

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Максимов Алексей Борисович

Должность: директор департамента по образовательной политике

Дата подписания: 12.10.2026 16:48:36

Уникальный идентификатор:

8db180d1a3f02ac9e60521a5672742735c18b1d6

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение
высшего образования**

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета

«Информационных технологий»



 / Д.Г. Демидов /

« 26 » февраль 2026 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность и защита информации**

Направление подготовки

09.03.01 Информатика и вычислительная техника

Профиль подготовки (образовательная программа)

«Информационные системы умных пространств»

Год начала обучения:

2026

Квалификация (степень) выпускника

Бакалавр

Форма обучения

Очная

Москва – 2026

Рабочая программа составлена на основе ФГОС ВО и учебного плана Московского политехнического университета по направлению (специальности) 09.03.01 Информатики и вычислительная техника, по профилю подготовки Информационные системы умных пространств.

Разработчик(и):

к. ф.-м. н., доцент кафедры



/ Т.Т. Идиатуллин /

Согласовано:

Заведующий кафедрой
«СМАРТ-технологии»,
к.т.н., доцент



/ Е.В. Петрунина /

Содержание

1. Цели, задачи и планируемые результаты обучения по дисциплине
2. Место дисциплины в структуре образовательной программы
3. Структура и содержание дисциплины
 - 3.1 Виды учебной работы и трудоемкость
 - 3.2 Тематический план изучения дисциплины (по формам обучения)
 - 3.3 Содержание дисциплины
 - 3.4 Тематика семинарских/практических и лабораторных занятий
 - 3.5 Тематика вопросов для самостоятельного изучения
4. Учебно-методическое и информационное обеспечение
 - 4.1 Нормативные документы и ГОСТы
 - 4.2. Основная литература
 - 4.3 Дополнительная литература
 - 4.4 Электронные образовательные ресурсы
 - 4.5 Лицензионное и свободно распространяемое программное обеспечение
 - 4.6 Современные профессиональные базы данных и информационные справочные системы
5. Материально-техническое обеспечение
6. Методические рекомендации
 - 6.1 Методические рекомендации для преподавателя по организации обучения
 - 6.2 Методические указания для обучающихся по освоению дисциплины
 - 6.3 Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
7. Фонд оценочных средств
 - 7.1 Методы контроля и оценивания результатов обучения
 - 7.2 Шкала и критерии оценивания результатов обучения
- Приложение 1
- Приложение 2

1 Цели, задачи и планируемые результаты обучения по дисциплине

К основным целям освоения дисциплины «Информационная безопасность и защита информации» следует отнести:

- формирование у обучающихся системного представления о содержании информационной безопасности, свойствах защищаемой информации и комплексном характере мер ее защиты;
- ознакомление обучающихся с правовыми, организационными, криптографическими, программными и техническими методами защиты информации, а также с требованиями действующих нормативных документов;
- формирование навыков применения средств защиты информации при эксплуатации и разработке информационных систем, а также оценки защищенности программных и аппаратных средств.

К основным задачам освоения дисциплины «Информационная безопасность и защита информации» следует отнести:

- изучение основных понятий информационной безопасности, свойств конфиденциальности, целостности и доступности информации;
- изучение классификации угроз безопасности информации, источников угроз и построения модели нарушителя;
- изучение правовых основ и системы стандартизации в области защиты информации в Российской Федерации;
- изучение математических основ и практических аспектов применения криптографических методов защиты информации, в том числе отечественных криптографических алгоритмов;
- изучение механизмов идентификации, аутентификации и разграничения доступа, реализуемых в операционных системах и прикладном программном обеспечении;
- приобретение навыков настройки программных средств защиты информации, обеспечения защищенного информационного обмена и контроля целостности данных;
- приобретение навыков выявления и устранения типовых уязвимостей программного обеспечения при его разработке и эксплуатации;
- изучение организационных мер защиты информации, порядка обработки персональных данных и реагирования на инциденты информационной безопасности.

Обучение по дисциплине «Информационная безопасность и защита информации» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-2. Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	ИОПК-2.1. Знает современные программные и программно-аппаратные средства защиты информации, в том числе отечественного производства. ИОПК-2.2. Умеет выбирать средства защиты информации в соответствии с характером обрабатываемой информации и выявленными угрозами. ИОПК-2.3. Владеет навыками применения современных средств защиты информации при решении задач профессиональной деятельности.
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИОПК-3.1. Знает основные понятия информационной безопасности, классификацию угроз, требования нормативных правовых актов и стандартов в области защиты информации. ИОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности с учетом требований информационной безопасности, выявлять угрозы и оценивать их актуальность. ИОПК-3.3. Владеет навыками применения организационных и технических мер защиты информации при работе с информационными системами и информационными ресурсами.
ОПК-5. Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем	ИОПК-5.1. Знает состав и назначение программных и программно-аппаратных средств защиты информации, порядок их установки и настройки. ИОПК-5.2. Умеет выполнять установку, настройку и проверку работоспособности средств защиты информации, в том числе средств криптографической защиты. ИОПК-5.3. Владеет методами установки и конфигурирования системного и прикладного программного обеспечения с учетом требований защищенности.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность и защита информации» относится к числу профессиональных учебных дисциплин базового цикла (Б1.1) основной образовательной программы бакалавриата по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль «Информационные системы умных пространств».

