

МИНОБРНАУКИ РОССИИ



Федеральное государственное автономное образовательное учреждение  
высшего образования  
**«Российский государственный гуманитарный университет»**  
**(ФГАОУ ВО «РГГУ»)**

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ  
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ  
Кафедра комплексной защиты информации

**ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО  
ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

*Код и наименование направления подготовки/специальности*

«Безопасность автоматизированных систем  
(по отрасли или в сфере профессиональной деятельности)»

*Наименование направленности (профиля)/ специализации*

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2026

*Оценка безопасности программного обеспечения автоматизированных систем*  
Рабочая программа дисциплины

Составитель:

Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

УТВЕРЖДЕНО

Протокол заседания кафедры  
комплексной защиты информации

№ 5 от 25.12.2025

## Оглавление

1. Пояснительная записка.....	4
1.1. Цель и задачи дисциплины.....	4
1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине: .....	4
1.3. Место дисциплины в структуре образовательной программы.....	5
2. Структура дисциплины.....	5
3. Содержание дисциплины.....	6
4. Образовательные технологии.....	6
5. Оценка планируемых результатов обучения.....	7
5.1. Система оценивания.....	7
5.2. Критерии выставления оценки по дисциплине.....	8
5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.....	9
6. Учебно-методическое и информационное обеспечение дисциплины.....	10
6.1. Список источников и литературы.....	10
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»... ..	11
6.3. Профессиональные базы данных и информационно-справочные системы.....	11
7. Материально-техническое обеспечение дисциплины.....	11
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья.....	12
9. Методические материалы.....	13
9.1. Планы практических занятий.....	13
<i>Приложение 1. Аннотация рабочей программы дисциплины.....</i>	<i>15</i>

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

Цель дисциплины – формирование систематизированных знаний о процессах разработки и оценки безопасности ПО АС на примере DLP-систем, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.

Задачи дисциплины:

- сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;
- сформировать представления об уязвимостях, присущих объектам информатизации, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;
- сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

<b>Компетенция</b> (код и наименование)	<b>Индикаторы компетенций</b> (код и наименование)	<b>Результаты обучения</b>
ПК-4 Способен обеспечивать работоспособность систем защиты информации при возникновении нештатных ситуаций	ПК-4.1 Знает методы и способы обеспечения отказоустойчивости автоматизированных систем, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; методы и способы отказоустойчивости работы автоматизированных систем
	ПК-4.2 Умеет применять типовые программные средства резервирования и восстановления информации, средства обеспечения отказоустойчивости в автоматизированных системах	Уметь: осуществлять настройку политики ученой записей, выполнения резервирования и архивирования, отказоустойчивости DLP-систем
	ПК-4.3 Владеет навыками обнаружения, устранения неисправностей в работе системы защиты ин-	Владеть: навыками обнаружения, устранения неисправностей в работе DLP-систем

	формации автоматизированной системы, резервирования программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций	
ПК-6 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик	Знать основные принципы оценки работоспособности и тестирования оборудования обработки и передачи данных, критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации. Уметь составлять и реализовывать планы тестирующих мероприятий,
	ПК-6.2 Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик	Уметь: составлять и реализовывать планы тестирующих мероприятий, моделировать и оценивать эффективность применяемых средств защиты
	ПК-6.3 Владеет навыками определения уровня защищенности и доверия средств защиты информации	Владеть: навыками эксплуатации и тестирования DLP-систем, определение профиля защиты.

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Оценка безопасности программного обеспечения автоматизированных систем» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

## 2. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 академических часа

### Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	28
7	Практические работы	32
Всего:		60

Объем дисциплины в форме самостоятельной работы обучающихся составляет 48 академических часа.

### 3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	<b>Понятие DLP-системы. Базовые знания по защите объектов информатизации</b>	Понятие, структура и состав DLP-систем. Классификация объектов информатизации с точки зрения безопасности. Принципы обеспечения информационной безопасности.
2	<b>Проектирование системы защиты конфиденциальной информации на примере DLP-систем</b>	Формирование требований к объекту информатизации. Моделирование угроз безопасности. Методы обеспечения защищенности объектов информатизации на этапе внедрения и эксплуатации
3	<b>Архитектура DLP-систем</b>	Структура и назначение системы защиты информации. Этапы построения системы защиты информации. Порядок разработки системы защиты конфиденциальной информации.
4	<b>Нормативно-правовые требования по сертификации DLP-систем</b>	Противоречия между необходимостью применения программно—технических средств защиты информации и требований по осуществлению контрольных мероприятий на основе подобных средств. В данном случае процедуры контрольных мероприятий могут осуществляться с использованием персональных данных работника, подвергающегося проверке. Комплекс нормативно — правовых документов, определяющих как категории и виды конфиденциальной информации, требования по обеспечения информационной безопасности подобных информационных ресурсов, так и перечень рекомендуемых для использования способов и средств защиты информации

