Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 05.09.2026 12:33:11
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"26" февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Технологии защищенного документооборота»

Направление подготовки
«10.05.03 Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист

Формы обучения
Очная

Москва, 2026 г.

Разработчик(и):

Заведующий кафедрой «Информационная безопасность»,
к.т.н., доцент  /И.В. Калуцкий/

Ассистент кафедры «Информационная безопасность»  /А.В. Шорников/

Согласовано:
Заведующий кафедрой «Информационная безопасность»,
к.т.н., доцент  /И.В. Калуцкий/

Руководитель образовательной программы
ст. преподаватель кафедры «Информационная безопасность»  /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 5
3 Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость ... 5
3.2 Тематический план изучения дисциплины ... 6
3.3 Содержание дисциплины ... 7
3.4 Тематика семинарских/практических и лабораторных занятий ... 11
3.5 Тематика курсовых проектов (курсовых работ) ... 11
4 Учебно-методическое и информационное обеспечение 12
4.1 Нормативные документы и ГОСТы ... 12
4.2 Основная литература ... 12
4.3 Дополнительная литература ... 12
4.4 Электронные образовательные ресурсы ... 12
4.5 Лицензионное и свободно распространяемое программное обеспечение ... 13
4.6 Современные профессиональные базы данных и информационные справочные системы ... 13
5 Материально-техническое обеспечение 13
6 Методические рекомендации 13
6.1 Методические рекомендации для преподавателя по организации обучения ... 13
6.2 Методические указания для обучающихся по освоению дисциплины ... 13
7 Фонд оценочных средств 15
7.1 Методы контроля и оценивания результатов обучения ... 15
7.2 Шкала и критерии оценивания результатов обучения ... 16
7.3 Оценочные средства ... 16

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Технологии защищенного документооборота» следует отнести:

- формирование у студентов компетенций в области разработки, внедрения и эксплуатации систем защищенного документооборота в соответствии с требованиями информационной безопасности;
- изучение принципов организации и функционирования систем защищенного документооборота;
- понимание современных методов и технологий защиты информации в документообороте;
- способность разрабатывать документацию с учетом требований безопасности;
- способность оценивать уровень защищенности систем документооборота;
- умение внедрять меры защиты информации в документооборот.

К **основным задачам** освоения дисциплины «Технологии защищенного документооборота» следует отнести:

- овладение навыками и приемами структурирования и форматирования документов, пригодных для человеко-машинной обработки;
- изучение и освоение теоретического материала, как в процессе контактной, так и в ходе самостоятельной работы;
- выполнение предоставленных практических заданий различных форм, как в процессе контактной, так и в ходе самостоятельной работы.

Обучение по дисциплине «Технологии защищенного документооборота» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-13. Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	ИПК-13.1. Знает ГОСТы по оформлению документов по разработке и регламентированию по обеспечению информационной безопасности. ИПК-13.2. Умеет: - разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем. ИПК-13.3. Владеет навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части Б1 «Дисциплины (модули)».

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы ИКТ», «Проектирование и администрирование баз данных».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	5	1-18
	В том числе:			
1.1	Лекции	-		
1.2	Семинарские/практические занятия	-		
1.3	Лабораторные занятия	72	5	1-18
2	**Самостоятельная работа**	**72**	5	1-18
3	**Промежуточная аттестация**		5	19-21
	Экзамен		5	19-21
	Итого			

3.1.2 Очно-заочная форма обучения

Не предусмотрена.

3.1.3 Заочная форма обучения

Не предусмотрена.

