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
Кафедра Информационных технологий

УТВЕРЖДАЮ
Директор ЛФ КНИТУ-КАИ
_____ Р.А. Шамсутдинов
«01» сентября 2017г.
Регистрационный номер 0428 10/17-16

РАБОЧАЯ ПРОГРАММА

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**

Лениногорск 2017

Рабочая программа составлена на основе требований федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 12 марта 2015г. №219 и в соответствии с рабочим учебным планом направления 09.03.02, утвержденным Ученым советом КНИТУ-КАИ «31» августа 2015г., протокол № 6.

Рабочая программа дисциплины (модуля) разработана ст.преподавателем Яншиной Т.А. _____.
(подпись преподавателя)

утверждена на заседании кафедры ИТ протокол № 2 от 01.09.2017 г.

И.о. заведующего кафедрой к.п.н. Ахмедзянова Ф.К._____

Рабочая программа дисциплины:	Наименование Подразделения	Дата	№ протокола	Подпись
СОГЛАСОВАНА	на заседании кафедры ИТ	01.09.2017	№2	_____ И.о. зав.кафедрой Ф.К. Ахмедзянова
ОДОБРЕНА	Учебно-методическая комиссия ЛФ КНИТУ-КАИ	01.09.2017	№2	_____ Председатель УМК З.И.Аскарова
СОГЛАСОВАНА	Научно-техническая библиотека	01.09.2017		_____ Библиотекарь А.Г. Страшнова

РАЗДЕЛ 1. ИСХОДНЫЕ ДАННЫЕ И КОНЕЧНЫЙ РЕЗУЛЬТАТ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Цели 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 Б1.В.17 относится к вариативной части Блока 1 Дисциплины (модули).

Логическая и содержательная связь дисциплин, участвующих в формировании представленных в п.1.5 компетенций:

Компетенция: ПК-28.

Предшествующие дисциплины: Технология обработки информации; Инструментальные средства информационных систем; Операционные системы; Инфокоммуникационные системы и сети; Надежность, эргономика и качество информационных систем; Управление проектированием информационных систем; Корпоративные информационные системы; Производственная практика по получению профессиональных умений и опыта профессиональной деятельности.

Дисциплины, изучаемые одновременно: Мультимедиа-технологии; Преддипломная практика.

Последующие дисциплины: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

Компетенция: ПК-34.

Предшествующие дисциплины: Технология обработки информации; Инструментальные средства информационных систем; Операционные системы; Инфокоммуникационные системы и сети; Надежность, эргономика и качество информационных систем; Управление проектированием информационных систем; Корпоративные информационные системы; Производственная практика по получению профессиональных умений и опыта профессиональной деятельности.

Дисциплины, изучаемые одновременно: Мультимедиа-технологии; Преддипломная практика.

Последующие дисциплины: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

1.4. Объем дисциплины (модуля) (с указанием трудоемкости всех видов работы)

Таблица 1а

Объем дисциплины (модуля) для очной формы обучения

Виды учебной работы	Общая Трудоемкость		Семестр 8	
	В ЗЕ	В часах	В ЗЕ	В часах
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	**2**	**72**	**2**	**72**
Контактная работа обучающихся с преподавателем (аудиторные занятия)	***1***	***36***	***1***	***36***
Лекции	0,5	18	0,5	18

Практические занятия	Не предусмотрены			
Лабораторные работы	0,5	18	0,5	18
Самостоятельная работа Обучающегося	***1***	***36***	***1***	***36***
Проработка учебного материала	1	36	1	36
Курсовой проект	Не предусмотрен			
Курсовая работа	Не предусмотрена			
Подготовка к промежуточной аттестации (зачет)				
Промежуточная аттестация	Зачет			

Таблица 1б

Объем дисциплины (модуля) для заочной формы обучения

Виды учебной работы	Общая Трудоемкость		Семестр	
			9	
	В ЗЕ	В часах	В ЗЕ	В часах
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	**2**	**72**	**2**	**72**
Контактная работа обучающихся с преподавателем (аудиторные занятия)	***0,3***	***12***	***0,3***	***12***
Лекции	0,2	8	0,2	8
Практические занятия	Не предусмотрены			
Лабораторные работы	0,1	4	0,1	4
Самостоятельная работа Обучающегося	***1,6***	***56***	***1,6***	***56***
Проработка учебного материала	1,6	56	1,6	56
Курсовой проект	Не предусмотрен			
Курсовая работа	Не предусмотрена			
Подготовка к промежуточной аттестации (зачету)	***0,1***	***4***	***0,1***	***4***
Промежуточная аттестация	Зачет			

