Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:
Разработка защищенных телекоммуникационных систем

Квалификация:
Специалист

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность телекоммуникационных систем»

_____ Бурлов В.Г.

Утверждаю
Председатель УМС _____И.И. Палкин

Рекомендована решением
Учебно-методического совета
10 мая 2018 г., протокол № 4

Рассмотрена и утверждена на заседании кафедры
17 мая 2018 г., протокол № 5
Зав. кафедрой _____ Бурлов В.Г.

Авторы-разработчики:
_____Бурлов В.Г.
_____Богданов П.Ю.

Санкт-Петербург 2018

1. Цели освоения дисциплины

Целью освоения дисциплины «Управление информационной безопасностью телекоммуникационных систем» является формирование способности планировать, реализовывать, оценивать и корректировать процессы управления (менеджмента) информационной безопасности телекоммуникаций.

Основными задачами дисциплины являются изучение:

- основ построения систем управления (менеджмента) информационной безопасности телекоммуникаций;
- процессов планирования, реализации, проверки (оценивания), совершенствования (корректировки) систем управления (менеджмента) информационной безопасности телекоммуникационных систем;
- основ обеспечения доверия к информационной безопасности

2.Место дисциплины в структуре ОПОП

«Управление информационной безопасностью телекоммуникационных систем» (Б1.Б.35.04) относится к дисциплинам специализации.

Для успешного усвоения данной дисциплины необходимо чтобы обучаемые владели знаниями, умениями и навыками, сформированными в процессе изучения следующих дисциплин: Введение в специальность, Основы информационной безопасности, Телекоммуникационные системы, Организационное и правовое обеспечение информационной безопасности, Защита операционных систем, Документоведение.

Освоение данной дисциплины необходимо для Защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ПК-1	способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем
ПК-5	способность проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов
ПСК-7.4	способность участвовать в разработке систем управления информационной безопасностью телекоммуникационных систем

В результате освоения компетенций в рамках дисциплины «Управление информационной безопасностью телекоммуникационных систем» обучающийся должен:

Код компетенции	Результаты обучения
ПК-1	Знать: современные международные и национальные стандарты; Уметь: анализировать научно-техническую информацию; Владеть: терминологией менеджмента информационной безопасности;
ПК-5	Знать: основы менеджмента безопасности сетей; Уметь: разрабатывать техническую документацию; Владеть: навыками анализа проектных решений по обеспечению безопасности;
ПСК-7.4	Знать: основы построения систем менеджмента информационной безопасности телекоммуникаций; Уметь: разрабатывать и внедрять практические меры по управлению информационной безопасностью; Владеть: навыками проведения аудита информационной безопасности

Основные признаки проявления формируемых компетенций в результате освоения дисциплины Управление информационной безопасностью телекоммуникационных систем сведены в таблице.

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Уровень освоения компетенции	Результат обучения	Результат обучения	Результат обучения
	ПК-1: Знать, уметь, владеть	ПК-5: Знать, уметь, владеть	ПСК-7.4:Знать, уметь, владеть
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Не знает
	не умеет	не выделяет основные идеи	Не умеет
	не знает	допускает грубые ошибки	Не владеет
базовый	Способен выделить основные идеи текста, работать с нормативными документами	знает основы менеджмента безопасности сетей	знает принципы построения систем менеджмента информационной безопасности телекоммуникаций
	Способен показать развитие системы менеджмента информационной безопасности	может разрабатывать техническую документацию	умеет разрабатывать и внедрять практические меры по управлению информационной безопасностью;
	Знает основные рабочие категории, однако не ориентируется в их специфике	владеет навыками анализа проектных решений, однако не ориентируется в их специфике	владеет навыками проведения аудита информационной безопасности
продвинутый	Способен грамотно обосновать собственную позицию относительно решения современных проблем в области менеджмента информационной безопасности	Видит источники современных проблем в менеджменте информационной безопасности, владеет подходами к их решению	Знает основы построения систем менеджмента информационной безопасности
	Свободно ориентируется в области менеджмента информационной безопасности. Понимает ее основания и умеет выделить практическое значение заданной области, аргументировать собственную позицию и ответственность	владеет навыками разработки технической документации, понимает ее практическую ценность	умеет разрабатывать и внедрять практические меры по управлению информационной безопасностью; может аргументировано объяснить их
	Может дать критический анализ современным проблемам в области менеджмента информационной безопасности	владеет навыками анализа проектных решений, ориентируется в их специфике	навыками проведения аудита информационной безопасности, может объяснить свои решения