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1. Организационно-технические технологии защищенного документооборота	40			20		20
1.1	Раздел 1. Уязвимость конфиденциального документа	8			4		4
1.2	Раздел 2. Технология издания конфиденциальных документов	8			4		4
1.3	Раздел 3. Технология учета конфиденциальных документов	8			4		4
1.4	Раздел 4. Технология защиты в процессе исполнения	8			4		4
1.5	Раздел 5. Обработка конфиденциальных документов в электронном виде	8			4		4
2	Тема 2. Криптографические технологии защищенного документооборота	68					
2.1	Раздел 1. Обеспечение конфиденциальности	16			8		8
2.2	Раздел 2. Обеспечение целостности	8			4		4
2.3	Раздел 3. Аутентификация в процессе документооборота	16			8		8
2.4	Раздел 4. Невозможность отказа от авторства или приписывания авторства	4			2		2
2.5	Раздел 5. Код аутентификации	8			4		4
2.6	Раздел 6. Электронная подпись	8			4		4
2.7	Раздел 7. Генерация ключей	8			4		4
3	Тема 3. Подготовка отчета о технологиях защищенного документооборота	36			18		18
3.1	Раздел 1. Построение блок-схемы защищенного документооборота	8			4		4
3.2	Раздел 2. Разработка набора электронных учетных форм для защищенного документооборота	8			4		4

3.3	Раздел 3. Формирование криптографического модуля с общим интерфейсом	12			6		6
3.4	Раздел 4. Отчет о технологиях защищенного документооборота	8			4		4
	Итого	**144**			**72**		**72**

3.2.2 Очно-заочная форма обучения

Не предусмотрена

3.2.2 Заочная форма обучения

Не предусмотрена

3.3 Содержание дисциплины

Тема 1. Организационно-технические технологии защищенного документооборота

Раздел 1. Уязвимость конфиденциального документа.

Потенциальные угрозы конфиденциальным документам, включая хищение носителей информации, несанкционированный доступ, утрату, повреждение и утечку данных. Анализ уязвимостей на этапах создания, регистрации, передачи, хранения документов и в системах резервного копирования. Классификация внутренних и внешних источников угроз. Последствия реализации угроз: компрометация данных, финансовые и репутационные потери. Методы выявления уязвимостей через аудит систем, анализ журналов доступа, тестирование на проникновение. Комплексная защита с применением правовых, организационных и технических мер на всех этапах жизненного цикла документа.

Раздел 2. Технология издания конфиденциальных документов.

Разработка и оформление конфиденциальных документов с учетом требований информационной безопасности, включая классификацию по степени конфиденциальности и присвоение грифа секретности. Создание документов в бумажном и электронном виде с соблюдением режима секретности. Процедура подготовки проектов, согласования, утверждения и тиражирования документов. Особенности учета, регистрации и контроля версий. Требования к оформлению бланков, нумерации экземпляров и защитных элементов. Правила использования средств защиты при издании документов. Организация электронного документооборота и защита информации при цифровом распространении документов. Нормативное регулирование процессов издания и ответственность за нарушения.

Раздел 3. Технология учета конфиденциальных документов.

Регистрация, маркировка, нумерация и систематизация документов по степени секретности. Организация хранения с соблюдением режима конфиденциальности, ведение журналов движения документов, контроль выдачи и возврата материалов. Процедура списания и уничтожения документов с истекшим сроком хранения, проверка наличия и состояния документов, формирование дел. Учет электронных версий документов, контроль доступа и использование специализированных систем документооборота. Документальное оформление всех операций по движению конфиденциальных материалов, ведение отчетности и инвентаризация.

Раздел 4. Технология защиты в процессе исполнения.

Организация защиты конфиденциальных документов в процессе исполнения, включая контроль доступа и использования. Применение технических и организационных мер защиты при работе с документами. Обеспечение режима конфиденциальности при передаче, копировании и хранении документов. Контроль исполнения документов и соблюдения сроков. Защита информации при внесении изменений и дополнений. Мониторинг действий пользователей и регистрация событий безопасности. Применение криптографических средств при обработке документов. Контроль уничтожения отработанных документов и носителей. Обеспечение целостности и подлинности документов в процессе использования.

Раздел 5. Обработка конфиденциальных документов в электронном виде.

Создание и обработка электронных документов с применением криптографической защиты, электронной подписи и средств аутентификации. Организация защищенного электронного документооборота, включая системы хранения и передачи данных. Применение механизмов шифрования, контроля доступа и целостности информации. Реализация резервного копирования, архивирования и уничтожения электронных документов. Защита каналов передачи данных, протоколов обмена и систем хранения. Обеспечение конфиденциальности, целостности и доступности электронных документов при их создании, хранении и передаче. Контроль версий, изменений и жизненного цикла электронных документов. Применение специализированных систем электронного документооборота и средств технической защиты информации.