1.5 Планируемые результаты обучения

Таблица 2

Формируемые компетенции

Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)	Уровни освоения составляющих компетенций		
	Пороговый	Продвинутый	Превосходный
ПК-28 – способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию			

Знание (ПК-28З) – положений по защите информации, основных средств защиты информации	Знание положений по защите информации, основных средств защиты информации	Знание положений по защите информации, основных средств защиты информации, видов угроз для информации	Знание положений по защите информации, основных средств защиты информации, видов угроз для информации, методов их устранения и программных средств защиты
Умение (ПК-28У) – устанавливать и использовать средства защиты информации, такие как антивирусы	Умение устанавливать и использовать средства защиты информации, такие как антивирусы	Умение устанавливать и использовать средства защиты информации, такие как антивирусы, программы проверки жестких дисков и флеш-накопителей	Умение устанавливать и использовать средства защиты информации, такие как антивирусы, программы проверки жестких дисков и флеш-накопителей, программы по шифрованию данных
Владение (ПК-28В) – навыками обнаружения и устранения сетевых угроз, распознавания стандартных вирусов	Владение навыками обнаружения и устранения сетевых угроз, распознавания стандартных вирусов	Владение навыками обнаружения и устранения сетевых угроз, распознавания стандартных вирусов, отслеживания и блокировки сетевых атак	Владение навыками обнаружения и устранения сетевых угроз, распознавания стандартных вирусов, отслеживания и блокировки сетевых атак, отслеживания программ по подбору паролей
ПК-34 – способностью к инсталляции, отладке программных и настройке технических средств для ввода информационных систем в опытную и промышленную эксплуатацию			
Знание (ПК-34З) - способов и методов инсталляции, отладки программных и настройки технических средств, для ввода информационных систем в опытную и промышленную эксплуатацию	Знание способов и методов обеспечения защиты компьютерной информации	Знание способов и методов обеспечения защиты компьютерной информации, принципов работы систем защиты информации	Знание способов и методов обеспечения защиты компьютерной информации, принципов работы систем защиты информации, способов использования систем защиты информации
Умение (ПК-34У) - производить инсталляцию, отладку программных и настройку технических средств, для ввода информационных систем в опытную и промышленную эксплуатацию	Умение производить инсталляцию систем компьютерной безопасности	Умение производить инсталляцию и отладку систем компьютерной безопасности	Умение производить инсталляцию и отладку систем компьютерной безопасности, настройку систем оповещения
Владение (ПК-34В) - навыками производить инсталляцию, отладку программных и настройку технических средств, для ввода информационных систем в опытную и промышленную эксплуатацию	Владение навыками работы с системами компьютерной безопасности	Владение навыками работы с системами компьютерной безопасности, мониторинга программно-аппаратных комплексов на предмет компьютерных угроз.	Владение навыками работы с системами компьютерной безопасности, мониторинга программно-аппаратных комплексов на предмет компьютерных угроз, ввод защищенных программно-аппаратных комплексов в эксплуатацию

РАЗДЕЛ 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) И ТЕХНОЛОГИЯ ЕЕ ОСВОЕНИЯ

2.1. Структура дисциплины (модуля) и ее трудоемкость

Таблица 3а

Распределение фонда времени по видам занятий
Очная форма

Наименование раздела и темы	Всего часов	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах/интерактивные часы)				Коды составляющих компетенций	Формы и вид контроля освоения составляющих компетенций (из фонда оценочных средств)
		лекции	лаб. раб.	пр. зан.	сам. раб.		
Раздел 1. Основы защиты информации							*ФОС ТК-1*
Основные понятия и определения. Концептуальные основы защиты информации	8	2		-	6	*ПК-28, ПК-34*	Текущий контроль
Организационно-правовые аспекты защиты информации. Политика безопасности и управление рисками	12	2	4	-	6	*ПК-28, ПК-34*	Текущий контроль
Раздел 2. Криптография и алгоритмы шифрования. Сетевая защита							*ФОС ТК-2*
Стандартизация в сфере ИТ-безопасности	16	4	4	-	8	*ПК-28, ПК-34*	Текущий контроль
Математические методы и модели в задачах защиты информации	16	4	4	-	8	*ПК-28, ПК-34*	Текущий контроль
Многоуровневая защита информации в компьютерных системах и сетях	20	6	6	-	8	*ПК-28, ПК-34*	Текущий контроль
Зачет						*ПК-28, ПК-34*	*ФОС ПА-1*
ИТОГО:	**72**	**18**	**18**	**-**	**36**		

