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»

УТВЕРЖДЕНА:
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

Рабочая программа дисциплины

«ЗАЩИТА ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ»

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: 22.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 23.06.2025	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 22.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Защита объектов критической информационной инфраструктуры» 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-3.1
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-4.3

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПК-3.1	Владеет методами организации работы коллектива исполнителей, принимает управленческие решения в условиях спектра мнений, определяет порядок выполнения работ	**Знать** базовые понятия в области обеспечения безопасности информации, обрабатываемой объектами критической информационной инфраструктуры; принципы организации систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечения их функционирования; процедуру категорирования объектов критической информационной инфраструктуры, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов критической информационной инфраструктуры. **Уметь** формировать сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости

		присвоения ему одной из таких категорий; выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта критической информационной инфраструктуры, а также возможных способов реализации угроз безопасности и последствий от их реализации. Обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта критической информационной инфраструктуры. **Владеть** навыками работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов критической информационной инфраструктуры; навыками работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов критической информационной инфраструктуры, в том числе зарубежными информационными ресурсами. Навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта критической информационной инфраструктуры.
ПК-4.3	Способен организовать управление информационной безопасностью	**Знать** нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов критической информационной инфраструктуры; основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий

		компьютерных атак на информационные ресурсы российской федерации; процедуру категорирования объектов критической информационной инфраструктуры, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов критической информационной инфраструктуры; процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; основные принципы выявления наличия критических процессов у субъекта критической информационной инфраструктуры. **Уметь** формировать сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта критической информационной инфраструктуры, возможных способов реализации угроз безопасности и последствий от их реализации; обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта критической информационной инфраструктуры; определять структуру системы безопасности значимого объекта критической информационной инфраструктуры. **Владеть** навыками разработки

		организационно - распорядительных документов по безопасности значимых объектов критической информационной инфраструктуры; эксплуатации системы безопасности значимого объекта критической информационной инфраструктуры; навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей; навыками проведения работ по контролю состояния безопасности объектов критической информационной инфраструктуры; навыками работы с информационными системами, информационно-телекоммуникационными сетями, автоматизированными системами управления субъектов критической информационной инфраструктуры.

2 Место дисциплины в структуре ООП

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

Дисциплина является предшествующей для дисциплин/практик: «Системы менеджмента информационной безопасности», «Математическое моделирование объектов и систем», «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	Законодательные акты в области обеспечения безопасности критической информационной инфраструктуры	1	5	1	5			1	4	Устный опрос
2	Методические документы и стандарты в области безопасности информации.	2	5	2	5			1	4	Устный опрос
3	Процедуры категорирования объектов критической информационной инфраструктуры.	3	5	3	5			1	4	Доклад
4	Принципы организации систем безопасности критической информационной инфраструктуры.	4	5	4	5			1	4	Устный опрос
5	Программные и программно-аппаратные средства для обеспечения безопасности критической информационной инфраструктуры.	5	5	5	5			1	4	Доклад
6	Государственный контроль в области обеспечения безопасности	6	5	6	5			1	4	Устный опрос

	критической информационной инфраструктуры.									
7	Роль защищенности критической информационной инфраструктуры при проведении компьютерных атак.	7	5	7	5			1	3	Доклад
8	Процедуры выявления и анализа угроз безопасности информации в объектах критической информационной инфраструктуры.	8	4	8	4			1	3	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	Нормативно-правовые акты в области КИИ			1	6			1	2	
2	Анализ потенциальных угроз объектов КИИ			2	5			1	2	Устный опрос
3	Категории значимости информации			3	5			1	2	Устный опрос
4	Организационно - распорядительные документы по безопасности значимых объектов КИИ			4	5			1	2	Устный опрос
5	Контроль состояния объектов критической информационной инфраструктуры			5	5			1	2	Устный опрос
	Промежуточная аттестация									Зачет
	Всего				26				10	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 2

№	Тема	Краткое содержание
1	Законодательные акты в области обеспечения безопасности критической информационной инфраструктуры	Определение критической информационной инфраструктуры. Законы и нормативные акты в области обеспечения безопасности критической информационной инфраструктуры. Роли и обязанности субъектов законодательства
2	Методические документы и стандарты в области безопасности информации.	Международные стандарты безопасности информации. Национальные методические документы. Процессы сертификации и аттестации.
3	Процедуры категорирования объектов критической информационной инфраструктуры.	Определение категорий критичности. Методы оценки рисков. Процедуры классификации и категоризации объектов
4	Принципы организации систем безопасности критической информационной инфраструктуры.	Принципы защиты информации. Архитектура систем безопасности. Управление доступом и аутентификация
5	Программные и программно-аппаратные средства для обеспечения безопасности критической информационной инфраструктуры.	Средства криптографической защиты. Системы мониторинга и обнаружения инцидентов. Средства защиты от DDoS-атак и вредоносных программ
6	Государственный контроль в области обеспечения безопасности критической информационной инфраструктуры.	Регулярные аудиты и проверки соответствия. Меры государственного регулирования. Отчетность перед государственными органами.
7	Роль защищенности критической информационной инфраструктуры при проведении компьютерных атак.	Типы компьютерных атак на критическую информационную инфраструктуру. Планирование и проведение учений по защите от атак. Реагирование на инциденты и восстановление после атаки.
8	Процедуры выявления и анализа угроз безопасности информации в объектах критической	Методы обнаружения угроз. Анализ уязвимостей и угроз. Разработка мер по предотвращению угроз.

