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

«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

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 «Управление информационной безопасностью» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК-1.1	Применяет методы научно-исследовательских и проектных работ в профессиональной деятельности	**Знать** методы информационной безопасности и защиты данных для использования в профессиональной деятельности. **Уметь** решать нестандартные профессиональные задачи, в том числе в ноной или незнакомой среде с применением информационной безопасности и зашиты данных. **Владеть** навыками теоретического и экспериментального исследования объектов профессиональной деятельности с применением технологий информационной безопасности и защиты данных, в том числе в новой или незнакомой среде.
ОПК-3.1	Разрабатывает проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной	**Знать** проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности. **Уметь** ставить цели и находить способы ее достижения используя научное представление о

	документации на системы и средства обеспечения информационной безопасности	результатах защиты информации. **Владеть** методиками постановки цели и способами ее достижения; научными представлениями о результатах обработки информации.
УК-2.1	Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления; разрабатывает модель внедрения, функционирования, мониторинга, анализа, поддержки и улучшения защиты информационных активов для достижения деловых целей, основанную на оценке риска и на принятии уровней риска организации, разработанную для эффективного рассмотрения и управления рисками	**Знать** основные требования к представлению менеджмента информационной безопасности, принципы формирования концепции проекта в рамках обозначенной проблемы; основные требования, предъявляемые к проектной работе и критерии оценки результатов проектной деятельности. **Уметь** спланировать и реализовать работу с учетом ресурсных ограничений и требований к результату ISO 27000, критически оценивать полученные результаты, в рамках обозначенной проблемы, формулируя цель, задачи, актуальность, значимость (научную, практическую, методическую и иную в зависимости от типа проекта), ожидаемые результаты и возможные сферы их применения. **Владеть** основными инструментами реализации менеджмента ИБ с учетом основных этапов жизненного цикла выполняемых работ, составления плана-графика реализации проекта в целом и плана-контроля его выполнения.
УК-3.1	Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов; проводит анализ требований для защиты информационных активов и применение соответствующих средств управления, чтобы обеспечить необходимую защиту этих информационных активов, способствует успешной реализации СМИБ	**Знать** общие формы организации деятельности коллектива; психологию межличностных отношений в группах разного возраста; основы стратегического планирования работы коллектива для достижения поставленной цели. **Уметь** создавать в коллективе психологически безопасную доброжелательную среду; учитывать в своей социальной и профессиональной деятельности интересы коллег; предвидеть результаты (последствия) как личных, так и коллективных действий; планировать командную работу, распределять поручения и

		делегировать полномочия членам команды. **Владеть** навыками постановки цели в условиях командой работы; способами управления командной работой в решении поставленных задач; навыками преодоления возникающих в коллективе разногласий, споров и конфликтов на основе учета интересов всех сторон.
УК-6.1	Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания	**Знать** способы эффективного планирования и организации своей деятельности; особенности оценки своих ресурсов и их пределы, для их оптимального использования в целях успешного выполнения порученного задания. **Уметь** выполнять критический анализ и сформулировать перечень недостающих знаний, необходимых для достижения целей. **Владеть** навыками четкого формулирования запроса на поиск новых знаний.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Управление информационной безопасностью» базируется на результатах освоения следующих дисциплин/практик: «Организационно-правовые механизмы обеспечения информационной безопасности»

Дисциплина является предшествующей для дисциплин/практик: «Комплексное обеспечение информационной безопасности», «Системы менеджмента информационной безопасности»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 1
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	52	52
лекции	26	26
лабораторные работы	0	0
практические/семинарские занятия	26	26
Самостоятельная работа (в т.ч. курсовое проектирование)	56	56
Трудоемкость промежуточной аттестации	0	0

Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет, Курсовой проект	Зачет, Курсовой проект