### 4. Образовательные технологии

#### Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Понятие DLP-системы. Базовые знания по защите объектов информатизации	Лекция 1	Традиционная лекция с использованием презентаций

		Практическое занятие 1	Выполнение заданий Работа с литературой
2	Проектирование системы защиты конфиденциальной информации на примере DLP-систем	Лекция 2.1 Лекция 2.2  Практическое занятие 2	Традиционная лекция с использованием презентаций  Выполнение заданий Работа с литературой
3	Архитектура DLP-систем	Лекция 3.1 Лекция 3.2 Лекция 3.3  Практическое занятие 3	Традиционная лекция с использованием презентаций  Выполнение заданий Работа с литературой
4	Нормативно-правовые требования по сертификации DLP-систем	Лекция 4.1 Лекция 4.2  Практическое занятие 4	Традиционная лекция с использованием презентаций  Выполнение заданий Работа с литературой

## 5. Оценка планируемых результатов обучения

### 5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- практическое занятие № 1	9 баллов	9 баллов
- практическое занятие № 2	17 баллов	17 баллов
- практическое занятие № 3	17 баллов	17 баллов
- практическое занятие № 4	17 баллов	17 баллов
Промежуточная аттестация - зачёт с оценкой (ответы на вопросы)		40 баллов
<b>Итого за семестр</b>		<b>100 баллов</b>

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55		E	
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

## 5.2. Критерии выставления оценки по дисциплине

<b>Баллы/ Шкала ECTS</b>	<b>Оценка по дисциплине</b>	<b>Критерии оценки результатов обучения по дисциплине</b>
100-83/ A,B	отлично	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	хорошо	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	удовлетворительно	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	неудовлетворительно	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

## 5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

**Вопросы к зачету**

<b>Контрольные вопросы</b>	<b>Реализуемые компетенции</b>
1. Понятие, структура и состав DLP-систем.	ПК-4., ПК-6

2. Классификация DLP-систем.	ПК-4., ПК-6
3. Принципы обеспечения информационной безопасности.	ПК-4., ПК-6
4. Жизненный цикл DLP-систем.	ПК-4., ПК-6
5. Моделирование угроз безопасности объекта информатизации.	ПК-4., ПК-6
6. Управление проектированием защищенных объектов информатизации.	ПК-4., ПК-6
7. Структура и назначение системы защиты информации на примере DLP-систем.	ПК-4., ПК-6
8. Этапы построения системы защиты информации.	ПК-4., ПК-6
9. Архитектура DLP-систем.	ПК-4., ПК-6
10. Оценка соответствия системы защиты.	ПК-4., ПК-6
11. Методики анализа рисков информационной безопасности.	ПК-4., ПК-6
12. Аттестация объектов информатизации по безопасности.	ПК-4., ПК-6
13. Противоречия между необходимостью применения программно—технических средств защиты информации и требований по осуществлению контрольных мероприятий на основе подобных средств.	ПК-4., ПК-6
14. База контентной фильтрации.	ПК-4., ПК-6
15. Два основных способа перехвата — серверный и агентский.	ПК-4., ПК-6
16. DLP-системы для учета рабочего времени сотрудников. Рабочий процесс каждого пользователя можно представить в виде статистики, которая позволяет проанализировать, насколько сотрудник вовлечен в трудовой процесс.	ПК-4., ПК-6
17. Требования, предъявляемые ФСТЭК к усилению мер информационной защиты DLP-систем.	ПК-4., ПК-6
18. Поддержка виртуальных и терминальных сред как расширение функционала подсистемы информационной безопасности при использовании различных решений виртуализации рабочих сред, созданных как в форме локальных виртуальных машин, так и терминальных сессий рабочих столов или опубликованных приложений на гипервизорах.	ПК-4., ПК-6
19. Инспекция содержимого перемещаемых данных в режиме реального времени с возможностью блокировки такой попытки или отправки тревожного оповещения.	ПК-4., ПК-6
20. Лингвистический анализ и статистические методы анализа.	ПК-4., ПК-6

