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

«ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

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 «Защищенные информационные системы» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.2
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК-2.2	Владеет навыками управления проектами сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты, самостоятельно проектирует сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты	**Знать** методы обработки результатов экспериментальных исследований и оформления научно-технических отчетов, касающиеся технологий обеспечения информационной безопасности больших данных; методы разработки программы и методики испытаний средств и систем обеспечения информационной безопасности; требования информационной безопасности закрытого и открытого контуров инфокоммуникационных систем. **Уметь** готовить по результатам выполненных исследований научные доклады и статьи, касающиеся технологий обеспечения информационной безопасности больших данных; разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности; строить модели нарушителей и угроз в закрытом и открытом контуре инфокоммуникационных систем. **Владеть** навыками обеспечения информационной безопасности больших данных; навыками разработки программы и методики

		испытаний средств и систем обеспечения информационной безопасности; инструментальными средствами защиты информации от несанкционированного доступа в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационной системы.
УК-3.2	Организует дискуссии по заданной теме и обсуждение результатов работы команды по анализу задач создания защищенных информационных систем с различных точек зрения; планирует командную работу для исследований в области защищенных информационных систем	**Знать** методы и способы защиты информационных систем. **Уметь** решать задачи в соответствии с заданной темой и обсуждением результатов работы команды по анализу задач создания защищенных информационных систем. **Владеть** навыками определения и постановки задач.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Защищенные информационные системы» базируется на результатах освоения следующих дисциплин/практик: «Управление информационной безопасностью», «Технологии защиты информации в автоматизированных информационных системах»

Дисциплина является предшествующей для дисциплин/практик: «Производственная практика: эксплуатационная практика», «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 № 3
Общая трудоемкость дисциплины	180	180
Аудиторные занятия, в том числе:	91	91
лекции	52	52
лабораторные работы	0	0
практические/семинарские занятия	39	39
Самостоятельная работа (в т.ч. курсовое проектирование)	53	53
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 № 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	Безопасность информационных систем	1	4			1	3	1	4	Устный опрос
2	Анализ активных заражений, работа с антивирусным ПО	2	4			2, 4	8	1	4	Устный опрос
3	Криптографические методы защиты информации	3	6			3	4	2	5	Устный опрос
4	Анализ и создание защищенных информационных систем	4	6					2	5	Устный опрос
5	Системная защита информации компьютерных сетей	5	6			5	4	1	5	Устный опрос
6	Создание защищенной информационной системы	6	5			6	6	1	6	Устный опрос
7	Разработка системы защиты информации	7	5			7	4	1	6	Доклад
8	Внедрение, подтверждение соответствия системы защиты информации	8	5			8	4	2	6	Устный опрос
9	Подтверждение соответствия системы защиты информации	9	6					1	6	Устный опрос
10	Этапы стадии эксплуатации системы защиты информации	10	5			9	6	2	6	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		52				39		89	

4.2 Краткое содержание разделов и тем занятий

Семестр № 3

№	Тема	Краткое содержание
1	Безопасность информационных	Обеспечение физической безопасности информационных систем. Управление

	систем	инцидентами информационной безопасности в вопросах противодействия внутренним угрозам и защите информации от несанкционированного доступа.
2	Анализ активных заражений, работа с антивирусным ПО	Анализ активных заражений и лечение инфицированных систем с помощью антивирусного ПО. Борьба с вредоносным ПО с помощью Антивирусных продуктов, включая фишинг (fishing) и хакерские атаки, максимально соответствующие ресурсам компьютера и требованиям пользователя. Работа с базами данных эвристического анализа и ревизорным модулем.
3	Криптографические методы защиты информации	Рассмотрены криптографические протоколы и стандарты. Симметричные криптосистемы, асимметричные криптосистемы, а также хеширование и цифровая подпись. Рассмотрены научные источники по криптографии, математическая база симметричной криптографии и способы защиты данных преимущественно криптографической защиты информации, принципы построения криптоалгоритмов и сетей засекреченной связи.
4	Анализ и создание защищенных информационных систем	Моделирование угроз с учетом жизненного цикла ИС. Применение мер по ИБ в процессе разработки приложения. Проведение мероприятий ИБ на этапе разработки концепции ИС.
5	Системная защита информации компьютерных сетей	Системы обнаружения и предотвращения вторжений, VPN-технологии, обеспечение безопасности беспроводных сетей. Этапы разработки защищенных информационных систем. Современные подходы к обеспечению анонимности работы в сети Интернет.
6	Создание защищенной информационной системы	Рассмотрены требования к системе защиты информации, а также этапы проведения работ: 1) принятие решения о необходимости защиты обрабатываемой информации; 2) классификация объекта по требованиям защиты информации (установление уровня защищенности обрабатываемой информации); 3) определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации; 4) определение требований к системе защиты информации. Решение о необходимости создания системы защиты информации принимается на основе анализа стоящих задач, обрабатываемой информации и нормативной базы.
7	Разработка системы защиты информации	Разработка системы защиты информации – организуется обладателем информации. На данном

