МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)
Электростальский институт (филиал)
Московского политехнического университета

Филиппова О.Д.
2026.10.26
14:22:38
+03'00'

УТВЕРЖДАЮ
Врио директора
Электростальского института (филиала)
Московского политехнического университета
_____/О.Д. Филиппова/
«16» июня 2023 г.

Рабочая программа дисциплины

«Информационная безопасность»

Направление подготовки

27.03.04 Управление в технических системах

Направленность образовательной программы

«Информационные технологии в управлении»

(набор 2023 года)

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная, заочная

Электросталь 2023

Рабочая программа дисциплины разработана в соответствии с:

1) Приказом Министерства науки и высшего образования Российской Федерации от 31 июля 2020 г. № 871, федеральный государственный образовательный стандарт высшего образования – бакалавриат по направлению подготовки 27.03.04 Управление в технических системах.

2) Профессиональным стандартом 40.178 Специалист в области проектирования АСУ ТП, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от «13» марта 2017 г. №272н.

3) Федеральный закон Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);

4) Приказ Министерства образования и науки Российской Федерации от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программа высшего образования – программа бакалавриата, программам специалитета, программам магистратуры».

5) Учебным планом (очной, заочной форм обучения) по направлению подготовки 27.03.04 Управление в технических системах.

Рабочая программа дисциплины включает в себя оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины).

Автор: Д.П. Посевин, доцент, к.ф.-м.н. кафедры ПМиИ
(указать ФИО, ученую степень, ученое звание или должность)

Программа одобрена на заседании кафедры ПМиИ (протокол № 7 от 22.05.2023 г.).

1 Цель и задачи освоения дисциплины

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с Федеральным государственным образовательным стандартом (ФГОС) высшего образования по направлению подготовки 27.03.04 Управление в технических системах.

Цель курса – изучение комплекса проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности, их информационных ресурсов.

Задачи курса – овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты предпринимательской информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения. Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

2 Место дисциплины в структуре ООП бакалавриата

Данная дисциплина относится к числу элективных дисциплин ООП бакалавриата.

Дисциплина «Информационная безопасность» занимает важное место в реализации задач программы подготовки бакалавров по направлению 27.03.04 Управление в технических системах.

Изучение курса «Информационная безопасность» предполагает освоение базовых средств вычислительной техники для решения практических задач. Это способствует повышению уровня информационной культуры каждого студента и обеспечивает конкурентоспособность будущих бакалавров в условиях информационного общества.

Дисциплина «Информационная безопасность» преподаётся в 9-м семестре и, опираясь практически на все предшествующие дисциплины, сама не является уже базовой для других дисциплин.

Студенты, начинающие обучаться данной дисциплине, должны знать основы математического анализа и линейной алгебры, основные структуры алгоритмов, иметь навыки модульного программирования и работы на ЭВМ.

3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций (Таблица 1):

Таблица 1

Код и название компетенции	Индикатор достижения компетенции	Перечень планируемых результатов обучения по дисциплине
УК-9. Способен к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм.	УК-9.1 Владеет навыками использования базовых дефектологических знаний в социальной и профессиональной сферах; УК-9.2 Нетерпимо относится к коррупционному поведению; УК-9.3 Принимает участие в формировании нетерпимого отношения к коррупционному поведению; УК-9.4 Способен проявлять активную гражданскую позицию.	**Знать**: – законодательство Российской Федерации в области защиты информации; – информационно-правовые аспекты безопасности информационных ресурсов, основные проблемы информационного права, информационно-правовых отношений, принципы и способы охраны интеллектуальной собственности; **Уметь**: разрабатывать политику информационной безопасности; **Владеть**: основными направлениями правовой защиты информации.

4 Структура и содержание дисциплины

Общая трудоемкость дисциплины «Информационная безопасность» составляет 4 зачетных единиц 144 часа (из них 128 часов – самостоятельная работа студентов заочной формы и 90 часов – очной формы обучения).

Разделы дисциплины очной формы изучаются в седьмом семестре: лекции – 36 часов, лабораторные занятия – 18 часов, форма контроля – экзамен.

Разделы дисциплины заочной формы изучаются в девятом семестре: лекции – 6 часов, лабораторные занятия – 10 часов, форма контроля – экзамен.

Структура и содержание дисциплины «Информационная безопасность» по срокам и видам работы отражены в Приложении А.

