоохранительных органах, финансовое обеспечение реализации программы специалитета должно осуществляться в пределах бюджетных ассигнований федерального бюджета, выделяемых федеральному органу исполнительной власти, в ведении которого находится указанная Организация.

## 6.5. Требования к применяемым механизмам оценки качества образовательной деятельности и подготовки обучающихся по программе специалитета

Качество образовательной деятельности и подготовки обучающихся по программе специалитета определяется в рамках системы внутренней оценки, а также системы внешней оценки, в которой Организация принимает участие на добровольной основе.

В целях совершенствования программы специалитета Организация при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по программе специалитета привлекает работодателей и (или) их объединения, иных юридических и (или) физических лиц, включая педагогических работников Организации.

В рамках внутренней системы оценки качества образовательной деятельности по программе специалитета обучающимся предоставляется возможность оценивания условий, содержания, организации и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик.

Внешняя оценка качества образовательной деятельности по программе специалитета в рамках процедуры государственной аккредитации осуществляется с целью подтверждения соответствия образовательной деятельности по программе специалитета требованиям ФГОС ВО.

Внешняя оценка качества образовательной деятельности и подготовки обучающихся по программе специалитета может осуществляться в рамках профессионально-общественной аккредитации, проводимой работодателями, их объединениями, а также уполномоченными ими организациями, в том числе иностранными организациями, либо авторизованными национальными профессионально-общественными организациями, входящими в международные структуры, с целью признания качества и уровня подготовки выпускников отвечающими требованиям профессиональных стандартов (при наличии) и (или) требованиям рынка труда к специалистам соответствующего профиля.

В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, внешняя оценка качества программы специалитета может осуществляться в рамках профессионально-общественной аккредитации, проводимой работодателями, их объединениями, а также уполномоченными ими организациями, с целью признания качества и уровня подготовки выпускников отвечающими требованиям профессиональных стандартов (при наличии) и (или) требованиям рынка труда к специалистам соответствующего профиля.

**Раздел 7. СПИСОК РАЗРАБОТЧИКОВ**

|  |  |
| --- | --- |
| Ф.И.О. разработчика | Должность |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Приложение 1

Перечень профессиональных стандартов,   
соответствующих профессиональной деятельности выпускников,  
освоивших образовательную программу по специальности  
10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

|  |  |  |
| --- | --- | --- |
| № п/п | Код профессионального стандарта | Наименование области профессиональной деятельности. Наименование профессионального стандарта |
| 06 Связь, информационные и коммуникационные технологии | | |
| 1. | 06.031 | Профессиональный стандарт «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 9 ноября 2016 г. № 611н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44398) |
| 2. | 06.033 | Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857) |
| 12 Обеспечение безопасности | | |
| 3. | 12.005 | Профессиональный стандарт «Специалист по противодействию иностранным техническим разведкам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 25 декабря 2015 г. № 15с (зарегистрирован Министерством юстиции Российской Федерации 22 января 2016 г., регистрационный № 40706) |
| 40 Сквозные виды профессиональной деятельности в промышленности | | |
| 4. | 40.178 | Профессиональный стандарт «Специалист в области проектирования автоматизированных систем управления технологическими процессами», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 13 марта 2017 г. № 272н (зарегистрирован Министерством юстиции Российской Федерации 4 апреля 2017 г., регистрационный № 46243) |

