МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____ / Д.Г.Демидов /
«15» февраля 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение системной и программной инженерии»

Направление подготовки
09.03.01 Информатика и вычислительная техника

Профиль
«Системная и программная инженерия»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2024 г.

Разработчик(и):

Доцент, к.т.н., доцент /И.В. Калуцкий/

ст.преподаватель /А.Ю.Гневшев/

Согласовано:
Заведующий кафедрой «Инфокогнитивные технологии»,

доцент, к.т.н. /Е.А.Пухова/

1 Цели, задачи и планируемые результаты обучения по дисциплине

К основным целям освоения дисциплины следует отнести:

- приобретение студентами знаний по организационному обеспечению защиты информации и формирование практических навыков работы в конкретных условиях, необходимых для комплексного обеспечения безопасности информации;
- обеспечение основ правовой подготовки специалистов в области защиты информации, развитие навыков работы с нормативно-правовыми документами, приобретение знаний и навыков, необходимых для комплексного обеспечения безопасности информации.

К основным задачам освоения дисциплины следует отнести:

- овладение студентами практическими навыками использования организационных и правовых принципов и норм для защиты информации.

Обучение по дисциплине «Организационное и правовое обеспечение системной и программной инженерии» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-9. Способен осваивать методики использования программных средств для решения практических задач	ИОПК-9.1. Знает примерный состав команды разработчиков ПО, основы реализации проекта, способы коммуникации с участниками проектной деятельности, технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии, технологии подготовки и проведения презентаций. ИОПК-9.2. Умеет осуществлять взаимодействие с заказчиком в процессе реализации проекта; принимать участие в командо-образовании и развитии персонала. ИОПК-9.3. Владеет навыками проведения презентаций, переговоров, публичных выступлений.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части основной профессиональной образовательной программы бакалавриата.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОПОП:

- Основы информационной безопасности.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, т.е. 72 академических часа.

.

3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			1	
1	**Аудиторные занятия**	**32**	32	
	В том числе:			
1.1	Лекции	2	2	
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	30	30	
2	**Самостоятельная работа**	**40**	40	
3	**Промежуточная аттестация**			
	Дифференцированные зачеты		Диф.зачет	
	Итого:	**72**	72	

3.2 Тематический план изучения дисциплины (по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1 Организационная защита информации	7	1		2		4
2	Тема 2 Организационные источники и каналы утечки информации. Силы, средства и условия организационной защиты информации	9	1		4		4
3	Тема 3 Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий	8			4		4
4	Тема 4 Подбор персонала на должности, связанные с работой с конфиденциальной информацией	8			4		4
5	Тема 5 Организация доступа и допуска к информации ограниченного доступа	10			4		6
6	Тема 6 Текущая работа с персоналом, обладающим конфиденциальной информацией	10			4		6
7	Тема 7 Организация служебного расследования по фактам	10			4		6

	разглашения персоналом конфиденциальной информации						
8	Тема 8 Организация охраны территории, зданий, помещений и персонала	10			4		6
Итого		**72**	**2**		**30**		**40**

3.3 Содержание дисциплины

Тема 1. *Понятие "Организационная защита информации".*
Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией. Понятия организационная защита информации и режим защиты информации. Различные подходы к определению понятия организация защиты информации. Определение понятия по целям, по функциям, по структуре т.д. Понятие режим защиты информации. Режим защиты информации как составная часть организационной защиты информации; субъекты и объекты системы организационной защиты информации.

Тема 2. *Организационные источники и каналы утечки информации. Силы, средства и условия организационной защиты информации.*
Комуникационный процесс и его базовые элементы: источник информации, отправитель, сообщение, канал, получатель. Источники конфиденциальной информации: люди, документы, изделия, технические носители и средства коммуникации. Организационные каналы передачи информации и каналы утечки информации и несанкционированного доступа к ней. Классификация организационных каналов утечки конфиденциальной информации. Основания классификации: по каналам коммуникации и источникам конфиденциальной информации; по источникам угроз; времени воздействия и места их возникновения; по направлениям деятельности организации и характеру конфиденциальной информации; по характеру взаимоотношений с партнерами; по способам и средствам несанкционированного доступа к конфиденциальной информации; по способам, средствам и методам защиты информации от утечки и несанкционированного доступа к ней; по степени формализации каналов утечки и т.д. Основные организационные каналы утечки и несанкционированного доступа к информации: разглашение информации персоналом организации: разглашение информации при осуществлении сотрудничества с другими организациями, в частности в ходе переговоров, при поведении совещаний, при приеме в организации посетителей; при осуществлении рекламной и публикаторской деятельности. Соотношение организационных и правовых методов защиты информации при взаимоотношениях с государственными и муниципальными организациями (налоговой инспекцией, санитарной и пожарной службами, органами статистики, правоохранительными органами и т.п.), с другими организациями на основе договоров (банками, адвокатскими конторами, аудиторскими фирмами, страховыми компаниями, службами связи, охранными агентствами и т.п.). Соотношение организационных и технических методов защиты информации при использовании технических, в том числе, электронных средств передачи, обработки, хранения конфиденциальной информации. Совокупности каждого из методов защиты информации, используемых для перекрытия каналов утечки информации, как основные направления организационной защиты информации.