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 1

№ 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	Информационная безопасность как объект управления	1	2			1	2	2	10	Устный опрос
2	Система управления информационной безопасностью	2	4			2	2	2	10	Устный опрос
3	Аудит информационной безопасности	3	4			3	4	1, 3	7	Устный опрос
4	Современные методы и средства анализа и управление рисками информационных систем компаний	4	4			4	4	1, 3	7	Устный опрос
5	Правовые меры обеспечения информационной безопасности	5	4			5, 6	8	4	6	Устный опрос
6	Организационные меры обеспечения информационной безопасности	6	4			7	2	4	6	Устный опрос
7	Программно-технические меры обеспечения информационной безопасности	7	2			8	2	5	5	Устный опрос
8	Управление инцидентами информационной безопасности	8	2			9	2	5	5	Устный опрос
	Промежуточная аттестация									Зачет, Курсовой проект
	Всего		26				26		56	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 1

№	Тема	Краткое содержание
1	Информационная безопасность как объект управления	Безопасность в информационном обществе. Информационная безопасность в системе национальной безопасности России. Основные определения и критерии классификации угроз. Современные проблемы информационнойбезопасности и пути их решения
2	Система управления информационной безопасностью	Системный подход к управлению информационной безопасностью. Система государственного управления информационной безопасностью. Стандартизация в сфере управления информационной безопасностью.
3	Аудит информационной безопасности	Назначение, цели и виды аудита ИБ. Требования к аудитору ИБ, особенности взаимодействия в процессе аудита. Оценка работы аудитора. Стандартизация в сфере аудита информационной безопасности. Содержание и организация процесса аудита информационной безопасности. Оценка рисков информационной безопасности. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита информационной безопасности
4	Современные методы и средства анализа и управление рисками информационных систем компаний	Обоснование необходимости инвестиций в информационную безопасность компании. Методика FRAP. Управление рисками. Основные этапы оценки риска. Методика OCTAVE (октэйв). Профиль угрозы. Идентификация инфраструктурных уязвимостей. Разработка стратегии и планов безопасности. Методика RiskWatch (риск вэтч). Генерация отчетов.
5	Правовые меры обеспечения информационной безопасности	Законодательное регулирование обеспечения информационной безопасности на предприятии. Локальные нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Юридическая ответственность за нарушение законодательства в сфере информационной безопасности.
6	Организационные меры обеспечения информационной безопасности	Особенности организационной защиты компьютерных информационных систем и сетей. Организация работы с документами и документируемой информацией. Организация использования технических средств. Организация работы по проведениюсистематического контроля на предприятии. Режимно-секретный отдел предприятия .Служба безопасности предприятия.
7	Программно-технические меры обеспечения информационной безопасности	Программные средства автоматизации процедур управления информационной безопасности и анализа политики информационной безопасности. Программные средства поддержки процессов управления информационной безопасности.

8	Управление инцидентами информационной безопасности	Деятельность по управлению компьютерными инцидентами. ГосСОПКА. Реагирование на инциденты информационной безопасности. Разработка политики управления компьютерными инцидентами. Организация взаимодействия между подразделениями внутри организации, а также с внешними организациями. Анализ результатов деятельности по управлению компьютерными инцидентами. Нормативное и методическое регулирование управления инцидентами информационной безопасности.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 1

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Основные определения и критерии классификации угроз информационной безопасности	2
2	Система государственного управления информационной безопасностью	2
3	Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита информационной безопасности.	4
4	Разработка стратегии и планов безопасности	4
5	Локальные нормативные акты предприятия по информационной безопасности	4
6	Юридическая ответственность за нарушение законодательства в сфере информационной безопасности	4
7	Режимно-секретный отдел предприятия. Служба безопасности предприятия	2
8	Программные средства автоматизации процедур управления информационной безопасности и анализа политики информационной безопасности	2
9	Нормативное и методическое регулирование управления инцидентами информационной безопасности	2

4.5 Самостоятельная работа

Семестр № 1

№	Вид СРС	Кол-во академических

		часов
1	Написание курсового проекта (работы)	10
2	Подготовка к практическим занятиям (лабораторным работам)	20
3	Подготовка к сдаче и защите отчетов	4
4	Подготовка презентаций	12
5	Проработка разделов теоретического материала	10

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: презентации с использованием различных вспомогательных средств с обсуждением, дискуссии, кейс-методы; работа в команде (групповая разработка моделей и их сравнение по различным критериям); коллективные решения творческих задач, деловые игры, работа в малых группах, моделирование производственных процессов и ситуаций

