

**Федеральное государственное автономное образовательное учреждение
высшего образования
"Национальный исследовательский университет
"Высшая школа экономики"**

МИЭМ
Департамент прикладной математики

**Рабочая программа дисциплины
Защита информации**

для образовательной программы 01.04 04 «Системы управления и обработки информации в инженерии»
направления подготовки 01.04.04 «Прикладная математика»
магистратура

Разработчики программы:

Лось Алексей Борисович, к.т.н., доцент, e-mail: alos@hse.ru

Сорокин Александр Владимирович, asorokin@hse.ru

Одобрена на заседании Кафедры компьютерной безопасности «30» августа 2018 г.

Зав. Кафедрой А. Б. Лось _____

Рекомендована Академическим советом образовательной программы
« » _____ 2018 г., № протокола _____

Утверждена « » _____ 2018 г.

Академический руководитель образовательной программы
/ _____ / _____

Москва, 2018

Настоящая программа не может быть использована другими подразделениями университета и другими вузами без разрешения подразделения-разработчика программы.



1 Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает минимальные требования к знаниям и умениям студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и студентов направления 01.04.04. «Системы управления и обработки информации в инженерии», изучающих дисциплину Защита информации.

Программа разработана в соответствии с:

- ФГОС по направлению подготовки 01.04.04. «Прикладная математика»;
- Образовательной программой направления подготовки 01.04.04. «Системы управления и обработки информации в инженерии»;
- Рабочим учебным планом университета по направлению подготовки 01.04.04. «Системы управления и обработки информации в инженерии», утвержденным в 2018 г.

2 Цели освоения дисциплины

Целью освоения дисциплины Защита информации является формирование у студентов навыков, необходимых для решения следующих предусмотренных образовательным стандартом направления подготовки 01.04.04. «Прикладная математика» профессиональных задач:

- Оценка надежности и качества функционирования объекта проектирования;
- Разработка и расчет вариантов решения проблемы, анализ этих вариантов, прогнозирование последствий, планирование реализации проекта;
- Организация защиты информации и безопасного использования программных средств в вычислительных системах.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

Знать:

- Основные свойства защищаемой информации;
- Основные виды угроз защищаемой информации;
- Классы методов и средств защиты информации;
- Современное состояние и области применения различных классов методов и средств защиты информации.

Уметь:

- Выбирать конкретные классы методов и средств защиты информации для защиты от конкретной угрозы;
- Оценивать обоснованность выбора методов и средств защиты информации;
- Давать рекомендации по совершенствованию уровня защиты информационной системы.

Иметь навыки (приобрести опыт):

- Планирования применения методов и средств защиты информации в конкретной информационной системе;
- Анализа готового решения по применению методов и средств защиты информации в конкретной информационной системе;
- Формирования требований, предъявляемых к методам средствам защиты информации.



В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
Готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	ОК-2	РБ Знает основные угрозы информации Знает основные классы методов и средств защиты информации Знает основные основные виды организационных методов защиты информации СД Способен сформулировать основные рекомендации по защите информации для конкретного объекта Способен аргументированно обосновать или указать недостатки проекта защиты информации для конкретного объекта МЦ Осознает важность защиты информации в информационной системе и на объекте информатизации	Лекции раздела «Организационные методы защиты информации», семинарские занятия
Способность проводить экономический анализ работ, обосновывать оптимальность решения с учетом различных требований	ОПК-1	РБ Знает основные свойства защищаемой информации Знает основные угрозы информации Знает основные классы методов и средств защиты информации СД Способен провести анализ проекта защиты информации для информационной системы с учетом требований обеспечения свойств информации и разумной целесообразности предлагаемых решений Способен аргументированно обосновать оптимальность предлагаемого решения по защите информации для информационной системы Способен предложить пути совершенствования предложенного проекта защиты информации для информационной системы МЦ Обосновывает важность всестороннего анализа предлагаемых проектов мер по защите информации перед их внедрением Излагает риски, возникающие при недостаточном анализе проектов по защите информации	Семинарские занятия



Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
Способность разрабатывать эффективные математические методы решения задач естествознания, техники, экономики и управления	ОПК-2	РБ Знает назначение криптографических средств защиты информации Знает основные категории криптографических средств защиты информации Знает примеры основных классов современных криптографических средств Знает принципы построения эффективных криптографических средств МЦ Обосновывает важность разработки эффективных криптографических средств для обеспечения защиты информации	Лекции раздела «Криптографические средства защиты информации»
Способность анализировать сложные технические системы управления	ПК-1	РБ Знает основные свойства защищаемой информации Знает основные угрозы информации Знает основные классы методов и средств защиты информации СД Способен провести анализ сложной технической системы с точки зрения обеспечения защиты информации Способен аргументированно оценить степень обеспечения защиты информации Способен сформулировать основные рекомендации по повышению уровня защиты информации в исследуемой системе МЦ Обосновывает важность обеспечения защиты информации в сложных технических системах Излагает риски при недостаточном уровне защиты информации в системах управления	
Готовность к принятию ответственности за свои решения в рамках профессиональной компетенции, способность принимать нестандартные решения, разрешать проблемные ситуации	ПК-6	РБ Знает основные угрозы информации Знает основные классы методов и средств защиты информации Знает основные основные виды организационных методов защиты информации СД	Лекции раздела «Организационные методы защиты информации», семинарские занятия



Компетенция	Код по ФГОС/НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
		Способен сформулировать основные рекомендации по защите информации для конкретного объекта Способен аргументированно обосновать или указать недостатки проекта защиты информации для конкретного объекта МЦ Осознает важность защиты информации в информационной системе и на объекте информатизации	

4 Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации» относится к числу дисциплин базовой (общепрофессиональной) части профессионального цикла.

Изучение данной дисциплины базируется на дисциплинах и компетенциях уровня бакалавриата направления подготовки 01.03.04 «Прикладная математика» или других инженерных направлений подготовки.

5 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы			Самостоятельная работа
			Лекции	Семинары	Практические занятия	
1	Задача защиты информации	14	2	4		8
2	Организационные методы защиты информации	18	2	4		12
3	Криптографические методы защиты информации	18	2	4		12
4	Технические средства защиты информации	13	1	4		8
5	Стеганографические методы защиты информации	13	1	4		8
	Всего:	76	8	20		48



6 Формы контроля знаний студентов

Тип контроля	Форма контроля	1 год				Параметры
		1	2	3	4	
Итоговый	Экзамен		+			Устный теоретический экзамен

6.1 Критерии оценки знаний, навыков

Экзамен проводится в виде устного опроса преподавателем по вопросам билета и прочим вопросам, вынесенным на Экзамен. Список вопросов, выносимых на экзамен, выдается преподавателем не позднее 7 недели 1 модуля, причем в случае, если какой-либо вопрос или вопросы не были изучены в ходе лекций или семинарских занятий, он обязан быть исключен из списка вопросов, выносимых на экзамен. Билет содержит 3 вопроса, относящихся ко всем разделам изучаемой дисциплины. При ответе на вопросы билета и дополнительные вопросы студент должен продемонстрировать освоение всей изучаемой дисциплины, выраженное в формировании у него всех компетенций, предусмотренных разделом 3, на предусмотренных уровнях. Преподаватель, принимающий экзамен, оценивает ответ на каждый из вопросов оценкой от 0 до 3 баллов. В этом случае оценки означают: 0 – ответ отсутствует или ответ свидетельствует о том, что соответствующий раздел дисциплины студентом не освоен, 1 – ответ студента свидетельствует об удовлетворительном освоении соответствующего раздела дисциплины, 2 – ответ студента свидетельствует о качественном освоении им соответствующего раздела дисциплины, 3 – ответ студента свидетельствует об отличном освоении им соответствующего раздела дисциплины, понимании материала, свободном владении им. Для уточнения оценки за ответ по конкретному вопросу преподаватель может задавать студенту дополнительные вопросы из списка вопросов, выносимых на экзамен, относящихся к тому же разделу изучаемой дисциплины, либо оценить уровень подготовки студента по конкретному вопросу билета, предложив 3 кратких и конкретных вопроса по вопросу билета, оценивая верный ответ на каждый из них 1 баллом, в результате чего студент имеет возможность получить за ответ на вопрос билета также от 0 до 3 баллов. Таким образом, оценка студента за ответ на вопросы билета может составить от 0 до 9 баллов. К данному результату студента, приступившего к ответу на вопросы билета, прибавляется 1 балл, так что итоговая оценка за экзамен составляет от 1 до 10 баллов. Оценка «0» выставляется при нарушении студентом норм академической этики или проведения итоговой аттестации либо в случае, если студент не приступил к ответу на вопросы экзаменационного билета по любой причине.

