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

МИЭМ
Департамент прикладной математики

Рабочая программа дисциплины
Информационная безопасность

для образовательной программы 09.03 03 «Прикладная информатика»
направления подготовки 09.00.00 «Информатика и вычислительная техника»
бакалавриат

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 «29» августа 2016 г.

Зав. Кафедрой А. Б. Лось _____

Рекомендована Академическим советом образовательной программы
« » _____ 201_ г., № протокола _____

Утверждена « » _____ 201_ г.
Академический руководитель образовательной программы
/_____ / _____

Москва, 2016

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 09.03.03. «Прикладная информатика», изучающих дисциплину Информационная безопасность.

Программа разработана в соответствии с:

- ФГОС по направлению подготовки 09.03.03. «Прикладная информатика»;
- Образовательной программой направления подготовки 09.03.03. «Прикладная информатика»;
- Рабочим учебным планом университета по направлению подготовки 09.03.03. «Прикладная информатика», утвержденным в 2016 г.

2 Цели освоения дисциплины

Целью освоения дисциплины Информационная безопасность является формирование у студентов навыков, необходимых для решения слежующих предусмотренных образовательным стандартом направления подготовки 09.03.03. «Прикладная информатика» профессиональных задач:

- Участие в организации ИТ-инфраструктуры и управлении информационной безопасностью ИС
- Анализ и выбор проектных решений по созданию и модификации ИС;
- Оценка затрат и рисков проектных решений, эффективности информационной системы.

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
Способность принимать участие в управлении проектами создания ИС на стадиях жизненного цикла	ПК-9	РБ Знает основные угрозы информации Знает классы методов и средств защиты информации Знает назначение основных классов методов и средств защиты информации СД Способен предложить проект системы информационной безопасности ИС Способен аргументированно оценить предложенный проект системы информационой безопасности ИС МЦ Обосновывает важность тщательного проектирования подсистемы информационной безопасности ИС	Лекции и практические занятия разделов «Организационные методы защиты информации», «Криптографические методы защиты информации», «Технические средства защиты информации»
Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	ПК-10	РБ Знает свойства защищаемой информации Знает основные угрозы информации Знает назначение организационных методов защиты информации Знает назначение основных классов методов и средств защиты информации СД Способен представить проект высокоуровневой политики безопасности объекта информатизации Способен агрументированно оценить проект высокоуровневой политики безопасности объекта информатизации Способен осуществлять поддержку высокоуровневой политики безопасности объекта информатизации на этапах ее жизненного цикла МЦ Осознает важность грамотного управления информационной безопасностью для обеспечения надлежащего уровня безопасности объекта информатизации	Лекции и практические занятия раздела «Организационные методы защиты информации»
Способность осуществлять и обосновывать выбор	ПК-12	РБ Знает классы методов и средств	Лекции и практические занятия разделов «Задача за-

Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
проектных решений по видам обеспечения информационных систем		защиты информации Знает назначение основных классов методов и средств защиты информации Знает основные виды криптографических средств защиты информации Знает основные виды технических средств защиты информации СД Способен осуществить обоснованный выбор средств защиты информации Способен предложить обоснованный проект использования выбранных средств защиты информации	щиты информации», «Криптографические методы защиты информации», «Технические средства защиты информации»
Способность анализировать рынок программно-технических средств, информационных продуктов и услуг для создания и модификации ИС	ПК-14	РБ Знает классы методов и средств защиты информации Знает назначение основных классов методов и средств защиты информации Знает основные виды криптографических средств защиты информации Знает основные виды технических средств защиты информации	Лекции и практические занятия разделов «Криптографические методы защиты информации», «Технические средства защиты информации»

4 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к числу дисциплин базовой части программы бакалавриата.

Изучение данной дисциплины базируется на основных естественнонаучных и математических дисциплинах.

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями и компетенциями:

- Знанием основных понятий и терминологии в области теории групп, колец и полей
- Знанием основных принципов электромагнетизма и распространения электромагнитных волн
- Понятием о кодировании различных типов информации, существовании различных кодировок текстовой инфоормации
- Умением совершать операции с действительными числами в различных позиционных системах счисления
- Знанием аппаратного устройства основных узлов компьютерных систем

5 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы			Самостоятельная работа
			Лекции	Семинары	Практические занятия	
1	Задача защиты информации	16	2		4	10
2	Организационные методы защиты информации	12	2		2	8
3	Криптографические методы защиты информации	18	4		6	8
4	Технические средства защиты информации	14	4		2	8
5	Стеганографические методы защиты информации	12	2		2	8

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 8 недели 2 модуля, причем в случае, если какой-либо вопрос или вопросы не были изучены в ходе лекций или практических занятий, он обязан быть исключен из списка вопросов, выносимых на экзамен. Билет содержит 5 вопросов, относящихся ко всем разделам изучаемой дисциплины. Преподаватель, принимающий экзамен, может оценить каждый из ответов оценкой от 0 до 2 баллов. В этом случае оценки означают: 0 – ответ отсутствует или ответ свидетельствует о том, что данный раздел дисциплины студентом не освоен, 1 – ответ студента свидетельствует об удовлетворительном освоении данного раздела дисциплины, 2 – ответ студента свидетельствует о качественном освоении им данного раздела дисциплины. Для уточнения оценки по конкретному вопросу преподаватель может задавать студенту дополнительные вопросы из списка вопросов, выносимых на экзамен, относящихся к тому же разделу изучаемой дисциплины. Итоговая оценка за экзамен в этом случае определяется суммой оценок за каждый вопрос и может равняться от 0 до 10 баллам. 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.

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 отдельных практических занятий применяется класс с проектором для демонстрации презентаци.

9 Порядок формирования оценок по дисциплине

Преподаватель оценивает работу студентов на семинарских занятиях: оенивается участие студентов в дискуссиях 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 окончанием 2 модуля перед итоговым контролем - $O_{ауд}$.

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

$$O_{накопленная} = O_{ауд}$$

Результирующая оценка за дисциплину рассчитывается следующим образом:

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

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

На пересдаче 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 отдельных семинарских занятий используется класс с проектором, подключенным к компьютеру и допукающий демонстрацию презентаций.