Приложение 2

Перечень обобщённых трудовых функций и трудовых функций,  
имеющих отношение к профессиональной деятельности выпускника  
образовательной программы по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Код и**  **наименование**  **профессионального стандарта** | **Обобщенные трудовые функции** | | | **Трудовые функции** | | |
| **Код** | **Наименование** | **Уровень**  **квалификации** | **Наименование** | **Код** | **Уровень (подуровень) квалификации** |
| 06.031 Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности | A | Применение ИАС в защищенном исполнении в процессах АИАД | 7 | Автоматизированная информационно-аналитическая поддержка процессов принятия решений | A/01.7 | 7 |
| Решение типовых задач обработки информации в ИАС государственных органов, обеспечивающих национальную безопасность | A/02.7 | 7 |
| Решение типовых задач анализа информации в ИАС государственных органов, обеспечивающих национальную безопасность | A/03.7 | 7 |
| C | Эксплуатация ИАС в защищенном исполнении | 7 | Настройка ИАС для решения задач в сфере профессиональной деятельности | C/01.7 | 7 |
| Обеспечение функционирования ИАС | C/02.7 | 7 |
| Обеспечение функционирования средств защиты информации в ИАС | C/03.7 | 7 |
| D | Организационное управление в ИАС в защищенном исполнении | 7 | Управление работой коллектива информационно-аналитических работников и специалистов по созданию и эксплуатации ИАС | D/01.7 | 7 |
| Разработка нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование ИАС | D/02.7 | 7 |
| Организация работ по выполнению в ИАС требований защиты информации ограниченного доступа | D/03.7 | 7 |
| 06.033 Специалист по защите информации в автоматизированных системах | A | Обслуживание систем защиты информации в автоматизированных системах | 5 | Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем | А/02.5 | 5 |
| C | Внедрение систем защиты информации автоматизированных систем | 6 | Установка и настройка средств защиты информации в автоматизированных системах | С/01.6 | 6 |
| D | Разработка систем защиты информации автоматизированных систем | 7 | Разработка проектных решений по защите информации в автоматизированных системах | D/02.7 | 7 |
| 40.178 Специалист в области проектирования автоматизированных систем управления технологическими процессами | A | Оформление технической документации на различных стадиях разработки проекта автоматизированных систем управления технологическими процессами | 6 | Разработка простых узлов, блоков автоматизированных систем управления технологическими процессами | A/04.6 | 6 |
| B | Разработка отдельных разделов проекта на различных стадиях проектирования автоматизированной системы управления технологическими процессами | 6 | Предпроектное обследование технологического процесса (объекта управления), для которого разрабатывается проект автоматизированной системы управления | В/01.6 | 6 |
| Разработка проектных решений отдельных частей автоматизированной системы управления технологическими процессами | В/02.6 | 6 |
| C | Разработка проекта автоматизированной системы управления технологическими процессами | 7 | Разработка концепции автоматизированной системы управления технологическими процессами | С/01.7 | 7 |