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационно-коммуникационных технологий», «Программирование», «Дискретная математика», «Алгоритмы и структуры данных», «Операционные системы».

Дисциплина обеспечивает изучение дисциплин «Базы данных», «Сети и телекоммуникации», «Веб-технологии», «Проектирование информационных систем», «Промышленная автоматизация и интернет вещей», а также выполнение курсовых работ и выпускной квалификационной работы в части обоснования мер защиты разрабатываемых решений.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, т.е. 108 академических часов, из них аудиторных — 54 часа, самостоятельная работа обучающихся — 54 часа. Форма промежуточной аттестации — экзамен в 3 семестре.

3.1 Виды учебной работы и трудоемкость

(по очной форме обучения)

№ п/п	Вид учебной работы	Количество часов	Семестр 3
1	Аудиторные занятия	54	54
	В том числе:		
1.1	Лекции	18	18
1.2	Семинарские/практические занятия	—	—
1.3	Лабораторные занятия	36	36
2	Самостоятельная работа	54	54
3	Промежуточная аттестация	экзамен	экзамен
	Итого:	108	108

3.2 Тематический план изучения дисциплины

(по очной форме обучения)

№ п/п	Разделы/темы дисциплины	Всего, час.	Лекции	Лабораторные занятия	Самостоятельная работа
1	Тема 1. Основные понятия информационной безопасности. Угрозы и модель нарушителя	12	2	4	6
2	Тема 2. Правовое и организационное обеспечение защиты информации. Стандартизация	12	2	4	6
3	Тема 3. Криптографические методы защиты информации. Симметричные криптосистемы	12	2	4	6
4	Тема 4. Асимметричная криптография, хеш-функции и электронная подпись	12	2	4	6
5	Тема 5. Идентификация, аутентификация и разграничение доступа	12	2	4	6
6	Тема 6. Защита операционных систем. Вредоносное программное обеспечение и антивирусная защита	12	2	4	6
7	Тема 7. Безопасность компьютерных сетей и защищенный информационный обмен	12	2	4	6
8	Тема 8. Безопасность приложений и баз данных. Защищенное программирование	12	2	4	6
9	Тема 9. Защита персональных данных. Управление инцидентами и обеспечение	12	2	4	6

№ п/п	Разделы/темы дисциплины	Всего, час.	Лекции	Лабораторные занятия	Самостоятельная работа
	непрерывности работы				
	Итого	108	18	36	54

3.3 Содержание дисциплины

3.3.1 Содержание лекционных занятий (18 часов)

Тема 1. Основные понятия информационной безопасности. Угрозы и модель нарушителя (2 ч)

Основные понятия и определения: информация, защищаемая информация, информационная безопасность, защита информации, безопасность информационной системы. Свойства защищаемой информации: конфиденциальность, целостность, доступность; дополнительные свойства — подлинность, подотчетность, неотказуемость. Категории информации ограниченного доступа. Объекты и субъекты защиты. Понятие угрозы безопасности информации, классификация угроз по источнику, характеру воздействия и нарушаемому свойству. Естественные и антропогенные, преднамеренные и непреднамеренные угрозы. Понятие уязвимости и канала утечки информации. Модель нарушителя: категории нарушителей, их мотивация, возможности и предположения о доступных ресурсах. Понятие риска информационной безопасности, оценка вероятности реализации угрозы и ущерба. Комплексный подход к защите информации: правовые, организационные, физические, технические, программные и криптографические меры. Банк данных угроз безопасности информации как источник исходных данных для моделирования угроз.