Тема 2. Криптографические технологии защищенного документооборота

Раздел 1. Обеспечение конфиденциальности.

Обеспечение конфиденциальности информации посредством криптографических преобразований, включая симметричное и асимметричное шифрование данных. Применение алгоритмов криптографической защиты при хранении, передаче и обработке конфиденциальных документов. Организация защищенного канала связи с использованием криптографических протоколов. Реализация электронной подписи для подтверждения подлинности и целостности документов. Управление криптографическими ключами, их генерация, распределение и хранение. Контроль доступа к зашифрованным данным и криптографическим средствам защиты. Обеспечение стойкости криптографических систем защиты информации. Применение сертифицированных криптографических средств в соответствии с требованиями нормативных документов.

Раздел 2. Обеспечение целостности.

Обеспечение целостности информации в документообороте с применением криптографических методов. Использование хеш-функций и алгоритмов вычисления контрольных сумм для фиксации исходного состояния документов. Применение механизмов контроля целостности при хранении, передаче и обработке документов. Организация проверки целостности на всех этапах жизненного цикла документа: от создания до архивирования. Выявление и регистрация фактов нарушения целостности данных. Использование сертифицированных криптографических средств и соответствие требованиям нормативных документов по защите информации. Мониторинг и аудит процедур контроля целостности в системе документооборота.

Раздел 3. Аутентификация в процессе документооборота.

Реализация механизмов аутентификации пользователей при работе с конфиденциальными документами, включая многофакторную проверку подлинности и

идентификацию субъектов доступа. Применение криптографических методов подтверждения личности, управление учетными данными и цифровыми идентификаторами. Организация защищенных сессий работы с документами, контроль полномочий и прав доступа. Внедрение протоколов взаимной аутентификации, защита от несанкционированного доступа и подмены субъектов. Обеспечение целостности и подлинности учетных данных, механизмов восстановления доступа и смены учетных записей. Реализация централизованного управления идентификационными атрибутами и политиками аутентификации в документообороте.

Раздел 4. Невозможность отказа от авторства или приписывания авторства.

Обеспечение юридической значимости электронных документов через невозможность отказа от авторства. Защита от несанкционированного приписывания авторства посредством криптографической аутентификации. Контроль целостности и подлинности электронных подписей. Управление сертификатами и ключами для подтверждения авторства. Применение протоколов подтверждения действий пользователей при работе с документами. Обеспечение доказательной базы авторства в судебных и административных процедурах.

Раздел 5. Код аутентификации.

Формирование и применение кодов аутентификации для подтверждения целостности и подлинности документов. Реализация алгоритмов вычисления контрольных сумм и хеш-функций. Внедрение механизмов проверки подлинности электронных документов при передаче и хранении. Обеспечение защиты от несанкционированного изменения данных с помощью криптографических методов. Организация верификации подлинности документов на всех этапах документооборота. Применение сертифицированных алгоритмов и протоколов формирования кодов аутентификации. Контроль корректности и актуальности используемых механизмов аутентификации.

Раздел 6. Электронная подпись.

Принципы и механизмы формирования электронной подписи документов, включая алгоритмы создания и проверки подписей. Методы обеспечения юридической значимости электронных документов через криптографическое подписание. Технологии верификации подлинности подписей и подтверждения авторства. Процедуры генерации, распределения и хранения ключей электронной подписи. Стандарты и протоколы реализации электронной подписи в системах документооборота. Контроль целостности подписанных документов и защита от несанкционированного изменения. Требования к инфраструктуре открытых ключей и сертификатам подписи. Реализация электронной цифровой подписи (ЭЦП) для подтверждения неизменности данных и авторства. Управление сертификатами и ключами проверки ЭЦП, обеспечение их актуальности и защищённости.

Раздел 7. Генерация ключей.

Разработка и управление криптографическими ключами для обеспечения защиты информации, включая генерацию, распределение, хранение и обновление ключей. Применение алгоритмов формирования ключей различной длины и сложности. Организация жизненного цикла ключей, контроль их актуальности и замены. Обеспечение безопасности хранения и передачи ключевой информации. Реализация механизмов защиты от компрометации ключей. Управление сертификатами открытых ключей и инфраструктурой открытых ключей. Контроль соответствия ключей установленным требованиям безопасности и нормативным документам. Обеспечение возможности восстановления доступа при компрометации ключей.