		этапе проводятся работы:- проектирование системы защиты информации;- разработка эксплуатационной документации на систему защиты информации. Подробно рассматриваются работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации, а также работы и услуги по проектированию в защищенном исполнении.
8	Внедрение, подтверждение соответствия системы защиты информации	Внедрение системы защиты информации – организуется обладателем информации (заказчиком) с привлечением оператора. Рассматривается основные пакет документов которые формируются по результатам исполнения работ на этапе внедрения системы защиты информации, а также состав обязательных организационно-распорядительных документов, разрабатываемых на этапе внедрения системы защиты информации.
9	Подтверждение соответствия системы защиты информации	Подтверждение соответствия системы защиты информации – организуется обладателем информации (заказчиком) или оператором. Перечень работ на данном этапе определяется в "программе" и методиках аттестационных испытаний, разрабатываемой до их начала. Документ формируется исполнителем работ и согласовывается с заявителем.
10	Этапы стадии эксплуатации системы защиты информации	Данные этапы связанны с следующими работами:- ввод системы защиты информации в постоянную эксплуатацию;- промышленная эксплуатация системы защиты информации.- вывод из эксплуатации системы защиты информации.Также оператор осуществляет администрирование системы защиты информации, выявление инцидентов и реагирование на них, управление конфигурацией объекта и его системой защиты информации, контроль за обеспечение необходимого уровня защищенности информации. Повторная аттестация ГИС осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 3

№	Темы практических (семинарских) занятий	Кол-во академических часов

1	Безопасность информационных систем	3
2	Анализ активных заражений, работа с антивирусным ПО	4
3	Криптографические методы защиты информации	4
4	Анализ и создание защищенных информационных систем	4
5	Системная защита информации компьютерных сетей	4
6	Создание защищенной информационной системы	6
7	Разработка системы защиты информации	4
8	Внедрение, подтверждение соответствия системы защиты информации	4
9	Этапы стадии эксплуатации системы защиты информации	6

4.5 Самостоятельная работа

Семестр № 3

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	31
2	Подготовка презентаций	22

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 практическим занятиям

https://el.istu.edu/mod/folder/view.php?id=326508

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/mod/folder/view.php?id=326509

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 3 | 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.

6.1.2 семестр 3 | Устный опрос

Описание процедуры.

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.

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-2.2	Способен продемонстрировать специализированные знания в области проектирования сложных систем (под-систем, компонентов системы) и комплексов управления информационной безопасностью. Правильно применяет приобретенные навыки по управлению и проектировке информационных систем, с учетом особенностей их защиты.	Устное собеседование по теоретическим вопросам и индивидуальные практические задания.
УК-3.2	1. Знает методы и способы защиты информационных систем. 2. Анализирует возможные варианты	Опрос, собеседование, компьютерные

	поиска и критического анализа 3. Разрабатывает наиболее оптимальные пути решения задач ИБ.	тесты. Вид промежуточной аттестации – экзамен.