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с нормативными документами и стандартами	Способен дать собственную аргументированную оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи управления с современными проблемами информационной безопасности
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход к решению проблем управления информационной безопасности
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции управления информационной безопасности , аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но затрудняется с пониманием их практической значимости	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные концепций менеджмента информационной безопасности, проводит их сравнение в заданной проблемной области	Способен выделить специфику концепций управления в проблемной области информационной безопасности
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Осмысливает современные принципы управления информационной безопасностью, владеет подходами к решению соответствующих проблем	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в развитии	Может понять практическое назначение основной идеи, но затрудняется выявить ее основания	Понимает особенности управления информационной безопасностью, ее практическую ценность, однако	Свободно ориентируется в области управления информационной безопасности. Понимает ее

				испытывает затруднения в описании сложных объектов анализа	основания и умеет выделить практическое значение
	не знает	допускает ошибки при выделении рабочей области анализа	Способен изложить основное содержание современных научных идей в рабочей области анализа	Знает основное содержание современных научных идей в управлении информационной безопасности, способен их сопоставить	Может дать критический анализ современным проблемам в области управления информационной безопасности

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 10 зачетных единиц, 360 часов.

Объем дисциплины по видам учебных занятий
в академических часах

Объём дисциплины	**Всего часов**		
	Очная форма обучения	**9**	**10**
Общая трудоёмкость дисциплины	**360**		
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	**154**		
в том числе:			
лекции	**68**	**36**	**32**
практические занятия	**54**	**54**	
Лабораторные работы	**32**		**32**
Самостоятельная работа (СРС) – всего:	**206**	**90**	**116**
в том числе:			
курсовая работа			
контрольная работа			
Вид промежуточной аттестации (зачет/экзамен)		**экзамен**	**экзамен**
Всего:	**360**		

4.1. Структура дисциплины

Очная форма обучения

№ п/п	**Раздел и тема дисциплины**	**Семестр**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемости**	**Занятия в активной и интерактивной форме, час.**	**Формируемые компетенции**
			Лекции	**Семинар Лаборат. Практич.**	**Самост. работа**			
1	Базовая терминология	9	**16**	**2**	**15**	**Опрос**		**ПК-1; ПК-5, ПСК-7.4**
2	Стандартизация систем и процессов управления	9	**20**	**10**	**25**	**Опрос**		**ПК-1; ПК-5, ПСК-7.4**

	информационной безопасностью							
3	Политика информационной безопасности	10	**16**	**10**	**25**	**Опрос**		**ПК-1; ПК-5, ПСК-7.4**
4	Управление и система управления информационной безопасностью	10	**16**	**10**	**25**	**Опрос**		**ПК-1; ПК-5, ПСК-7.4**
	ИТОГО							

4.2. Содержание разделов дисциплины

4.2.1 Базовая терминология

Система. Процесс. Управление. Системный и процессный подход. Циклическая модель улучшения процессов. Системный и процессный подходы к управлению организацией

4.2.2 Стандартизация систем и процессов управления информационной безопасностью

Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности» Стандарты на отдельные процессы управления информационной безопасностью и оценку безопасности информационных технологий. Отраслевые стандарты в области управления информационной безопасностью – стандарты банковской системы Российской Федерации.

4.2.3 Политика информационной безопасности

Политика обеспечения информационной безопасности и политика информационной безопасности организации.

4.2.4 Управление и система управления информационной безопасностью

Управление информационной безопасностью информационно-телекоммуникационных технологий организации. Система управления

информационной безопасностью организации. Процессный подход в рамках управления информационной безопасностью. Работа с процессами Стратегии построения и внедрения системы управления информационной безопасностью

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тематика практических занятий	Форма проведения	Формируемые компетенции
	Базовая терминология	**Формальное описание структуры информационной системы.**	**лабораторная работа**	**ПК-1; ПК-5, ПСК-7.4**
	Оценка рисков информационной безопасности	**Анализ рисков информационной безопасности на основе построения модели информационных потоков.**	**лабораторная работа**	**ПК-1; ПК-5, ПСК-7.4**
	Политика информационной безопасности	**Формирование требований к политике информационной безопасности.**	**лабораторная работа**	**ПК-1; ПК-5, ПСК-7.4**
	Оценка рисков информационной безопасности	**Анализ рисков на основе модели угроз и уязвимостей.**	**лабораторная работа**	**ПК-1; ПК-5, ПСК-7.4**
	Оценка рисков информационной безопасности	**Анализ рисков на основе международного стандарта ISO 17799.**	**лабораторная работа**	**ПК-1; ПК-5, ПСК-7.4**

5. Учебно-методическое обеспечение самостоятельной работы студентов и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Текущий контроль проводится путем проверки выполнения творческих заданий, дискуссий, устного опроса.

