МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ Жуковский А. Г.
« 21 » 08 2022 г.

Разработка безопасного программного обеспечения Б1.В.05

рабочая программа дисциплины

Кафедра **«Информатика и вычислительная техника»**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	5	180/5сем		
Контактная работа, в том числе (по семестрам, курсам):		90/5сем		
Лекции		30/5сем		
Лабораторных работ		30/5сем		
Практических занятий		30/5сем		
Семинаров				
Самостоятельная работа		90/5сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам)				
Число КП (по семестрам)				
Число зачетов с разбивкой по семестрам				
Число экзаменов с разбивкой по семестрам (курсам)		1/5сем		

Программу составил:
Доцент кафедры ИВТ к.т.н. Швидченко С. А.

Рецензент(ы):
Зав. кафедрой ИВТ, д. т. н., профессор Соколов С. В.

Рабочая программа дисциплины
«Разработка безопасного программного обеспечения»

Разработана в соответствии с ФГОС ВО
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. N 1427.

Составлена на основании учебных планов
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Одобрена на заседании кафедры
"Информатика и вычислительная техника"

Протокол от «29» 08 2022 г. № 1

Зав. кафедрой _____ Соколов С. В.

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР_____________________
« __» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от « _» ________ 20__ г. № _
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР_____________________
« __» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «_» ________ 20__ г. № _
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР_____________________
« __» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «_» ________ 20__ г. № _
Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР_____________________
« __» _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
«Информатика и вычислительная техника»

Протокол от «_» ________ 20__ г. № _
Зав. кафедрой _____________________

---

1. Цели изучения дисциплины

Целью освоения дисциплины «Разработка безопасного программного обеспечения» является получение обучающимися знаний, формирование у них умений и навыков, необходимых при разработке безопасного программного обеспечения для решения задач в профессиональной деятельности, соответствующих общепрофессиональных компетенций в соответствии с ООП, а также основных знаний и умений в области разработки безопасного программного обеспечения.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способность решать профессиональные задачи в соответствии с ***проектной деятельностью.***

Задачи освоения дисциплины:

− получение знаний об основных уязвимостях и угрозах безопасности информации при разработке ПО и их источниках; о требованиях к безопасному программному обеспечению (ПО) и программно-методической документации; о методологии оценки безопасности ПО и уровнях доверия и оценке рисков безопасности ПО; об организационных и технических мерах по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО, в том числе о целях этих мер и о требованиях, предъявляемых к их реализации; руководящих документах, регламентирующих процесс создания и содержание этапов создания безопасного ПО; руководящих документах, регламентирующих анализ (аудит, экспертизу) безопасности ПО и оценку степени соответствия выявленной безопасности ПО предъявленным требованиям; о документах, которые необходимо разрабатывать при выполнении работ по созданию безопасного ПО; о периодичности, основных этапах и методах тестирования и анализа ПО; об инструментальных средствах, применяемые для тестирования ПО, его анализа и поиска в нем уязвимостей;

− приобретение умения выявлять угрозы и уязвимости ПО; проводить тестирование и анализ ПО; разрабатывать необходимую документацию в процессе создания безопасного ПО; разрабатывать организационные и технические меры по созданию безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО; оценивать безопасность ПО, уровнях доверия и риски безопасности ПО; оценивать степень соответствия выявленной безопасности ПО предъявленным требованиям;

− приобретение практических навыков выявления угроз и уязвимостей ПО; тестировании и анализе ПО; разработке необходимой документации; разработке организационных и технических мер по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла созданию безопасного ПО; оценке безопасность ПО, уровне доверия и риске безопасности ПО; оценке степени соответствия выявленной безопасности ПО предъявленным требованиям.

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях
Знать:
- принципы построения компьютерных сетей; - стек сетевых протоколов операционных систем; - стек протоколов сетевого оборудования; - порядок реализации методов и средств межсетевого экранирования; - принципы функционирования сетевых протоколов, включающих криптографические алгоритмы; - виды политик управления доступом и информационными потоками в компьютерных сетях; -источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению;

- состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;
- методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации;
- принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации;
- программно-аппаратные средства и методы защиты информации в компьютерных сетях;
- нормативные правовые акты в области защиты информации;
- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- организационные меры по защите информации.

Уметь:

- оценивать угрозы безопасности информации в компьютерных сетях;
- настраивать правила фильтрации пакетов в компьютерных сетях;
- обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях;
- конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях;
- выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;
- проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях;
- производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях;
- оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях.