Тема 3. Подготовка отчета о технологиях защищенного документооборота

Раздел 1. Построение блок-схемы защищенного документооборота.

Разработка блок-схемы защищенного документооборота, отражающей последовательность этапов движения документов и взаимодействия участников процесса. Визуализация процедур создания, согласования, утверждения, регистрации, хранения и уничтожения документов. Отображение механизмов контроля доступа, шифрования и аутентификации в документообороте. Представление алгоритмов обработки документов в электронном и бумажном виде. Схематичное отображение систем защиты информации, используемых на каждом этапе документооборота. Демонстрация взаимосвязей между компонентами системы документооборота и средствами обеспечения безопасности. Формирование наглядной модели процессов с указанием временных и логических связей между операциями.

Раздел 2. Разработка набора электронных учетных форм для защищенного документооборота.

Разработка унифицированных форм документации для учета и контроля защищенного документооборота, включая регистрационные журналы, акты, ведомости и отчеты. Создание шаблонов учетных карточек, сопроводительных документов и сопроводительной документации. Внедрение электронных форм учета с применением средств криптографической защиты. Разработка процедур заполнения, хранения и актуализации учетных форм. Обеспечение соответствия форм требованиям нормативных документов по защите информации. Организация системы контроля заполнения и ведения учетных документов. Формирование методических рекомендаций по работе с учетными формами. Внедрение автоматизированных систем учета документооборота с сохранением конфиденциальности данных.

Раздел 3. Формирование криптографического модуля с общим интерфейсом.

Проектирование архитектуры модуля, включающей базовые криптографические операции, алгоритмы шифрования и электронной подписи. Реализация механизмов генерации и управления ключами, протоколов обмена ключами и аутентификации. Создание API для взаимодействия с прикладными системами, обеспечивающего выполнение криптографических преобразований. Внедрение средств контроля целостности и проверки подлинности данных. Обеспечение совместимости модуля с различными платформами и операционными системами. Тестирование производительности и безопасности реализованных криптографических функций. Документирование интерфейсов и алгоритмов работы модуля для последующего использования в системах документооборота.

Раздел 4. Отчет о технологиях защищенного документооборота

Систематизация данных о криптографических алгоритмах, механизмах аутентификации и контроля доступа. Оценка эффективности реализованных решений по защите конфиденциальных документов. Формирование рекомендаций по оптимизации процессов документооборота на основе полученных результатов. Документирование архитектуры системы защищенного документооборота, включая описание взаимодействий компонентов и применяемых протоколов безопасности. Представление результатов тестирования криптографических модулей и учетных форм. Составление методических указаний по эксплуатации системы защищенного документооборота. Формирование выводов о соответствии реализованных решений требованиям информационной безопасности.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

Тема 1. Организационно-технические технологии защищенного документооборота

Лабораторная работа №1.1. Подготовка Инструкции по конфиденциальному делопроизводству

Лабораторная работа №1.2. Разработка Приказа об утверждении Инструкции по конфиденциальному делопроизводству

Лабораторная работа №1.3. Формы учета

Лабораторная работа №1.4. Настройки безопасности в MS Word

Лабораторная работа №1.5. Настройки безопасности в MS Excel

Тема 2. Криптографические технологии защищенного документооборота

Лабораторная работа №2.1. Обеспечение конфиденциальности. Шифрование файлов по алгоритмам Магма и Кузнечик

Лабораторная работа №2.2. Обеспечение целостности. Режим выработки имитовставки

Лабораторная работа №2.3. Аутентифицированное шифрование с ассоциированными данными

Лабораторная работа №2.4. Невозможность отказа от авторства или приписывания авторства

Лабораторная работа №2.5. Код аутентификации. Хэширование Стрибог

Лабораторная работа №2.6. Электронная цифровая подпись

Лабораторная работа №2.7. Генерация ключей

Тема 3. Подготовка отчета о технологиях защищенного документооборота

Лабораторная работа №3.1. Построение блок-схемы защищенного документооборота на предприятии

