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

«ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ 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: 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 «Организационно-правовые механизмы обеспечения информационной безопасности» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПК-2 Способность участвовать в планировании и реализации процессов контроля над информационной безопасностью или процессов информационно-аналитических систем безопасности	ПК-2.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПК-2.1	Способен применить экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем	**Знать** основы российской правовой системы и законодательства, правового статуса личности, организации деятельности органов государственной власти Российской Федерации по защите информации; характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ; виды и степень ответственности за правонарушения и преступления в информационной сфере; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. **Уметь** определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; анализировать правовые акты и осуществлять правовую оценку информации; предпринимать необходимые меры по восстановлению нарушенных прав; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. **Владеть** навыками поиска нормативной правовой информации,

		необходимой для профессиональной деятельности навыками работы с нормативными правовыми актами; навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности и обеспечения режима секретности, а также организации и управления деятельностью службы защиты информации на предприятии.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Защита персональных данных при обработке в автоматизированных информационных системах»

Дисциплина является предшествующей для дисциплин/практик: «Комплексное обеспечение информационной безопасности», «Защита объектов критической информационной инфраструктуры», «Производственная практика: научно-исследовательская работа (научно-исследовательский семинар)»

3 Объем дисциплины

Объем дисциплины составляет – 4 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 1
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	52	52
лекции	26	26
лабораторные работы	26	26
практические/семинарские занятия	0	0
Самостоятельная работа (в т.ч. курсовое проектирование)	56	56
Трудоемкость промежуточной аттестации	36	36
Вид промежуточной аттестации (итогового контроля по дисциплине)	Экзамен	Экзамен

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 1

№	Наименование	Виды контактной работы	СРС	Форма

п/п	раздела и темы дисциплины	Лекции		ЛР		ПЗ(СЕМ)				текущего контроля
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Информационные отношения и правовой режим защиты информации ограниченного доступа	1	4	1	2			2	10	Проверочная работа
2	Правовая защита различных видов конфиденциальной информации	2	4	2, 3	4			2	10	Проверочная работа
3	Защита персональных данных и государственное регулирование деятельности по защите информации	3	4	4, 5, 6	8			5	10	Проверочная работа
4	Организационное обеспечение информационной безопасности	4	4	7, 8, 9	6			1	10	Проверочная работа
5	Организация охраны, режима и работы с персоналом	5	2	10	2			3	4	Проверочная работа
6	Организация защиты информации в различных направлениях деятельности предприятия (организации)	6	4	11	2			4	6	Проверочная работа
7	Организация взаимодействия с федеральными органами исполнительной власти в сфере обеспечения информационной безопасности	7	4	12	2			4	6	Проверочная работа
	Промежуточная аттестация								36	Экзамен
	Всего		26		26				92	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 1

№	Тема	Краткое содержание
1	Информационные отношения и правовой	Информационные отношения как объект правового регулирования. Законодательство

	режим защиты информации ограниченного доступа	Российской Федерации в области информационной безопасности. Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующие обеспечение информационной безопасности в Российской Федерации Понятие и виды информации ограниченного доступа по законодательству РФ. Правовой режим защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Правовой режим защиты информации конфиденциального характера. Понятие информации конфиденциального характера по российскому законодательству. Основные виды конфиденциальной информации. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
2	Правовая защита различных видов конфиденциальной информации	Институт правовой защиты служебной тайны. Правовые основы защиты служебной тайны. Нормативно-правовые акты, регулирующие правовую защиту служебной тайны. Защита в режиме служебной тайны сведений, доступ к которым ограничивается в соответствии с законодательством, при обращении и хранении таких сведений (информации) в органах государственной власти и органах местного самоуправления. Институт правовой защиты коммерческой тайны. Правовые основы защиты коммерческой тайны. Объекты и субъекты права на коммерческую тайну. Права и обязанности обладателя коммерческой тайны. Ответственность за нарушение прав на коммерческую тайну. Институт правовой защиты банковской тайны. Институт правовой защиты профессиональной тайны.
3	Защита персональных данных и	Институт правовой защиты персональных данных. Правовые основы защиты информации

