Федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский университет
Государственной противопожарной службы МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ СВЯЗИ И УСТРОЙСТВАХ ТЕЛЕКОММУНИКАЦИЙ

Направление подготовки
10.06.01 Информационная безопасность

Направленность
«Управление в социальных и экономических системах»

уровень подготовки кадров высшей квалификации

Санкт-Петербург

1. Цель и задачи дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций»

Цель изучения дисциплины: формирование системы теоретических знаний и умений, необходимых для нахождением проблем в области информационной безопасности сетей связи, телекоммуникационного оборудования и успешного их решения.

В процессе освоения дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций» обучающийся формирует и демонстрирует нормативно заданные общепрофессиональные и профессиональные компетенции (таблица 1).

Перечень компетенций, формируемых в процессе изучения дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций»

Таблица 1

Компетенции	Содержание
ОПК-1	способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологию научных исследований, внедрять полученные результаты в практическую деятельность
ОПК-5	способность выбирать, разрабатывать и применять модели, методы, научные и научно-технические решения, связанные с анализом, проектированием и разработкой средств и систем защиты информации в области, соответствующей направленности программы адъюнктуры и объекту исследования
ПК-2	способность применять компьютерные и мультимедийные технологии, математическое, программное и информационное обеспечение для решения задач при осуществлении научно-исследовательской работы
ПК-4	способность исследовать способы повышения противодействия угрозам нарушения информационной безопасности для любого вида информационных систем

Задачами изучения дисциплины является:

1) знать основные принципы построения защищенных распределенных компьютерных систем;
2) владеть навыками и средствами проектирования систем обеспечения информационной безопасности, объектов информатизации на базе телекоммуникационных систем;
3) владеть навыками анализа проблем и пути их решения в области информационной безопасности сетей связи и на устройствах телекоммуникаций;
4) владеть основными методами верификации программ, способами настройки систем обнаружения компьютерных атак;
5) владеть навыками использования программных средств и работы в компью-

терных сетях, использования ресурсов Интернет.

2. Перечень планируемых результатов обучения дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций», соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты обучения, характеризующие этапы формирования компетенций	**Планируемые результаты освоения образовательной программы**
В результате освоения обучающийся должен **демонстрировать способность и готовность**	В результате освоения образовательной программы обучающийся должен владеть компетенциями в соответствии с этапом формирования
применять методологию научных исследований области обеспечения информационной безопасности и внедрять полученные результаты в практическую деятельность	ОПК-1
применять модели, методы, научные и научно-технические решения, связанные с анализом, проектированием и разработкой средств и систем защиты информации в области, соответствующей направленности программы адъюнктуры и объекту исследования	ОПК-5
в области научно-исследовательской деятельности:	
оценивание степени соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности; исследование научных основ теории и методологии обеспечения информационной безопасности и защиты информации; исследование методов, аппаратно-программных и организационных средств защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида; исследование методов, моделей и средств выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса; исследование способов повышения противодействия угрозам нарушения информационной безопасности для любого вида информационных систем; анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.	ПК-2, ПК-4

3. Место дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций» в структуре основной профессиональной образовательной программы (далее ОПОП ВО)

Дисциплина «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций» относится к числу факультативных дисциплин основной профессиональной образовательной программы по направлению подготовки 10.06.01 «Информационная безопасность» (квалификация «Исследователь. Преподаватель-исследователь»).

4.Структура и содержание дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций»

4.1. Объем дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций» и виды учебной работы

Для очной формы обучения

Вид учебной работы	Всего часов	4 семестр
Общая трудоемкость дисциплины в часах	**72**	36
Контактные часы (всего)	**36**	36
В том числе:		
Лекции	**24**	24
Практические занятия	**12**	12
Контроль:		
Форма контроля - зачет		+
Самостоятельная работа (всего)	**36**	36

Для заочной формы обучения

Вид учебной работы	Всего часов	2 курс	3 курс
Общая трудоемкость дисциплины в часах	**72**	36	36
Контактные часы (всего)	**16**	6	10
В том числе:			
Лекции	**12**	6	6
Практические занятия	**4**		4
Контроль:			
Форма контроля - зачет			+
Самостоятельная работа (всего)	**56**	30	26

4.2. Темы дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций»

очная форма обучения

Наименование тем	Всего часов	Количество часов			Самостоятельная работа	Примечания
		Лекции	Практические занятия	Контроль		
4 семестр						
Тема 1. Аппаратные и программные средства защиты сети	20	6	4		10	
Тема 2. Информационная безопасность в мобильных системах связи	16	6			10	
Тема 3. Принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности	20	6	4		10	
Тема 4. Методы оценки защищенности информации и информационной безопасности объекта	16	6	4		6	
Зачет				+		
Итого по дисциплине	**72**	**24**	**12**		**36**	