Содержание разделов дисциплины

Лекции

№ раздела	Основное содержание
1	Понятие безопасности. Национальная безопасность. Доктрина безопасности Российской Федерации. Безопасность в экономической сфере России. Цели экономической безопасности, ее содержание и структура. Концепция информационной безопасности России. Международные договоры, доктрины в области информационной безопасности. Информационные права граждан. Соперничество в информационной сфере, информационные войны. Информационная безопасность как институт информационного права. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг. Законодательство о безопасности и защите информации, его структура и содержание. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание. Безопасность функционирования предпринимательской структуры. Основные задачи и уровни реализации информационной безопасности. Понятие атаки на информацию, базовые понятия криптографии.
	Информационное общество, информационная сфера. Определение и эволюция термина «информационная безопасность». Цели, задачи, направления исследования и практической реализации информационной безопасности. Основные угрозы жизненно важным интересам личности, общества, государства, предпринимательства в информационной сфере. Место, цели и задачи информационной безопасности в бизнесе. Информационная безопасность и компьютеризация информационной среды. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации. Симметричные шифры, алгоритм скремблера
	Симметричные шифры, система Фейштеля
	Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения. Соотношение понятий информационной безопасности и безопасности информации. Взаимосвязь понятий информационной безопасности и защиты информации. Научные взгляды, теории и дискуссии. Концепция защиты информации. Понятие и цели защиты информации, формирование и эволюция понятия. Обеспечивающий технологический аспект защиты информации. Асимметричные алгоритмы. Алгоритм RSA
	Понятие аналитической работы, ее цели и задачи. Аналитическая работа по выявлению каналов несанкционированного доступа к информации. Аналитическая работа с источником конфиденциальной информации. Аналитическая работа с источником угрозы конфиденциальной информации. Аналитическая работа с каналом объективного распространения информации. Стадии аналитической работы. Порядок и методика сбора исходных сведений, их анализа и оценки. Экспертные системы. Результаты аналитической работы как основа формирования системы защиты информации и ее совершенствования. Система PGP, операции с ключами и файлами

	Понятие, цели и задачи системы защиты конфиденциальной информации. Принципы построения системы, ее технологичность, иерархичность и факторы эффективности. Принцип разграничения доступа. Принцип регламентации состава защищаемой информации. Принцип персональной ответственности. Принцип коллегиальности контроля. Принципы надежности и превентивности. Принцип эволюции структуры системы в условиях реальных угроз информации. Обязательная совокупность простейших (несистемных) методов и средств защиты конфиденциальной предпринимательской информации. Преимущества и недостатки. Компьютерные технологии и формирование основ системы защиты информации. Место системы в обеспечении безопасности информации в компьютерах, вычислительных системах и сетях. Комплексность системы защиты. Уровни сетевых атак, основные виды сетевых атак.
2	Структура комплексной системы защиты информации (КСЗИ). Содержание элемента правовой защиты информации. Содержание элемента организационной защиты информации. Содержание элемента инженерно-технической защиты информации и технических средств охраны. Содержание элемента программно-аппаратной защиты информации. Содержание элемента криптографической защиты информации. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом предпринимательской структуры и видами угроз. Система защиты информации в малом бизнесе. Стоимость системы и критерии выбора системы. Сертификация систем и средств защиты информационных систем и информационных ресурсов. Понятие межсетевого экрана, его базовые компоненты и их функции.
	Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Критерии оценки защищённости систем информационной безопасности. Международные критерии. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации. Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макро-вирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Методика применения антивирусных программ. Архитектура межсетевых экранов, типы архитектур
	Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. Основные виды вирусов, классификация антивирусных программ

Лабораторные занятия

№ раздела	План занятия, основное содержание
1	Алгоритм скремблера, бинарные файлы
	Система Фейштеля, текстовые файлы, бинарные файлы
	Система PGP, операции с ключами ,буфером обмена и файлами
	Деловая игра «Задание»
2	Конфигурирование межсетевого экрана Winroute
	Конфигурирование антивируса ESET

Самостоятельная работа обучающегося

Кол.час	Основное содержание
90/128	Изучение учебного материала по конспектам лекций, литературным источникам без составления конспекта, плана
	Система Фейштеля. Российский стандарт симметричного шифра.
	Система PGP, операции с ключами, буфером обмена и файлами
	Межсетевой экран, его базовые компоненты и их функции.
	Конфигурирование межсетевого экрана Winroute.

5 Образовательные технологии

При подаче лекционного материала используются:

– электронные средства представления информации по курсу (электронная версия конспекта лекций, презентаций к лекциям и материала для индивидуальных работ).

– мультимедийные средства при подаче лекционного материала.

При реализации учебной работы используются такие виды активной и интерактивной формы проведения занятий, как разбор задач, тестовые задания.