Таблица 3б

Распределение фонда времени по видам занятий
Заочная форма

Наименование раздела и темы	Всего часов	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах/интерактивные часы)				Коды составляющих компетенций	Формы и вид контроля освоения составляющих компетенций (из фонда оценочных средств)
		лекции	лаб. раб.	пр. зан.	сам. раб.		
Раздел 1. Основы защиты информации							*ФОС ТК-1*
Основные понятия и определения. Концептуальные основы защиты информации	13	2		-	11	*ПК-28, ПК-34*	Текущий контроль
Организационно-правовые аспекты защиты информации. Политика безопасности и управление рисками	13	1	1	-	11	*ПК-28, ПК-34*	Текущий контроль
Раздел 2. Криптография и алгоритмы шифрования. Сетевая защита							*ФОС ТК-2*
Стандартизация в сфере ИТ-безопасности	14	2	1	-	11	*ПК-28, ПК-34*	Текущий контроль
Математические методы и модели	13	1	1	-	11	*ПК-28, ПК-34*	Текущий контроль

в задачах защиты информации							
Многоуровневая защита информации в компьютерных системах и сетях	15	2	1	-	12	*ПК-28, ПК-34*	Текущий контроль
Зачет	4					*ПК-28, ПК-34*	*ФОС ПА-1*
ИТОГО:	**72**	**8**	**4**	**-**	**56**		

Таблица 4

Матрица компетенций по разделам РП

Наименование раздела (тема)	Формируемые компетенции (составляющие компетенций)					
	ПК-28			ПК-34		
	ПК-28З	ПК-28У	ПК-28В	ПК-34З	ПК-34У	ПК-34В
Раздел 1						
Тема 1.1	+	+	+			+
Тема 1.2	+	+	+			+
Раздел 2						
Тема 2.1	+	+		+	+	+
Тема 2.2	+	+		+	+	+
Тема 2.3	+	+		+	+	+

2.2. Содержание дисциплины (модуля)

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.

Литература: [2]; [3]; [5].

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.

Литература: [2]; [3]; [5].

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.

Литература: [1]; [3]; [4].

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.

Литература: [1]; [3]; [4].

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.

Литература: [1]; [2]; [5].

2.3. Курсовое проектирование

Курсовое проектирование по данной дисциплине в соответствии с учебным планом не предусмотрено.

РАЗДЕЛ 3. ОЦЕНОЧНЫЕ СРЕДСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ И КРИТЕРИИ ОЦЕНОК ОСВОЕНИЯ КОМПЕТЕНЦИЙ

3.1. Оценочные средства для текущего контроля

Фонд оценочных средств для проведения текущего контроля (ФОС ТК) является составной частью РП дисциплины (модуля) и хранится на кафедре.

Таблица 5

Фонд оценочных средств текущего контроля

№ п/п	Наименование раздела (модуля)	Вид оценочных средств	Примечание
1	2	3	4
1.	Раздел 1. Основы защиты информации	ФОС ТК-1	Тест по первому разделу Лабораторный практикум
2.	Раздел 2. Криптография и алгоритмы шифрования. Сетевая защита	ФОС ТК-2	Тест по второму разделу Лабораторный практикум

Типовые оценочные средства для текущего контроля: ФОС ТК-1.

Перечень лабораторных работ:

- Реализация дискретной модели политики безопасности
- Количественная оценка стойкости парольной защиты

Тест

№1 Антивирусная программа – специализированная программа для обнаружения компьютерных вирусов, нежелательных программ вообще и восстановления зараженных такими программами файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.

Antivirus Kaspersky
DrWeb
Avast
Nod 32

№2 Сервисы безопасности это
Обеспечение безопасного восстановления
Инверсия паролей
Контроль целостности
Регулирование конфликтов
Шифрование
Кэширование записей
Экранирование

№3 Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза

Активная
Умышленная
Пассивная

№4 Основные угрозы конфиденциальности информации
блокирование

маскарад
злоупотребления полномочиями
переадресовка
перехват данных

№5 Элементы знака охраны авторского права
Года первого выпуска программы
Наименование охраняемого объекта
Наименования (имени) правообладателя

Типовые оценочные средства для текущего контроля: ФОС ТК-2.

