Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных (121)»

УТВЕРЖДЕНА:
на заседании совета института ИТиАД им. Е.И.Попова
Протокол №8 от 16 февраля 2026 г.

Рабочая программа дисциплины

«СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление: 10.04.01 Информационная безопасность

Безопасность киберфизических систем

Квалификация: Магистр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Маринов Александр Андреевич Дата подписания: 17.06.2026	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 18.06.2026	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 18.06.2026

Год набора – 2026

Иркутск, 2026 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Системы менеджмента информационной безопасности» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПК-3 Способность использования навыков составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области информационной безопасности или в области информационно-аналитических систем безопасности	ПК-3.2
ПК-4 Способность использования навыков разработки эксплуатационной документации на объектах информации и проводить экспериментально-исследовательские работы при проведении сертификации средств защиты информации по требованиям безопасности информации	ПК-4.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПК-3.2	Владеет методологией для экспериментов по моделированию процессов обработки информации в специальных АИС; способен разработать процедуру интеграции модулей защиты в бизнес-процессы менеджмента информационной безопасности	**Знать** современные подходы к управлению ИБ и направлениях их развития; принципы построения СУИБ; взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; подходы к интеграции СУИБ в общую систему управления предприятием. **Уметь** анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; применять процессный подход к управлению ИБ в различных сферах деятельности; используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; разрабатывать и внедрять СУИБ и оценивать ее эффективность. **Владеть** навыками управления

		информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ; навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.
ПК-4.2	Владеет методами внедрения и применение политики информационной безопасности, установление целей, процессов и процедур СМИБ, относящихся к менеджменту риска и улучшению информационной безопасности в целях достижения непрерывного улучшения СМИБ	**Знать** современные подходы к управлению ИБ и направлениях их развития; основные стандарты, регламентирующие управление ИБ ;принципы разработки процессов управления ИБ. **Уметь** используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи формализации разрабатываемых процессов управления ИБ; разрабатывать и внедрять СУИБ и оценивать ее эффективность. **Владеть** навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Системы менеджмента информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Защита объектов критической информационной инфраструктуры»

Дисциплина является предшествующей для дисциплин/практик: «Математическое моделирование объектов и систем», «Защита объектов критической информационной инфраструктуры», «Производственная практика: преддипломная практика»

3 Объем дисциплины

Объем дисциплины составляет – 5 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)		
	Всего	Семестр № 2	Семестр № 3
Общая трудоемкость дисциплины	180	144	36
Аудиторные занятия, в том числе:	104	78	26

лекции	39	39	0
лабораторные работы	65	39	26
практические/семинарские занятия	0	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	40	30	10
Трудоемкость промежуточной аттестации	36	36	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет, Экзамен	Экзамен	Зачет

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 2

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Проведение экспериментов по моделированию процессов обработки информации	1	7	1	7			1	6	Устный опрос
2	Разработка требований к разрабатываемым процессам управления ИБ	2	8	2	8			1	6	Устный опрос
3	Разработка процедуры интеграции модулей защиты в бизнес-процессы менеджмента информационной безопасности	3	8	3	8			1	6	Доклад
4	Современные подходы к управлению рисками ИБ	4	8	4	8			1	6	Устный опрос
5	Задачи формализации разрабатываемых процессов управления ИБ	5	8	5	8			1	6	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		39		39				66	

Семестр **№ 3**

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Разработка и внедрение СУИБ			1	4			3	2	Устный опрос
2	Экспериментально-исследовательские работы при проведении сертификации средств защиты информации			2	5			2	3	Доклад
3	Оценка эффективности внедрения СУИБ			3	6					Устный опрос
4	Интеграция модулей защиты в бизнес-процессы менеджмента ИБ			4	5			1	2	Устный опрос
5	Интеграция СУИБ в общую систему управления предприятием			5	6			2	3	Доклад
	Промежуточная аттестация									Зачет
	Всего				26				10	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 2