заочная форма обучения

Наименование тем	Всего часов	Количество часов			Самостоятельная работа	Примечания
		Лекции	Практические занятия	Контроль		
2 курс						
Тема 1. Аппаратные и программные средства защиты сети	20	4			16	
Тема 2. Информационная безопасность в мобильных системах связи	16	2			14	
Итого за 2 курс	**36**	**6**			**30**	
3 курс						
Тема 3. Принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной без-	20	4			16	

Наименование тем	Всего часов	Количество часов			Самостоятельная работа	Примечания
		Лекции	Практические занятия	Контроль		
опасности						
Тема 4. Методы оценки защищенности информации и информационной безопасности объекта	16	2	4		10	
Зачет				+		
Итого за 3 курс	**36**	**6**	**4**		**26**	
Итого по дисциплине	**72**	**12**	**4**		**56**	

4.3. Содержание дисциплины

Тема 1. Аппаратные и программные средства защиты сети

Лекция. Аппаратные средства защиты информации. Шлюзы безопасности. Сетевые экраны.

Программные средства защиты информации. Антивирусное программное обеспечение. Устройства шифрования протокола. Аутентификация личности. Криптография.

Практическое занятие. Программно-аппаратный комплекс защиты информации

Самостоятельная работа. Современные программно-аппаратные средства защиты.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1, 2].

Тема 2. Информационная безопасность в мобильных системах связи

Лекция. Особенности построения и функционирования. Система обеспечения защиты информации. Понятие и классификация угроз. Виды представления информации и возможные каналы ее утечки.

Самостоятельная работа. Законодательство в области информационной безопасности и связи. Незаконный доступ. Утечка информации. Криптопровайдеры. Анализ и мониторинг защищенности.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1, 2].

Тема 3. Принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности

Лекция. Принципы создания новых средств защиты информации и обеспечения информационной безопасности. Принципы совершенствования существующих средств защиты информации и обеспечения информационной безопасности.

Практическое занятие. Известные технические, математические и организационные решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Самостоятельная работа. Частные технические, математические и организационные решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1, 2].

Тема 4. Методы оценки защищенности информации и информационной безопасности объекта

Лекция. Методологические подходы к оценке информационной безопасности. Критерии и показатели определения требуемого уровня защищенности объекта. Методы, используемые для оценки защищенности информации и информационной безопасности: экспертный опрос, нечеткая логика, решение задач на графах, нормативные и стандартизированные методики.

Практическое занятие. Решение типовых задач оценки защищенности информации и информационной безопасности объекта: определение а) требуемого и текущего количества установленных средств защиты, б) требуемой и текущей меры структурной защищенности объекта, в) оптимального расположения точек контроля на графе объекта, г) определения оптимального уровня всех точек контроля через анализ структурной защищенности.

Самостоятельная работа. Принципы построения защищенного объекта.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1, 2].

5. Методические рекомендации по организации изучения дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций»

При реализации программы дисциплины используются следующие виды занятий: лекция и практическое занятие.

Лекция:

Лекция составляет основу теоретического обучения и должна давать систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки и техники, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

Ведущим методом в лекции выступает устное изложение учебного материала, сопровождающееся демонстрацией слайдов, использованием компьютерной техники.

Практические занятия:

Практическое занятие проводится в целях: выработки практических умений и приобретения навыков, закрепления пройденного материала по соответствующий теме дисциплины. Главным их содержанием является практическая работа каждого обучающегося.

При подготовке к практическим занятиям и семинарам обучающимся необходимо ориентироваться на рабочую программу дисциплины.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим практическим занятиям и зачету.

6. Оценочные средства для проведения промежуточных аттестаций обучающихся по дисциплине

6.1. Типовые контрольные вопросы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов для зачета

1. Защищенные каналы связи.
2. Антивирусная защита.
3. Принципы обеспечения информационной безопасности.
4. Модели дискреционного доступа.
5. Модели мандатного доступа.
6. Ролевые модели доступа.
7. Модели безопасности информационных потоков.
8. Классификационные признаки и известные классификации угроз нарушения информационной безопасности.
9. Идентификация и категорирование уязвимостей.
10. Анализ уязвимости процессов переработки информации: скомпрометированные процессы и процессы, обладающие недекларированными возможностями.
11. Инструментальные средства анализа рисков информационной безопасности.
12. Методы обеспечения безопасности информации.
13. Классификация аппаратно-программных средства защиты информационных систем и ресурсов.

14. Организационные средства защиты информационных систем и ресурсов.
15. Понятие идентификации, аутентификации и авторизации.
16. Технологии идентификации: кодовая, радиочастотная, биометрическая, смарт-карточная.
17. Технологии аутентификации: однофакторная и многофакторная, одноразовые и многоразовые пароли, цифровые сертификаты.
18. Системы разграничения доступа: требования к реализации диспетчера доступа и представление матрицы управления доступом.
19. Методы, используемые для оценки защищенности информации и информационной безопасности.
20. Методы оценки качества и эффективности комплексной системы обеспечения информационной безопасности.