Владеть:

- определением состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях;
- разработкой порядка применения программно-аппаратных средств защиты информации в компьютерных сетях;
- формированием шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях;
- настройкой программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации;
- управлением функционированием программно-аппаратных средств защиты информации в компьютерных сетях;
- контролем корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях;
- управлением средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями.

ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения

Знать:

- архитектуру подсистем защиты информации в операционных системах;
- принципы построения систем управления базами данных;
- основные средства и методы анализа программных реализаций;
- принципы построения антивирусного программного обеспечения;
- виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению;
- источники угроз информационной безопасности программного обеспечения и меры по их предотвращению;
- уязвимости используемого программного обеспечения и методы их эксплуатации;

- виды и формы функционирования вредоносного программного обеспечения; - характерные признаки наличия вредоносного программного обеспечения; - средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения; - принципы функционирования программных средств криптографической защиты информации; - порядок обеспечения безопасности информации при эксплуатации программного обеспечения; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации..
Уметь:
- анализировать угрозы безопасности информации программного обеспечения; - формулировать правила безопасной эксплуатации программного обеспечения; - обосновывать правила безопасной эксплуатации программного обеспечения; - анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия; - производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации; - осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения; - определять порядок функционирования программного обеспечения с целью обеспечения защиты информации; - анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения.
Владеть:
- определением порядка установки программного обеспечения с целью соблюдения требований по защите информации; - контролем над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение; - формулированием требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения; - выполнением работ по обнаружению вредоносного программного обеспечения; - ликвидацией обнаруженного вредоносного программного обеспечения и последствий его функционирования; - формулированием требований к встроенным средствам защиты информации программного обеспечения.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина опирается на знания, умения и навыки довузовской подготовки по основам Б1.О.03 «Информатика».
2	Б1.О.11 «Основы информационной безопасности»
3	Б1.В.01 «Введение в профессию»
4	Б1.О.10 «Языки программирования»
5	Б1.О.17 «Технологии и методы программирования»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.29 «Основы управления информационной безопасностью»
2	Б1.В.31 «Защита информации от вредоносного программного обеспечения»

3	Б1.О.31 «Безопасность компьютерных сетей»
4	Б1.О.33 «Программно-аппаратные средства защиты информации»
5	Б1.О.39 «Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)»
6	Б1.О.40 «Администрирование средств защиты информации в компьютерных системах и сетях»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 180 часов , 90 аудиторных часа, 90 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компе-тенции	УМИО
1	2	3	4	5	6
Курс 3, Семестр 5.					
Модуль 1: Основные понятия угроз и уязвимостей информационной безопасности при разработке ПО. (86 часов 42час. + 44СР)					
1.1	Лекция 1. ВВЕДЕНИЕ В ДИСЦИПЛИНУ. БАЗОВАЯ ТЕРМИНОЛОГИЯ. Угрозы и уязвимости информационной безопасности при разработке ПО. Безопасное ПО. Тестирование и анализ ПО. Фаззинг. Инструментальные среды и средства разработки и анализа ПО. Управление конфигурацией ПО. Документация разработчика ПО. Цели создание безопасного ПО и меры по их достижению.	Лек.	4	ПК-2 ПК-3	Л1.1,
1.2	АЛГОРИТМЫ ШИФРОВАНИЯ ДАННЫХ	ПЗ1	4	ПК-2	Л1.1, Л3,2.
1.3	МЕТОДЫ ПОИСКА И СБОРА ИНФОРМАЦИИ. МЕТОДИКА УСТРАНЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.	ЛР1	4	ПК-3	Л1.1, Л1,2. Л3.1
1.4	1. Знакомство с ГОСТ ГОСТ Р 56939-2016 2. Формирование требований к ПО и составление технического задания с учетом требований ГОСТ ГОСТ Р 56939-2016 3. Принципы безопасной разработки. Построение модели угроз.	СР	20	ПК-2 ПК-3	Л1.2, Л1,3.
1.5	Лекция 2. ОСНОВНЫЕ НОРМАТИВНО-ПРАВОВЫЕ АКТЫ В ОБЛАСТИ СОЗДАНИЯ БЕЗОПАСНОГО ПО Обзор основных ГОСТов: - ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения; - ГОСТ Р 56546-2015 Классификация уязвимостей информационных систем; - ГОСТ Р 58412-2019 Защита информации. Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО;	Лек.	6	ПК-2 ПК-3	Л1.2, Л1,4.