Лабораторные занятия проходят в виде проверки знаний путём опроса, анализа практических примеров (комплексных бизнес-кейсов), полученных в лекционном материале знаний, обсуждения типичных проблемных ситуаций, тестирования.

6 Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- вопросы для устного опроса,
- вопросы к экзамену,
- фонд тестовых заданий.

Образцы контрольных вопросов и заданий для проведения текущего контроля приведены в Приложении Б.

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	Содержание компетенции
УК-9	Способен к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм.

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.2 Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (Таблица 2).

Таблица 2

Показатель	Критерии оценивания			
	2	3	4	5
УК-9. Способен к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм.				
Знать: – законодательство Российской Федерации в области защиты информации; – информационно-правовые аспекты безопасности информационных ресурсов, – основные проблемы информационного права, информационно-правовых отношений, принципы и способы охраны интеллектуальной собственности.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие знаний, законодательство Российской Федерации в области защиты информации.	Обучающийся демонстрирует неполное соответствие знаний, информационно-правовые аспекты безопасности информационных ресурсов. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие знаний, основные проблемы информационного права, информационно-правовых отношений, принципы и способы охраны интеллектуальной собственности, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие необходимых знаний основных проблем информационного права, информационно-правовых отношений, принципы и способы охраны интеллектуальной собственности, свободно оперирует приобретенными знаниями.
Уметь: разрабатывать политику информационной безопасности.	Обучающийся не умеет или в недостаточной степени умеет разрабатывать политику информационной безопасности	Обучающийся демонстрирует неполное соответствие умений, разрабатывать политику информационной безопасности. Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие умений, разрабатывать политику информационной безопасности. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, разрабатывать политику информационной безопасности. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
Владеть: основными направлениями правовой защиты информации.	Обучающийся не владеет или в недостаточной степени владеет основными направлениями правовой защиты информации	Обучающийся владеет основными направлениями правовой защиты информации в неполном объеме, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет основными направлениями правовой защиты информации, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет основными направлениями правовой защиты информации свободно применяет полученные навыки в ситуациях повышенной сложности.

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».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Информационная безопасность» (прошли промежуточный контроль, выполнили практические работы).

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в Приложении Б к рабочей программе.

7 Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1 Господарик Ю.П., Пашковская М.В. Международная экономическая безопасность: учебник. – М.: Университет «Синергия», 2016. – 417с. https://biblioclub.ru/index.php?page=book_red&id=455420&sr=1

2 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы– М.: Питер, 2009. - 958 с.

б) дополнительная литература:

1 Расторгуев С.П. Основы информационной безопасности: Учебное пособие. – М.: Академия, 2007. – 192 с.

2 Фомичёв В.М. Дискретная математика и криптология. – М.: Диалог-МИФИ, 2003. – 456 с.

3 Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: «Наука и техника», 2010. – 325 с.

в) программное обеспечение и интернет-ресурсы

Программное обеспечение:

– Операционная система Windows 7 DreamSpark № 9d0e9d49-31d1-494a-b303-612508131616

– Офисные приложения, Microsoft Office 2013 (или ниже) – Microsoft Open License. Лицензия № 61984042

– Microsoft Project 2013 Standart 32- bit/x64 Russian.

– Антивирусное ПО Avast (бесплатная версия)

– Turbo C++ (свободная лицензия)

– TurboPascal 7.1 (свободная лицензия)

– VBA 7.0 (свободная лицензия)

– Delphi 7.0 (бесплатно для образовательных целей)

– LinuxUbuntu (свободная лицензия)

– Arduino 1.6.5 (свободная лицензия)

– 1С: Предприятие 8.2 (версия для обучения)

– AnyLogic (версия пакета имитационного моделирования бесплатно для образовательных целей)

– ForexOptimizer, LiteUpdateDevelop – программное обеспечение для работы на учебном сегменте рынка Форекс (свободная лицензия)

– XAMPP (свободная лицензия)

– MySQL (свободная лицензия).

Каждый студент обеспечен индивидуальным неограниченным доступом к электронным библиотекам университета (elib.mgup; lib.mami.ru/lib/content/elektronyy-katalog), к электронным каталогам вузовских библиотек и крупнейших библиотек Москвы (http://window.edu.ru), к электронно-библиотечным системам (электронным библиотекам):

Электронно-библиотечная система «Лань» (www.e.lanbook.com): Доступ к коллекциям «Инженерно-технические науки», «Экономика и менеджмент»;

ЭБС «Университетская библиотека онлайн» (https://biblioclub.ru);

Национальная электронная библиотека (http://нэб.рф);

Электронная библиотека Московского политехнического университета **(**http://lib.mami.ru/**);**

Научная электронная библиотека «КИБЕРЛЕНИНКА» (http://cyberleninka.ru/)

Изучение дисциплины «Информационная безопасность» предполагает использование мультимедийных учебных аудиторий или аудиторий, оснащенных видеопроектором и компьютером.