6.2. Методика оценивания совокупности знаний, умений и навыков, характеризующих этапы формирования компетенций

В процессе изучения дисциплины процедурами оценивания образовательных достижений обучающихся при завершении этапа формирования компетенций является экзамен.

Промежуточная аттестация: зачет

№	Показатели достижения планируемого уровня компетенций	Шкала оценивания
1	Обучающийся показывает всесторонние и глубокие знания программного материала, знание основной и дополнительной литературы; последовательно и четко отвечает на вопросы билета и дополнительные вопросы; уверенно ориентируется в проблемных ситуациях; демонстрирует способность применять теоретические знания для анализа практических ситуаций, делать правильные выводы, проявляет творческие способности в понимании, изложении и использовании программного материала.	*Зачтено*
2	Обучающийся имеет существенные пробелы в знаниях основного учебного материала по дисциплине; не способен аргументировано и последовательно его излагать, допускает грубые ошибки в ответах, неправильно отвечает на задаваемые вопросы или затрудняется с ответом.	*Не зачтено*

7. Требования к условиям реализации. Ресурсное обеспечение дисциплины «Современные проблемы обеспечения информационной безопасности в сетях связи и устройствах телекоммуникаций»

Программное обеспечение, в том числе лицензионное:

1. Microsoft Windows Professional, Russian – Системное программное обеспечение. Операционная система. [Коммерческая (Volume Licensing)]; ПО-BE8-834;

2. Microsoft Office Standard (Word, Excel, Access, PowerPoint, Outlook, One-Note, Publisher) – Пакет офисных приложений [Коммерческая (Volume Licensing)]; ПО-D86-664;

3. Adobe Acrobat Reader DC – Приложение для создания и просмотра электронных публикаций в формате PDF [Бесплатная]; ПО-F63-948;

4. Google Chrome – Браузер [Открытая]; ПО-F2C-926.

Современные профессиональные базы данных и информационно-справочные системы:

При реализации дисциплины используются следующие современные базы данных и информационно-справочные системы, обеспечивающие индивидуальный неограниченный доступ:

1. Международная реферативная база данных научных изданий Scopus [Электронный ресурс]. – Режим доступа: https://www.scopus.com/, доступ только после самостоятельной регистрации;

2. Международная реферативная база данных научных изданий Web of Science [Электронный ресурс]. – Режим доступа: https://www.clarivate.ru/products/web-of-science/, доступ только после самостоятельной регистрации;

3. Научная электронная библиотека «eLIBRARY.RU» [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/, доступ только после самостоятельной регистрации;

4. Справочная правовая система «КонсультантПлюс: Студент» [Электронный ресурс]. – Режим доступа: http://student.consultant.ru/, свободный доступ;

5. Информационно-правовой портал «Гарант» [Электронный ресурс]. – Режим доступа: http://www.garant.ru/, свободный доступ.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Безопасность информационных систем и защита информации в МЧС России: учебное пособие: [гриф МЧС] / Ю.И. Синещук [и др.]; ред. В.С. Артамонов; С.-Петерб. гос. ун-т гос. противопож. службы МЧС России. – СПб.: СПбУ ГПС МЧС России, 2012. – 300 с. Режим доступа: http://elib.igps.ru/?4&type=card&cid=ALSFR-6d86bbe6-aeac-49db-bc2e-068c7a55cb8d&remote=false

2. Синещук, Ю.И. Информационные технологии и защита информации в автоматизированных системах управления МЧС России: учебное пособие: [гриф МЧС] / Ю.И. Синещук, С.Н. Терехин, В.В. Духанин; ред. В.С. Артамонов; МЧС

России. – СПб.: СПбУ ГПС МЧС России, 2010. – 284 с. Режим доступа: http://elib.igps.ru/?6&type=card&cid=ALSFR-a2e62800-d42d-4e9c-9bc9-4c1d7b9f0f55&remote=false

Дополнительная литература

1. Информационная безопасность и применение информационных технологий при обеспечении безопасности граждан: методические рекомендации / Антюхов В.И., Иванов А.Ю., Исаков С.Л., Ходасевич Г.Б. – Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, 2008. – 20 с. Режим доступа: http://elib.igps.ru/?8&type=card&cid=ALSFR-1b1a800e-94af-426a-ac90-dabb1b33fd47&remote=false

2. Башлы, П. Н. Информационная безопасность и защита информации: учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. Режим доступа: http://www.iprbookshop.ru/10677.html

Материально-техническое обеспечение дисциплины:

Для проведения и обеспечения занятий используются специальные помещения, представляющие собой учебные аудитории, а также помещения для самостоятельной работы.

Технические средства обучения:

- Мультимедийный проектор,
- Проекционный экран,
- Персональный компьютер.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.06.01 Информационная безопасность (уровень подготовки кадров высшей квалификации).

Авторы: доктор технических наук, профессор Буйневич М.В.