5.2. Методические указания по организации самостоятельной работы

Целью самостоятельной работы является повышение уровня знаний студентов, их умения ориентироваться в аспектах профессиональной деятельности, приобретение навыков, практических знаний в дальнейшей профессиональной деятельности.

Самостоятельная работа дает возможность студентам проверить, а преподавателю ре-шить задачи контроля уровня усвоения рассматриваемых тем, выявить пробелы в знаниях и наметить пути их устранения. Самостоятельная работа способствует выработке у студентов умений грамотно и четко формировать и излагать свои мысли, вести творческую дискуссию, отстаивать свои мнения и убеждения. По темам дисциплины дан перечень наиболее важных вопросов курса, а также список литературы. При подготовке к семинарскому занятию необходимо обращаться к конспекту лекций и первоисточникам.

Важным этапом самостоятельной подготовки является изучение соответствующих разделов в учебниках и учебных пособиях, и только после этого, когда уже имеется теоретическая база для уяснения более сложного материала, нужно приступить к выполнению практических и лабораторных заданий.

5.3. Промежуточный контроль: зачет, экзамен

Перечень вопросов к экзамену(9 семестр):

1. Цель и этапы анализа объектов защиты.
2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.
3. Идентификация и классификация объектов защиты.
4. Типизация информационных систем. Данные об информационной системе,

необходимые для построения модели документооборота.

5. Подходы к разграничению доступа в рамках организации. Структура документов, регламентирующих разграничение доступа.

6. Подходы к построению модели нарушителя.

7. Классификация нарушителей (ФСТЭК).

8. Классификация угроз безопасности персональных данных (ФСТЭК).

9. Методика определения актуальных угроз (ФСТЭК).

10. Методика оценки ущерба, нанесённого при реализации угроз информационной безопасности.

11. Угрозы, источником которых является персонал организации.

12. Методы «социальной инженерии» и способы защиты от них.

13. Обязанности сотрудников Службы безопасности при приёме сотрудников на работу.

14. Нормативная документация, обязательная к ознакомлению и подписанию при приёме на работу.

15. Предоставление сотруднику доступа к конфиденциальной информации. Основные разделы Инструкции по внесению изменений в списки пользователей.

16. Обязанности сотрудников Службы безопасности при обучении и увольнении сотрудников.

17. Упрощённая модель классификации субъектов.

18. Основные положения инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации.

19. Основные положения регламента контроля использования технических средств обработки и передачи информации.

20. Основные положения инструкции по организации парольной защиты.

21. Основные положения документов, регламентирующих использование средств аутентификации и носителей ключевой информации.

22. Основные положения инструкции по организации антивирусной защиты.

23. Основные положения инструкции по работе с электронной почтой.

24. Типы чрезвычайных ситуаций. Структура аварийного плана. Причины изменения аварийного плана.

25. Классификация объектов при составлении аварийного плана.

26. Требования к различным классам объектов и их резервированию.

27. Основные положения плана обеспечения непрерывной работы и восстановления работоспособности.

28. Приведите примеры источников информации об инцидентах информационной безопасности.

29. Перечислите аспекты анализа инцидентов информационной безопасности, направленные на совершенствование системы управления информационной безопасностью.

30. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.

Перечень вопросов к экзамену(10 семестр):

1 Понятие система. Системный подход

2. Понятие процесс. Процессный подход

3. Понятие управление

4 Понятие Информационная безопасность.

5 Модель нарушителя

6 Смысл и содержание стандарта ISO/IEC 27000 СМИБ. Общий обзор и терминология

7 Перечислите этапы оценки рисков информационной безопасности автоматизированных систем

8) Смысл и содержание стандарта ISO/IEC 27001 "СМИБ.Требования"

9 Смысл и содержание стандарта ISO/IEC 27003 "СМИБ. Руководство по реализации системы менеджмента информационной безопасности"

10 Смысл и содержание стандарта ISO/IEC 27004 "СМИБ. Измерения"

11 Смысл и содержание стандарта ISO/IEC 27005 "СМИБ. Менеджмент риска информационной безопасности."

