КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Основы управления информационной безопасностью» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Целью преподавания и изучения дисциплины «Основы управления информационной безопасностью» является получение студентами знаний об основных подходах к разработке организационно-распорядительной документации, аудиту, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью информационных систем для успешной профессиональной деятельности.

Задачами дисциплины являются:

- -изучение основ управления информационной безопасностью информационных систем;
- обучение и воспитание культуры информационной безопасности;
- практическая разработка политики безопасности, которая должна охватывать все аспекты информационной безопасности — от методов защиты данных и контроля доступа до правил использования корпоративных устройств и удалённой работы;
- получение практических навыков управления информационной безопасностью в процессе мониторинга, реагирования на инциденты, аудите системы информационной безопасности на предприятии.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ОПК-1.2, ОПК-5.2	Основы информационной безопасности	**Основы управления информационной безопасностью**	

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК1.2. Демонстрирует умение оценивать роль информационной безопасности при решении задачи профессиональной деятельности	Знать: основы информационной безопасности и её составляющие; методы и средства обеспечения информационной безопасности; нормативно-правовую базу в сфере информационной безопасности; потенциальные угрозы и риски, связанные с нарушением режима информационной безопасности. Уметь: анализировать потенциальные угрозы информационной безопасности в своей профессиональной деятельности; разрабатывать меры и мероприятия по обеспечению информационной безопасности; применять специализированные инструменты и системы защиты информации. Владеть: практическими навыками реализации мероприятий по защите информации.
ОПК5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК5.2. Демонстрирует умение решать стандартные профессиональные задачи с целью выполнения требований нормоконтролеров РФ	Знать: процедура прохождения нормоконтроля; стандартные формы отчетности и документирования; порядок действий при проведении проверок контролирующими органами. Уметь: готовить документацию и материалы к проверке нормами контроля; решать проблемы и исправлять недостатки, выявленные проверяющими инстанциями; эффективно взаимодействовать с представителями органов нормоконтроля. Владеть: навыками подготовки и оформления отчетной документации; технологией взаимодействия с представителями государственных структур; способностью оперативно реагировать на запросы и предписания нормоконтролирующих организаций.

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности		ак.часов	
		Всего	По семестрам
			9
1. Контактная работа обучающихся с преподавателем:		51	51
Аудиторные занятия, часов всего, в том числе:		50	50
• занятия лекционного типа		16	16
• занятия семинарского типа:		34	34
практические занятия		-	-
лабораторные занятия		34	34
в том числе занятия в форме практической подготовки		-	-
Консультации		0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		57	57
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		27	27
- выполнение домашних заданий по практическим занятиям		30	30
- подготовка к зачету		-	-
Промежуточная аттестация: зачет		-	-
ИТОГО:	часов	108	108
общая трудоемкость	зач. ед.	3	3

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Основы управления информационной безопасностью.

Концепция информационной безопасности (ИБ). Основные составляющие информационной безопасности. Угрозы информационной безопасности. Базовые вопросы управления информационной безопасностью. Типы управления (иерархический и органический). Метод управления. Цели и задачи управления. Основные черты современных систем управления. Менеджмент – наука управления. Функции управления. Циклическая модель улучшения процессов. Системный подход к управлению. Процессный подход. Система управления. Основные этапы процесса организации информационной безопасностью.

Тема 2. Стандартизация систем и процессов управления

информационной безопасностью

Стандарты информационной безопасности. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на процессы управления информационной безопасности. Оценочные стандарты в информационной безопасности. Отраслевые стандарты в области управления информационной безопасностью. Сертификация системы информационной безопасности.

Тема 3. Политика информационной безопасности

Основные понятия политики безопасности. Понятие политики обеспечения ИБ и политики ИБ организации. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ. Верхний, средний и нижний уровни политики безопасности. Содержание политики ИБ. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности.

Тема 4. Системы управления информационной безопасностью (СУИБ

Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Деятельность по обеспечению ИБ, связь с остальной деятельностью организации. Цель и основные задачи управления по обеспечения ИБ. Область действия СУИБ организации. Модели обеспечения ИБ. Документальное обеспечение СУИБД. Иерархия документов. Функциональная структура управления ИБ организации. Роль высшего руководства в организации системы управления информационной безопасностью.

Тема 5. Оценка рисков информационной безопасности

Основные понятия и определения управления информационными рисками. Анализ рисков информационной безопасности. Процесс управления рисками информационной безопасности. Понятие актива. Инвентаризация активов. Типы активов. Шкала ценности активов. Количественные, качественные и смешанные методы оценки рисков. Шкалы вероятности угроз и уязвимостей, Оценка уровня риска выявление существующих контролей (контрмер). Этапы обработки риска. Управление информационными рисками, стандарты, нормативные документы, рекомендации. Программные средства, используемые для анализа и управления рисками

Тема 6. Процессы управления информационной безопасностью

Основные процессы СУИБ. Циклическая модель процессов СУИБД. Планирование СУИБД. Реализация СУИБД. Этапы внедрения СУИБД, Положение о применимости. Управление инцидентами информационной безопасности. Аудит информационной безопасности. Проверка СУИБД. Совершенствование СУИБД, Документирование процессов СУИБД.