Перечень лабораторных работ:

- Ассиметричные алгоритмы шифрования данных
- Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра

Тест

№1 Отметьте составные части современного
Модем
Принтер
Сканер
Межсетевой экран
Монитор

№2 Вредоносные программы - это
Шпионские программы
Программы, наносящие вред данным и программам, находящимся на компьютере
Антивирусные программы
Программы, наносящие вред пользователю, работающему на зараженном компьютере
Троянские утилиты и сетевые черви

№3 К вредоносным программам относятся
Потенциально опасные программы
Вирусы, черви, трояны
Шпионские и рекламмные программы
Вирусы, программы-шутки, антивирусное программное обеспечение
Межсетевой экран, брандмауэр

№4 Сетевые черви это
Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты
Вирусы, которые проникнув на компьютер, блокируют работу сети
Вирусы, которые внедряются в документы под видом макросов
Хакерские утилиты управляющие удаленным доступом компьютера
Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

№5 Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется

Загрузочный вирус
Макровирус
Троян
Сетевой червь
Файловый вирус

3.2. Оценочные средства для промежуточного контроля

Фонд оценочных средств для проведения промежуточной аттестации (ФОС ПА) является составной частью РП дисциплины, разработан в виде отдельного документа, в соответствии с положением о ФОС ПА.

Первый этап: типовые тестовые задания

№1 Свойство вируса, позволяющее называться ему загрузочным – способность …
Заражать загрузочные сектора жестких дисков
Заражать загрузочные дискеты и компакт-диски
Вызывать перезагрузку компьютера-жертвы
Подсвечивать кнопку Пуск на системном блоке

№2 К классу условно опасных относятся программы …
О которых нельзя однозначно сказать, что они вредоносны
Последствия выполнения которых нельзя предугадать
Которые можно выполнять только при наличии установленного антивирусного программного обеспечения
Характеризующиеся способностью при срабатывании заложенных в них выполнять какое-либо действие, например, удаление файлов. В остальное время они безвредны

№3 Типы методов антивирусной защиты
Теоретические
Практические
Организационные
Технические
Программные

№4 Главное преимущество встроенного в Microsoft Windows брандмауэра по сравнению с устанавливаемыми отдельно персональными брандмауэрами
Более ясный и интуитивно понятный интерфейс
Отсутствие необходимости отдельно покупать его и устанавливать
Наличие более полного функционала
Возможность более точно задавать исключения

№5 Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет
Трудности с регулярным автоматическим получением новых антивирусных баз
Невозможность использовать антиспамовую программу в режиме реального времени
Ложные срабатывания в работе персонального брандмауэра
Невозможность запуска антивирусной проверки в режиме реального времени

Второй этап: вопросы к зачету

1. Компьютерная информация: определение, основные категории с точки зрения безопасности
2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности.
3. Политика безопасности информационных систем и ее основные элементы
4. Обзор нормативных правовых актов РФ в области информационной защиты.
5. Дискреционный и мандатный доступ к ресурсам информационных систем.
6. Классификация угроз информационным системам. Фундаментальные, базовые и первичные угрозы
7. Атаки типа переполнения стека
8. Основные услуги безопасности, предоставляемые информационными системами
9. Механизмы реализации услуг безопасности в информационных системах
10. Классификация криптографических алгоритмов
11. Структурная схема симметричной криптосистемы
12. Структурная схема асимметричной криптосистемы
13. Математические определения шифра, процедур шифрования и дешифрации
14. История развития криптоалгоритмов: шифр Цезаря, афинная криптосистема, шифры Виженера и Вернома
15. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы
16. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования
17. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля
18. Алгоритм шифрования TEA: структура, достоинства и недостатки
19. Алгоритм шифрования DES: структура, достоинства и недостатки
20. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB
21. Поточные шифры: принципы функционирования, структура
22. Криптоатаки на поточные шифры, построение ЛРС с последовательностями наибольшей длины
23. Методы построения нелинейных поточных шифров
24. Асимметричные криптосистемы: принципы функционирования, трудновычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов
25. RSA: математические основы криптоалгоритма
26. RSA: структура криптоалгоритма
27. RSA: возможные криптоатаки и криптостойкость алгоритма
28. Алгоритм асимметричного шифрования Рабина
29. Криптосистема ЭльГемаля: структура, криптостойкость
30. Метод ключевого обмена Диффи-Хелмана
31. Асимметричные криптоалгоритмы рюкзачного типа
32. Алгоритмы генерации случайных чисел для криптоарлгоритмов,
33. Алгоритмы генерации и поверки простых чисел в современных криптосистемах
34. Хэш-функции: назначение и основные свойства
35. Итеративно-последовательная схема построения хэш-функций. Хэш-функции на основе блочных шифров
36. Электронная цифровая подпись: назначения, структура системы ЭЦП на основе алгоритма RSA
37. Система ЭЦП на основе алгоритма ЭльГемаля
38. Система ЭЦП на основе эллиптических кривых
39. Криптосистема: структура, основные функции
40. Современные схемы разделения ключей
41. Сертификация открытых ключей. Структура сертификата. Инфраструктура PKI.