Тема 2. Правовое и организационное обеспечение защиты информации. Стандартизация (2 ч)

Система нормативных правовых актов Российской Федерации в области информационной безопасности. Доктрина информационной безопасности Российской Федерации. Законодательство об информации, информационных технологиях и о защите информации. Правовые режимы информации ограниченного доступа: государственная тайна, коммерческая тайна, служебная тайна, персональные данные. Правовое регулирование применения электронной подписи. Законодательство о безопасности критической информационной инфраструктуры. Ответственность за правонарушения в сфере компьютерной информации. Государственное регулирование и лицензирование деятельности в области защиты информации, функции

уполномоченных органов. Сертификация средств защиты информации и аттестация объектов информатизации. Стандартизация в области защиты информации: национальные стандарты, стандарты серии, посвященной системам менеджмента информационной безопасности. Организационные меры защиты: политика информационной безопасности организации, регламенты и инструкции, разграничение зон ответственности, работа с персоналом, режим доступа в помещения, контроль выполнения требований.

Тема 3. Криптографические методы защиты информации.

Симметричные криптосистемы (2 ч)

Основные понятия криптографии: открытый текст, шифртекст, ключ, шифрование и расшифрование, криптоанализ, криптографическая стойкость. Классификация криптографических систем. Исторические шифры замены и перестановки, их криптоанализ на основе частотного метода. Понятие абсолютно стойкого шифра и условия его реализации. Симметричные криптосистемы: поточные и блочные шифры. Принципы построения блочных шифров: подстановочно-перестановочные сети, сеть Фейстеля, раундовые преобразования и ключевое расписание. Отечественные стандарты блочного шифрования и их характеристики. Режимы работы блочных шифров: простой замены, гаммирования, гаммирования с обратной связью, выработки имитовставки; область применения и особенности каждого режима. Требования к качеству ключевой информации, генерация случайных и псевдослучайных последовательностей. Управление ключами: генерация, распределение, хранение, смена и уничтожение ключей. Задача распределения ключей в симметричных системах.

Тема 4. Асимметричная криптография, хеш-функции и электронная подпись (2 ч)

Идея криптографии с открытым ключом. Односторонние функции и функции с секретом. Математические основы: модульная арифметика, задачи факторизации больших чисел и дискретного логарифмирования, в том числе в группе точек эллиптической кривой. Схемы асимметричного шифрования и их вычислительная сложность в сравнении с симметричными. Протоколы согласования ключей. Гибридные криптосистемы. Криптографические хеш-функции: свойства стойкости к нахождению прообраза и коллизий, области применения, отечественный стандарт хеширования. Контроль целостности данных, коды аутентификации сообщений. Электронная подпись: назначение, схема формирования и проверки, отечественный стандарт электронной подписи. Виды электронной подписи в соответствии с законодательством.

Инфраструктура открытых ключей: сертификат ключа проверки подписи, удостоверяющий центр, цепочки доверия, списки отозванных сертификатов. Средства криптографической защиты информации и требования к ним.

Тема 5. Идентификация, аутентификация и разграничение доступа (2 ч)

Понятия идентификации, аутентификации и авторизации. Факторы аутентификации: основанные на знании, владении и биометрических характеристиках. Парольная аутентификация: требования к паролям, хранение паролей в виде хеш-значений, применение соли, атаки на парольные системы и меры противодействия. Многофакторная аутентификация, одноразовые пароли, аппаратные носители ключевой информации. Биометрическая аутентификация: показатели ошибок первого и второго рода. Аутентификация в распределенных системах, протоколы взаимной аутентификации, единый вход, технологии федеративной аутентификации. Модели разграничения доступа: дискреционная, мандатная, ролевая, атрибутная. Матрица доступа, списки управления доступом, метки конфиденциальности. Принципы наименьших привилегий и разделения обязанностей. Реализация механизмов разграничения доступа в операционных системах. Аудит доступа и регистрация событий безопасности.

Тема 6. Защита операционных систем. Вредоносное программное обеспечение и антивирусная защита (2 ч)

Модель безопасности операционной системы: субъекты, объекты, монитор обращений, доверенная вычислительная база. Механизмы защиты, реализуемые операционными системами: изоляция процессов, защита памяти, уровни привилегий, управление учетными записями, политики безопасности. Настройка защищенной конфигурации операционной системы, отключение неиспользуемых служб, управление обновлениями. Журналирование событий безопасности и его настройка. Классификация вредоносного программного обеспечения: вирусы, черви, троянские программы, программы-вымогатели, шпионские программы, скрытые каналы управления. Механизмы распространения и признаки заражения. Методы обнаружения вредоносного программного обеспечения: сигнатурный анализ, эвристический анализ, поведенческий анализ, контроль целостности, изолированные среды исполнения. Организация антивирусной защиты в организации, централизованное управление и обновление баз. Средства доверенной загрузки и контроля съемных носителей. Отечественные средства антивирусной защиты и защищенные операционные системы.