	- ГОСТ Р ИСО/МЭК 18045-2013 Методология оценки безопасности информационных технологий; - ГОСТ Р ИСО-МЭК 27034-1 Информационные технологии. Безопасность приложений. Часть 1. Безопасность приложений; - ГОСТ Р ИСО-МЭК 27034-7-2020 Информационные технологии. Безопасность приложений. Часть 7. Основы прогнозирования доверия				
1.6	ЗАЩИТА ОТ КОПИРОВАНИЯ	ПЗ2	4	ПК-2	Л1.1, Л3.2
1.7	УЯЗВИМОСТИ WINDOWS. ЗАЩИТА ОТ КОПИРОВАНИЯ ПЕРЕНОСНЫХ НОСИТЕЛЕЙ	ЛР2	4	ПК-3	Л1.1, Л3.1
1.8	1. Реализация ПО. Анализ кода уязвимого приложения 2. Тестирование ПО на изменение плоскости атак. 3. Планирование реагирования на инциденты. 4. Фаззинг-тестирование ПО.	СР	24	ПК-2 ПК-3	Л1.1, Л2.3.
1.9	Лекция 3. УГРОЗЫ, УЯЗВИМОСТИ, РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ ПО - ИХ ВЫЯВЛЕНИЕ И ОЦЕНКА. Угрозы безопасности информации при разработке ПО (по ГОСТ Р 58412-2019). Классификация уязвимостей информационных систем (по ГОСТ Р 56546—2015). Выявление угроз безопасности информации при разработке ПО. Оценка уровня доверия безопасности ПО (степени соответствия выявленной безопасности ПО предъявленным требованиям) (по ГОСТ Р ИСО-МЭК 27034-7). Методы и средства оценки рисков информационной безопасности при создании ПО.	Лек.	5	ПК-2 ПК-3	Л1.1, Л2.3.
1.10	ЗАЩИТА ОТ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ И НАВОДОК.	ПЗ3	4	ПК-2	Л3.2
1.11	МОДЕЛИ РАСПРОСТРАНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	ЛР3	4	ПК-3	Л3.1
Модуль 2: Безопасная разработка программного обеспечения (ПО). 94 часа (48 час. + 46СР)					
2.1	Лекция 4. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРЫ ПО РАЗРАБОТКЕ БЕЗОПАСНОГО ПО, РЕАЛИЗУЕМЫХ НА РАЗЛИЧНЫХ СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА РАЗРАБОТКИ БЕЗОПАСНОГО ПО Меры по разработке безопасного ПО, реализуемые при выполнении анализа требований к ПО.	Лек.	4	ПК-2 ПК-3	Л1.1, Л1.1, Л1,3.

	Меры по разработке безопасного ПО, реализуемые при выполнении проектирования архитектуры ПО. Меры по разработке безопасного ПО, реализуемые при выполнении конструирования и комплексирования ПО. Меры по разработке безопасного ПО, реализуемые при выполнении квалификационного тестирования ПО. Меры по разработке безопасного ПО, реализуемые при выполнении инсталляции ПО и поддержки приемки ПО. Меры по разработке безопасного ПО, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента документацией и конфигурацией программы. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента инфраструктурой среды разработки ПО. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента людскими ресурсами. Меры по разработке безопасного ПО, реализуемые при выполнении. Меры по разработке безопасного ПО, реализуемые при выполнении. Меры по разработке безопасного ПО, реализуемые при выполнении.				
2.2	ВИДЫ ШИФРОВ. АЛГОРИТМЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ	ПЗ4	4	ПК-3	Л3.2
2.3	АППАРАТНЫЕ КЛЮЧИ ЗАЩИТЫ. КОЛИЧЕСТВЕННАЯ ОЦЕНКА СТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ.	ЛР4	4	ПК-2	Л3.1
2.4	Лекция 5. ТЕСТИРОВАНИЕ И АНАЛИЗ ПО Виды тестирования ПО. Статический анализ ПО. Динамический анализ ПО. Защита ПО от взлома и несанкционированного использования	Лек.	6	ПК-2	Л1.1, Л1,2.
2.5	СИММЕТРИЧНЫЕ АЛГОРИТМЫ	ПЗ5	6	ПК-2	Л3.2
2.6	ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. БЕЗОПАСНАЯ РАБОТА В ИНТЕРНЕТ	ЛР5	6	ПК-2	Л1.1, Л3.1.
2.7	1. Отечественные и зарубежные стандарты в области разработки безопасного ПО. 2. Обеспечение безопасной разработки на фазе формирования требований к ПО. 3. Обеспечение безопасной разработки на фазе проектирования ПО.	СР	20	ПК-2 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4
2.8	Лекция 6. ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА РАЗРАБОТКИ БЕЗОПАСНЫХ ПРОГРАММ Инструментальные средства для безопасной	Лек.	6	ПК-2 ПК-3	Л1.3