42. Иерархическая и сетевая модели сертификации открытых ключей.
43. Роль сжатия информации в криптосистемах. Алгоритм сжатия Хаффмана
44. Роль сжатия информации в криптосистемах. Алгоритм сжатия Лемпела-Зива
45. Аутентификация в информационных системах: назначение, разновидности, угрозы подсистемам аутентификации
46. Системы аутентификации с защищенными паролями и с проверкой на стороне сервера
47. Система аутентификации по схеме «запрос-ответ»
48. Обзор современных протоколов аутентификации.
49. Обзор современных защищенных сетевых протоколов.
50. Угрозы безопасности в глобальных сетях
51. Межсетевые экраны: назначение, основные функции, состав
52. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки
53. Proxy-сервера : назначение, основные функции, достоинства и недостатки
54. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона
55. Модель безопасности ОС Windows. Идентификация пользователей: идентификатор безопасности и маркер доступа субъекта, привилегии.
56. Модель безопасности ОС Windows. Реализация дискреционной модели защиты доступа к ресурсам системы.
57. Модель безопасности ОС Windows: политика аудита.
58. Модель безопасности ОС Windows. Файловая система EFS.
59. Вредоносные программы: определение, классификация
60. Эксплойты: определение. Атаки на переполнение буфера и методы защиты от них.
61. Эксплойты: определение. SQL-инъекции и методы .защиты от них
62. Компьютерные вирусы: определение, методы заражения и маскировки. Методы защиты от вирусов.

3.3. Форма и организация промежуточной аттестации по итогам освоения дисциплины

По итогам освоения дисциплины проведение зачета проводится в два этапа: **тестирование** и **письменного задания.**

Первый этап проводится в виде тестирования. **Тестирование** ставит целью оценить **пороговый** уровень освоения обучающимися заданных результатов, а также знаний и умений, предусмотренных компетенциями.

Для оценки **превосходного и продвинутого** уровня усвоения компетенций проводится **второй этап** в виде **письменного задания**, в которое входит письменный ответ на вопросы.

3.4. Критерии оценки промежуточной аттестации

Таблица 6

Система оценки промежуточной аттестации

Описание оценки в требованиях к уровню и объему компетенций	Выражение в баллах	Словесное выражение
Освоен превосходный уровень усвоения Компетенций	от 86 до 100	Зачтено
Освоен продвинутый уровень усвоения Компетенций	от 71 до 85	Зачтено
Освоен пороговый уровень усвоения Компетенций	от 51 до 70	Зачтено
Не освоен пороговый уровень усвоения Компетенций	до 51	Не зачтено

РАЗДЕЛ 4. ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

4.1. Учебно-методическое обеспечение дисциплины

4.1.1. 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

4.1.2. 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

4.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6. Аникин, Игорь Вячеславович И.В. Методы и средства защиты компьютерной информации: лабораторный практикум. [Электронный ресурс]: учебное пособие для студ. вузов / И. В. Аникин, В. И. Глова. - Казань: Издательство КГТУ им. А.Н. Туполева, 2011 . - 131 с. – Режим доступа: http://e-library.kai.ru/reader/hu/flipping/Resource-84/1.pdf/index.html

7. Гусева А.И. Вычислительные системы, сети и телекоммуникации: учебник.- М.: ИЦ Академия, 2014. - 288 с. Рек. УМО

8. Петровский, Владимир Владимирович. Комплексная защита информации на предприятии: Методы и способы противодействия средствам технических разведок [Электронный ресурс]: учебное пособие / В. В. Петровский, В. И. Петровский, В. И. Глова. - Казань: Издательство КГТУ им. А.Н. Туполева, 2012. - 628 с. – Режим доступа: http://e-library.kai.ru/reader/hu/flipping/Resource-1471/811871_0001.pdf/index.html

9. Варлатая С.К, Шаханова М.В. Защита информационных процессов в компьютерных сетях: учебно-методический комплекс.- М: Проспект, 2017. - 224 с.