Лабораторная работа №3.2. Разработка набора электронных учетных форм для защищенного документооборота

Лабораторная работа №3.3. Формирование криптографического модуля с общим интерфейсом

Лабораторная работа №3.4. Отчет о технологиях защищенного документооборота

3.5 Тематика курсовых проектов (курсовых работ)

Не предусмотрено учебным планом.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон №63-ФЗ «Об электронной подписи» от 06.04.2010.
2. ГОСТ Р 7.0.109-2024 Система стандартов по информации, библиотечному и издательскому делу.
3. ГОСТ Р 53898-2013 Системы электронного документооборота. Система электронного архива. Общие требования.
4. ГОСТ Р ИСО 15489-1-2007 Система стандартов по информации, библиотечному и издательскому делу.
5. ГОСТ Р 7.0.8-2013 Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело.
6. ГОСТ Р ИСО 23081-1-2008 Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Метаданные для документов.
7. Постановление Правительства РФ №1233 от 03.11.2015 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения».
8. Приказ Росархива от 15.06.2020 №69 «Об утверждении Требований к системам электронного документооборота государственных органов».

4.2 Основная литература

1. Куняев Н.Н., Дёмушкин А.С., Кондрашова Т.В., Фабричнов А.Г. Конфиденциальное делопроизводство и защищённый электронный документооборот: учебник / Н.Н. Куняев, А.С. Дёмушкин, Т.В. Кондрашова, А.Г. Фабричнов. – М.: ИНФРА-М, 2023.
2. Караваева А.В. Технология защищённого документооборота: учебно-методическое пособие / А.В. Караваева. – М.: Юрайт, 2024.
3. Смирнова Г.Н. Электронные системы управления документооборотом: учебное пособие / Г.Н. Смирнова. – СПб.: Питер, 2023.

4.3 Дополнительная литература

1. Кришталюк А. Конфиденциальное делопроизводство и защита коммерческой тайны: учебное пособие / А. Кришталюк. – М.: КноРус, 2023.
2. Грозова О.С. Делопроизводство: учебное пособие для вузов / О.С. Грозова. – М.: Юрайт, 2024.
3. Шувалова Н.Н., Иванова А.Ю. Основы делопроизводства. Язык служебного документа: учебник и практикум / Н.Н. Шувалова, А.Ю. Иванова. – М.: Юрайт, 2024.

4.4 Электронные образовательные ресурсы

1. Электронный курс «Технологии защищенного документооборота» [Электронный ресурс] // Электронная информационно-образовательная среда Московского политеха / URL: https://online.mospolytech.ru/local/crw/course.php?id=9457.

4.5 Лицензионное и свободно распространяемое программное обеспечение

Не предусмотрено.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. КонсультантПлюс: справочная правовая система [Электронный ресурс]. – Режим доступа: свободный. URL: https://www.consultant.ru/.
2. Гарант: информационно-правовой портал [Электронный ресурс]. – Режим доступа: свободный. URL: https://www.garant.ru/
3. eLIBRARY.RU: научная электронная библиотека [Электронный ресурс]. – Режим доступа: свободный. URL: https://elibrary.ru/.
4. Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/ – Режим доступа: для авториз. пользователей.
5. Образовательная платформа «Юрайт» : [сайт]. – URL: https://urait.ru/ – Режим доступа: для авториз. пользователей.
6. Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprsmart.ru/ – Режим доступа: для авториз. пользователей.

5 Материально-техническое обеспечение

Лабораторные работы и самостоятельная работа студентов должны проводиться в специализированной аудитории, оснащенной современной оргтехникой и персональными компьютерами с программным обеспечением в соответствии с тематикой изучаемого материала. Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов. Рабочее место преподавателя должно быть оснащено современным компьютером с подключенным к нему проектором на настенный экран, или иным аналогичным по функциональному назначению оборудованием.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов является самостоятельная работа, а также посещение аудиторных занятий.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях. Оценивание результатов обучения по дисциплине осуществляется на основе балльно-рейтинговой системы (далее – БРС). Максимальный совокупный балл за академический период составляет 100.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

