Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»

Лениногорский филиал

(наименование института, в состав которого входит кафедра, ведущая дисциплину)

Кафедра Машиностроения и информационных технологий

(наименование кафедры, ведущей дисциплину)

АННОТАЦИЯ

к рабочей программе

дисциплины (модуля)

«Защита информации»

Индекс по учебному плану: **Б1.В.17**

Направление подготовки**: 09.03.02 Информационные системы и технологии**

Квалификация: **бакалавр**

Направленность (профиль) программы: **Информационные системы**

Виды профессиональной деятельности: **проектно-технологическая; монтажно-наладочная**

Разработчик: старший преподаватель кафедры ЕНГД Т.А. Яншина

Лениногорск 2018 г.

1.1. Цель изучения дисциплины (модуля)

Целью изучения дисциплины является: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.2. Задачи дисциплины (модуля)

– освоение защиты информации как систематической научно-практической деятельности, носящей прикладной характер;

– знание базовых теоретических понятий, лежащих в основе процесса защиты информации;

– усвоение методов и способов защиты информации.

1.3. Место дисциплины (модуля) в структуре ОП ВО

Дисциплина «Защита информации» входит в состав вариативной части Блока 1 Дисциплины (модуля).

1.4 Осваиваемые компетенции, результаты освоения:

ПК-28 - способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию.

ПК-34 - способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию.

1.5 Трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 2 зачётные единицы или 72 часа. Формы промежуточной аттестации – зачет.

1.6 Содержание дисциплины

Раздел 1. Основы защиты информации.

Тема 1.1. Основные понятия и определения. Концептуальные основы защиты информации.

Становление и развитие понятия «информационная безопасность». Современные подходы к определению понятия. Сущность информационной безопасности, характеристика ее составляющих. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия “информационная безопасность”.

Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации. Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности.

Тема 1.2. Организационно-правовые аспекты защиты информации. Политика безопасности и управление рисками.

Современная концепция информационной безопасности Российской Федерации. Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их

достижения. Виды и состав угроз информационной безопасности. Состояние информационной безопасности Российской Федерации и основные задачи по их обеспечению. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в различных сферах общественной жизни. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Организационная основа системы обеспечения информационной безопасности.

Раздел 2. Криптография и алгоритмы шифрования.

Тема 2.1. Стандартизация в сфере ИТ-безопасности. Правовые основы стандартизации и сертификации в РФ и зарубежных странах. Гармонизация российской системы стандартизации и сертификации с европейскими и международными правилами. Закон о техническом регулировании. Основные понятия. Закон о техническом регулировании. Понятия технических регламентов и стандартизации.

Организационная структура технического комитета ИСО 176, модель описания системы качества в стандартах ИСО 9001 и 9004 и модели функционирования системы менеджмента качества (СМК), основанной на процессном подходе.

Схемы сертификации, инфраструктура сертификации ИКТ в образовании, сертификация в жизненном цикле программной продукции и результаты экспертной оценки.

Тема 2.2. Математические методы и модели в задачах защиты информации.

Основные понятия криптографии. Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома.

Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома. Симметричные системы шифрования. Основные понятия и определения. Классификация симметричных систем шифрования: поточные шифры, блочные шифры. Блочные шифры. Сеть Фейштеля. Алгоритм TEA. Алгоритм DES. Алгоритм ГОСТ 28147-89. Сравнение алгоритмов DES и ГОСТ 28147-89. Модификация алгоритма DES: тройной DES с двумя и тремя ключами. Алгоритм AES. Режимы выполнения алгоритмов шифрования: EBC, CBC, CFB и OFB.

Потоковые шифры. Алгоритм RC4. Математические основы криптографических методов. Основные понятия и определения теории информации. Основные теоремы теории чисел (арифметика вычетов, малая теорема Ферма, теорема Эйлера, разложение числа на простые сомножители). Наибольший общий делитель. Алгоритм Евклида. Обобщенный алгоритм Евклида. Возведение в степень по модулю. Дискретные логарифмы в конечном поле. Понятия однонаправленной функции и однонаправленной функции с лазейкой. Элементы теории сложности проблем.

Классы сложности проблем.

Тема 2.3. Многоуровневая защита информации в компьютерных системах и сетях.

Принципы многоуровневой защиты информации. Обеспечение безопасности операционных систем. Протоколы защищенных каналов.

Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей VPN. Защита удаленного доступа. Технологии обнаружения и предотвращения вторжений. Технологи защиты от вредоносных программ и спама.

1.7 Учебно-методическое обеспечение дисциплины

1.7.1. Основная литература:

1. Малюк А.А. Теория защиты информации. [Электронный ресурс]. - М.: Издательство Горячая линия-Телеком, 2012. - 184 с.- Режим доступа: https://e.lanbook.com/reader/book/5170/#1

2. Информационная безопасность и защита информации. [Электронный ресурс]: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование).- Режим доступа: http://znanium.com/bookread2.php?book=763644

1.7.2. Дополнительная литература:

3. Платонов В.В. Программно-аппаратные средства защиты информации: учебник.- М.: ИЦ Академия, 2014. - 336 с.

4. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие / И. В. Аникин, В. И. Глова, Л. И. Нейман, А.Н. Нигматуллина. - Казань: Издательство КГТУ им. А.Н. Туполева, 2008. - 280 с. – Режим доступа: http://e-library.kai.ru/reader/hu/flipping/Resource-1282/%D0%9C465.pdf/index.html

5. Мельников В.П. Защита информации: учебник.- М. ИЦ Академия, 2014. - 304 с. - Рек. УМО

1.8 Информационное обеспечение дисциплины (модуля)

1.8.1 Основное информационное обеспечение

- e-library.kai.ru – Библиотека Казанского национального исследовательского технического университета им. А.Н. Туполева
- elibrary.ru – Научная электронная библиотека
- e.lanbook.ru - ЭБС «Издательство «Лань»
- ibook.ru - Электронно-библиотечная система Айбукс
- http://znanium.com

1.8.2 Перечень информационных технологий, включая перечень программного обеспечения и информационных справочных систем

- Microsoft Visual Studio
- Microsoft Windows Professional 7 Russian
- Microsoft Office Professional Plus 2010 Russian
- Microsoft Office Professional Plus 2007 Russian
- Антивирусная программа Kaspersky Endpoint Security 10, 8

1.9 Кадровое обеспечение

1.9.1 Базовое образование

Высшее образование в предметной области информационные технологии и /или наличие ученой степени и/или ученого звания в указанной области и /или наличие дополнительного профессионального образования – профессиональной переподготовки в области информационных технологий.

1.9.2 Профессионально-предметная квалификация преподавателей

Профессионально-предметная деятельность преподавателей связана с информационными технологиями. Направления научных и прикладных работ имеют непосредственное отношение к содержанию и требованиям дисциплины.

Преподаватель участвует в научно-исследовательской работе кафедры, в семинарах и конференциях по направлению исследований кафедры в рамках своей дисциплины. Руководит научно-исследовательской работой студентов, систематически выступает на региональных и международных научных конференциях, публикует научные работы.

1.9.3 Педагогическая (учебно-методическая) квалификация преподавателей

К ведению дисциплины допускаются кадры, имеющие стаж научно-педагогической работы (не менее 1 года); практический опыт работы в данной области.

Обязательное прохождение повышения квалификации (стажировки) не реже чем один раз в три года в соответствующей области, либо в области педагогики.