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по курсовому проектированию/работе:

https://el.istu.edu/course/view.php?id=7963

5.1.2 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/course/view.php?id=7963

5.1.3 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/course/view.php?id=7963

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 1 | 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
ОПК-1.1	Определяет основные методики решения нестандартных профессиональных задач разработки программного обеспечения, в том числе в новой или незнакомой среде с применением математических, естественнонаучных и профессиональных знаний	Опрос, собеседование, практикоориентированные задания, тесты письменные и/или компьютерные, дискуссия. Вид промежуточной аттестации – зачет.
ОПК-3.1	Способен продемонстрировать специализированные знания по объектам информатизации воздействие на структуры управления и угрозы нарушения безопасности информации, которые могут быть реализованы путем деструктивного воздействия на информационные ресурсы.	Опрос, собеседование, практикоориентированные задания, дискуссия. Вид промежуточной аттестации – зачет.
УК-2.1	Способен применять современные средства поиска информации; Способен анализировать связи и определять наиболее важные из них.	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий
УК-3.1	Знает основные командные роли, корректирует работу команды с учетом интересов, особенностей поведения и мнении ее членов.	Опрос, собеседование, практикоориентированные задания, тесты. Вид промежуточной аттестации – зачет.
УК-6.1	Опрос, собеседование, практикоориентированные задания, тесты. Вид промежуточной аттестации – зачет.	Тестирование, представление и защита презентации, аннотация. Вид промежуточной аттестации – зачет.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 1, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

Перечень теоретических вопросов, практических заданий и ситуаций, выносимых на зачет, доводятся преподавателем до студентов в начале изучения программы. Формулировки вопросов, заданий должны быть четкими, краткими, понятными, исключающими двойное толкование. Могут быть применены тестовые задания или задания комбинированного характера. Количество вариантов для устных заданий должно быть больше чем число студентов, сдающих экзамен не менее, чем на 3. Количество вариантов для письменных заданий должно быть не менее двух. Вопросы к зачету:
1. Современные технологии поиска информации
2. Поиск информации для проведения научного исследования с использованием современных технологий
3. Преимущества современных технологий по сравнению с традиционными методами поиска информации?
4. Влияние современных технологий на эффективность поиска информации
5. Ограничения и недостатки существуют при использовании современных технологий и методов поиска информации в научных исследованиях
6. Лидерские и поддерживающие роли в команде
7. Причины возникновения и способы минимизации конфликтов в команде
8. Учет мнений и интересов команды при принятии решений
9. Синергетический эффект командной работы
10. Методы и инструменты корректировки работы команды
11. Принципы эффективного планирования собственной деятельности
12. Инструменты организации рабочего времени?
13. Способы преодоления прокрастинации при планировании и организации задач
14. Управление приоритетами при планировании деятельности
15. Преимущества регулярного обновления и корректировки плана деятельности
16. Принципы методики решения нестандартных профессиональных задач в разработке программного обеспечения
17. Влияние математических и естественнонаучных знаний на процесс решения нестандартных задач в программировании
18. Роль профессиональных знаний в разработке программного обеспечения при решении нестандартных задач
19. Влияние методики адаптации к новой или незнакомой среде
20. Применение методов исследования при решении нестандартных профессиональных задач в программировании
21. Значение организационно-распорядительных документов в обеспечении информационной безопасности
22. Роль технической документации при внедрении и поддержке средств обеспечения информационной безопасности
23. Элементы эксплуатационной документации информационной безопасности
24. Требования к документам, регламентирующих информационную безопасность, с учетом соблюдения законодательства и стандартов
25. Как организация может использовать документы по информационной безопасности в обучении сотрудников и повышении их информационной грамотности?