### *Примерные задания для тестирования*

1. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это:
  - a) аудит
  - b) аутентификация
  - c) авторизация
  - d) идентификация
  
2. Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется:
  - a) избирательным
  - b) мандатным
  - c) привилегированным

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1. Список источников и литературы

#### Источники основные

1. Методический документ. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств. Утверждён ФСТЭК России 30 июня 2025 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-30-iyunya-2025-g>, свободный. – Загл. с экрана.
2. *Руководящий документ*. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-1>, свободный. – Загл. с экрана.
3. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-3>, свободный. – Загл. с экрана.
4. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-2>, свободный. – Загл. с экрана.
5. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-25-iyulya-1997-g>, свободный. – Загл. с экрана.

#### Литература Основная

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/452368>.
2. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2025. — 216 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2206781>. – Режим доступа: по подписке.
3. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под. ред. А. В. Душкина. - Москва : Горячая линия-Телеком, 2022. - 248 с. - ISBN 978-5-9912-

- 0470-5. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1911635>. – Режим доступа: по подписке.
4. Лозовецкий, В. В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей : учебное пособие для вузов / В. В. Лозовецкий, Е. Г. Комаров, В. В. Лебедев ; под редакцией В. В. Лозовецкий. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 488 с. — ISBN 978-5-507-47615-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/397355>. — Режим доступа: для авториз. пользователей.
  5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1843022>. – Режим доступа: по подписке.

## **6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».**

Национальная электронная библиотека (НЭБ) [www.rusneb.ru](http://www.rusneb.ru)  
 ELibrary.ru Научная электронная библиотека [www.elibrary.ru](http://www.elibrary.ru)  
 Электронная библиотека Grebennikon.ru [www.grebennikon.ru](http://www.grebennikon.ru)

## **6.3. Профессиональные базы данных и информационно-справочные системы**

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

## **7. Материально-техническое обеспечение дисциплины**

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

- 1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. KasperskyEndpointSecurity

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint

- 2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. Kaspersky Endpoint Security

4. Mozilla Firefox
5. Vmware Player 15.5
6. Microsoft Share Point 2010

## **8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья**

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
  - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
  - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
  - письменные задания оформляются увеличенным шрифтом;
  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих:
  - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
  - письменные задания выполняются на компьютере в письменной форме;
  - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - письменные задания выполняются на компьютере со специализированным программным обеспечением;
  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
  - в печатной форме увеличенным шрифтом;
  - в форме электронного документа;

- в форме аудиофайла.
- для глухих и слабослышащих:
  - в печатной форме;
  - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - в печатной форме;
  - в форме электронного документа;
  - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемые эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

## 9. Методические материалы

### 9.1. Планы практических занятий

#### **Практическое занятие 1(2 ч.) «Общая архитектура DLP-систем»**

Задания:

1. Обсудить понятие, структуру и состав DLP-систем. Дать классификацию объектов информатизации по заданию преподавателя.

#### **Практическое занятие 2 (8 ч.) «Анализ угроз конфиденциальной информации»**

Задания:

1. Формирование требований по уровню защищенности.
2. Моделирование угроз безопасности .

#### **Практическое занятие 3(6 ч.) «Проектирование DLP-систем»**

Задания:

1. Порядок разработки системы защиты DLP.
2. Оценка соответствия системы защиты.

#### **Практическое занятие 4 (6 ч.) «Нормативно-правовые требования в области создания DLP-систем»**

Задания:

3. Порядок сертификации и процедура ввода в эксплуатацию
4. Умение поддерживать непрерывный цикл анализа защищенности



## **АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ**

Цель дисциплины – формирование систематизированных знаний о процессах разработки защищенных объектов информатизации и систем защиты информации на примере DLP-систем, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.

Задачи дисциплины:

- сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;
- сформировать представления об уязвимостях, присущих объектам информатизации, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;
- сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.

В результате освоения дисциплины обучающийся должен:

Знать: архитектуру подсистем безопасности, смысл базовых понятий, таких как идентификация и аутентификация, разграничение доступа и т.д.; методы и способы отказоустойчивости работы автоматизированных систем

Уметь: настраивать и эксплуатировать DLP-системы, составлять и реализовывать планы тестирующих мероприятий, моделировать и оценивать эффективность применяемых средств защиты.

Владеть: методами и инструментами анализа защищенности объектов информатизации с помощью DLP-систем.