Приложение 3

Примерный учебный план   
образовательной программы по специальности  
10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Индекс | Наименование дисциплин (модулей), практик, аттестационных испытаний | | Формы промежуточной аттестации | | Трудоемкость | | | | | | | Примерное распределение по семестрам | | | | | | | | | | | | | | | | | | | | Коды форми-руемых компетен-ций |
| з.е. | | | часы | | | |
| всего | | контактная работа | | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | | 8 | | 9 | | 10 | |
| 1 | 2 | | 3 | | 4 | | | 5 | | 6 | | 7 | | 8 | | 9 | | 10 | | 11 | | 12 | | 13 | | 14 | | 15 | | 16 | | 17 |
| **Б.1** | **Блок 1. Дисциплины (модули)** | |  | | **Не менее 210** | | | **Не менее 7560** | | **Не менее 3780** | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| **Б.1.О** | **Обязательная часть** | |  | | **Не менее 153** | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| Б.1.О.1 | История (История России, Всеобщая история) | | экзамен | | 4 | | | 144 | |  | | х | |  | |  | |  | |  | |  | |  | |  | |  | |  | | УК-5,  ОПК-1 |
| Б.1.О.2 | Физическая культура | | зачет | | 2 | | | 72 | |  | | х | |  | |  | |  | |  | |  | |  | |  | |  | |  | | УК-7 |
| Б.1.О.3 | Иностранный язык | | 3 зачета, экзамен | | 9 | | | 324 | |  | | х | | х | | х | | х | |  | |  | |  | |  | |  | |  | | УК-4 |
| Б.1.О.4 | Философия | | зачет, экзамен | | 5 | | | 180 | |  | |  | |  | | х | | х | |  | |  | |  | |  | |  | |  | | УК-1,  ОПК-2 |
| Б.1.О.5 | Безопасность жизнедеятельности | | зачет | | 3 | | | 108 | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | | УК-8 |
| Б.1.О.6 | Политология | | экзамен | | 3 | | | 108 | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | |  | | УК-5,  ОПК-1 |
| Б.1.О.7 | Логика | | зачет | | 2 | | | 72 | |  | |  | |  | | х | |  | |  | |  | |  | |  | |  | |  | | УК-1 |
| Б.1.О.8 | Экономика | | зачет | | 2 | | | 72 | |  | |  | |  | | х | |  | |  | |  | |  | |  | |  | |  | | УК-2, УК-9 |
|  | **Группа учебных дисциплин (модулей) "Математические основы обеспечения информационной безопасности"** | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| Б.1.О.9 | Математика | | 2 экзамена | | 7 | | | 252 | |  | | х | | х | |  | |  | |  | |  | |  | |  | |  | |  | | ОПК-3 |
| Б.1.О.10 | Прикладная математика | | 2 экзамена | | 6 | | | 216 | |  | |  | |  | | х | | х | |  | |  | |  | |  | |  | |  | | ОПК-3 |
| Б.1.О.11 | Математические основы обработки информации | | зачет | | 4 | | | 144 | |  | |  | |  | |  | |  | | х | |  | |  | |  | |  | |  | | ОПК-3 |
| Б.1.О.12 | Дискретная математика | | экзамен | | 4 | | | 144 | |  | |  | | х | |  | |  | |  | |  | |  | |  | |  | |  | | ОПК-3 |
|  | **Группа учебных дисциплин (модулей)  "Физико-технические основы обеспечения информационной безопасности"** | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| Б.1.О.13 | Физика | | 2 экзамена | | 7 | | | 252 | |  | |  | | х | | х | |  | |  | |  | |  | |  | |  | |  | | ОПК-3 |
| Б.1.О.14 | Основы электротехники и радиоэлектроники | | экзамен | | 4 | | | 144 | |  | |  | |  | |  | | х | |  | |  | |  | |  | |  | |  | | ОПК-6 |
| Б.1.О.15 | Основы электро-, радиоизмерений | | экзамен | | 3 | | | 108 | |  | |  | |  | |  | |  | | х | |  | |  | |  | |  | |  | | ОПК-6 |
|  | **Группа учебных дисциплин (модулей) "Информационные технологии и программирование"** | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| Б.1.О.16 | Информатика и информационные технологии в правоохранительной деятельности | | зачет, экзамен | | 5 | | | 180 | |  | | х | | х | |  | |  | |  | |  | |  | |  | |  | |  | | ОПК-9, ОПК-10, ОПК-11 |
| Б.1.О.17 | Средства вычислительной техники | | экзамен | | 4 | | | 144 | |  | |  | | х | |  | |  | |  | |  | |  | |  | |  | |  | | ОПК-7 |
| Б.1.О.18 | Программирование: языки, методы и технологии | | зачет, экзамен | | 7 | | | 252 | |  | | х | | х | |  | |  | |  | |  | |  | |  | |  | |  | | ОПК-7 |