№	Тема	Краткое содержание
1	Проведение экспериментов по моделированию процессов обработки информации	Рассматривается схема взаимосвязи моделей базовой информационной технологии в информационной безопасности. Специальные (конкретные) ИТ в вопросах информационной безопасности и задают обработку данных в определенных типах задач пользователей, используя модели: модель представления знаний; модель организации информационных процессов; модель обработки данных; модель обмена данными; модель накопления данных.
2	Разработка требований к разрабатываемым процессам управления ИБ	Стандарты ISO 27000, Cobit. Разработка технического задания. Внесение требований в локально-нормативные правовые акты.
3	Разработка процедуры интеграции модулей защиты в бизнес-процессы менеджмента информационной безопасности	Этапы интеграции модулей, защиты бизнес-процессов менеджмента информационной безопасности. Организационные и технические аспекты интеграции модулей защиты, бизнес-процессы менеджмента информационной безопасности, а также документирование.

4	Современные подходы к управлению рисками ИБ	Анализ рисков в области защиты информации. Управление рисками и международные стандарты. Технологии анализа рисков ИБ. Инструментальные средства анализа рисков. Анализ защищенности информационной системы, обнаружение атак и управление рисками, а также основные вопросы при проведении этапов аудита информационной безопасности.
5	Задачи формализации разрабатываемых процессов управления ИБ	Рассмотрены вопросы обеспечения безопасности сотрудников и организации, при реализации процессов формализации для соответствующей системы управления информационной безопасностью. Также рассмотрены меры безопасности из стандарта ИСО/МЭК 27001 как один из способов реализации политики, относительно формализации затрагивающих процессов.

Семестр **№ 3**

№	Тема	Краткое содержание
1	Разработка и внедрение СУИБ	Подходы к построению СУИБ, выявление уязвимостей в информационной инфраструктуре организации, формулировка цели и задач СУИБ. Базовые роли СУИБ, разработка документации. Возможность внедрения СУИБ: управление непрерывностью бизнеса и управление безопасностью.
2	Экспериментально-исследовательские работы при проведении сертификации средств защиты информации	Сертификационные испытания средства защиты информации. Оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия. Выдача (отказ в выдаче) сертификата соответствия. Внесение изменений в сертифицированное средство защиты информации. Переоформление сертификата соответствия. Продление, приостановление и прекращение действия сертификата соответствия.
3	Оценка эффективности внедрения СУИБ	Стандарт ИСО/МЭК 27001. Достоверность результатов оценки эффективности внедрения СУИБ. Преимущества оценки эффективности внедрения СУИБ.
4	Интеграция модулей защиты в бизнес-процессы менеджмента ИБ	Преимущества интеграции модулей защиты в бизнес-процессы менеджмента информационной безопасности. Критерии выбора модулей защиты и основные проблемы для интеграции в бизнес-процессы менеджмента информационной безопасности. Также рассмотрены методы и стратегии эффективной интеграции модулей защиты в бизнес-процессы.
5	Интеграция СУИБ в общую систему	Базовые приоритеты в отношении системы менеджмента информационной безопасности.

	управления предприятием	Оценка возможных рисков, выбор необходимых мер безопасности, внедрение выбранных методов и средств защиты в которых следует отметить: повышение доверия клиентов, партнеров и других заинтересованных сторон за счет подтверждения соответствия определенному уровню защищенности информации; эффективность организации на внутреннем и внешнем рынке; интеграция процессов управления информационной безопасностью в общую систему корпоративного управления.