Тема 7. Безопасность компьютерных сетей и защищенный информационный обмен (2 ч)

Уязвимости стека сетевых протоколов и типовые сетевые атаки: перехват трафика, подмена адресов, атаки на отказ в обслуживании, атаки типа «человек посередине». Сегментация сети и принципы построения защищенной сетевой архитектуры, демилитаризованная зона. Межсетевые экраны: типы, принципы фильтрации, правила и порядок их формирования. Трансляция сетевых адресов. Системы обнаружения и предотвращения вторжений: методы обнаружения, размещение датчиков, реагирование на события. Виртуальные частные сети: назначение, схемы построения, протоколы туннелирования. Защита канала передачи данных с применением протокола TLS: установление защищенного соединения, проверка сертификатов, типовые ошибки конфигурирования. Безопасность беспроводных сетей: механизмы аутентификации и шифрования, характерные угрозы. Средства защиты электронной почты. Мониторинг сетевой активности и анализ трафика. Средства защиты информации отечественного производства для сетевой инфраструктуры.

Тема 8. Безопасность приложений и баз данных. Защищенное программирование (2 ч)

Уязвимости программного обеспечения и причины их появления. Классификация типовых уязвимостей приложений. Недостаточная проверка входных данных как источник большинства уязвимостей: внедрение операторов языка запросов, внедрение команд операционной системы, межсайтовое выполнение сценариев, некорректная обработка путей к файлам. Ошибки управления сессиями и аутентификацией, небезопасные прямые ссылки на объекты, недостатки конфигурации. Ошибки работы с памятью в программах на низкоуровневых языках. Принципы защищенного программирования: проверка и нормализация входных данных, параметризованные запросы, экранирование выводимых данных, минимизация привилегий, безопасная обработка ошибок и исключений, безопасное хранение секретов. Безопасность баз данных: разграничение доступа, шифрование данных при хранении и передаче, аудит операций, резервное копирование. Тестирование защищенности программного обеспечения: статический и динамический анализ кода, анализ зависимостей, применение процессов разработки безопасного программного обеспечения. Требования национальных стандартов к разработке безопасного программного обеспечения.

Тема 9. Защита персональных данных. Управление инцидентами и обеспечение непрерывности работы (2 ч)

Понятие персональных данных, их категории и правовые основания обработки. Оператор персональных данных, его обязанности, права субъекта персональных данных. Информационные системы персональных данных, уровни защищенности и состав необходимых мер защиты. Порядок обработки, трансграничная передача, требования к локализации баз персональных данных. Организационно-распорядительная документация оператора. Понятие инцидента информационной безопасности. Организация мониторинга событий безопасности, средства сбора и корреляции событий. Этапы реагирования на инцидент: обнаружение, локализация, устранение, восстановление, анализ причин. Взаимодействие с государственной системой обнаружения и предупреждения компьютерных атак. Обеспечение непрерывности деятельности: резервное копирование и восстановление данных, стратегии резервирования, планы восстановления после сбоев, показатели допустимого времени восстановления и допустимой потери данных. Аудит информационной безопасности: виды, порядок проведения, оформление результатов. Повышение осведомленности персонала, социальная инженерия и меры противодействия ей.

3.3.2 Содержание лабораторных занятий (36 часов)

Лабораторная работа № 1. Анализ угроз безопасности информации и построение модели нарушителя (4 ч)

Описание информационной системы по индивидуальному заданию, выделение защищаемых информационных активов. Определение перечня актуальных угроз с использованием банка данных угроз безопасности информации. Построение модели нарушителя с обоснованием его категорий и возможностей. Качественная оценка рисков и ранжирование угроз, формирование перечня необходимых мер защиты. Оформление отчета в виде фрагмента модели угроз.

Лабораторная работа № 2. Разработка организационно-распорядительных документов по защите информации (4 ч)

Изучение структуры и содержания политики информационной безопасности организации. Разработка фрагмента политики информационной безопасности для заданной организации: цели, область действия, требования к парольной защите, правила работы со съемными носителями и электронной почтой. Разработка инструкции пользователя по обеспечению

информационной безопасности. Обоснование принятых решений ссылками на нормативные документы.

Лабораторная работа № 3. Симметричное шифрование и режимы работы блочных шифров (4 ч)

Изучение исторических шифров и их криптоанализ на основе частотного анализа. Применение средств симметричного шифрования для защиты файлов и контейнеров данных. Исследование режимов работы блочного шифра, сравнение результатов шифрования одинаковых данных в различных режимах, оценка влияния режима на защищенность. Изучение порядка генерации, хранения и смены ключевой информации.