	государственное регулирование деятельности по защите информации	персонального характера. ФЗ «О персональных данных», подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных. Государственный надзор и контроль обработки персональных данных. Государственное регулирование деятельности в области защиты информации. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Правовые основы сертификации в области защиты информации. Правонарушения в информационной сфере и особенности защиты от них. Особенности правонарушений в информационной сфере. Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Правовая защита информационных систем. Правовая защита результатов интеллектуальной деятельности.
4	Организационное обеспечение информационной безопасности	Понятие организационной защиты информации. Сущность организационных методов защиты информации. Соотношение организационных мер защиты информации с мерами правового и технического характера. Основные термины, связанные с организацией защиты информации. Организация режима секретности. Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Особенности системы организационной защиты государственной тайны. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны. Организация деятельности режимно-секретных органов. Установление и изменение степени секретности сведений, отнесенных к государственной тайне. Понятие «рассекречивание сведений». Основания для рассекречивания сведений. Допуск к государственной тайне. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы.

		Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности. Организация доступа к сведениям, составляющим государственную тайну.
5	Организация охраны, режима и работы с персоналом	Понятие «охрана». Цели и задачи охраны. Объекты охраны. Виды, способы и особенности охраны различных объектов. Понятие о рубежах охраны. Многорубежная система охраны. Факторы выбора методов и средств охраны. Организация режимных мероприятий. Понятие «режим», цели и задачи режимных мероприятий. Виды режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Виды пропускных документов. Порядок организации работы бюро пропусков. Контрольно-пропускные пункты, их оборудование и организация работы. Понятие «внутриобъектовый режим» и его общие требования. Противопожарный режим и его обеспечение. Работа с персоналом, обладающим конфиденциальной информацией. Подбор и расстановка кадров. Организация обучения персонала. Основные формы обучения и методы контроля знаний. Мотивация персонала к выполнению требований по защите информации. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. Организационные меры по защите информации при увольнении сотрудника.
6	Организация защиты информации в различных направлениях деятельности предприятия (организации)	Организация подготовки и проведения конфиденциальных переговоров. Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров. Основные этапы проведения конфиденциальных переговоров. Подготовка помещения для проведения конфиденциальных переговоров. Организация защиты информации при приеме в организации посетителей, командированных лиц, иностранных представителей. Требования режима защиты информации при приеме в организации посетителей. Организация работы с иностранными

		представителями. Требования к помещениям, в которых проводится прием иностранных представителей. Обеспечение защиты информации при выезде за рубеж командируемых лиц. Организация работы службы безопасности предприятия. Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников. Варианты организационных структур, обеспечивающих защиту информации. Основные документы службы информационной безопасности.
7	Организация взаимодействия с федеральными органами исполнительной власти в сфере обеспечения информационной безопасности	Организационно-правовая структура, цели, функции и задачи Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ (Роскомнадзор). Организационно-правовое взаимодействие служб ИБ организаций (предприятий) с ФСБ России, ФСТЭК России и Роскомнадзором. Характеристика ФЗ "О безопасности критической информационной инфраструктуры". Нормативные, методические и руководящие документы ФСБ России и ФСТЭК России в сфере обеспечения информационной безопасности и защиты информации.

4.3 Перечень лабораторных работ

Семестр № 1

№	Наименование лабораторной работы	Кол-во академических часов
1	Информационные отношения как объект правового регулирования	2
2	Правовой режим защиты государственной тайны	2
3	Правовой режим защиты информации конфиденциального характера	2
4	Институт правовой защиты персональных данных	4
5	Государственное регулирование деятельности в области защиты информации	2
6	Преступления в сфере компьютерной информации	2
7	Понятие и сущность организационной защиты информации	2

8	Организация режима секретности	2
9	Допуск к государственной тайне	2
10	Организация служебного расследования по фактам утраты информации	2
11	Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам	2
12	Организационно-правовое взаимодействие с регуляторами в сфере информационной безопасности	2

4.4 Перечень практических занятий

Практических занятий не предусмотрено

4.5 Самостоятельная работа

Семестр № 1

№	Вид СРС	Кол-во академических часов
1	Оформление отчетов по лабораторным и практическим работам	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 лабораторным работам:

https://el.istu.edu/course/view.php?id=6885

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/mod/folder/view.php?id=335350

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 | Проверочная работа

Описание процедуры.