12 Смысл и содержание стандарта ISO/IEC 27007 "СМИБ. Руководства по аудиту систем менеджмента информационной безопасности"
13 Смысл и содержание стандарта СТО БР ИББС-1.1 «Аудит информационной безопасности»
14 Смысл и содержание стандарта СТО БР ИББС-1.2 Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2
15 Понятия политики обеспечения ИБ и политики ИБ
16. Содержание политики ИБ
17 Жизненный цикл политики ИБ
18 Деятельность по обеспечению ИБ организации как процесс.
19 Система управления ИБ организации
20 Смысл и содержание стандарта ISO/IEC 27002 СМИБ. «Свод норм и правил менеджмента информационной безопасности»
21 Смысл и содержание стандарта СТО БР ИББС-1.3-2016 «Сбор и анализ технических данных при выявлении и расследовании инцидентов информационной безопасности при осуществлении переводов денежных средств».
22 Смысл и содержание стандарта СТО БР ИББС-1.4-2018 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском информационной безопасности при аутсорсинге»
23 Методы «социальной инженерии» и способы защиты от них
24 Основные положения плана обеспечения непрерывной работы и восстановления работоспособности.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1) Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. «Основы управления информационной безопасностью» Издательство: Горячая линия-Телеком. 2014г. 244с

2) Бурлов В.Г., «Теоретические основы управления риском», Издательство НПО «Стратегия будущего», СПБ, 2008,

3) Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799:2005 Информационные технологии. Практические правила управления информационной безопасностью

4) Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001:2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

5) Национальный стандарт Российской Федерации ГОСТ Р 54581-2011 "Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 1. Обзор и основы".

6) Национальный стандарт Российской Федерации ГОСТ Р 54582-2011 "Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий- Часть 2. Методы доверия "

7) Федеральный закон от 4 мая 2011 г. N 99-ФЗ О лицензировании отдельных видов деятельности

8) Федеральный закон от 27 декабря 2002 г. N 184-ФЗ О техническом регулировании

9) Положение по аттестации объектов информатизации по требованиям безопасности информации Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.

б) дополнительная литература:

1) Ярочкин В.И. «Информационная безопасность», Издательство «Гаудемус»

,М. 2004г. -543с.

2) Бурлов В.Г. «Математические методы моделирования в экономике. Часть 1» Издательство НПО «Стратегия будущего», 2008, СПБ, 330с.

3) Бурлов В.Г. «Основы моделирования социально-экономических и политических процессов. Часть1. » (Методология. Методы.) С-Пб. НП «Стратегия будущего», 2007. 287с.

4) Бурлов В.Г. «Основы моделирования социально-экономических и политических процессов. Часть 2.» (Модели. Технологии.) С-Пб. НП «Стратегия будущего», 2007. 276с.

5) Бурлов В.Г. и др. Материалы международной конференции «13th International Conference on Cyber Warfare & Security» ICCWS 2018, 8-9 March 2018, National Defense University, Washington DC, USA, 707 pp

6) Бурлов В.Г. и др. Материалы международной конференции «17th European Conference on Cyber Warfare and Security», 28 - 29 June 2018, University of Oslo, Oslo, Norway, 641 pp

7) Бурлов и др. Материалы международной конференции «5th European Conference on Social Media», 21 - 22 June 2018, Limerick, Ireland , 507 pp

8) Обеспечение информационной безопасности бизнеса/ В.В. Андрианов, С.Л. Зефиров, В.Б. Голованов, Н.А. Голдуев; Под ред.А.П. Курило – М.: Издательство Альпина Паблишерз, 2011 – 373 с.

9) Курило А.П., Зефиров С.Л., Алексеев В.М. и др. Аудит информационной безопасности.- М.: .: Издательская группа БДЦ-пресс, 2006 – 304с.

7. Методические указания для обучающихся по освоению дисциплины

Для усвоения материала рекомендуется вести конспект лекций и семинаров. При самостоятельной работе, в особенности при подготовке докладов, возможно и нужно обращаться за консультациями к преподавателю в индивидуальном режиме, что можно сделать как в личном общении, так и через электронные средства связи

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Базовая терминология	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	MS PowerPoint
Стандартизация систем и процессов управления информационной безопасностью	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	MS PowerPoint
Политика информационной безопасности	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и рационального воздействия; сочетание индивидуального и коллективного обучения	MS PowerPoint
Управление и система управления информационной безопасностью	Чтение лекций с использованием слайд-презентаций, интерактивное взаимодействие педагога и студента; использование деятельностного подхода; сочетание средств эмоционального и	MS PowerPoint

	рационального воздействия; сочетание индивидуального и коллективного обучения	

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий используются обычные, и в некоторых случаях, мультимедийные аудитории. Лабораторные занятия проводятся в компьютерном классе с ЛВС, связанной Интернетом.