Лабораторная работа № 4. Хеш-функции, контроль целостности и электронная подпись (4 ч)

Вычисление хеш-значений файлов с применением отечественного и распространенных зарубежных алгоритмов хеширования. Организация контроля целостности набора файлов и обнаружение внесенных изменений. Формирование ключевой пары, создание самоподписанного сертификата, формирование и проверка электронной подписи документа. Изучение структуры сертификата ключа проверки подписи и проверка цепочки доверия.

Лабораторная работа № 5. Настройка идентификации, аутентификации и разграничения доступа (4 ч)

Настройка политики паролей и политики блокировки учетных записей в операционной системе. Создание учетных записей и групп, назначение прав доступа к файловым объектам, реализация принципа наименьших привилегий. Настройка ролевого разграничения доступа для учебного приложения. Настройка многофакторной аутентификации с применением одноразовых паролей. Настройка аудита событий доступа и анализ журналов.

Лабораторная работа № 6. Защищенная конфигурация операционной системы и антивирусная защита (4 ч)

Приведение конфигурации операционной системы к защищенному состоянию: отключение неиспользуемых служб, настройка обновлений, ограничение запуска программ, контроль подключения съемных носителей. Настройка средства антивирусной защиты: параметры проверки, реакция на обнаруженные объекты, обновление баз, формирование отчетов. Проверка работоспособности защиты с применением тестового файла EICAR. Анализ журналов средства защиты.

Лабораторная работа № 7. Защита сетевого взаимодействия (4 ч)

Настройка правил межсетевого экрана для разграничения сетевого доступа на учебном стенде. Анализ сетевого трафика средствами анализатора протоколов, сравнение передачи данных по защищенному и незащищенному протоколам. Настройка защищенного соединения с применением протокола TLS, проверка сертификата сервера. Настройка защищенного туннеля между узлами учебной сети и проверка его работоспособности.

Лабораторная работа № 8. Выявление и устранение типовых уязвимостей приложения (4 ч)

Изучение типовых уязвимостей на специально подготовленном учебном стенде в изолированном сегменте сети. Анализ исходного кода учебного приложения и выявление недостатков проверки входных данных, обработки ошибок и хранения учетных данных. Внесение изменений в код приложения: применение параметризованных запросов, экранирование выводимых данных, корректная обработка исключений, безопасное хранение паролей. Проверка результативности принятых мер и оформление отчета.

Лабораторная работа № 9. Резервное копирование, реагирование на инциденты и аудит защищенности (4 ч)

Разработка схемы резервного копирования данных учебной информационной системы, выполнение полного и инкрементального копирования, проверка восстановления данных. Настройка сбора и централизованного хранения журналов событий безопасности. Разбор учебного сценария инцидента информационной безопасности: анализ журналов, определение последовательности событий, формирование перечня мер по локализации и устранению последствий. Оформление акта по результатам проверки защищенности информационной системы.

3.3.3 Содержание самостоятельной работы обучающихся (54 часа)

Самостоятельная работа обучающихся включает следующие виды деятельности:

- проработка конспектов лекций и изучение разделов дисциплины, вынесенных на самостоятельное изучение, по рекомендованной литературе и электронным образовательным ресурсам;
- изучение нормативных правовых актов и национальных стандартов в области защиты информации;
- изучение методических документов уполномоченных органов и материалов банка данных угроз безопасности информации;

- подготовка к выполнению и защите лабораторных работ, оформление отчетов;
- выполнение индивидуального задания по разработке комплекса мер защиты информации для заданной информационной системы;
- изучение документации на применяемые средства защиты информации, в том числе сертифицированные средства отечественного производства;
- подготовка обзора (реферата) по одному из направлений защиты информации;
- подготовка к тестированию и к экзамену.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
7. Приказ Минобрнауки России от 19.09.2017 № 929 (ред. от 08.02.2021) «Об утверждении федерального государственного образовательного стандарта высшего образования — бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника» (Зарегистрировано в Минюсте России 10 октября 2017 г. № 48489).
8. Академический учебный план. Направление подготовки: 09.03.01 Информатика и вычислительная техника. Профиль: Информационные системы умных пространств. Форма обучения: очная.

9. Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования «Московский политехнический университет» (утверждено приказом Московского Политеха от 01.12.2022 № 1375ОД).
10. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
11. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
12. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
13. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
14. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
15. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.
16. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
17. ГОСТ Р ИСО/МЭК 27001-2021. Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования.

4.2 Основная литература

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2017. — 702 с.
2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд. — Москва : РИОР : ИНФРА-М, 2018. — 336 с.

3. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — 5-е изд. — Москва : ФОРУМ : ИНФРА-М, 2016. — 432 с.
4. Олифер, В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. — Москва : Горячая линия — Телеком, 2016. — 644 с.
5. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие / А. А. Малюк. — Москва : Горячая линия — Телеком, 2016. — 280 с.