Приветствуется обсуждение самих заданий с другими студентами: можно как давать, так и получать советы по общей стратегии выполнения и изучения материала, давать и получать помощь в проверке гипотез и задумок. Однако выполнять задания и оформлять отчетные материалы студент должен самостоятельно. Делиться отчетными материалами или создавать их совместно запрещено.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

Приведенные ниже правила выставления оценок могут быть изменены, если преподаватель сочтет это необходимым. Важно, чтобы обучающиеся регулярно просматривали план курса, выложенный в СДО, на предмет его обновления или изменения. Достижение компетенций оценивается с помощью лабораторных работ и рубежных контролей. По усмотрению преподавателя студенту могут начисляться дополнительные баллы за активную работу в семестре, участие в научных мероприятиях, нестандартные решения задач и другие достижения. Такие баллы суммируются с основной оценкой, но итоговый результат не может превышать 100 баллов.

После сдачи (загрузки в СДО) лабораторной работы студент должен ее защитить. Во время защиты лабораторной работы преподаватель проверяет содержание отчета, таблиц, исходного кода и других отчетных материалов, а также выполнение критериев и требований задания, а студент отвечает на вопросы преподавателя по предоставленным отчетным материалам, а также теоретическим вопросам, приведенных после текста задания лабораторной работы (при их наличии). Если студент отказывается отвечать на вопросы, или дает полностью неверные ответы, или ответы не по теме, то работа может считаться сданной, но при этом она не оценивается, либо оценка будет снижена на усмотрение преподавателя.

За каждую лабораторную работу устанавливается максимально возможное количество рейтинговых баллов в соответствии с пунктом 7.2. При несвоевременной сдаче работы (позднее срока, установленного в календарно-тематическом плане) количество начисляемых баллов может быть снижено:

- при сдаче работы с опозданием до 3 календарных дней – максимально возможное количество баллов снижается на 10% (оценка за лабораторную работу выставляется с коэффициентом – 0.9);
- при сдаче работы с опозданием от 4 до 7 календарных дней – максимально возможное количество баллов снижается на 25% (оценка за лабораторную работу выставляется с коэффициентом – 0.75);
- при сдаче работы с опозданием свыше 7 календарных дней – начисляется не более 50% от максимально возможного количества баллов за задание (оценка за лабораторную работу выставляется с коэффициентом – 0.5).

В случае наличия уважительных причин для несвоевременной сдачи работы, студент должен обратиться к преподавателю. При возможности, студенты должны заранее сообщать о том, что у них могут возникнуть трудности со своевременной сдачей лабораторной работы или иного полученного задания.

Работа должна быть выполнена студентом самостоятельно: в отчетных материалах должны содержаться результаты работы только за его авторством, по отчетным материалам можно проследить как велась работа, студент может объяснить ход выполнения работы, если же обозначенное выше не соблюдается, то такая работа не считается сданной и не оценивается.

Рубежные контроли выполняются в аудитории индивидуально по варианту задания, выданному преподавателем в назначенные дни. При отсутствии студента в день написания контрольной работы ему дается еще один шанс ее написать на другом занятии в семестре (в том числе и в рамках консультаций преподавателя), но обязательно очно.

7.2 Шкала и критерии оценивания результатов обучения

За посещение аудиторных занятий начисляется до 9 баллов (по 0,5 балла за каждое занятие при условии регулярного посещения). При пропуске занятий количество баллов уменьшается пропорционально количеству пропусков.

За выполнение лабораторных работ начисляется до 47 баллов, более конкретное распределение баллов за лабораторные работы представлено ниже:

- лабораторные работы №1.1–№1.5 – до 2 баллов.
- лабораторные работы №2.1–№2.7 – до 3 баллов.
- лабораторные работы №3.1–№3.4 – до 4 баллов.

За прохождение рубежного контроля начисляется до 8 баллов. За первый и второй рубежный контроль можно получить до 2 баллов, за третий рубежный контроль можно получить до 3 баллов.

Итого, по результатам текущего контроля, не считая дополнительных баллов, студент может получить до 64 баллов.

В свою очередь, по результатам промежуточной аттестации студент может получить до 36 баллов. Студенты, получившие оценку «неудовлетворительно» в ходе промежуточной аттестации, сохраняют ранее накопленную оценку за текущий контроль.