7 Содержание дисциплины

Разделы	Темы	
1		Задача защиты информации
	1.1	Свойства защищаемой информации
	1.2	Основные угрозы информации
	1.3	Категории методов и средств защиты информации
	1.4	Принципы выбора методов и средств защиты информации
2.		Организационные методы защиты информации
	2.1	Организация управления потоками информации и разграничения прав доступа
	2.2	Контроль трафика в каналах связи
	2.3	Межсетевые экраны
	2.4	Регламентация действий персонала
	2.5	Политика безопасности организации



	2.6	Управление рисками в информационной безопасности
3		Криптографические методы защиты информации
	3.1	Криптографические примитивы – шифры замены и перестановки
	3.2	Криптоанализ простейших шифров
	3.3	Эволюция шифров с целью их усиления
	3.4	Многоалфавитные шифры
	3.5	Криптоанализ шифра Вижинера
	3.6	Понятие абсолютно стойкого шифра
	3.7	Современные блочные шифры
	3.8	Электронная цифровая подпись и хэш-функции
4		Технические средства защиты информации
	4.1	Физические основы появления ПЭМИН.
	4.2	Каналы утечки данных
	4.3	Поиск каналов утечки данных
	4.4	Методы предотвращения съема данных через физические каналы
5		Стеганографические методы защиты информации
	5.1	Основные понятия стеганографии
	5.2	Исторические примеры стеганографической защиты информации
	5.3	Современные методы стеганографической защиты информации

8 Образовательные технологии

Для проведения занятий применяется класс с проектором для демонстрации презентации.

9 Порядок формирования оценок по дисциплине

Преподаватель оценивает работу студентов на семинарских занятиях: оценивается участие студентов в дискуссиях, выступление с докладами и аргументированность представляемых на обсуждение проектов. Оценки за работу на семинарских занятиях преподаватель выставляет в рабочую ведомость. Накопленная оценка по 10-ти балльной шкале за работу на семинарских занятиях определяется перед итоговым контролем - $O_{\text{ауд}}$.

Накопленная оценка по дисциплине равна накопленной оценке за работу на семинарских занятиях.

$$O_{\text{накопленная}} = O_{\text{ауд}}$$

Результирующая оценка за дисциплину рассчитывается следующим образом:

$$O_{\text{результ}} = 0,7 * O_{\text{накопл}} + 0,3 * O_{\text{экз}}$$

Способ округления накопленной оценки итогового контроля в форме экзамена: арифметический.

На передаче студенту не предоставляется возможность получить дополнительный балл для компенсации накопленной оценки.

10 Учебно-методическое и информационное обеспечение дисциплины

10.1 Базовый учебник



Кабанов А. С., Лось А. Б., Трунцев В. И. Основы информационной безопасности. – М.: МГИЭМ, 2012.

10.2 Основная литература

1. Кабанов А. С., Лось А. Б., Першаков А. С. Теоретические основы компьютерной безопасности. – М.: МГИЭМ, 2012.
2. Хорев П. Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2006
3. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. - М.: Астрель, 2007.
4. Соболева Т. А. История шифровального дела в России. — М.: ОЛМА-ПРЕСС Образование, 2002.
5. Бабаш А. В., Шанкин Г. П. Криптография (аспекты защиты). — М.: СОЛОН-ПРЕСС, 2007.
6. Чмора А. Л. Современная прикладная криптография. – М.: “Гелиос АРВ”, 2001.

10.3 Дополнительная литература

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. - М.: “Гелиос АРВ”, 2001. – 480 с.

11 Материально-техническое обеспечение дисциплины

При проведении занятий используется класс с проектором, подключенным к компьютеру и допускающий демонстрацию презентаций.