4.3 Дополнительная литература

1. Столлингс, В. Криптография и защита сетей: принципы и практика / В. Столлингс ; пер. с англ. — 2-е изд. — Москва : Вильямс, 2001. — 672 с.
2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер ; пер. с англ. — Москва : Триумф, 2012. — 816 с.
3. Смарт, Н. Криптография / Н. Смарт ; пер. с англ. — Москва : Техносфера, 2005. — 528 с.
4. Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. — Москва : Горячая линия — Телеком, 2013. — 229 с.
5. Скабцов, Н. Аудит безопасности информационных систем / Н. Скабцов. — Санкт-Петербург : Питер, 2018. — 272 с.
6. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд. — Москва : ДМК Пресс, 2017. — 434 с.
7. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. — 5-е изд. — Москва : Академия, 2011. — 336 с.

4.4 Электронные образовательные ресурсы

1. Курс в ЛМС Московского политехнического университета. — <https://lms.mospolytech.ru/>
2. Официальный сайт Федеральной службы по техническому и экспортному контролю. — <https://fstec.ru/>
3. Банк данных угроз безопасности информации ФСТЭК России. — <https://bdu.fstec.ru/>
4. Информационные ресурсы Национального координационного центра по компьютерным инцидентам. — <https://safe-surf.ru/>

5. Портал государственных стандартов Российской Федерации. — <https://protect.gost.ru/>
6. Документация по применению средств криптографической защиты информации КриптоПро. — <https://docs.cryptopro.ru/>
7. Документация проекта OpenSSL. — <https://docs.openssl.org/>
8. Единый реестр российских программ для электронных вычислительных машин и баз данных. — <https://reestr.digital.gov.ru/>
9. Электронно-библиотечная система «Лань». — <https://e.lanbook.com/>
10. Электронно-библиотечная система «Юрайт». — <https://urait.ru/>

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Операционная система Windows 10 (или выше) — Microsoft Open License.
2. Офисные приложения Microsoft Office 2016 (или выше) — Microsoft Open License.
3. Операционная система специального назначения Astra Linux Common Edition — отечественное программное обеспечение (свободно распространяемая редакция).
4. Средство криптографической защиты информации «КриптоПро CSP» — отечественное программное обеспечение (учебная лицензия или демонстрационный режим).
5. Криптографическая библиотека и утилиты OpenSSL — свободно распространяемое ПО (лицензия Apache 2.0).
6. Средство шифрования данных VeraCrypt — свободно распространяемое ПО (лицензия Apache 2.0).
7. Средство работы с электронной подписью и шифрованием GnuPG — свободно распространяемое ПО (лицензия GPL).
8. Средство антивирусной защиты Kaspersky Endpoint Security (или Dr.Web Enterprise Security Suite) — отечественное программное обеспечение (академическая лицензия).
9. Анализатор сетевых протоколов Wireshark — свободно распространяемое ПО (лицензия GPL).
10. Система виртуализации Oracle VirtualBox — свободно распространяемое ПО (лицензия GPL).
11. Средство централизованного сбора и анализа журналов событий (Elastic Stack или аналогичное) — свободно распространяемое ПО.
12. Интерпретатор языка программирования Python и система контроля версий Git — свободно распространяемое ПО.

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, компьютер, экран) — 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерного класса, оборудованного современной вычислительной техникой из расчета одно рабочее место на одного обучающегося, а также следующего материально-технического обеспечения:

- персональные компьютеры с установленным программным обеспечением средств защиты информации и системой виртуализации — из расчета одно рабочее место на одного обучающегося;
- изолированный сегмент локальной вычислительной сети (или комплекс виртуальных машин), не имеющий выхода в сеть Интернет, для выполнения работ по анализу защищенности учебных стендов;
- сервер (или выделенная виртуальная машина) для развертывания учебных стендов, средств централизованного сбора журналов и служб каталога;
- персональные носители ключевой информации (USB-токены или смарт-карты) со считывателями — не менее одного комплекта на два рабочих места;
- сетевое оборудование с возможностью настройки правил фильтрации трафика для выполнения работ по защите сетевого взаимодействия;
- доступ к электронной информационно-образовательной среде университета, электронно-библиотечным системам и справочно-правовой системе.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

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, выдержки из нормативных документов, задания для лабораторных работ и учебные стенды, а также заранее проверить работоспособность средств защиты информации и изолированность учебного сегмента сети.

При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия. Лабораторные работы целесообразно выстраивать от анализа угроз и разработки организационных мер к применению криптографических средств, настройке механизмов защиты операционных систем и сетевого взаимодействия и далее к устранению уязвимостей приложений, что формирует у обучающихся представление о комплексном характере защиты информации.

