

МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)

Утверждаю:

Проректор по учебной работе

Павлов В. Н.

2017 г.



РАБОЧАЯ ПРОГРАММА

дисциплины

«ЗАЩИЩЕННЫЕ ПРОГРАММНЫЕ СИСТЕМЫ»

для подготовки аспирантов

по направлению

09.06.01 – «Информатика и вычислительная техника»

по направленности

«Вычислительные машины, комплексы и компьютерные сети»

Санкт-Петербург

2017

СТРУКТУРА ДИСЦИПЛИНЫ

№№ учебных планов: 7909150

Обеспечивающий факультет: ФКТИ

Обеспечивающая кафедра: ВТ

Общая трудоемкость (ЗЕТ) 3

Курс 1

Семестр 2

Виды занятий

Лекции (академ. часов) 36

Все аудиторные (контактные) занятия (академ. часов) 36

Самостоятельная работа (академ. часов) 72

Всего (академ. часов) 108

Вид аттестации

Дифференцированый зачет (семестр) 2

Рабочая программа рассмотрена и одобрена на заседании кафедры вычислительной техники (ВТ) 16.05.2017, протокол № 3.

Рабочая программа рассмотрена и одобрена учебно-методической комиссией факультета компьютерных технологий и информатики (ФКТИ) 18.05.2017, протокол № 5.

АННОТАЦИЯ ДИСЦИПЛИНЫ

«Защищенные программные системы»

Дисциплина «Защищенные программные системы» имеет целью изучение основных понятий, методологии и практических приемов проектирования, разработки и внедрения информационных и программных систем в защищенном исполнении с учетом требований по обеспечению информационной безопасности.

SUBJECT SUMMARY

«Protected Software Intensive Systems»

Discipline is designed to study the basic concepts, methodologies and practices of design, development and implementation of protected software intensive systems to meet the security requirements.

Received competences are to be used during working at PHD thesis.

ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

- 1. Знания о нормативно-методическом регулировании процессов создания информационных и программных систем в защищённом исполнении (ИСЗИ), изучение безопасных продуктов и систем информационных технологий.**
- 2. Формирование умений в области разработки ИСЗИ, отдельных компонентов информационных и программных систем, с учётом требований нормативно-технической и методической документации по обеспечению безопасности информации.**
- 3. Освоение современных методов, технологий и средств защиты информации в информационных и программных системах, изучение методов и технологий проектирования ИСЗИ, приобретение практических навыков работы с нормативно-методическими документами и стандартами в области разработки ИСЗИ, разработка основных документов на этапах создания и эксплуатации ИСЗИ.**

Перечень компетенций, в формировании которых участвует дисциплина, приведен в матрице компетенций, прилагаемой к ОПОП.

Настоящая программа составлена на основе «Программы кандидатских экзаменов по истории и философии науки, иностранному языку и специальным дисциплинам», утвержденной приказом Минобрнауки России от 8 октября 2007 г. № 274 (зарегистрирован Минюстом России 19 октября 2007 г., регистрационный № 10363).

МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина «Защищенные программные системы» относится к вариативной части ОПОП. Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Современные методы и средства работы со знаниями»;
2. «Педагогика высшего образования».

и обеспечивает подготовку выпускной научной квалификационной работы (диссертации).

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Введение (2 академ. часа = 2 ауд. ч.)

Введение в дисциплину. Разъяснение ФСТЭК по поводу терминологии «автоматизированная система» (АС) и «информационная система» (ИС). Основные понятия и положения защиты информации в АС. Этапы развития АС. Классификация задач, решаемых с использованием АС. Модели данных, систем и процессов защиты информации в АС. Требования к моделям защиты информации в АС.

Тема 1. Определение и содержание понятия «угрозы безопасности АС» (16 академ. ч. = 4 ауд. ч.+ 12 ч. сам. раб.)

Особенности современных АС как объектов информационного воздействия, критерии оценки их защищенности. Уязвимости информационно технологических ресурсов АС. Основные угрозы безопасности информации АС и их классификация. Понятие модели нарушителя в автоматизированной системе. Мониторинг угроз безопасности АС.

Тема 2. Оценка угроз безопасности АС (18 академ. ч. = 6 ауд. ч.+ 12 ч. сам. раб.)

Цели и задачи оценки угроз безопасности АС. Понятие базовой модели угроз безопасности информации. Порядок разработки модели угроз и нарушителей информационной безопасности АС. Методы и модели анализа угроз. Базовая модель угроз информационной системы и порядок ее использования. Оценка угроз безопасности информационных систем персональных данных.

Тема 3. Критерии оценки защищенности АС (18 академ. ч. = 6 ауд. ч.+ 12 ч. сам. раб.)

Международные стандарты оценки защищенности. Оценка защищенности на основе отечественных стандартов. История формирования общих критериев. Общий подход к формированию критериев оценки безопасности информационных технологий. Последовательность формирования требований и спе-

цификаций. Понятие профиля защиты и его особенности. Требования общих критериев и результаты оценки.