Мониторинг и изменение параметров процесса СУИБД, Стратегии построения и внедрения СУИБ. Организация работы службы безопасности предприятия

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	
1	Основы управления информационной безопасностью	4	6/6	10	ОПК-1.2, ОПК-5.2
2	Стандартизация систем и процессов управления информационной безопасностью	4	6/6	10	ОПК-1.2, ОПК-5.2
3	Политика информационной безопасности	2	6/6	10	ОПК-1.2, ОПК-5.2
4	Системы управления информационной безопасностью (СУИБ)	2	6/6	10	ОПК-1.2, ОПК-5.2
5	Оценка рисков информационной безопасности	2	6/6	10	ОПК-1.2, ОПК-5.2
6	Процессы управления информационной безопасностью	2	4/4	7	ОПК-1.2, ОПК-5.2
	Всего	**16**	**34/34**	**57**	

6. Практические занятия

Практические занятия не предусмотрены.

7. Лабораторные работы

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
1.	Основы управления информационной безопасностью	Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности	6

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
		информации. Угроза раскрытия параметров автоматизированной системы.	
2.	Стандартизация систем и процессов управления информационной безопасностью	Изучение стандартов информационной безопасности. Серия стандартов ISO/IEC 27000 «Информационные технологии.» Анализ методов обеспечения безопасности. Изучение стандартов на процессы управления информационной безопасности. Оценочные стандарты в информационной безопасности. Отраслевые стандарты в области управления информационной безопасностью Изучение методов . сертификации системы информационной безопасности.	6
3.	Политика информационной безопасности	Анализ основных этапов разработки политики безопасности организации. Анализ структуры политики безопасности организации. Примеры частных политик организаций информационной безопасности.	6
4.	Системы управления информационной безопасностью (СУИБ)	Разработка цели и основных задачи управления по обеспечения информационной безопасности организации. Разработка модели обеспечения информационной безопасности организации. Функциональная структура управления ИБ организации.	6
5.	Оценка рисков информационной безопасности	Количественные, качественные и смешанные методы оценки рисков. Шкалы вероятности угроз и уязвимостей, Инвентаризация активов. Типы активов. Шкала ценности активов. Количественные, качественные и смешанные методы оценки рисков. Оценка уровня риска выявление существующих контролей (контрмер). Этапы обработки риска.	6
6.	Процессы управления информационной безопасностью	Управление инцидентами информационной безопасности. Планирование СУИБД. Основные этапы организации работы службы безопасности предприятия. Документирование процессов СУИБД. Аудит состояния информационной безопасности организации.	4
	Всего		**34**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Основы управления информационной безопасностью» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Варианты контрольных работ.

Контрольная работа 1. «Стандартизация систем и процессов управления информационной безопасностью».

Вариант 1.

Задание 1. Структура государственной системы защиты информации.

Задание 2. Идентификация рисков работы со сторонними организациями.

Вариант 2.

Задание 1. Основные документы, определяющие политику РФ в сфере информационной

безопасности.

Задание 2. Методика оценки рисков информационной безопасности по двум и трем факторами.

1. Контрольная работа 2. «Процессы управления информационной безопасностью»

Вариант 1.

Задание 1. Цели аудита состояния информационной безопасности

Задание 2. Этапы процесса реагирования на инциденты

Вариант 2.

Задание. 1 Этапы проведения аудита информационной безопасности

Задание 2. Процедуры идентификация нападающего в процессе реагирования на инцидент

Расчетно-графическое задание

Частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания в области управления информационной безопасностью информации и аргументировать собственную точку зрения. Выполняется группой обучающихся из 3-4 человек. Тема творческого задания:

«Разработка политики безопасности локального и нижнего уровней на экономическом объекте». В качестве объекта исследования группа выбирает и описывает виртуальное предприятие, работающего в различных областях и занимающегося различными сферами деятельности (государственное образовательное учреждение, адвокатская контора, предприятие, занимающееся электронной коммерцией, предприятие связи, поликлиника, аутсорсинговая компания, страховая компания, банк).

Содержание о задания:

1) Описание хозяйственной деятельности выбранного объекта защиты, положения на рынке, конкуренты, контрагенты, клиенты, перечень предоставляемых услуг.

2) Построение модели угроз и нарушителя информационной безопасности.

3) Оценка уровня защищенности выбранного предприятия.

4) Разработка политики безопасности верхнего уровня.