Все работы, связанные с анализом защищенности, проводятся исключительно на специально подготовленных учебных стендах в изолированном сегменте сети. Перед началом выполнения таких работ следует довести до обучающихся требования законодательства об ответственности за неправомерный доступ к компьютерной информации и правила работы в учебной лаборатории. При проверке работ и отчетов следует учитывать не только достигнутый технический результат, но и обоснованность выбранных мер защиты ссылками на нормативные документы, полноту анализа угроз и корректность оформления документов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи с учебным планом. Основой теоретической подготовки обучающихся являются лекции.

В процессе самостоятельной работы обучающиеся закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, изучают нормативные правовые акты, национальные стандарты и документацию на применяемые средства защиты информации, готовятся к защите лабораторных работ и к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Особое внимание при подготовке следует уделять работе с нормативными документами и умению обосновывать выбор мер защиты, а также практическому освоению средств защиты информации. Все практические действия по анализу защищенности допускается выполнять только в отношении учебных стендов и собственных информационных ресурсов; применение изученных методов к сторонним информационным системам без разрешения их владельцев является противоправным.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы обучающихся, оценочные средства текущего контроля успеваемости и промежуточной аттестации:

- подготовка к решению прикладных задач;
- выполнение и защита лабораторных работ, оформление отчетов;
- выполнение индивидуального задания по разработке комплекса мер защиты информации;
- подготовка домашних работ и их защита;
- подготовка обзора (реферата) по направлениям защиты информации;
- тест;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю).

ОПК-2. Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

ОПК-5. Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем.

Показатель	2	3	4	5
знать: основные понятия и свойства информационной безопасности, классификацию угроз и уязвимостей, требования нормативных правовых актов и стандартов, криптографические методы защиты, механизмы разграничения	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие указанных знаний	Обучающийся демонстрирует неполное соответствие указанных знаний, освещена основная, наиболее важная часть материала, допущена одна значительная ошибка или неточность	Обучающийся демонстрирует частичное соответствие указанных знаний, допускаются 2—3 незначительные ошибки и неточности	Обучающийся демонстрирует полное соответствие указанных знаний, свободно оперирует материалом дисциплины

Показатель	2	3	4	5
доступа и защиты сетевого взаимодействия				
уметь: выявлять актуальные угрозы безопасности информации, обосновывать выбор мер защиты со ссылкой на нормативные документы, применять криптографические средства, настраивать механизмы разграничения доступа и выявлять типовые уязвимости приложений	Обучающийся не умеет или в недостаточной степени умеет выполнять указанные действия	Обучающийся демонстрирует неполное соответствие указанных умений, испытывает значительные затруднения при переносе умений на новые ситуации	Обучающийся демонстрирует частичное соответствие указанных умений, допускает незначительные ошибки и неточности	Обучающийся демонстрирует полное соответствие указанных умений, уверенно применяет их в нестандартных ситуациях
владеть: навыками установки и настройки средств защиты информации, обеспечения защищенного информационного обмена и контроля целостности данных, разработки организационно-распорядительных документов и реагирования на инциденты	Обучающийся не владеет или в недостаточной степени владеет указанными навыками	Обучающийся владеет указанными навыками, но допускаются значительные ошибки, проявляется недостаточность навыков по ряду показателей	Обучающийся частично владеет указанными навыками, допускаются незначительные ошибки и затруднения при аналитических операциях	Обучающийся в полном объеме владеет указанными навыками, свободно оперирует приобретенным и знаниями

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по

дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю), методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, свободно оперирует приобретенными знаниями, умениями и навыками, применяет их в ситуациях повышенной сложности. Все лабораторные работы выполнены и защищены, индивидуальное задание выполнено в полном объеме. Присутствовал более чем на $\frac{3}{4}$ занятий по дисциплине.
хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует неполное, но правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо при этом были допущены 2—3 несущественные ошибки. Присутствовал более чем на $\frac{3}{4}$ занятий по дисциплине.
удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. Присутствовал более чем на $\frac{1}{2}$ занятий по дисциплине.
неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, обучающийся испытывает значительные затруднения при оперировании

Шкала оценивания	Описание
	знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Список вопросов для экзамена