Тема 4. Реализация моделей безопасности АС (18 академ. ч. = 6 ауд. ч.+ 12 ч. сам. раб.)

Модель реализации многоуровневой защиты автоматизированной системы. Реализация «ядра безопасности». Основные меры по защите информации в АС (организационные, правовые, программно-аппаратные, криптографические, технические). Механизмы и методы защиты в распределенных АС. Условия, способствующие повышению эффективности защиты информации в АС. Архитектура механизмов защиты распределенных АС. Анализ и синтез структурных и функциональных схем защищенных АС.

Тема 5. Особенности разработки информационных систем персональных данных (18 академ. ч. = 6 ауд. ч.+ 12 ч. сам. раб.)

Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности. Особенности защиты среды виртуализации.

Тема 6. Основные категории средств защиты ИС (18 академ. ч. = 6 ауд. ч.+ 12 ч. сам. раб.)

Рекомендации по выбору средств защиты. Руководящие документы средства вычислительной техники, системы обнаружения вторжений, межсетевые экраны, антивирусы, средства защиты от несанкционированного доступа, средства гарантированного уничтожения информации. Сертификация средств защиты информационных систем. Технологические процедуры парольной политики, использования других средств идентификации и аутентификации, криптографических средств.

Заключение (2 академ. часа = 2 ауд. ч.)

Перспективы расширения областей применения защищенных информационных систем. Системы тайного голосования через интернет. Задача обеспечения анонимности. Роль стандартизации в области информационной безопасности.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**Перечень основной и дополнительной учебной литературы,
необходимой для освоения дисциплины**

№	Название, библиографическое описание	Се- мestr	К-во экз. в библ. (на каф.)
Основная литература			
1	Столлингс В. Криптография и защита сетей. Принципы и практика. – М. : Вильямс, 2001.	1	420)
2	Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности : Учеб. пособие. – М. : Изд. Молгачева , 2001. - 351 с	1	20 (0)
Дополнительная литература			
1	Даниленко А.Ю. Безопасность систем электронного документооборота: Технология защиты электронных документов. – М. : URSS, 2015	1	4 (0)
2	Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. – М. : URSS, 2016	1	4 (0)
3	Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. – М. : URSS, 2017	1	4 (0)
4	Перервенко А.В. Модели и методы формирования политик безопасности автоматизированных систем на основе данных активного аудита. – СПб. : Изд-во СПбГЭТУ "ЛЭТИ", 2005.	1	3 (0)
5	Анин Б.Ю. Защита компьютерной информации. – СПб. : БХВ-Петербург, 2000.	1	18 (0)
6	Трубачев, А.П. Формирование требований безопасности автоматизированных систем. – М: Защита информации. Инсайд. – 2005.	1	1 (0)
7	Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М. : Academia, 2005.	1	5 (0)

Зав. отделом учебной литературы Т.В. Киселева

Киселев 4.11.17.

**Перечень ресурсов информационно-телекоммуникационной сети
«Интернет», используемых при освоении дисциплины**

№	Электронный адрес
1	http://fstec.ru/
2	http://fsb.ru/
3	http://government.ru/
4	http://pd.rkn.gov.ru/
5	http://rkn.gov.ru/
6	http://www.gost.ru/
7	http://gostexpert.ru/
8	http://garant.ru/
9	http://consultant.ru/
10	http://www.ispdn.ru/
11	http://iso27000.ru/
12	http://www.securitylab.ru/
13	http://abiss.ru/standards/document_library/

Информационные технологии (операционные системы, программное обеспечение общего и специализированного назначения, а также информационные справочные системы) и материально-техническая база, используемые при осуществлении образовательного процесса по дисциплине, соответствуют требованиям федерального государственного образовательного стандарта высшего образования.

Описание информационных технологий и материально-технической базы приведено в УМКД дисциплины.

Конкретные формы и процедуры текущего контроля знаний и промежуточной аттестации, включая перечень экзаменационных вопросов (Приложение 1), а также методические указания для обучающихся по самостоятельной работе при освоении дисциплин (содержащиеся в ОПОП) доводятся до сведения обучающихся на первом занятии.

ЛИСТ СОГЛАСОВАНИЯ

Разработчики

д.т.н., профессор



Водяхо А.И.

Рецензент

к.т.н., профессор



Мустафин Н. Г.

Зав. кафедрой вычислительной техники,

д.т.н., профессор



Куприянов М.С.

Декан факультета компьютерных технологий

и информатики (ФКТИ),

д.т.н., профессор

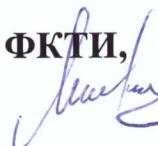


Куприянов М.С.

Согласовано

Председатель учебно-методической комиссии ФКТИ,

к.т.н., доцент



Михалков В.А.

Начальник методического отдела

д.т.н., профессор



Грязнов А.Ю.

Заведующий отделом докторантуры и аспирантуры

к.ф.-м.н.



Кучерова О.В.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№	Дата	Изменение	Дата заседания УМК, № прот-ла	Автор	Нач. МО
1					