Тема 3. *Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий.*
Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну,

к различным степеням секретности. Присвоение грифа и изменение грифа секретности работам, документам и изделиям. Понятие рассекречивание сведений. Основания для рассекречивания конфиденциальных сведений, документов и изделий.

Тема 4. *Подбор персонала на должности, связанные с работой с конфиденциальной информацией.*
Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения. Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией. Должности, составляющие с точки зрения защиты информации группы риска: руководящий состав организации,средний управленческий персонал, исполнители, сотрудники, осуществляющие технологические процессы передачи, обработки и хранения информации и др. Оценка кандидатов на должности, связанные с доступом к конфиденциальной информации. Основные критерии оценки: уровень профессиональной подготовки, знаний, умений и наличие практического опыта работы; личностные характеристики. Методы проверки кандидатов на должности. Состав документов, необходимых при подборе и приеме сотрудников на должности, связанные с доступом к конфиденциальной информации. Особенности документирования трудовых отношений с персоналом, обладающим конфиденциальной информацией.

Тема 5. *Организация доступа и допуска к информации ограниченного доступа.*
Понятие допуск. Формы допусков, их назначение и классификация. Основные принципы допускной работы. Понятие доступ к защищаемой информации. Условия правомерного доступа. Задачи режима защиты информации, решаемые в процессе регулирования доступа. Понятие разрешительной системы доступа, основные требования, предъявляемые к ней.

Тема 6. *Текущая работа с персоналом, обладающим конфиденциальной информацией.*
Профессиональная ориентация и обучение персонала. Ознакомление сотрудника с правилами, процедурами и методами защиты информации. Организация обучения персонала. Основные формы обучения и методы контроля знаний. Мотивация персонала к выполнению требований по защите информации. Основные формы воздействия на персонал как методы мотивации: использование различных форм вознаграждения, управление карьерой, привлечение к участию в прибылях, воспитание фирменного патриотизма и др. Организация контроля за соблюдением персоналом требований режима защиты информации. Методы проверки персонала. Основные меры по защите информации при увольнении сотрудника. Документирование процедуры увольнения сотрудника.

Тема 7. *Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.*
Понятие служебное расследование по фактам разглашения информации. Цели изадачи служебного расследования. Основания для проведения служебного расследования.Процедура служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования.

Тема 8. *Организация охраны территории, зданий, помещений и персонала.*
Понятие охрана. Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы и другие материальные и финансовые ценности. Особенности их охраны. Виды и способы охраны. Понятие о рубежах охраны. Многорубежная система охраны. Факторы выбора приемов и средств охраны.

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. Приказ Минобрнауки России от 19.09.2017 N 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. N 48489).

3. Академический учебный план Направление подготовки: 09.03.01 Информатика и вычислительная техника Профиль: Системная и программная инженерия Форма обучения: очная.

4. 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).

4.2 Основная литература

- «Череватова, Т. Ф. Нормативное обеспечение в сфере информационных технологий и систем / Т. Ф. Череватова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 84 с. — ISBN 978-5-507-47262-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/349997
- Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2016. — 201 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155246

4.2. Дополнительная литература

1 Паршин, К. А. Методы и средства проектирования информационных систем и технологий : учебно-методическое пособие / К. А. Паршин. — Екатеринбург : , 2018. — 129 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/121337

4.3.Электронные образовательные ресурсы

Ссылка на электронный образовательный ресурс Организационное и правовое обеспечение информационной безопасности

https://lms.mospolytech.ru/course/view.php?id=5803

5 Материально-техническое обеспечение

5.1 Требования к оборудованию и помещению для занятий

Практические занятия (семинары) и самостоятельная работа студентов должна проводиться в специализированных аудиториях с комплектом мультимедийного оборудования и/или доской для записей материалов. Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов.

5.2 Требования к программному обеспечению

Для проведения практических занятий (семинаров) специального программного обеспечения для освоения дисциплины не требуется.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

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

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

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются аудиторные занятия, семинары и практики.

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

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

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

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

Текущий контроль осуществляется на аудиторных занятиях, промежуточный контроль осуществляется на зачете в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

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

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

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

- Дифференцированный зачет.

7.2 Шкала и критерии оценивания результатов обучения

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

Показатель	Критерии оценивания			
	2	3	4	5
ОПК-9. Способен осваивать методики использования программных средств для решения практических задач				
ИОПК-9.1. Знает примерный состав команды разработчиков ПО, основы реализации проекта, способы коммуникации с участниками проектной деятельности, технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии, технологии подготовки и проведения презентаций. ИОПК-9.2. Умеет осуществлять взаимодействие с заказчиком в процессе реализации проекта; принимать участие в командо-образовании и развитии персонала. ИОПК-9.3. Владеет навыками	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. 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 следующих знаний, указанных в индикаторах компетенций дисциплины. Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Свободно оперирует приобретенными знаниями.