4.3 Перечень лабораторных работ

Семестр № 2

№	Наименование лабораторной работы	Кол-во академических часов
1	Построение диаграммы IDEF0	7
2	Разработка требований к разрабатываемым процессам управления ИБ	8
3	Разработка процедуры интеграции модулей защиты в бизнес-процессы менеджмента информационной безопасности	8
4	Применение технологий анализа рисков ИБ	8
5	Описание управления ИБ	8

Семестр **№ 3**

№	Наименование лабораторной работы	Кол-во академических часов
1	Подходы к построению СУИБ	4
2	Экспериментально-исследовательские работы при проведении сертификации средств защиты информации	5
3	Оценка эффективности внедрения СУИБ	6
4	Разработка алгоритма интеграции модулей защиты в бизнес-процессы менеджмента ИБ	5
5	Разработка алгоритма интеграции СУИБ в общую систему управления предприятием	6

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Семестр № 2

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	30

	(лабораторным работам)	

Семестр **№ 3**

№	Вид СРС	Кол-во академических часов
1	Ведение терминологического словаря	2
2	Подготовка к практическим занятиям (лабораторным работам)	6
3	Подготовка презентаций	2

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: брейн-ринг; банк-вопросов; интеллектуальный биатлон

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по лабораторным работам:

https://el.istu.edu/mod/folder/view.php?id=324722

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/mod/folder/view.php?id=324722

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 2 | Доклад

Описание процедуры.

Публичное выступление по теме доклада с использованием презентации

Критерии оценивания.

Оценка доклада определяется следующими критериями:
- формулировка цели и задач проекта – 30 б.;
- качество анализа и обоснование выводов по теме проекта – 30 б.;
- логика и структура презентации доклада – 20 б.;
- качество оформления презентации – 10 б.;
- организация речи докладчика – 10 б.

Критерии оценки за доклад определяются по числу баллов за защиту выпускной аттестационной работы:
- менее 54 б. – неудовлетворительно;
- от 55%-74 б. – удовлетворительно;
- от 75%-84 б. – хорошо;
- от 85% -100 б. – отлично.

Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на

выяснение объема знаний, обучающегося по определенному разделу, теме.

6.1.2 семестр 2 | Устный опрос

Описание процедуры.

Устный опрос проводится по окончанию лекционных занятий путем опроса студентов по списочному составу (при наличии бюджета времени после обсуждения установленных вопросов).

Критерии оценивания.

опрашиваемым студентом должны быть даны верные (по смыслу) ответы на поставленные вопросы; допускается помощь в ответах со стороны аудитории (давшие правильный ответ освобождаются от персональной очереди отвечающих по списку).

6.1.3 семестр 3 | Доклад

Описание процедуры.

Публичное выступление по теме доклада с использованием презентации

Критерии оценивания.

- формулировка цели и задач проекта – 30 б.;
- качество анализа и обоснование выводов по теме проекта – 30 б.;
- логика и структура презентации доклада – 20 б.;
- качество оформления презентации – 10 б.;
- организация речи докладчика – 10 б.

Критерии оценки за доклад определяются по числу баллов за защиту выпускной аттестационной работы:
- менее 54 б. – неудовлетворительно;
- от 55%-74 б. – удовлетворительно;
- от 75%-84 б. – хорошо;
- от 85% -100 б. – отлично.

Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме.

6.1.4 семестр 3 | Устный опрос

Описание процедуры.

Устный опрос проводится по окончанию лекционных занятий путем опроса студентов по списочному составу (при наличии бюджета времени после обсуждения установленных вопросов).

Критерии оценивания.

опрашиваемым студентом должны быть даны верные (по смыслу) ответы на поставленные вопросы; допускается помощь в ответах со стороны аудитории (давшие правильный ответ освобождаются от персональной очереди отвечающих по списку).

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ПК-3.2	Способен продемонстрировать специализированные знания в области моделированию процессов обработки информации в специальных АИС: разработать процедуру интеграции модулей защиты в бизнес-процессы менеджмента информационной безопасности.	Устное собеседование по теоретическим вопросам и индивидуальные практические задания.
ПК-4.2	Осуществляет поиск и анализ информации, процессов и процедур СМИБ, относящихся к менеджменту риска и улучшению информационной безопасности принципы разработки процессов управления ИБ; взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ.	Устное собеседование по теоретическим вопросам и индивидуальные практические задания.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 2, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

Вопросы к экзамену:

1) Каким образом проводятся эксперименты по моделированию процессов обработки информации?
2) Схема взаимосвязи моделей базовой информационной технологии.
3) Модель представления знаний.
4) Модель обработки данных.
5) Модель обмена данными.
6) Модель накопления данных
7) Какие основные шаги и методики необходимо применять при разработке требований к разрабатываемым процессам управления информационной безопасностью?
8) Стандарты 180 27000. СоЬп
9) Разработка технического задания.
10) Внесение требований к разрабатываемым процессам управления МБ в локальные-

нормативно правовые акты.
11) Какие ключевые этапы и рекомендации необходимо учесть при разработке процедуры интеграции модулей защиты в бизнес-процессы менеджмента информационной безопасности?
12) Этапы интеграции модулей защиты бизнес-процессы менеджмента информационной безопасности.
13) Технические аспекты интеграции модулей защиты бизнес-процессы менеджмента информационной безопасности.
14) Документирование интеграции модулей защиты бизнес-процессы менеджмента информационной безопасноеги.
15) Организационные аспекты интеграции модулей защиты бизнес-процессы менеджмента информационной безопасности.
16) Какие современные подходы и методики широко применяются в управлении рисками информационной безопасности?
17) Анализ рисков в области защиты информации.
18) Управление рисками и международные стандарты.
19) Технологии анализа рисков ИБ.
20) Инструментальные средства анализа рисков.

Пример задания:

1. Подходы к построению СУИБ
2. Прекращение действия сертификата соответствия средств защиты информации

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
На высоком уровне демонстрирует знание основных современных подходов к управлению ИБ и направлений их развития; основных стандартов. регламентирующих управление ИБ принципов разработки процессом управления ИБ. Может используя современные методы и средств разрабатывать процессы	С незначительными неточностями демонстрирует знание основных современных подходов к управлению ИБ и направлений их развития. Основных стандартов, регламентирующих управление ИБ; принципов разработки процессов управления ИБ. Может используя современные методы и средства разрабатывать	Частично демонстрирует знание основных современных подходов к управлению ИБ и направлений их развития. Не может используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач. Допускает ошибки в ответах на вопросы.	Демонстрирует отсутствие знания основных современных подходов к управлению ИВ и направлений их развития. Допускает грубые ошибки в ответах на вопросы.

управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; практически решать задачи нормализации разрабатываемых процессов управления ИБ: разрабатывать и внедрять СУИБ и оценивать ее эффективность	процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач.		

6.2.2.2 Семестр 3, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.2.1 Описание процедуры

Выделены на этапах формирования (категория «Знать»), умения (категория «Уметь»), навыки и (или) опыт деятельность (категория «Владеть»). В процедуру оценивания компетенций включен самоанализ (самооценка) сформированности компетенций обучающимися.
Допуском к зачету является подготовка и полные ответы по пройденному материалу на лабораторных занятиях, защищенные обучающимся.
Во время экзамена для оценки знаний используются вопросы, приведенные в п. 6.2.2.1

Пример задания:

1) Подходы к построению СУИБ.
2) Базовые роли СУИБ.
3) Каким образом проводятся эксперименты по моделированию процессов обработки информации?
4) Сертификационные испытания средства защиты информации.
5) Оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия.
6) Выдача (отказ в выдаче) сертификата соответствия средств защиты информации.
7) Предоставление дубликата сертификата соответствия средств защиты информации.
8) Маркирование средств защиты информации.
9) Внесение изменений в сертифицированное средство средств защиты информации.
10) Переоформление сертификата соответствия средств защиты информации.
11) Продление срока действия сертификата соответствия средств защиты информации.
12) Приостановление действия сертификата соответствия средств защиты информации.
13) Прекращение действия сертификата соответствия средств защиты информации.