|  | **Группа учебных дисциплин (модулей) "Методы и средства обеспечения информационной безопасности"** | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| Б.1.О.19 | Системы и сети передачи информации | | зачет, экзамен | | 9 | | | 324 | |  | |  | |  | |  | |  | | х | | х | |  | |  | |  | |  | | ОПК-8 |
| Б.1.О.20 | Теория информационной безопасности и методология защиты информации | | зачет, экзамен | | 6 | | | 216 | |  | |  | |  | | х | | х | |  | |  | |  | |  | |  | |  | | ОПК-4, ОПК-5 |
| Б.1.О.21 | Информационное право | | зачет | | 2 | | | 72 | |  | |  | |  | | х | |  | |  | |  | |  | |  | |  | |  | | ОПК-4 |
| Б.1.О.22 | Правовая защита информации | | экзамен | | 4 | | | 144 | |  | |  | |  | |  | |  | | х | |  | |  | |  | |  | |  | | ОПК-4 |
| Б.1.О.23 | Организационная защита информации | | зачет, экзамен | | 6 | | | 216 | |  | |  | |  | |  | |  | |  | |  | | х | | х | |  | |  | | ОПК-4, ОПК-5 |
| Б.1.О.24 | Документоведение | | зачет | | 3 | | | 108 | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | |  | | ОПК-9, ОПК-11 |
| Б.1.О.25 | Технологии защищенного документооборота | | экзамен | | 4 | | | 144 | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | | ОПК-5, ОПК-8 |
| Б.1.О.26 | Техническая защита информации | | экзамен | | 7 | | | 252 | |  | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | | ОПК-8 |
| Б.1.О.27 | Программно-аппаратная защита информации | | экзамен | | 4 | | | 144 | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | | ОПК-8 |
| Б.1.О.28 | Криптографическая защита информации | | экзамен | | 3 | | | 108 | |  | |  | |  | |  | |  | | х | |  | |  | |  | |  | |  | | ОПК-8 |
| Б.1.О.29 | Специальные информационные технологии в правоохранительной деятельности | | зачет, экзамен | | 6 | | | 216 | |  | |  | |  | |  | |  | |  | |  | | х | | х | |  | |  | | ОПК-9, ОПК-10, ОПК-11 |
| Б.1.О.30 | Правоохранительные органы | | зачет | | 2 | | | 72 | |  | | х | |  | |  | |  | |  | |  | |  | |  | |  | |  | | УК-10, ОПК-1, ОПК-2 |
|  | Элективные дисциплины по физической культуре и спорту | |  | | 0 | | | 328 | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | | УК-7 |
|  | **Дисциплины (модули) образовательной организации  (при необходимости)** | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
|  | **Элективные дисциплины (модули) образовательной организации (при необходимости)** | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| **Б.1.С** | **Дисциплины (модули) специализации** | |  | | **Не менее 51** | | | **Не менее  1836** | | **Не менее  918** | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| Б.1.С.4 | *Специализация № 4. Компьютерная экспертиза* | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| Б.1.С.4.1 | Компьютерная криминалистика | | зачет, экзамен | | 7 | | | 252 | |  | |  | |  | |  | |  | |  | |  | | х | | х | |  | |  | | ПК-Р4.1, ПК-Р4.3 |
| Б.1.С.4.2 | Расследование компьютерных инцидентов | | экзамен | | 5 | | | 180 | |  | |  | |  | |  | | х | |  | |  | |  | |  | |  | |  | | ПК-Р4.1, ПК-Р4.2 |
| Б.1.С.4.3 | Инструментальное обеспечение компьютерной экспертизы | | зачет с оценкой | | 5 | | | 180 | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | |  | | ПК-Р4.1 |
| Б.1.С.4.4 | Методы хранения, восстановления и анализа данных | | экзамен | | 7 | | | 252 | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | | ПК-Р4.2 |
| Б.1.С.4.5 | Следообразование в компьютерных системах | | экзамен | | 7 | | | 252 | |  | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | | ПК-Р4.2 |
| Б.1.С.4.6 | Правовые и организационные основы компьютерной экспертизы | | зачет с оценкой | | 5 | | | 180 | |  | |  | |  | |  | |  | |  | |  | |  | |  | | х | |  | | ПК-Р4.3 |
| Б.1.С.4.7 | Безопасность сетей ЭВМ | | зачет с оценкой экзамен | | 10 | | | 360 | |  | |  | |  | |  | |  | | х | | х | |  | |  | |  | |  | | ОПК-8 |
| Б.1.С.4.8 | Интеллектуальные технологии в задачах информационной безопасности | | экзамен | | 5 | | | 180 | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | | ОПК-9, ОПК-10, ОПК-11 |