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 3, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 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 экзамену является подготовка и полные ответы по пройденному материалу на практических занятиях, защищенные обучающимся.
Во время экзамена для оценки знаний используются следующие вопросы:
1) Управление рисками безопасности информационных систем.
2) Технологии обнаружения и предотвращения кибератак.
3) Стандарты и нормативы информационной безопасности.
4) Обучение и повышение осведомленности сотрудников в области информационной безопасности.
5) Классификация и анализ активных заражений
6) Методы обнаружения и удаления вирусов
7) Защита от резидентного вируса в установленном антивирусном ПО, имитирующая копию вируса.
8) Исследование новых угроз и разработка антивирусных программ.
9) Принципы и алгоритмы шифрования данных.
10) Обзор криптографических методов и стандартов.
11) Применение криптографии в современных системах защиты.
12) Развитие квантовых вычислений и их влияние на шифрование.
13) Оценка уязвимостей информационных систем.
14) Методики тестирования на проникновение.
15) Интеграция механизмов безопасности в разработку информационных систем.
16) Создание корпоративных стандартов безопасности информации.
17) Система контроля доступа к информации в компьютерной сети.
18) Защита от сетевых атак и вторжений.
19) Безопасность беспроводных сетей и мобильных устройств.
20) Безопасность облачных и виртуализированных сред.
21) Моделирование угроз и оценка рисков для информационных систем
22) Внедрение механизмов идентификации и аутентификации
23) Применения блокчейн технологии для создания защищенных систем
24) Использование искусственного интеллекта и машинного обучения для защиты информации
25) Выбор и обоснование средств защиты информации.
26) Разработка политик и процедур безопасности.
27) Управление инцидентами и непрерывностью бизнеса.
28) Защита персональных данных и конфиденциальной информации.
29) Проведение аудита и оценки соответствия системы защиты.

30) Сертификация и лицензирование в области информационной безопасности.
31) Контроль выполнения требований безопасности на предприятии.
32) Расследование инцидентов и восстановление систем после сбоев.
33) Подготовка документации и отчетов для подтверждения соответствия.
34) Выбор сертификационных органов и программ.
35) Получение и продление сертификатов безопасности.
36) Оценка эффективности системы защиты информации на основании сертификатов.
37) Планирование и управление обновлениями системы защиты.
38) Мониторинг и анализ инцидентов безопасности.
39) Корректирующие и превентивные меры в процессе эксплуатации.
40) Поддержка пользователей и обучение персонала в области защиты информации.

Пример задания:

1 Управление рисками безопасности информационных систем
2. Защита от резидентного вируса в установленном антивирусном ПО, имитирующая копию вируса.

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
На высоком уровне демонстрирует знание основных современных подходов к управлению проектами сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты, самостоятельно проектирует сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты.	С незначительными неточностями демонстрирует знание основных современных подходов к управлению проектами сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты, самостоятельно проектирует сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты.	Частично демонстрирует знание основных современных подходов к управлению проектами сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты. Не может используя современные методы и средства разрабатывать разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности. Допускает ошибки в ответах на вопросы.	Демонстрирует отсутствие знания основных современных подходов к управлению проектами сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты. Допускает грубые ошибки в ответах на вопросы.

	Может строить модели нарушителей и угроз в закрытом и открытом контуре инфокоммуникационных систем.		

7 Основная учебная литература

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

2. Введение в SQL : методическое пособие для специальностей 0719 " Информационные системы и технологии (системы поддержки принятия решений)" ... / Иркут. гос. техн. ун-т, 2004. - 32.

3. 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.

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. 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. 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.

3. Макаровский Б.Н. Информационные системы и структуры данных : учеб. пособие для вузов по специальности "Орг. механизир. обраб. экон. информ. " / Б.Н. Макаровский, 1980. - 199.

4. Криптографическая защита информации : учебное пособие : для студентов бакалавриата, магистратуры, аспирантов, обучающихся по направлениям "Информационная безопасность", "Бизнес информатика", "Инфокоммуникационные технологии и системы связи" по профилю "Защищенные системы и сети связи" / С. О. Крамаров [и др.]; под редакцией С. О. Крамарова, 2018. - 319.

5. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие для вузов по направлению 09.03.01 "Информатика и вычислительная техника" / В. Ф. Шаньгин, 2019. - 591.

6. Сумароков Л. Н. Интегрированные информационные системы : Осн. понятия, проблемы и методол. вопр. создания / Л. Н. Сумароков, Ю. М. Горностаев, 1972. - 60.

7. Арсеньев Ю. Н. Информационные системы и технологии. Экономика. Управление. Бизнес : учеб. пособие для вузов по направлениям 080500 "Менеджмент" и 080100 "Экономика" / Ю. Н. Арсеньев, С. И. Шелобаев, Т. Ю. Давыдова, 2006. - 447.

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