14) Процедуры прохождения сертификационного аудита на соответствие требованиям стандарта ISO 27001.
15) Достоверность результатов оценки эффективности внедрения СУИБ.
16) Преимущества оценки эффективности внедрения СУИБ.
17) Какие основные преимущества интеграции модулей защиты в бизнес-процессы менеджмента информационной безопасности?
18) Какие модули защиты следует интегрировать в бизнес-процессы для обеспечения эффективной защиты информации?
19) Какие проблемы могут возникнуть при интеграции модулей защиты в бизнес-процессы, и как их можно решить?
20) Какие критерии следует учитывать при выборе модулей защиты для интеграции в бизнес-процессы менеджмента информационной безопасности?
21) Какие методы и стратегии можно использовать для эффективной интеграции модулей защиты в бизнес-процессы, чтобы минимизировать возможные риски и обеспечить безопасность информации?
22) Лидерство и приверженность в отношении системы менеджмента информационной безопасности.
23) Политика информационной безопасности.
24) Роли, обязанности и полномочия в организации в области внедрения СМИБ.
25) Планирование СМИБ.
26) Обеспечение и поддержка СМИБ.
27) Функционирование СМИБ.
28) Оценка исполнения СМИБ.
29) Улучшение СМИБ

6.2.2.2.2 Критерии оценивания

Зачтено	Не зачтено
Ответ правильный, логически выстроен, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	Ответы неправильные или неполные.

7 Основная учебная литература

1. Попова Е. С. Информационная безопасность и защита информации [Электронный ресурс] : курс лекций / Е. С. Попова, 2009. - 68.

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files/er-4183.pdf

2. Нагаев И. В. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методическое пособие для бакалавров технических вузов / И. В. Нагаев, 2012. - 213.

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files/er-6789.pdf

3. Глухов Н. И. Информационная безопасность предприятия [Электронный ресурс] : монография / Н. И. Глухов, 2008. - 197.

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files/er-5013.pdf

4. Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие по специальностям 090103 "Организация и технология защиты информации", 090104 "Комплексная защита объектов информатизации" / В. Я. Ищейнов, М. В. Мецатунян, 2014. - 255.

8 Дополнительная учебная литература и справочная

1. Серенков П. С. Методы менеджмента качества. Методология организационного проектирования инженерной составляющей системы менеджмента качества / П. С. Серенков, 2016. - 490.

2. Проблемы управления информационной безопасностью : сб. тр. / Рос. акад. наук, Ин-т систем. анализа, 2002. - 221.

3. Бажин И. И. Информационные системы менеджмента : [Новая эра упр.] / И. И. Бажин, 2000. - 687.

4. Высокие технологии. Организация внедрения системы менеджмента качества на предприятии : в 2т. Т. 2 / Л. Д. Подлипаев, Е. А. Бельтюкова, Н. И. Гордин et al., 2003. - 374.

5. Соболев А.Н. Физические основы технических средств обеспечения информационной безопасности : учеб. пособие для вузов по специальностям 075500 "Комплекс. обеспечение информ. безопасности автоматизир. систем" и 075200 "Компьютер. безопасность" / А.Н. Соболев, В.М. Кириллов, 2004. - 221, [2].

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional (Microsoft Windows Seven Starter) - Seven, Vista, XP_prof_64, XP_prof_32 - поставка 2010

2. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional [1x100] RUS (проведен апгрейд с Microsoft Windows Seven Starter [1x100]) - поставка 2010

3. Свободно распространяемое программное обеспечение Microsoft Windows Server Standard 2008 R2 Russian Academic OPEN 1 License No Level

12 Материально-техническое обеспечение дисциплины

1. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

2. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

3. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

4. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

5. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

6. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

7. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

8. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

9. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

10. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

11. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

12. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

13. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

14. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

15. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

16. МФУ FS-1128 MFP

17. Сервер CPU Intel Core i7-960/GA-X58A-UD3R/DDR-IIIDimm 2Gb/HDD 1 Tb/DVD-RW/512MB PCI-E/блок пит.+ПО

18. Проектор Epson EB-W04LCD.WXGA 1280*800.3000:1.2800 ANSI Lumens