| Б.1.С.5 | *Специализация № 5. Организация и технология информационной безопасности* | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| Б.1.С.5.1 | Аудит информационной безопасности | | экзамен | | 7 | | | 252 | |  | |  | |  | |  | |  | |  | |  | | х | | х | |  | |  | | ПК-Р5.2 |
| Б.1.С.5.2 | Администрирование вычислительных сетей | | зачет, экзамен | | 10 | | | 360 | |  | |  | |  | |  | | х | |  | |  | |  | |  | |  | |  | | ПК-Р5.3 |
| Б.1.С.5.3 | Безопасность операционных систем | | экзамен | | 7 | | | 252 | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | |  | | ПК-Р5.2 |
| Б.1.С.5.4 | Разработка и эксплуатация автоматизированных систем в защищенном исполнении | | экзамен | | 7 | | | 252 | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | | ПК-Р5.1, ПК-Р5.2, ПК-Р5.3 |
| Б.1.С.5.5 | Безопасность персональных данных | | зачет с оценкой | | 5 | | | 180 | |  | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | | ПК-Р5.1 |
| Б.1.С.5.6 | Безопасность сетей ЭВМ | | зачет с оценкой экзамен | | 10 | | | 360 | |  | |  | |  | |  | |  | | х | | х | |  | |  | |  | |  | | ОПК-8 |
| Б.1.С.5.7 | Интеллектуальные технологии в задачах информационной безопасности | | экзамен | | 5 | | | 180 | |  | |  | |  | |  | |  | |  | |  | | х | |  | |  | |  | | ОПК-9, ОПК-10, ОПК-11, ПК-Р5.3 |
|  | Дисциплины (модули) образовательной организации  (при необходимости) | |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  |
| **Б.1.В** | **Часть, формируемая участниками образовательных отношений (распределение дисциплин (модулей) по периодам обучения определяется образовательной организацией самостоятельно)** |  | | | |  |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |
|  | **Дисциплины (модули) образовательной организации** |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |
|  | **Элективные дисциплины (модули) образовательной организации (при необходимости)** |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |
| **Б.2** | **Блок 2. Практика** |  | | **Не менее 24** | | | **Не менее 864** | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |
| **Б.2.О** | **Обязательная часть** |  | | **Не менее  6** | | | **Не менее 216** | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |
| Б.2.О.1 | Производственная (преддипломная) практика |  | | Не менее 6 | | | Не менее 216 | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | | х | | УК-3, УК-6,  ОПК-1 … ОПК-11,  ПК-Р4.1,  ПК-Р4.2,  ПК-Р4.3 | |
|  | Учебная практика (тип (типы) определяются образовательной организацией) (при необходимости) |  | |  | | |  | |  | |  | | х | | х | | х | | х | | х | | х | | х | | х | |  | |  | |
|  | Производственная практика (тип (типы) определяются образовательной организацией) (при необходимости) |  | |  | | |  | |  | |  | | х | | х | | х | | х | | х | | х | | х | | х | |  | |  | |
| **Б.2.В** | **Часть, формируемая участниками образовательных отношений** |  | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |
|  | Учебная практика (тип (типы) определяются образовательной организацией) (при необходимости) |  | |  | | |  | |  | |  | | х | | х | | х | | х | | х | | х | | х | | х | |  | |  | |
|  | Производственная практика (тип (типы) определяются образовательной организацией) (при необходимости) |  | |  | | |  | |  | |  | | х | | х | | х | | х | | х | | х | | х | | х | |  | |  | |
| **Б.3** | **Блок 3. Государственная итоговая аттестация** |  | | **Не  менее  6** | | | **Не  менее  216** | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |
| **Б.3.О** | **Обязательная часть** |  | | **Не  менее  6** | | | **Не  менее  216** | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | |
| Б.3.О.1 | Подготовка к защите и защита выпускной квалификационной работы |  | | 6 | | | 216 | |  | |  | |  | |  | |  | |  | |  | |  | |  | |  | | х | |  | |
|  | **Итого по образовательной программе** |  | | **300** | | | **11128** | |  | | **х** | | **х** | | **х** | | **х** | | **х** | | **х** | | **х** | | **х** | | **х** | | **х** | |  | |