8 Материально-техническое обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория лекционного типа № 501, учебно-лабораторный корпус, 144000, Московская область, г. Электросталь, ул. Первомайская, д.7	Комплект мебели, переносной мультимедийный комплекс (проекционный экран, проектор, ноутбук)
Учебная аудитория для занятий семинарского типа № 303, учебно-лабораторный корпус, 144000, Московская область, г. Электросталь, ул. Первомайская, д.7	Комплект мебели, компьютеры, проектор.
Компьютерные классы № 305, 306, учебно-лабораторный корпус, 144000, Московская область, г. Электросталь, ул. Первомайская, д.7	Комплект мебели, компьютеры, проектор.

9 Методические рекомендации для самостоятельной работы студентов

Время, отводимое на самостоятельную работу должно затрачиваться студентами для изучения лекционного материала, выполнение практических задач и подготовку к лабораторным работам (при их наличии). Самостоятельная работа студентов в ходе семестра является важной составной частью учебного процесса и необходима для закрепления и углубления знаний, полученных в период сессии на лекциях, практических и интерактивных занятиях, а также для индивиду-

ального изучения дисциплины в соответствии с программой и рекомендованной литературой.

Лекции и частично практические занятия базируются на литературных источниках, указанных в основном и дополнительном списках литературы, приведенных в рабочей программе. Более детальные и подробные рекомендации по использованию в самостоятельной работе литературных источников, а также программного обеспечения, даются на занятиях преподавателем. На этих же занятиях преподаватель передает студентам интернет-ссылки или на флэшке видеоматериалы по лабораторным работам.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. В конце рабочей программы есть контрольные вопросы, по которым студент имеет возможность самоконтроля выполненной работы.

В ряде дисциплин предусмотрены домашние задания, которые выполняются студентами в указанные преподавателем периоды времени (семестра). При этом студентом используются возможности представления выполненной работы в виде реферата, презентации или эссе.

При подготовке к контрольным мероприятиям, в том числе, защите курсовых проектов (работ), экзаменам и зачетам студент пользуется конспектами лекций, примерами выполнения практических расчетов, видеоматериалами и заполненными на лабораторных работах бланками по их выполнению. Преподавателем контроль качества самостоятельной работы может осуществляться с помощью устного опроса на лекциях или практических занятиях, тестирования, проведения коллоквиума, защиты презентации, эссе или рефератов, проверки письменных контрольных работ и реферативных обзоров. Перед контрольными мероприятиями преподаватель выдает примерные вопросы, основная доля которых представлена в рабочей программе.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельной темы учебной дисциплины. Самостоятельная работа является обязательной для каждого обучающегося, ее объем определяется учебным планом. При самостоятельной работе студент взаимодействует с рекомендованными материалами при участии преподавателя в виде консультаций. Для выполнения самостоятельной работы предусмотрено методическое обеспечение. Электронно-библиотечной система (электронная библиотека) обеспечивает возможность индивидуального доступа каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет.

10 Методические рекомендации для преподавателя

1. Изучив глубоко содержание учебной дисциплины, целесообразно разработать матрицу наиболее предпочтительных методов обучения и форм самостоятельной работы студентов, адекватных видам лекционных и семинарских занятий.
2. Необходимо предусмотреть развитие форм самостоятельной работы, выводя студентов к завершению изучения учебной дисциплины на её высший уровень.
3. Организуя самостоятельную работу, необходимо постоянно обучать студентов методам такой работы.
4. Вузовская лекция - главное звено дидактического цикла обучения. Её цель – формирование у студентов ориентировочной основы для последующего усвоения материала методом самостоятельной работы. Содержание лекции должно отвечать следующим дидактическим требованиям:

- изложение материала от простого к сложному, от известного к неизвестному;
- логичность, четкость и ясность в изложении материала;
- возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности студентов;
- опора смысловой части лекции на подлинные факты, события, явления, статистические данные;
- тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью студентов.

Преподаватель, читающий лекционные курсы в вузе, должен знать существующие в педагогической науке и используемые на практике варианты лекций, их дидактические и воспитывающие возможности, а также их методическое место в структуре процесса обучения.