5) Разработка политики безопасности среднего уровня по направлениям (менеджмент активов, физическая безопасность, безопасность финансовой деятельности, управление доступом, менеджмент непрерывности бизнеса, менеджмент инцидентов).

6) Разработка должностной инструкции специалиста-пользователя информационными ресурсами предприятия.

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

1. Концепция информационной безопасности (ИБ). Основные составляющие информационной безопасности.

2. Угрозы информационной безопасности. Базовые вопросы управления информационной безопасностью.

3. Типы управления (иерархический и органический). Метод управления. Цели и задачи управления. Основные черты современных систем управления

4. Менеджмент – наука управления. Функции управления. Циклическая

модель улучшения процессов.

5. Системный подход к управлению. Процессный подход.

6. Система управления. Основные этапы процесса организации информационной безопасностью.

7. Стандарты информационной безопасности. Серия стандартов ISO/IEC 27000«Информационные технологии. Методы обеспечения безопасности».

8. Стандарты на процессы управления информационной безопасностью.

9. Оценочные стандарты в информационной безопасности. Отраслевые стандарты в области управления информационной безопасностью.

10. Сертификация системы информационной безопасности.

11. Основные понятия политики безопасности. Понятие политики обеспечения ИБ и политики ИБ организации.

12. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ. Верхний, средний и нижний уровни политики безопасности. Содержание политики ИБ.

13. Структура политики безопасности организации. Базовая политика безопасности.

14. Специализированные политики безопасности.

15. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием.

16. Деятельность по обеспечению ИБ, связь с остальной деятельностью организации. Цель и основные задачи управления по обеспечения ИБ.

17. Область действия СУИБ организации . Модели обеспечения ИБ.

18. Документальное обеспечение СУИБД. Иерархия документов.

19. Политика СУИБ. Роль высшего руководства в организации системы управления информационной безопасностью.

20. Анализ рисков информационной безопасности.

21. Инвентаризация активов. Понятие актива. Типы активов.

22. Угрозы и уязвимости информационной безопасности. Оценка рисковинформационной безопасности.

23. Основные процессы СУИБ. Циклическая модель процессов СУИБД.

24. Планирование СУИБД. Реализация СУИБД.

25. Этапы внедрения СУИБД, Положение о применимости.

26. Управление инцидентами информационной безопасности. Аудит информационной безопасности.

27. Проверка СУИБД. Совершенствование СУИБД,

28. Документирование процессов СУИБД.

29. Мониторинг и изменение параметров процесса СУИБД,

30. Стратегии построения и внедрения СУИБ.

31. Организация работы службы безопасности предприятия.

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Аверченков, В. И. Служба защиты информации: организация и управление : учебноепособие / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. –186 с. – URL: https://biblioclub.ru/index.php?page=book&id=93356 . – Текст: электронный

2. .Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. —161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный //Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268

3. Парфёнов, Ю. П. Средства управления и защиты информационных ресурсов автоматизированных систем : учебное пособие / Ю. П. Парфёнов. — 2-е изд. — Москва : ФЛИНТА, 2022. — 120 с. — ISBN 978-5-9765-5016-2. — Текст: электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/231707 — Режим доступа: для авториз. пользователей.

4. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш . - 4-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2022. - 336 с. - URL: https://znanium.com/catalog/product/1861657 - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01761-6. - Текст : электронный.

5. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. —URL: https://e.lanbook.com/book/293009 — Режим доступа: для авториз. пользователей

Дополнительная литература:

1.Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : СевероКавказский Федеральный университет (СКФУ), 2015. – 222 с. – URL: https://biblioclub.ru/index.php?page=book&id=458204 – Текст : электронный

2.Внуков, А. А. Защита информации в банковских системах : учебное

пособие длявузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512269

3.Расторгуев, С. П. Основы информационной безопасности : учебное пособие для студентов вузов / С. П. Расторгуев. - 2-е изд., стер. - М. : Академия, 2009. - 187 с. : ил. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 180-181. - ISBN 9785769564864 : 240.90. - Текст : непосредственный.

4.Галатенко, В. А. Основы информационной безопасности : учебное пособие для студентов вузов / В. А. Галатенко ; под ред. В. Б. Бетелина. - Изд. 4-е. - М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2008. - 205 с. -19 (Основы информационных технологий). - Библиогр.: с. 200-202. - ISBN 9785947748215 : 224.00. - Текст : непосредственный.

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/
5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search
6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в

Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, лабораторных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения лабораторных занятий. Лаборатория сетей и систем передачи информации, безопасности компьютерных сетей

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» - - 15, сетевое оборудование; стенды; коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак, средства анализа защищенности компьютерных сетей

Учебная аудитория для проведения лабораторных занятий. Аудитория

информационных технологий

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» - 15, сетевое оборудование.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____