Образовательная организация в пределах требований, установленных ФГОС, при формировании образовательной программы высшего образования в отношении учебных дисциплин (модулей), указанных в настоящем примерном учебном плане, вправе: конкретизировать наименование; увеличивать трудоемкость; уменьшать трудоемкость не более чем на 2 з.е. при условии, что итоговая величина составит не менее 3 з.е.; устанавливать периоды обучения, в которых изучается учебная дисциплина (модуль), а также формы промежуточной аттестации по их окончании; разделять учебные дисциплины (модули) при условии сохранения общей трудоемкости и индикаторов достижения формируемых компетенций, установленных примерной основной образовательной программой для исходной учебной дисциплины (модуля).

Федеральные государственные образовательные организации, находящиеся в ведении федеральных государственных органов, указанных в части 1 статьи 81 Федерального закона от 29 декабря 2012 г. "Об образовании в Российской Федерации", при формировании образовательной программы высшего образования в целях реализации квалификационных требований к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого они находятся, в отношении учебных дисциплин (модулей), указанных в настоящем примерном учебном плане, вправе: изменять наименование и трудоемкость в пределах требований, установленных ФГОС ВО.

Приложение 4

Примерный календарный учебный график  
образовательной программы по специальности  
10.05.05 «Безопасность информационных технологий в правоохранительной сфере»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Месяц | Сентябрь | | | | | Октябрь | | | | Ноябрь | | | | | Декабрь | | | | Январь | | | | | | | | | | | | Февраль | | | | | | | | Март | | | | | | | | | | Апрель | | | | | | | | Май | | | | | | | | | | Июнь | | | | | | | | Июль | | | | | | Август | | | |
| Неделя | 1 | | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | | 19 | | 20 | | | | 21 | | | 22 | 23 | | 24 | | 25 | | 26 | | 27 | | 28 | | 29 | | 30 | | 31 | | 32 | | 33 | | 34 | | 35 | | 36 | | 37 | | 38 | | 39 | | 40 | | 41 | | 42 | | 43 | | 44 | | 45 | | 46 | | 47 | 48 | 49 | 50 | 51 | 52 |
| 1 курс |  | | | | | | | | | | | | | | | | | | \* | | \* | | Э | | Э | | | К | | | К | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | Э | | Э | | К | | К | | К | К | К | К | К | К |
| 2 курс |  | | | | | | | | | | | | | | | | | | \* | | \* | | Э | | Э | | | К | | | К | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | Э | | Э | | К | | К | | К | К | К | К | К | К |
| 3 курс |  | | | | | | | | | | | | | | | | | | \* | | \* | | Э | | Э | | | К | | | К | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | Э | | Э | | К | | К | | К | К | К | К | К | К |
| 4 курс |  | | | | | | | | | | | | | | | | | | \* | | \* | | Э | | Э | | | К | | | К | |  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | Э | | Э | | К | | К | | К | К | К | К | К | К |
| 5 курс | |  | | | | | | | | | | | | | | | | | | \* | | \* | | Э | | Э | | | К | | | К | | П | | П | | П | | П | | П | | П | | П | | П | | П | | П | | П | | П | | П | | П | | П | | П | | Г | | Г | | Г | | Г | | Г | | К | | К | К | К | К | К | К | К |

Обозначения:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  | Э |  |  |  |  | Г |  |  |  |  | П |  |  |  |  | К |  |  | \* |  |  |  |  |  |  |  |  |
| теоретическое обучение | | | | | экзаменационные сессии | | | | | итоговая государственная аттестация | | | | | практика | | | | | каникулы | | | | | выходные, праздничные дни | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. Федеральные государственные образовательные организации, осуществляющие подготовку кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка, находящиеся в ведении федеральных государственных органов, указанных в части 1 статьи 81 Федерального закона от 29 декабря 2012 г. «Об образовании в Российской Федерации», при формировании образовательной программы высшего образования устанавливают индикаторы достижения компетенции самостоятельно на основе квалификационных требований к военно-профессиональной подготовке, специальной профессиональной подготовке выпускников, устанавливаемых федеральным государственным органом, в ведении которого они находятся [↑](#footnote-ref-1)
2. В федеральных государственных организациях, осуществляющих подготовку кадров в интересах обороны и безопасности государства, обеспечения законности   
   и правопорядка, дисциплина (модуль) может быть исключена. [↑](#footnote-ref-2)
3. *В Календарном плане указаны государственные праздники Российской Федерации. В него также должны быть включены ключевые даты, которые значимы на уровне субъекта Российской Федерации, а также для отраслей, под нужды которых осуществляется подготовка кадров в образовательной организации.* [↑](#footnote-ref-3)