	разработки в среде Windows: - Microsoft Threat Modeling Tool 2014 — средство моделирования атак; - SDL MiniFuzz File Fuzzer — средство фаззинг-тестирования; - Attack Surface Analyzer — анализатор плоскости атаки; - Анализатор кода C/C++ из состава Microsoft Visual Studio.				
2.9	АСИМЕТРИЧНЫЕ АЛГОРИТМЫ	ПЗ6	6	ПК-2	Л1.2 Л3.2
2.10	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ СЕТИ. НАСТРОЙКА ПАРАМЕТРОВ БЕЗОПАСНОСТИ БРАУЗЕРА	ЛР6	6	ПК-2	Л1.1, Л3.1
2.11	1. Обеспечение безопасной разработки на фазе реализации ПО 2. Обеспечение безопасной разработки на фазе тестирования ПО 3. Обеспечение безопасной разработки на фазах выпуска и поддержки ПО	СР	26	ПК-2 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4
	Экзамен			ПК-2 ПК-3	Л1.1 Л1.2 Л1.3 Л1.4
Итого – 180 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1 Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Брылева А. А.	Программные средства создания интернет-приложений : учебное пособие / А. А. Брылева.	Минск : РИПО, 2019. - 377 с.	Э1
Л1.2	Лисьев Г. А., Романов П.Ю., Аскерко Ю.И.	Программное обеспечение компьютерных сетей и web-серверов : учебное пособие / Г.А. Лисьев, П.Ю. Романов, Ю.И. Аскерко	Москва : ИНФРА-М, 2023. — 145 с.	Э2
Л1.3	Коробко И. В.	Справочник системного администратора по программированию Windows : практическое руководство / И. В. Коробко	Санкт-Петербург : БХВ-Петербург, 2009. - 576 с.	Э3

Л1.4	Исаченко О. В.	Программное обеспечение компьютерных сетей : учебное пособие / О.В. Исаченко.	Москва : ИНФРА-М, 2022. — 158 с.	Э4
5.1.2 Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Клейн Т.	Дневник охотника за ошибками: путешествие через джунгли проблем безопасности программного обеспечения : практическое руководство	Москва : ДМК Пресс, 2015. - 240 с.	Э5
Л2.2	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика : учебное пособие	Москва : Директ-Медиа, 2020. - 270 с.	Э6
Л2.3	Петров А. А.	Компьютерная безопасность: криптографические методы защиты: практическое руководство	Москва : ДМК Пресс, 2008. - 448 с.	Э7
Л2.4	Чио К., Фримэн Д.	Машинное обучение и безопасность: защита систем с помощью данных и алгоритмов : практическое руководство / К. Чио, Д. Фримэн.	Москва : ДМК Пресс, 2020. - 388 с.	Э8
6.1.3 Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Швидченко С.А.	Методические указания для проведения лабораторных работ	Ростов н/Д: СКФ МТУСИ, 2022	Э9
Л3.2	Швидченко С.А.	Методические указания для проведения практических занятий	СКФ МТУСИ: Ростов-на-Дону, 2022 г.	Э10
5.2 Электронные образовательные ресурсы				
Э1	*https://znanium.com/catalog/product/1088292*			
Э2	*https://znanium.com/catalog/product/1878635*			
Э3	*https://znanium.com/catalog/product/1768239*			
Э4	*https://znanium.com/catalog/product/1860121*			
Э5	*https://znanium.com/catalog/product/1907788*			
Э6	*https://znanium.com/catalog/product/1908082*			
Э7	*https://znanium.com/catalog/product/1908428*			
Э8	*https://znanium.com/catalog/product/1908430*			
Э9-Э10	http://www.skf-mtusi.ru/?page_id=659			

5.3. Программное обеспечение		
П.1	1. AVAST Free Antivirus 2. AVG AntiVirus Free 3. Dr.Web Antivirus 4. Антивирус Касперского 5. ESET NOD32 Антивирус 6. AVZ Antivirus	Антивирусное ПО. Свободное, условно свободное или триал-версии.