5. При изложении материала важно помнить, что почти половина информации на лекции передается через интонацию. В профессиональном общении исходить из того, что восприятие лекций студентами заочной формы обучения существенно отличается по готовности и умению от восприятия студентами очной формы.
6. При проведении аттестации студентов важно всегда помнить, что систематичность, объективность, аргументированность – главные принципы, на которых основаны контроль и оценка знаний студентов. Проверка, контроль и оценка знаний студента, требуют учета его индивидуального стиля в осуществлении учебной деятельности. Знание критериев оценки знаний обязательно для преподавателя и студента.

11 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение по дисциплине «Информационная безопасность» инвалидов и лиц с ограниченными возможностями здоровья (далее ОВЗ) осуществляется преподавателем с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучающиеся с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

По дисциплине «Информационная безопасность» обучение инвалидов и лиц с ограниченными возможностями здоровья может осуществляться как в аудитории, так и дистанционно с использованием возможностей электронной образовательной среды (образовательного портала) и электронной почты.

Приложение А к рабочей программе

Структура и содержание дисциплины «Информационная безопасность»
по направлению подготовки 27.03.04 Управление в технических системах
(бакалавр)
Заочная форма обучения

n/n	Раздел	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов *						Формы аттестации	
		Л	П/С	Лаб	СРС	КСР	ДС	УО	РЗЗ	К.Р	К/р	Т	Э	З
	Девятый семестр													
1.1	Основы практической криптографии	4		6	66			+				+		
1.2	Сетевая и антивирусная защита	2		4	62			+				+		
	Форма аттестации							**1**				**1**	**Э**	
	Всего часов по дисциплине в девятом семестре	**6**		**10**	**128**									

Очная форма обучения

n/n	Раздел	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов *						Формы аттестации	
		Л	П/С	Лаб	СРС	КСР	ДС	УО	РЗЗ	К.Р	К/р	Т	Э	З
	Седьмой семестр													
1.1	Основы практической криптографии	20		12	45			+				+		
1.2	Сетевая и антивирусная защита	16		6	45			+				+		
	Форма аттестации							**1**				**1**	**Э**	
	Всего часов по дисциплине в седьмом семестре	**36**		**18**	**90**									

*** – Сокращения форм оценочных средств см. в Приложении** В.

Приложение Б к рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)
Электростальский институт (филиал)
Московского политехнического университета

Направление подготовки **27.03.04 Управление в технических системах**

ОП (образовательная программа**) «Информационные технологии в управлении»**

Форма обучения: **очная, заочная**

Виды профессиональной деятельности:

проектно-конструкторская;

организационно-управленческая деятельность

Кафедра Прикладной математики и информатики

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Информационная безопасность»

(набор 2023 года)

Состав: 1) Паспорт фонда оценочных средств
2) Описание оценочных средств:
вопросы для устного опроса,
вопросы и задачи к экзамену,
фонд тестовых заданий.

Составители:

Д.П. Посевин

Электросталь 2023

Паспорт
фонда оценочных средств по дисциплине
«Информационная безопасность»

Направление подготовки

27.03.04 Управление в технических системах

Направленность образовательной программы

«Информационные технологии в управлении»

Уровень
бакалавриат
Форма обучения
очная, заочная

Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1 Основы практической криптографии	УК-9	УО, Т
2 Сетевая и антивирусная защита	УК-9	УО, Т
Промежуточная аттестация		экзамен

Показатель уровня сформированности компетенций

Информационная безопасность				
ФГОС ВО **27.03.04 Управление в технических системах**				
КОМПЕТЕНЦИИ **Индекс** **Формулировка**	**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средства****	**Степени уровней освоения компетенций**
УК-9 Способен к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм.	**Знать**: – законодательство Российской Федерации в области защиты информации; – информационно-правовые аспекты безопасности информационных ресурсов, основные проблемы информационного права, информационно-правовых отношений, принципы и способы охраны интеллектуальной собственности; **Уметь**: разрабатывать политику информационной безопасности; **Владеть**: основными направлениями правовой защиты информации.	лекции, самостоятельная работа, лабораторные занятия	УО, Т; Э	**Базовый уровень:** воспроизводство полученных знаний в ходе текущего контроля **Повышенный уровень:** практическое применение полученных знаний в процессе подготовки к лабораторным работам.

Формы текущего контроля успеваемости студентов: защита лабораторных работ по индивидуальным вариантам, тестирование.

Форма промежуточной аттестации: экзамен в письменной форме.