Проведение лабораторной работы путем выполнения письменной проверочной работы. Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приѐмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности. Основной целью политики информационной безопасности является общее описание правил работы с информацией компании. Наличие сформулированных и закрепленных на бумаге правил обеспечения информационной безопасности позволит достичь:

1. Стабильность защиты.
2. Независимость защиты от личных и профессиональных качеств исполняющего персонала.
3. Возможность контроля как защиты, так и процедур обработки информации.

Перед разработкой политики информационной безопасности должен быть проведен анализ активов, включающий их учет и оценку.

Готовая политика должна иметь в своем составе отдельный раздел для каждого обнаруженного актива, группы взаимосвязанных активов или обособленной части актива компании в зависимости от ранее проведенного анализа их структуры и взаимосвязи.

В дополнение и исходя из политики информационной безопасности могут быть разработаны другие документы, такие как руководства или стандарты. В отличие от политик они более конкретны, что выражается в привязке к определенному оборудованию, версиям программ или в точном указании необходимой последовательности действий для достижения заданного результата.

Политика информационной безопасности разрабатывается специалистами информационной безопасности компании для использования остальными сотрудниками компании. Поэтому, она должна быть изложена максимально просто, на обычном языке с использованием минимума специальной лексики только там, где это необходимо.

Критерии оценивания.

ответ раскрыт полностью – 5 баллов
ответ раскрыт частично – 2-4 баллов
имеет только общее представление о проблеме – 1 балл
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-2.1	Демонстрирует высокий уровень знаний нормативных правовых актов РФ и стандартов в сфере информационной безопасности киберфизических систем, руководящих и	Устное собеседование по теоретическим вопросам и/или выполнение практических

	методических документов ФСТЭК России и ФСБ России при применении экспертных систем комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем.	заданий.

6.2.2 Типовые оценочные средства промежуточной аттестации

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

6.2.2.1.1 Описание процедуры

Перечень теоретических вопросов, практических заданий и ситуаций, выносимых на экзамен, 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.

Пример задания:

1. Какие нормативно-правовые акты РФ регулируют информационную безопасность киберфизических систем?
2. Какие стандарты применяются в сфере информационной безопасности киберфизических систем?
3. Какие руководящие и методические документы ФСТЭК России и ФСБ России регулируют применение экспертных систем комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем?
4. Какие требования предъявляются к экспертным системам комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем в соответствии с нормативно-правовыми актами РФ?
5. Какие основные принципы обеспечения информационной безопасности киберфизических систем определены в документах ФСТЭК России и ФСБ России?
6. Основные понятия, термины и определения; предмет и объект защиты;
7. Уязвимости и угрозы безопасности информации в АИС; риски информационной безопасности (ИБ) и методы их оценки;
8. Институт правовой защиты служебной тайны.
9. Правовые и организационные методы защиты информации в АИС; аудит ИБ;
10. Правонарушения в информационной сфере и особенности защиты от них.
11. Правовая защита информационных систем
12. Понятие организационной защиты информации.
13. Основные термины, связанные с организацией защиты информации.
14. Организационные меры, направленные на защиту государственной тайны.
15. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
16. Организационно-правовое взаимодействие служб ИБ организаций (предприятий) с ФСБ России, ФСТЭК России и Роскомнадзором

17. Правовое регулирование деятельности Федеральной службы по техническому и экспортному контролю РФ.
18. Нормативные, методические и руководящие документы ФСБ России и ФСТЭК России в сфере обеспечения информационной безопасности и защиты информации.
19. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа;
20. Электронный замок Соболь-PCI: настройка и эксплуатация; управление пользователями; диагностика устройства; настройка контроля целостности; регистрация событий;
21. Требования к симметричным и асимметричным криптосистемам;
22. Алгоритм DES; свойства стандарта AES;
23. Функции хэширования, алгоритм MD5;

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.

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

8 Дополнительная учебная литература и справочная

1. Рассолов М. М. Информационное право : учеб. пособие / М. М. Рассолов, 1999. - 398.

2. Основы информационной безопасности : учеб. пособие для вузов по специальностям в обл. информ. безопасности / Е. Б. Белов [и др.], 2006. - 544.

3. Новиков В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения : учебное

пособие для вузов по дополнительным профессиональным программам в области информационной безопасности / В. К. Новиков, 2015. - 175.

4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры вузов по юридическим направлениям и специальностям / Т. А. Полякова [и др.]; под ред. Т. А. Поляковой и А. А. Стрельцова, 2016. - 324.

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