1. Информационная безопасность и защита информации: основные понятия и определения.
2. Свойства защищаемой информации: конфиденциальность, целостность, доступность.
3. Категории информации ограниченного доступа и их правовые режимы.
4. Угрозы безопасности информации: понятие и классификация.
5. Уязвимости и каналы утечки информации.
6. Модель нарушителя: назначение, категории нарушителей, их возможности.
7. Понятие риска информационной безопасности и порядок его оценки.
8. Комплексный подход к защите информации. Классификация мер защиты.
9. Банк данных угроз безопасности информации и его применение при моделировании угроз.
10. Система нормативных правовых актов Российской Федерации в области информационной безопасности.
11. Доктрина информационной безопасности Российской Федерации: основные положения.
12. Правовое регулирование обработки персональных данных.
13. Правовое регулирование применения электронной подписи.
14. Лицензирование деятельности в области защиты информации. Сертификация средств защиты информации.
15. Стандартизация в области защиты информации. Системы менеджмента информационной безопасности.
16. Политика информационной безопасности организации: назначение, структура, содержание.
17. Организационные меры защиты информации. Работа с персоналом и режим доступа.
18. Основные понятия криптографии. Криптографическая стойкость.
19. Шифры замены и перестановки. Частотный криптоанализ.
20. Абсолютно стойкий шифр и условия его реализации.

21. Поточные и блочные шифры: сравнительная характеристика.
22. Принципы построения блочных шифров. Сеть Фейстеля.
23. Отечественные стандарты блочного шифрования.
24. Режимы работы блочных шифров и области их применения.
25. Управление ключами: генерация, распределение, хранение и смена ключей.
26. Криптография с открытым ключом: основная идея и математические основы.
27. Схемы асимметричного шифрования. Гибридные криптосистемы.
28. Протоколы согласования ключей.
29. Криптографические хеш-функции: свойства и применение.
30. Контроль целостности данных. Коды аутентификации сообщений.
31. Электронная подпись: схема формирования и проверки, отечественный стандарт.
32. Виды электронной подписи в соответствии с законодательством.
33. Инфраструктура открытых ключей. Сертификаты и удостоверяющие центры.
34. Идентификация, аутентификация и авторизация: соотношение понятий.
35. Парольная аутентификация: требования к паролям, хранение и защита паролей.
36. Многофакторная аутентификация. Одноразовые пароли и аппаратные носители ключей.
37. Биометрическая аутентификация: показатели ошибок первого и второго рода.
38. Дискреционная и мандатная модели разграничения доступа.
39. Ролевая и атрибутная модели разграничения доступа.
40. Принципы наименьших привилегий и разделения обязанностей. Аудит доступа.
41. Модель безопасности операционной системы. Доверенная вычислительная база.
42. Механизмы защиты, реализуемые операционными системами.
43. Настройка защищенной конфигурации операционной системы. Управление обновлениями.
44. Классификация вредоносного программного обеспечения и механизмы его распространения.
45. Методы обнаружения вредоносного программного обеспечения.
46. Организация антивирусной защиты в организации.
47. Типовые сетевые атаки и меры противодействия им.

48. Сегментация сети и построение защищенной сетевой архитектуры.
49. Межсетевые экраны: типы и принципы фильтрации трафика.
50. Системы обнаружения и предотвращения вторжений.
51. Виртуальные частные сети: назначение и схемы построения.
52. Защита канала передачи данных с применением протокола TLS.
53. Безопасность беспроводных сетей.
54. Уязвимости приложений, связанные с недостаточной проверкой входных данных.
55. Ошибки управления сессиями и аутентификацией в приложениях.
56. Принципы защищенного программирования.
57. Безопасность баз данных: разграничение доступа, шифрование, аудит.
58. Тестирование защищенности программного обеспечения. Статический и динамический анализ кода.
59. Персональные данные: понятие, категории, обязанности оператора.
60. Уровни защищенности информационных систем персональных данных и состав мер защиты.
61. Инцидент информационной безопасности. Этапы реагирования на инцидент.
62. Мониторинг событий безопасности. Средства сбора и корреляции событий.
63. Резервное копирование данных и планирование восстановления после сбоев.
64. Аудит информационной безопасности: виды и порядок проведения.
65. Социальная инженерия и меры противодействия ей. Повышение осведомленности персонала.

7.3.2 Примерные темы индивидуальных заданий и обзоров

- Разработка модели угроз безопасности информации для заданной информационной системы.
- Разработка комплекса организационных и технических мер защиты информации для организации заданного профиля.
- Сравнительный анализ отечественных средств криптографической защиты информации.
- Применение электронной подписи в электронном документообороте организации.
- Сравнительный анализ моделей разграничения доступа и их реализации в операционных системах.

- Организация защиты информационной системы персональных данных заданного уровня защищенности.
- Анализ типовых уязвимостей веб-приложений и методов их устранения.
- Построение защищенной сетевой архитектуры предприятия.
- Организация мониторинга событий безопасности и реагирования на инциденты.
- Планирование резервного копирования и восстановления работоспособности информационной системы.