	информационной инфраструктуры.	

Семестр **№ 3**

№	Тема	Краткое содержание
1	Нормативно-правовые акты в области КИИ	Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Принципы обеспечения безопасности критической информационной инфраструктуры. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры. Категорирование объектов критической информационной инфраструктуры. Реестр значимых объектов критической информационной инфраструктуры. Права и обязанности субъектов критической информационной инфраструктуры. Система безопасности значимого объекта критической информационной инфраструктуры. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Оценка безопасности критической информационной инфраструктуры. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. Ответственность за нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов
2	Анализ потенциальных угроз объектов КИИ	Анализ возможных источников угроз и действий предполагаемых нарушителей. Актуальные типы угроз. Возможные сценарии атак.
3	Категории значимости информации	Параметры классов защищенности государственных информационных систем. Классы защищенности автоматизированных систем.
4	Организационно - распорядительные документы по безопасности значимых объектов КИИ	Определение принадлежности к субъектам КИИ. Создание комиссии по категорированию. Формирование перечня критических процессов. Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию.

5	Контроль состояния объектов критической информационной инфраструктуры	Требования по контролю защищенности объектов КИИ. Современная сетевая атака. Подходы к тестированию защищенности. Отчетность.

4.3 Перечень лабораторных работ

Семестр № 2

№	Наименование лабораторной работы	Кол-во академических часов
1	Исследование действующих законодательных актов о безопасности критической информационной инфраструктуры в РФ	5
2	Изучение международных стандартов безопасности информации и их применение на практике	5
3	Определение категорий критичности информационных объектов в организации	5
4	Анализ существующих принципов защиты информации и их применение в организации	5
5	Исследование существующих программных и программно - аппаратных средств для защиты от DDoS-атак и вредоносных программ	5
6	Разработка плана мероприятий по устранению нарушений и недочетов	5
7	Анализ последствий успешной и неуспешной защиты от компьютерных атак	5
8	Проведение анализа угроз безопасности информации объектов критической информационной инфраструктуры	4

Семестр **№ 3**

№	Наименование лабораторной работы	Кол-во академических часов
1	Анализ нормативно-правовых актов в области КИИ	6
2	Оценка потенциальных угроз объектов КИИ: анализ и план действий	5
3	Категоризация значимости информации: методы и применение	5
4	Организационно-распорядительные документы по безопасности КИИ: разработка и внедрение	5
5	Контроль состояния объектов КИИ: мониторинг и аудит безопасности	5

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 (лабораторным работам)	30

Семестр **№ 3**

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям (лабораторным работам)	10

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: В теоретическом курсе предусматривается проведение интерактивной лекции по темам: «Роль защищенности критической информационной инфраструктуры при проведении компьютерных атак», «Процедуры выявления и анализа угроз безопасности информации в объектах критической информационной инфраструктуры», «Анализ потенциальных угроз объектов КИИ», «Контроль состояния объектов критической информационной инфраструктуры»(Темы №7,8,10, 13). - при проведении практических работ предусматривается решение задач разработки плана мероприятий по устранению нарушений и недочетов, анализа последствий успешной и неуспешной защиты от компьютерных атак, анализа нормативно-правовых актов в области КИИ, а также проведение при решении задач по индивидуальным заданиям «разбора конкретных ситуаций».

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=334055

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/mod/folder/view.php?id=334057&forceview=1

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 | Устный опрос

Описание процедуры.

Проведение устного опроса в форме «вопрос-ответ»

Критерии оценивания.

ответ раскрыт полностью 8-10 баллов
ответ раскрыт частично 4-7 баллов
имеет только общее представление о проблеме 2-4 баллов
не ответил – 0 баллов

6.1.2 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.

6.1.3 семестр 3 | Устный опрос

Описание процедуры.

Проведение устного опроса в форме «вопрос-ответ»

Критерии оценивания.