Контрольные вопросы и задачи для проведения промежуточного контроля формирование компетенций УК-9	
№	**Вопросы**
1	Понятие атаки на информацию. Статистика атак.
2	Основные категории информационной безопасности.
3	Базовые понятия криптографии. Основные характеристики алгоритмов шифрования.
4	Понятие hash-функции, цифровые подписи.
5	Алгоритм скремблера, работа шифра
6	Последовательности ключей максимальной длины, неприводимые многочлены
7	Алгоритм-схема Фейштеля в симметричных алгоритмах.
8	Асимметричные алгоритмы, общий алгоритм работы
9	Алгоритм RSA, пример
10	Система PGP, общая схема работы, генерация ключей
11	Система PGP, основные операции с ключами и файлами, буфером обмена
12	Понятие достоверности ключа и методы её определения в системе PGP.
13	Понятие межсетевого экрана, его базовые компоненты и их функции.
14	Архитектура межсетевых экранов, типы архитектур
15	Фильтрация пакетов. Информация для правил фильтрации. Стеки правил.
16	Механизм NAT и его использование
17	Классификация компьютерных вирусов
18	Основные возможности пакета ESET, настройка.
19	Компоненты межсетевого экрана Winroute
20	Фильтрация пакетов с помощью экрана Winroute
Задачи	
1	Закодировать шифром «скремблер» с разрядностью n=5 и маской mask=27 число 30, рассматривая его как последовательность бит.
2	Построить в виде таблицы стек правил фильтрации на сетевом интерфейсе cIP-адресом 132.151.141.65, который обеспечивает реализацию следующей политики: а) пропускаются пакеты TELNET-службы только от(для) сервера с IP-адресом 10.99.99.10; б) не допускаются входящие подключения службы FTP: в) не допускаются входящие запросы PING. Считать, что фильтр обеспечивает анализ всех основных признаков пакетовпротоколов TCP,UDP,ICMP.
3	Закодировать шифром «скремблер» с разрядностью n=5 и маской mask=11 число 17, рассматривая его как последовательность бит.
4	Написать процедуру зашифровки блока данных с длиной N=128 по схеме Фейштеля, используя ключ с длиной L=96 и производящую функцию F(X,Key):F(X,Key)=((X shl 5)-Key[*]) XOR ((X shr 3)-Key[*]). Основная шифрующая операция – операция сложения.
5	Закодировать шифром «скремблер» с разрядностью n=6 и маской mask=17 число 34, рассматривая его как последовательность бит.
6	Написать процедуру расшифровки блока данных с длиной N=128, если он был зашифрован по схеме Фейштеля с длиной ключа L=96 и производящей функцией F(X,Key): F(X,Key)=((Xshr 5) XORKey[1]) + ((Xshl 7) XORKey[2])+Key[3].Последовательность шифрования блоков – циклическая (1←2←3 …←n←1),основная шифрующая операция – операция вычитания, число раундов равно 16.
7	Написать процедуру расшифровки блока данных с длиной N=96, если он был зашифрован по схеме Фейштеля с длиной ключа L=96 и производящей функцией F(X,Key): F(X,Key)=)=((Xshl 5)-Key[1]) XOR ((Xshr 3)-Key[2]) XORKey[3].Последовательность шифрования блоков – циклическая (1←2←3 …←n←1),основная шифрующая операция – операция сложения, число раундов равно 32.
8	Построить в виде таблицы стек правил фильтрации на сетевом интерфейсе cIP-адресом

	72.154.211.31, который обеспечивает реализацию следующей политики: а) пропускаются пакеты FTP-службы только от (для) прокси-сервера с IP-адресом 10.201.1.100; б) не допускаются входящие подключения службы TELNET: в) не допускаются исходящие запросы PING. Считать, что фильтр обеспечивает анализ всех основных признаков пакетовпротоколов TCP,UDP,ICMP.

Контрольные вопросы и задания для проведения текущего контроля
формирование компетенций УК-9