4.1.4 Методические рекомендации для студентов, в том числе по выполнению самостоятельной работы

Изучение дисциплины производится в тематической последовательности. Успешное освоение материала студентами обеспечивается посещением лекций и лабораторных работ, написанием конспекта по темам самостоятельной работы.

Для изучения дисциплины «Защита информации» рекомендуется использовать следующие источники:

1) Учебники и учебные пособия, программное обеспечение и интернет-ресурсы
2) Дидактический материал по всем разделам курса «Защита информации»:

- оценочных средств текущего контроля;
- оценочных средств по промежуточной аттестации.

4.1.5 Методические рекомендации для преподавателей

Успешное освоение материала обеспечивается тесной связью теоретического материала, преподносимого на лекциях и теоретико-экспериментальной работой студентов на лабораторных занятиях.

Лекционные занятия проводятся в форме лекций с использованием презентаций, видеороликов, При чтении лекционного курса непосредственно в аудитории необходимо

контролировать усвоение материала основной массой студентов, путем проведения экспресс-опросов по конкретным темам, тестового контроля знания, опроса студентов.

При проведении лабораторного практикума необходимо создать условия для максимально самостоятельного выполнения лабораторных работ.

Любая лабораторная работа должна включать самостоятельную проработку теоретического материала, изучение методик проведения и планирования эксперимента, освоение измерительных средств, обработку и интерпретацию экспериментальных данных.

4.2 Информационное обеспечение дисциплины (модуля)

4.2.1 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

1.2.2 Дополнительное справочное обеспечение

1. Habrahabr.ru
2. Citforum.ru

4.2.3 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

4.3 Кадровое обеспечение

4.3.1 Базовое образование

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

4.3.2 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.

4.3.3 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.

4.4. Материально-техническое обеспечение дисциплины

Для реализации учебного процесса требуется следующее материально-техническое обеспечение:

Таблица 7

Материально-техническое обеспечение дисциплины

Наименование раздела (темы) дисциплины	Наименование учебной лаборатории, аудитории, класса	Перечень лабораторного оборудования, специализированной мебели и технических средств обучения
Раздел 1-3	Учебная аудитория для проведения занятий лекционного типа (Л. 209)	- мультимедийный проектор (1 шт.); - ноутбук (1 шт.); - настенный экран (1 шт.); - акустические колонки (1 комплект); - учебные столы (15 шт.), стулья (30 шт.); - доска (1 шт.); - стол преподавателя (1 шт.); - учебно – наглядные пособия.
Раздел 1-2	Компьютерная аудитория (Л. 201)	- учебные столы (7 шт.), стулья (7 шт.); - доска (1 шт.); - стол преподавателя (1 шт.); - компьютерные столы (12 шт.), стулья (12 шт.); - персональные компьютеры (12 шт.); - локальная вычислительная сеть; - ЖК мониторы 23”(12 шт.); - доска интерактивная (1 шт.); - мультимедиа-проектор (1 шт.).
Раздел 1-2	Помещение для самостоятельной работы студента (Л. 112)	- персональный компьютер (9 шт.); - ЖК монитор 19” (9 шт.); - столы компьютерные (9 шт.); - учебные столы (8 шт.), стулья (25 шт.).

5. Вносимые изменения и утверждения

5.1 Внесение изменений в рабочую программу учебной дисциплины

Лист регистрации изменений, вносимых в рабочую программу учебной дисциплины

п.п.	№ раздела внесения изменений	Дата внесения изменений	Содержание изменений	«Согласовано» заведующий кафедрой	«Согласовано» председатель УМК филиала
1.	титульный лист	09.01.18	Наименование кафедры читать в следующей редакции: Кафедра машиностроения и информационных технологий		
2	4.2.1	01.10.2018	Дополнить электронная библиотечная система «ЮРАЙТ» http: //biblio-online.ru		
3	Титульный лист	01.02.2019	Изменение наименования учредителя университета. В соответствии с утверждением устава федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» в новой редакции (Приказ № 1042 от 26.11.2018) наименование «Министерство образования и науки Российской Федерации» читать как «Министерство науки и высшего образования Российской Федерации»		

5.2 Лист утверждения рабочей программы дисциплины (модуля) на учебный год

Рабочая программа дисциплины (модуля) утверждена на ведение учебного процесса в учебном году:

Учебный год	**«Согласовано»** Зав. каф. ИТ	**«Согласовано»** председатель УМК филиала
2017/2018		
2018/2019		
2019/2020		
2020/2021		
2021/2022		
2022/2023		