Итоговая оценка по дисциплине (модулю) определяется по следующим критериям:

- «неудовлетворительно» (2) – 0-54 баллов;
- «удовлетворительно» (3) – 55-69 баллов;
- «хорошо» (4) – 70-84 баллов;
- «отлично» (5) – 85-100 баллов.

7.3 Оценочные средства

7.3.1 Текущий контроль

Оценочными средствами текущего контроля являются лабораторные работы, выложенные в курсе СДО по данной дисциплине (модулю), а также прохождение рубежных контролей.

7.3.2 Промежуточная аттестация

Формой оценки знаний в рамках промежуточной аттестации является ***экзамен***.

В ходе промежуточной аттестации студенту выдается билет, содержащий 3 вопроса. За ответ на каждый вопрос студент может получить до 12 баллов. Билет формируется из перечня вопросов, расположенного ниже:

1. Перечислите основные виды угроз конфиденциальным документам и их источники.
2. Опишите методы выявления уязвимостей в системах документооборота.
3. Какие правовые меры защиты применяются к конфиденциальным документам?
4. Каковы основные требования к оформлению конфиденциальных документов?

5. Опишите процедуру подготовки и утверждения конфиденциальных документов.

6. Какие существуют способы маркировки конфиденциальных документов?

7. Как организуется учет и регистрация конфиденциальных документов?

8. Опишите систему контроля версий документов.

9. Какие меры защиты применяются при передаче конфиденциальных документов?

10. Как организуется хранение конфиденциальных документов?

11. Опишите процедуру уничтожения конфиденциальных документов.

12. Какие технические средства защиты используются при работе с документами?

13. Как осуществляется контроль доступа к электронным документам?

14. Опишите систему резервного копирования документов.

15. В чем заключается принцип обеспечения конфиденциальности информации?

16. Опишите основные алгоритмы симметричного шифрования.

17. Как работает система асимметричного шифрования?

18. Какие протоколы используются для организации защищенного канала связи?

19. Как формируется электронная подпись документа?

20. Опишите процесс управления криптографическими ключами.

21. Какие механизмы обеспечивают целостность информации?

22. Как работают хеш-функции в системах защиты?

23. Опишите процесс аутентификации пользователей.

24. Какие существуют методы многофакторной аутентификации?

25. Как обеспечивается невозможность отказа от авторства?

26. Что такое код аутентификации и как он формируется?

27. Опишите жизненный цикл криптографических ключей.

28. Как организуется инфраструктура открытых ключей?

29. Какие технические средства защиты применяются при издании документов?

30. Опишите систему контроля доступа к документам.

31. Как обеспечивается защита при копировании документов?

32. Какие меры защиты применяются при внесении изменений в документы?

33. Опишите систему мониторинга действий пользователей.

34. Как организуется криптографическая защита документов?

35. Какие средства используются для защиты каналов передачи данных?

36. Опишите систему защищенного электронного документооборота.

37. Как организуется шифрование электронных документов?

38. Какие механизмы контроля доступа применяются в электронном документообороте?

39. Опишите систему архивирования электронных документов.
40. Как обеспечивается конфиденциальность при передаче документов?
41. Какие протоколы используются для защиты данных при обмене документами?
42. Опишите систему управления версиями документов.
43. Как проводится аудит систем документооборота?
44. Опишите процедуру тестирования на проникновение.
45. Какие меры предпринимаются при обнаружении утечки информации?
46. Как организуется восстановление после инцидентов безопасности?
47. Опишите систему реагирования на инциденты безопасности.
48. Какие нормативные документы регулируют защиту документов?
49. Каковы последствия нарушения режима конфиденциальности?
50. Как проводится обучение персонала правилам работы с конфиденциальными документами?

Пример экзаменационного билета

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_
по дисциплине

«ТЕХНОЛОГИИ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА»

Направление подготовки
10.05.03 Информационная безопасность автоматизированных систем

ВОПРОСЫ:

1. Что такое код аутентификации и как он формируется?
2. Опишите систему архивирования электронных документов.
3. Опишите процедуру подготовки и утверждения конфиденциальных документов.

Утверждено: _____ / _____ / «__» _____ 20__г.