



Национальный исследовательский университет «Высшая школа экономики»
Программа дисциплины Защита информации для направления 09.03.01 «Информатика и
вычислительная техника» подготовки бакалавра

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

Московский институт электроники и математики
Департамент компьютерной инженерии

**Рабочая программа дисциплины
Защита информации**

для образовательной программы «Информатика и вычислительная техника»
направления подготовки 09.03.01. Информатика и вычислительная техника
уровень академический бакалавр

Разработчик программы
Акатов М. С., к.т.н., Makatov@hse.ru

Одобрена на заседании Департамента компьютерной инженерии
« 30 » августа 2016 г.
Руководитель департамента В.А. Старых _____

Утверждена Академическим советом образовательной программы
« 1 » сентября 2016 г., № протокола _____

Академический руководитель образовательной программы
Т.А. Потапова _____

Москва, 2016

*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 отчётности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и студентов, обучающихся на образовательной программе «Информатика и вычислительная техника», изучающих дисциплину «Защита информации». уровень академический бакалавр

Программа разработана в соответствии с:

- по направлению подготовки 09.03.01 «Информатика и вычислительная техника» уровень академический бакалавр;
- рабочим учебным планом университета образовательной программы «Информатика и вычислительная техника», утверждённым в 2016 г.

2 Цели освоения дисциплины

Цель дисциплины «Защита информации» - заложить практические правила защитой информации, научить проводить анализ угроз безопасности, приобрести навыки защиты информации; изучить методы и средства обеспечения защиты информации.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

Знать:

- основные требования нормативно-правовой базы информационной безопасности к защите информации от несанкционированного доступа, программных средств скрытого информационного воздействия, утечки информации по техническим каналам;
- задачи информационной безопасности, основные тенденции и направления формирования и функционирования комплексной системы защиты информации.

Уметь:

- применять методы определения причин, видов, источников и каналов утечки, искажения информации.

Иметь навыки (приобрести опыт):



- применения методов и форм защиты информации;
- формирования требований к защите 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	ОК-2	Знает основные угрозы информации Знает основные методы и средства защиты информации Знает основные виды организационных методов защиты информации Способен сформулировать основные рекомендации по защите информации Способен аргументированно обосновать или указать недостатки проекта защиты информации	Лекции, Практические Занятия
Способность анализировать сложные технические системы управления	ПК-1	Знает основные свойства защищаемой информации Знает основные угрозы информации Знает основные классы и средства защиты информации Способен аргументированно оценить степень обеспечения защиты информации Способен сформулировать основные рекомендации по повышению уровня защиты информации	Лекции, Практические Занятия
Готовность к принятию ответственности за свои решения, способность принимать нестандартные решения, разрешать проблемные ситуации	ПК-6	Знает основные угрозы информации Знает основные классы методов и средств защиты информации Знает основные виды организационных методов защиты информации Способен сформулировать основные рекомендации по защите информации для конкретного объекта	Лекции, Практические занятия

4 Место дисциплины в структуре образовательной программы

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



4.1 Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы Вид учебной работы	Всего часов	1 модуль		2 модуль	
Аудиторные занятия	56	28		28	
Лекции (Л)	24	12		12	
Семинары (С)					
Практические (лабораторные) занятия	32	16		16	
Самостоятельная работа	124	62		62	
Вид контроля				ДЗ, Э	
Общая трудоемкость (часы)	180	90		90	

5 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы		Сам. работа
			Лекции	Практические занятия	
1	Информационная безопасность	2	2		
2	Основы информационной безопасности и защиты информации	2	2		
3	Нормативно-правовая база информационной безопасности	6	2	5	
4	Виды и особенности угроз информационной безопасности	32	2	5	24
5	Каналы утечки информации	32	4	5	24
6	Организационные основы защиты информации организации	32	4	5	24
7	Инженерно-технические и программные методы защиты информации в организации	36	4	6	24
8	Оценка эффективности мероприятий по защите информации в организации	38	4	6	28
	Всего	180	24	32	124



6 Формы контроля знаний студентов

Тип контроля	Форма контроля	1 год				Параметры
		1	2	3	4	
Промежуточный	Домашнее задание		+			Письменная работа
Итоговый	Экзамен		+			Устный теоретический экзамен

7 Критерии оценки знаний, навыков

Итоговый контроль на курсе – устный экзамен с оценкой, включающий 2 теоретических вопроса.

Итоговая оценка за экзамен определяется суммой оценок за каждый вопрос и может равняться от 0 до 10 баллов. При ответе на вопросы билета и дополнительные вопросы студент должен продемонстрировать освоение всей изучаемой дисциплины, выраженное в формировании у него всех компетенций.