1 Системы управления доступом в Интернет и контроля корпоративной электронной почты
2. Утечки информации: источники, правовые и технологические аспекты борьбы.
3. Утилизация данных: проблемы повторного использования.
4. SELinux: реализация мандатного (принудительного) контроля доступа.
5. Распределенные системы управления доступом LDAP и ActiveDirectory: описание и сравнение.
6. Rootkits –примеры (для Windows, для *nix), методы и средства выявления и противодействия
7. Применение технологий «honeypots» для обеспечения сетевой безопасности.
8. SQL-инъекции: принципы атак, способы их обнаружения и противодействия.
9. Атаки межсайтового скриптинга (XSS-атаки): принципы атак, способы их обнаружения и противодействия.
10.Проблемы противодействия фишингу и фармингу.
11.P2P-приложения: тенденции развития и аспекты безопасности.
12.Безопасность Web-браузеров.
13.Безопасность беспроводных технологий.
14.Виртуальные частные сети (VPN) – технологии и средства организации.
15.Биометрические системы аутентификации: принципы, технологии и перспективы.
16.Средства взлома парольных систем и противодействие им.
17.Распределенные атаки отказ в обслуживании и противодействие им.
18.«Электронное государство» - общее понятие, технологии, аспекты безопасности
19.Проблемы безопасности «виртуальных» инфраструктур e-commerce.
20.Расследование ИТ-инцидентов
21.Эволюция вредоносного ПО (malware) и средств борьбы с ним.
22.СПАМ: способы распространения, принципы и средства противодействия
23.Методы защиты от нелегального использования ПО (и др. ITресурсов).
24.Безопасность информационных систем построенных с использованием с использованием технологий виртуализации.
25.Методы и средства борьбы и противодействия внутренним нарушителям.
26.Защита персональных данных, типовые решения.
27.Аспекты защиты информации в системах автоматизированного управления технологическими процессами.
28.Понятие политики безопасности

Критерии оценки устного опроса (собеседования)

Оценка «отлично» выставляется студенту, если студент ориентируется в теоретическом материале; имеет представление об основных подходах к излагаемому материалу; знает определения основных теоретических понятий излагаемой темы, умеет применять теоретические сведения для анализа практического материала, в основном демонстрирует готовность применять теоретические знания в практической деятельности и освоение большинства показателей формируемых компетенций.

Оценка «хорошо» выставляется студенту, если студент ориентируется в теоретическом материале; имеет представление об основных подходах к излагаемому материалу, но затрудняется в ответах на некоторые вопросы; знает определения основных теоретических понятий из-

лагаемой темы, но не в полной мере отражает суть рассматриваемой проблемы, в основном умеет применять теоретические сведения для анализа практического материала, в основном демонстрирует готовность применять теоретические знания в практической деятельности и освоение большинства показателей формируемых компетенций.

Оценка «удовлетворительно» выставляется студенту, если показаны недостаточные знания теоретического материала, основных понятий излагаемой темы, не всегда с правильным и необходимым применением специальных терминов, понятий и категорий; анализ практического материала был нечёткий.

Оценка «неудовлетворительно» выставляется в случаях, когда не выполнены условия, позволяющие выставить оценку «удовлетворительно».

Тест по дисциплине
формирование компетенций УК-9
Как выполнять тест

1 При работе с тестами сборника нельзя пользоваться дополнительными материалами.
2 Выполнять задания нужно самостоятельно, не отвлекаясь, в порядке их следования.
3 Выбирать надо ответ, который представляется наиболее правильным.
4 Время тестирования определяет преподаватель (как правило 20- 30 минут).
5 Не нужно долго размышлять над заданием. Если не удалось его выполнить за 2-3 минуты, переходите к следующему заданию. При работе с тестом следует выполнять сначала самые легкие, доступные задания. Если останется время, можно потом вернуться к заданию, вызвавшему затруднения.
6 Во время тестирования с вопросами обращайтесь только к преподавателю.

Как оценить свой результат

Успешность выполнения одного тематического теста, ориентировочно можно оценить, исходя из следующего соответствия:

- удовлетворительно 50 %-74%;
- хорошо 75%-94 %;
- отлично 95%-100 %.

Преподаватель может скорректировать шкалу оценок с учетом особенностей группы.

Вариант №1

1. Свойства информации в форме сообщения:
(укажите правильный вариант)
a. идеальность субъективность
c. информационная неуничтожаемость
d. динамичность
e. материальность
f. накапливаемость
2. Свойства информации в форме сведений: (укажите правильный вариант)
a. материальность
b. измеримость
c. сложность
d. проблемная ориентированность
e. накапливаемость
3. Информационная сфера – это … , … , … , … .
4. Первая классификация национальных интересов:
a. интересы …
b. интересы …
c. интересы …
5. Общие методы обеспечения информационной безопасности:
a. …
b. …

c. …

6. Информация – наиболее ценный … современного общества.

7. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?

a. Документы
b. Персонал
c. Организационные единицы
d. Промышленные образцы
e. Научный инструментарий

8. Поставьте в порядке важности национальные интересы:

a. Информационное обеспечение государственной политики Российской Федерации.
b. Развитие современных информационных технологий, отечественной индустрии информации.
c. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.
d. Защита информационных ресурсов от несанкционированного доступа

9. Допишите различные подходы к понятию информации:

a. информация …
b. информация …
c. … информация

10. Составляющие национальной безопасности:

a. …
b. …
c. …
d. …
e. …
f. …
g. …
h. …

11. Общие методы обеспечения национальной безопасности:

a. …
b. …
c. …

12. Основные объекты воздействия в информационной войне?

a. …
b. …
c. …
d. …
e. …

13. Перечислите информационное оружие:

a. …
b. … средства
c. … генераторы
d. средства …
e. средства …

14. Война, есть продолжение … другими, насильственными средствами.

15. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов … , … , … .

Вариант №2

1. Допишите различные подходы к понятию информации:

d. информация …
e. информация …
f. … информация

2. Составляющие национальной безопасности:

i. … b. … c. … d. …
e. … f. … g. …

3. Информация – наиболее ценный … современного общества.

4. Поставьте в порядке важности национальные интересы:

e. Информационное обеспечение государственной политики Российской Федерации.
f. Развитие современных информационных технологий, отечественной индустрии информации.
g. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.
h. Защита информационных ресурсов от несанкционированного доступа

5. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?

f. Документы
g. Персонал
h. Организационные единицы
i. Промышленные образцы
j. Научный инструментарий

6. Война, есть продолжение … другими, насильственными средствами.

7. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов … , … , … .

8. Перечислите информационное оружие:

f. …
g. … средства
h. … генераторы
i. средства …
j. средства …

9. Информационная сфера – это … , … , … , … .

10. Первая классификация национальных интересов:

d. интересы …
e. интересы …
f. интересы …

11. Общие методы обеспечения информационной безопасности:

d. … b. … c. …

12. Общие методы обеспечения национальной безопасности:

d. …
e. …
f. …

13. Основные объекты воздействия в информационной войне?

j. … b. … c. … d. … e. …

14. Свойства информации в форме сведений: (укажите правильный вариант)

f. материальность
g. измеримость
h. сложность
i. проблемная ориентированность
j. накапливаемость

15. Свойства информации в форме сообщения:
(укажите правильный вариант)

g. субъективность
h. информационная неуничтожаемость
i. динамичность
j. материальность
k. накапливаемость

Вариант №3

1. Какой метод обеспечения информационной безопасности отсутствует в перечне :

k. Организационный l. Правовой m. Технический
n. Экономический o. Идеологический

2. Совокупность информации, информационной инфраструктуры, субъектов и системы регулирования общественных отношений являются составляющими частями … … .

3. Автономная информация – информация , существующая … от какого-либо субъекта.

4. Информационная сфера – являясь системообразующим фактором жизни общества, активно влияет на сосояние … , … , … и др. составляющих безопасности Российской Федерации.

5. Информация взаимодействия - … одного субъекта на другого, имеющее целью …, моделей внешней среды двух субъектов или коллектива. 6. Информация воздействия - … знания, … модели окружающего мира.

7. Информационная безопасность - … защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью … интересов личности, общества и государства. 8. Составляющие национальной безопасности:

i. соблюдение … Российской Федерации.
j. Правовое … всех участников процесса информационного взаимодействия.
k. Соблюдение … прав и свобод человека и гражданина в области получения информации и пользования ею.
d. Приоритетное … отечественных современных информационных и телекоммуникационных технологий9. Общая схема национальной безопасности:
k. Формулировка …
l. Формирование перчня …
m. Оценка … и …
n. Разработка …
o. Принятие …

10. Для информационной войны обычно четко определена … … .

11. Вторая классификация национальных интересов:

g. по принадлежности интересов h. по важности интересов
i. по национальным признакам j. по экономическим признакам

12. Классификация информации как объекта исследования:

f. … информация
g. информация…
h. информация…

13. Программные продукты являются следующей составляющей информационных ресурсов (выберите правильный вариант):

a. документы b. персонал c. организационные интересы
d. промышленные образцы e. научный инструментарий

14. Свойства информации в форме сообщения:
(укажите правильный вариант)

a. идеальность c. динамичность a. информационная неуничтожаемость
b. субъективность d. накапливаемость b. измеримость

15. Свойства информации в форме сведений: (укажите правильный вариант)

k. материальность l. динамичность c. проблемная ориентированность
a. измеримость e. сложность

Приложение В к рабочей программе

Перечень оценочных средств по дисциплине

«Информационная безопасность»

№ ОС	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Устный опрос собеседование (УО)	Средство контроля, организованное как специальная беседа педагогического работника с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	Тест (Т)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
3	Экзамен (Э)	Итоговая форма оценки знаний. В высших учебных заведениях проводится во время сессии.	Вопросы к экзамену