проведения презентаций, переговоров, публичных выступлений.				

Шкала оценивания результатов промежуточной аттестации и её описание

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой дисциплины.

Шкала оценивания	**Описание**
Зачтено	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.
Не зачтено	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.

7.3 Оценочные средства

7.3.1 Вопросы для дифференцированного зачета

1. Организационная и правовая защита информации как составные части системы комплексного противодействия информационным угрозам.
2. Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране.
3. Основные цели и задачи организационного обеспечения информационной безопасности на предприятии.
4. Угрозы информационной безопасности. Виды угроз.
5. Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ.
6. Структура и содержание документа «Политика информационной безопасности предприятия».
7. Концепция информационной безопасности предприятия как составная часть «Политики информационной безопасности предприятия».
8. Служба информационной безопасности предприятия. Состав, задачи службы информационной безопасности предприятия.

9. Служба информационной безопасности предприятия. Состав, основные направления деятельности службы информационной безопасности предприятия.
10. Порядок засекречивания и рассекречивания сведений, составляющих информацию ограниченного доступа.
11. Порядок учета и хранения сведений, составляющих информацию ограниченного доступа.
12. Кадровая политика предприятия. Возможные источники пополнения предприятия кадрами для работы с конфиденциальной информацией.
13. Кадровая политика предприятия. Этапы подбора кадров для работы с конфиденциальной информацией.
14. Отражение вопросов информационной безопасности в трудовых договорах.
15. Организация доступа и допуска сотрудников к конфиденциальной информации.
16. Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность.
17. Основные направления деятельности при текущей работе с персоналом, допущенным к конфиденциальной информации.
18. Организация служебного расследования по фактам утраты конфиденциальной информации.
19. Организация охраны объектов информатизации. Составные элементы системы охраны.
20. Организация режима охраны объекта. Факторы, влияющие на выбор приёмов и средств охраны.
21. Организация внутриобъектового и пропускного режимов на объектах информатизации.
22. Атрибутивный и биометрический способы идентификации сотрудников. Их преимущества и недостатки.
23. Общие требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы.
24. Аттестация помещений, в которых обрабатывается конфиденциальная информация.
25. Организация защиты информации при взаимодействии со сторонними организациями. Отражение вопросов защиты информации при подготовке договоров о сотрудничестве.
26. Организация защиты информации при взаимодействии со сторонними организациями. Порядок отбора и подготовки информации к оглашению.
27. Контроль функционирования системы защиты информации. Формы контроля.
28. Аудит информационной безопасности.
29. Закон «Об информации информационных технологиях и о защите информации». Информация как объект правовых отношений.
30. Правовое определение понятий: «информация», «информационные технологии», «информационные системы» и «информационно-телекоммуникационные сети»
31. Закон «Об информации информационных технологиях и о защите информации». Обладатель информации.
32. Закон «Об информации информационных технологиях и о защите информации». Общедоступная информация.
33. Закон «Об информации информационных технологиях и о защите информации». Право на доступ к информации.
34. Закон «Об информации информационных технологиях и о защите информации». Ограничение доступа к информации.
35. Закон «Об информации информационных технологиях и о защите информации». Распространение информации или предоставление информации.
36. Закон «Об информации информационных технологиях и о защите информации». Защита информации.

37. Закон «Об информации информационных технологиях и о защите информации». Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
38. Закон «О персональных данных». Согласие субъекта персональных данных на обработку его персональных данных.
39. Закон «О персональных данных». Меры по обеспечению безопасности персональных данных при их обработке.
40. Закон «О персональных данных». Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных.
41. Закон «О персональных данных». Принципы обработки персональных данных.
42. Перечень сведений, составляющих государственную тайну.
43. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
44. Закон «О государственной тайне». Ограничение прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием.
45. Допуск должностных лиц и граждан к государственной тайне.
46. Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ.
47. Условия прекращения допуска должностного лица или гражданина к государственной тайне.
48. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне.
49. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.
50. Правовое определение понятий: «коммерческая тайна», «информация, составляющая коммерческую тайну», «обладатель информации, составляющей коммерческую тайну», «разглашение информации, составляющей коммерческую тайну».
51. Сведения, которые не могут составлять коммерческую тайну в соответствии с законом «О коммерческой тайне».
52. Правовое определение понятий: «доступ к информации, составляющей коммерческую тайну», «передача информации, составляющей коммерческую тайну», «контрагент», «предоставление информации, составляющей коммерческую тайну».
53. Права обладателя информации, составляющей коммерческую тайну.
54. Закон «О коммерческой тайне». Охрана конфиденциальности информации.
55. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений.
56. Предоставление информации, составляющей коммерческую тайну. Охрана конфиденциальности информации при ее предоставлении.