8 Содержание дисциплины

№	Наименование раздела дисциплины	Содержание раздела
1	Информационная безопасность	Основные понятия и определения. Современное состояние и перспективы развития защиты информации
2	Основы информационной безопасности и защиты информации	Принципы организации системы защиты, политика информационной безопасности, направления, способы и методы защиты.
3	Нормативно-правовая база информационной безопасности	Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Международные правовые акты по защите информации. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций. Виды тайн и законодательство по ограничениям оборота информации, относимой к различным тайнам
4	Виды и особенности угроз информационной безопасности	Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Предпосылки и причины.
5	Каналы утечки информации	Понятие и классификация каналов утечки



		информации. Характеристика каждого канала. Классификация каналов.
6	Организационные основы защиты информации организации	Понятие, цели и задачи системы защиты информации. Принципы построения системы, её технологичность, иерархичность и факторы эффективности. Принцип разграничения доступа. Принцип регламентации состава защищаемой информации. Принцип персональной ответственности. Принципы надёжности и превентивности.
7	Инженерно-технические и программные методы защиты информации в организации	Технические средства противодействия. Защита СВТ и носителей информации. Защита каналов связи. Защита программ и электронных баз данных.
8	Оценка эффективности мероприятий по защите информации в организации	Проведение мероприятий по защите информации в организации и оценка их эффективности

9 Образовательные технологии

Основное внимание при изучении дисциплины должно уделяться решению практических задач защиты информации в организации.

10 Оценочные средства для текущего контроля и аттестации студента

Тематика заданий текущего контроля

Примерные вопросы/ задания для [Укажите название текущего контроля, проводимого в письменной форме - контрольной работы, коллоквиума, домашнего задания]:

1. Вопрос
- 2.

Тематика [Укажите название текущего контроля - курсовые, эссе или другое] :

1. Тема
- 2.

Тема [Укажите название текущего контроля - эссе, рефераты или другое] для каждого студента утверждается преподавателем в индивидуальном порядке.

Вопросы для оценки качества освоения дисциплины

Примерный перечень вопросов к зачету (экзамену) по всему курсу или к каждому промежуточному и итоговому контролю для самопроверки студентов.

Примеры заданий промежуточного /итогового контроля

По желанию автора программы, приводятся примеры билетов с вопросами и задачами, заданий для зачета или экзамена, тренировочные тесты по дисциплине.



11 Порядок формирования оценок по дисциплине

Текущий и промежуточный контроль первого семестра:

- **Q1дом.зад.** – оценка за домашнее задание. Оценка выставляется по десятибалльной шкале при условии сдачи задания в срок.
- **Q1вопрос1, Q1вопрос2** – оценки за ответ на вопросы на устном экзамене. Каждый ответ оценивается по пятибалльной шкале.
- **Qитоговая** - итоговая оценка по дисциплине формируется по десятибалльной шкале и рассчитывается по формуле:

$$Q_{итоговая} = 0,5Q_{1дом.} + 0,5(Q_{1вопрос1} + Q_{1вопрос2})$$

Способ округления оценки: арифметический.

12 Учебно-методическое и информационное обеспечение дисциплины

12.1 Основная литература:

Научно-методические основы обеспечения безопасности защищаемых объектов

Автор: Ю.Б. Михайлов, Издательство: Горячая Линия - Телеком, ISBN 978-5-9912-0485-9; 2015 г.

Безопасность компьютерных сетей Автор: В.Г. Олифер, Н.А. Олифер, Издательство: Горячая Линия - Телеком, ISBN 978-5-9912-0420-0; 2015 г.

Методы оценки несоответствия средств защиты информации Авторы: А.С. Марков, В.Л. Цирлов, А.В. Барабанов, Издательство: Радио и связь, ISBN 5-89776-015-2; 2012 г.

Информационная безопасность открытых систем Автор: Д.А. Мельников, Издательство: Флинта, ISBN 978-5-02-037923-7; 2013 г.

Научно-методические основы обеспечения безопасности защищаемых объектов
Автор: Ю.Б. Михайлов, Издательство: Горячая Линия - Телеком, ISBN 978-5-9912-0485-9; 2015 г.

Стандарты информационной безопасности Автор: В. А. Галатенко, Издательство: Интернет-университет информационных технологий, Серия: Основы информационных технологий, ISBN 978-5-9556-0053-6; 2010 г.;

Организационно-правовое обеспечение информационной безопасности Редактор Анатолий Стрельцов, Издательство: Академия, Серия: Высшее профессиональное образование, ISBN 978-5-7695-4240-4; 2008 г.;



Защита информации в сети. Анализ технологий и синтез решений Галицкий А. В., Рябко С. Д., Шаньгин В. Ф., Издательство: ДМК Пресс, 2004 г., Твердый переплет, 616 стр., ISBN 5-94074-244-0;

Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей Автор: В. В. Платонов, Издательство: Академия, Серия: Высшее профессиональное образование, ISBN 5-7695-2706-4; 2006 г.

12.2 Дополнительная литература:

Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий Автор: В. А. Сердюк, Издательство: Высшая Школа Экономики (Государственный Университет), ISBN 978-5-7598-0698-1; 2011 г.

13 Материально-техническое обеспечение дисциплины

При проведении отдельных семинарских занятий используется класс с проектором, подключённым к компьютеру и допускающий демонстрацию презентаций.