ответ раскрыт полностью 8-10 баллов
ответ раскрыт частично 4-7 баллов
имеет только общее представление о проблеме 2-4 баллов
не ответил – 0 баллов

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-3.1	Способен продемонстрировать специализированные знания в области	Экзамен, зачет, практико -

	организации работы коллектива исполнителей: принимает управленческие решения, определяет порядок выполнения работ в области защиты ПДн.	ориентированные задания, тесты
ПК-4.3	Способен применять нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. Применять программные и (или) программно-аппаратные средства на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов. Показывает навыки работы с информационными системами, информационно-телекоммуникационными сетями, автоматизированными системами управления субъектов критической информационной инфраструктуры.	Устное собеседование по теоретическим вопросам и индивидуальные практические задания. Вид промежуточной аттестации – экзамен.

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

Примерный перечень вопросов:
1. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры.
2. Принципы обеспечения безопасности критической информационной инфраструктуры
3. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
4. Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры
5. Категорирование объектов критической информационной инфраструктуры
6. Реестр значимых объектов критической информационной инфраструктуры
7. Права и обязанности субъектов критической информационной инфраструктуры
8. Система безопасности значимого объекта критической информационной инфраструктуры
9. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
10. Оценка безопасности критической информационной инфраструктуры
11. Государственный контроль в области обеспечения безопасности значимых объектов

критической информационной инфраструктуры.
12. Ответственность за нарушение требований закона о безопасности КИИ и принятых в соответствии с ним иных нормативных правовых актов
13. Анализ возможных источников угроз и действий предполагаемых нарушителей
14. Актуальные типы угроз КИИ
15. Возможные сценарии атак на КИИ
16. Параметры классов защищенности государственных информационных систем
17. Классы защищенности автоматизированных систем
18. Определение принадлежности к субъектам КИИ.
19. Создание комиссии по категорированию объектов КИИ.
20. Формирование перечня критических процессов.
21. Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию
22. Требования по контролю защищенности объектов КИИ
23. Современные сетевые атаки на КИИ
24. Подходы к тестированию защищенности
25. Отчетность о контроле состояния объектов КИИ

Пример задания:

1. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры.
2. Анализ возможных источников угроз и действий предполагаемых нарушителей.

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	76 - 89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Обучающийся в целом правильно интерпретирует полученный результат.	75 - 61 – ответ в основном правильный, логически выстроен, использована профессиональная терминология.	менее 60 – ответы на теоретическую часть неправильные или неполные.

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 знания (категория "Знать"), умения (категория "Уметь"), навыки и (или) опыт деятельности (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 зачета для оценки знаний используются следующие вопросы:
1. Регулирование кибербезопасности в финансовой сфере
2. Законодательство о персональных данных
3. Регулирование безопасности критической информационной инфраструктуры
4. Законодательство об электронной подписи
5. Анализ потенциальных угроз объекта КИИ - банк
6. Анализ потенциальных угроз объекта КИИ - государственное ведомство
7. Анализ потенциальных угроз объекта КИИ - производственное предприятие
8. Анализ потенциальных угроз объекта КИИ - медицинское учреждение
9. Выбор правильных категорий для секретной информации
10. Ограничение доступа к конфиденциальной информации
11. Учет информации для текущего контроля объектов КИИ
12. Влияние категорий значимости информации на виды защиты
13. Анализ и оценка действующих организационно-распорядительных документов по безопасности значимых объектов КИИ
14. Разработка и установление документов по безопасности значимых объектов КИИ
15. Актуализация и обновление организационно-распорядительных документов по безопасности значимых объектов КИИ
16. Обучение и контроль исполнения организационно-распорядительных документов по безопасности значимых объектов КИИ
17. Контроль состояния серверов, на которых хранится критическая информация
18. Сбой в электропитании объекта КИИ
19. Пропуск инцидента в систему безопасности объекта КИИ
20. Вторжение или утечка данных от внутренних пользователей объекта КИИ

Пример задания:

1. Регулирование кибербезопасности в финансовой сфере
2. Ограничение доступа к конфиденциальной информации

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. Прокофьев И.В. Защита информации в информационных интегрированных системах : учеб. для вузов по специальности "Управление качеством" / И.В. Прокофьев, 2002. - 137.

2. Хорев П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев, 2012. - 351.

3. Информационная безопасность и защита информации : учебное пособие для вузов по направлению "Информационные системы и технологии" / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова, Н. Г. Шахов, 2016. - 383.

8 Дополнительная учебная литература и справочная

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

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

3. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для студентов высшего профессионального образования ; под ред. С. А. Клейменова / В. П. Мельников, С. А. Клейменов, А. М. Петраков, 2011. - 336.

4. Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин, 2017. - 701.

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. 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

17. 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

18. 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

19. МФУ FS-1128 MFP

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

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