Пример задания:

1. Современные технологии поиска информации
2. Влияние математических и естественнонаучных знаний на процесс решения нестандартных задач в программировании

6.2.2.1.2 Критерии оценивания

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

6.2.2.2 Семестр 1, Типовые оценочные средства для курсовой работы/курсового проектирования по дисциплине

6.2.2.2.1 Описание процедуры

Темы курсовых работ

1. Сравнительный анализ различных подходов к оценке ущерба, возникающего вследствие инцидента информационной безопасности.
2. Разработка методики выявления инцидентов информационной безопасности, связанных с нарушением политики использования информационных ресурсов организации.
3. Информационная безопасность в управлении персоналом.
4. Задачи аналитической работы в сфере защиты информации.
5. Задачи аналитической работы по выявлению угроз и каналов утраты конфиденциальной информации.
6. Направления использования результатов аналитической работы для формирования системы защиты информации.
7. Содержание процедуры разработки перечня ценных и конфиденциальных сведений.
8. Назначение и содержание перечня конфиденциальных документов фирмы.
9. Оценочные стандарты в информационной безопасности.
10. Стандартизация в области управления информационной безопасностью.
11. Современные методы и средства анализа и управление рисками информационных систем компаний.
12. Нормативные акты предприятия по информационной безопасности.
13. Регулирование использования средств криптографической защиты.
14. Проверка технического соответствия требованиям безопасности.
15. Меры управления аудитом информационных систем.
16. Процессный подход в рамках управления информационной безопасностью.
17. Система управления информационной безопасностью организации.
18. Особенности управления информационной безопасностью в рекламной сфере.
19. Особенности управления информационной безопасностью в федеральных органах исполнительной власти.
20. Экономические методы обеспечения информационной безопасности.
21. Особенности управления информационной безопасностью организации при переводе на дистанционный режим работы.

22. Порядок взаимодействия с федеральными органами исполнительной власти при расследовании инцидентов информационной безопасности.
23. Взаимодействие отдела информационной безопасности предприятия с правоохранительными органами при расследовании компьютерных правонарушений.
24. Уголовная ответственность за преступления в сфере компьютерной информации.
25. Уголовная ответственность в сфере информационной безопасности.
26. Административная ответственность в сфере информационной безопасности.
27. Дисциплинарная ответственность в сфере информационной безопасности.
28. Государственная система управления информационной безопасностью.
29. Функции, цели и задачи деятельности Федеральной службы безопасности РФ в сфере обеспечения информационной безопасности.
30. Функции, цели и задачи деятельности Федеральной службы по техническому и экспортному контролю РФ в сфере обеспечения информационной безопасности.

6.2.2.2.2 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.

7 Основная учебная литература

1. Прохорова О. В. Информационная безопасность и защита информации : учебное пособие / О. В. Прохорова, 2020. - 124 с

2. Глухих В. И. Информационная безопасность и защита данных : учебное пособие / В. И. Глухих, 2012. - 244.

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.

4. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие для вузов по направлениям подготовки и специальностям укрупненной группы 10.00.00 (090000) "Информационная безопасность" / В. С. Горбатов [и др.]; под общ. ред. Ю. Н. Лаврухина, 2014. - 557.

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

6. 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.

7. Краковский Ю. М. Информационная безопасность и защита информации : учебное пособие для вузов по направлению подготовки 09.03.01 "Информатика и вычислительная техника" (протокол № 528 от 10 августа 2015 года) / Ю. М. Краковский, 2016. - 223.

8 Дополнительная учебная литература и справочная

1. 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.

2. Курушин Владимир Дмитриевич. Компьютерные преступления и информационная безопасность : справочник / Владимир Дмитриевич Курушин, Владимир Александрович Минаев, 1998. - 256.

3. Милославская Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью : учебное пособие для вузов по направлению подготовки 090900 - "Информационная безопасность" (уровень - магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой, 2016. - 165.

4. Милославская Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов по направлению подготовки 090900- "Информационная безопасность" (уровни- бакалавр, магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой, 2014. - 213.

5. Милославская Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов по направлению подготовки 090900- "Информационная безопасность" (уровень-магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой, 2014. - 168.

6. Милославская Н. Г. Управление рисками информационной безопасности : учебное пособие для вузов по направлению подготовки 090900- "Информационная безопасность" (уровень-магистр) / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой, 2014. - 130.

7. 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. МФУ FS-1128 MFP

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

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