	7. Avira Free Antivirus	
	8. Norton AntiVirus	
	9. McAfee Antivirus	
	10. Emsisoft Anti-Malware	
	11. BullGuard Antivirus	
	12. Protector Plus Antivirus	
	13. Panda Antivirus	
	14. Ashampoo Anti-Virus	
	14. G Data AntiVirus	
	16. K7 AntiVirus	
	17. VIRUSfighter	
	18. Twister Antivirus	
П.2	1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker 6. Folder Guard 7. DEKSI USB Security 8. Locker (защита папок и дисков) 9. Advanced Hider 10. Hide Folders XP 11. Hide Files	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
П.3	1. TrustPort Tools 2. Cryptic Disk 3. Locker (скрытие файлов) 4. Max File Encryption 5. Secure Disk 6. Masker 7.1 7. Fox Secret 8. HideInPicture 1.0 9. Шифровальщик 10. Advanced Encryption Package 11. Gpg4win 12. Cryptic Disk Professional 13. CyberSafe Files Encryption 14. Steganos Privacy Suite 15. Lavasoft Privacy Toolbox 16. pkiImage Free Edition	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
П.4	1. Hetman Partition Recovery 2. Active File Recovery 3. R-Studio 7.6 4. Auslogics File Recovery 5. Active UNDELETE 6. Paragon Rescue Kit 7. Wise Data Recovery 8. Puran File Recovery 9. O&O DiskRecovery	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.

	10. Tenorshare Any Data Recovery	
	11. Power Data Recovery	
	12. GetDataBack	
	13. Recover My Files	
	14. R-Undelete	
	15. Handy Recovery	
	16. Ashampoo Undeleter	
П.5	1. Iperius Backup 2. FBackup 3. Backup4all 4. Uranium Backup Free 5. Simple Data Backup 6. Personal Backup 7. Back4Sure 8. SyncBackFree 9. Handy Backup 10. EASEUS Todo Backup 8.0 Free Edition 11. Exiland Backup Free 4.0 12. Nero BackItUp 13. Paragon Rescue Kit 14.0 Free 14. Action Backup 15. LimBackup 16. AVSbackup 17. ExtraBackup 18. Cobian Backup 19. Backup & Recovery 10 Build 9169 Free Edition 20. Information Backup System	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
П.6	MS Word – с лицензией	
П.7	Power Point – с лицензией	

6 . Материально - техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические рекомендации указания для обучающихся по самостоятельной работе

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение

учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную баз) учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/

Таблица 7.1 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 90	Неделя
Модуль 1 – 44 часа			
1	Знакомство с ГОСТ ГОСТ Р 56939-2016	4	1
2	Формирование требований к ПО и составление технического задания с учетом требований ГОСТ ГОСТ Р 56939-2016.	4	2
3	Принципы безопасной разработки. Построение модели угроз. 4.	4	3
4	Тестирование ПО на изменение плоскости атак.	4	4
5	Планирование реагирования на инциденты.	4	5
6	Фаззинг-тестирование ПО	4	6
7	Предпосылки для введения методологии безопасной разработки программ. Понятие безопасной разработки ПО. Модели безопасной разработки компаний Cisco и Microsoft. ГОСТ ГОСТ Р 56939-2016	6	7
8	Формирование требований безопасности к ПО. Определение минимальных приемлемых уровней безопасности. Определение шкалы ошибок и их влияния на безопасность. Проведение оценки рисков безопасности.	6	8
Модуль 2 – 46 часов			
9	Проверка спецификаций разработки на соответствие функциональным спецификациям. Анализ возможных плоскостей атак на ПО и противодействие им. Моделирование угроз.	4	9
10	Формирование и утверждения списка разрешенных инструментальных средств разработки, а также используемых стандартов. Выявление устаревших или опасных библиотечных функций. Статический анализ кода до компиляции.	4	10
11	Динамический анализ кода. Фаззинг-тестирование. Тестирование на изменение плоскости атак.	4	11
12	Планирование реагирования на инциденты с ПО. Проведение окончательного обзора безопасности ПО. Сертификация ПО и создание архива документации по проекту. Реагирование на инциденты и выпуск обновлений безопасности.	4	12
13	Резервное копирование программ, системных параметров и файлов	4	13
14	Использование методов замены для шифрования данных Использование методов перестановки для шифрования данных	4	14
15	Обеспечение безопасности локальной сети. Настройка параметров безопасности браузера	6	15
16	Инструментальные средства для безопасной разработки в среде Windows	6	16

Дополнения и изменения в рабочей программе