МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

«СОГЛАСОВАНО»
Руководитель ОП
_____ Артемьева И.Л.

«УТВЕРЖДАЮ»
И.о. директора департамента
_____ Смагин С.В.

«15» июля 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Защита информации
Направление подготовки 09.03.04 Программная инженерия
(Программная инженерия)
Форма подготовки (очная)

курс 4 семестр 7
лекции 36 час.
практические занятия 00 час.
лабораторные работы 18 час.
в том числе с использованием МАО лек. 0 /пр. 0 /лаб. 18 час.
всего часов аудиторной нагрузки 54 час.
в том числе с использованием МАО 18 час.
самостоятельная работа 54 час.
в том числе на подготовку к экзамену 00 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 7 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.04 Программная инженерия, утвержденный приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 920 (с изменениями и дополнениями).

Рабочая программа обсуждена на заседании кафедры прикладной математики, механики, управления и программного обеспечения, протокол № 7.1 от « 04 » июля 2019 г.

Заведующий кафедрой прикладной математики, механики, управления и программного обеспечения д.т.н., профессор Артемьева И.Л.
Составители: заведующая кафедрой прикладной математики, механики, управления и программного обеспечения д.т.н., профессор Артемьева И.Л., начальник отдела защиты информации департамента комплексной безопасности ДВФУ Зимин В.В.

Владивосток
2021

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры прикладной математики, механики, управления и программного обеспечения:

Протокол от «09» июля 2021 г. № 7.1

Заведующий кафедрой _____ Артемьева И.Л.
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента программной инженерии и искусственного интеллекта:

Протокол от «17» сентября 2021 г. № 9.1

И.о. директора департамента _____ Смагин С.В.
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины – изучение методов защиты информации в программных системах.

Задачи дисциплины:

дать основы

- обеспечения информационной безопасности государства;
- методологии создания систем защиты информации;
- защищенности процессов сбора, передачи и накопления информации;
- методов и средств защищенности и обеспечения информационной безопасности компьютерных систем.

В результате теоретического изучения дисциплины студент должен:

иметь представление:

- о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства, организации, гражданина;
- о методологии создания систем защиты информации;
- о перспективных направлениях развития средств и методов защиты информации;

знать:

- роль и место информационной безопасности в системе национальной безопасности страны;
- угрозы информационной безопасности государства, организации, гражданина;
- современные подходы к построению систем защиты информации;
- компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

уметь:

- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.

Планируемые результаты обучения по данной дисциплине (знания, умения, владения), соотнесенные с планируемыми результатами освоения образовательной программы.

Общепрофессиональные компетенции выпускников и индикаторы их достижения:

Наименование категории (группы) общепрофессиональных компетенций	**Код и наименование общепрофессиональной компетенции**	**Код и наименование индикатора достижения общепрофессиональной компетенции**
	ОПК-7. Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой	ОПК-7.1. Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий. ОПК-7.2. Умеет применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ. ОПК-7.3. Имеет навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач

Профессиональные компетенции выпускников и индикаторы их достижения:

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ иных требований, предъявляемых к выпускникам
Тип задач профессиональной деятельности: производственно-технологический				

Проведение работ по инсталляции программного обеспечения автоматизированных систем и загрузки баз данных; настройка параметров ИС и тестирование результатов настройки; ведение технической документации; техническое сопровождение ИС в процессе эксплуатации; применение Web технологий при реализации удаленного доступа в системах клиент – сервер и распределенных вычислений	Программное обеспечение	ПК-11. Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	ПК-11.1. Знает концепции и атрибуты качества ПО ПК-11.2. Умеет определять атрибуты качества ПО ПК-11.3. Имеет навыки в использовании методов, инструментов и технологий обеспечения качества ПО	06.028 Системный программист 06.022 Системный аналитик 06.004 Специалист по тестированию в области информационных технологий 06.001 Программист

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита информации» применяются следующие методы активного/ интерактивного обучения: метод круглого стола.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекционный материал (36 час.)

Тема 1. Основные понятия информационной безопасности (2 час.)

Понятие национальной безопасности. Информационная безопасность в системе национальной безопасности РФ

Тема 2. Концепция информационной безопасности (2 час.)

Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности. Угрозы конфиденциальной информации. Действия, приводящие к неправомерному овладению конфиденциальной информацией.

Тема 3. Направления обеспечения информационной безопасности (2 час.)

Правовая защита. Организационная защита. Инженерно-техническая защита

Тема 4. Выявление технических каналов утечки информации (6 час.)

Классификация технических каналов утечки информации. Классификация технических средств выявления каналов утечки информации. Индикаторы поля, интерсепторы и измерители частоты. Специальные сканирующие радиоприемники. Обнаружители диктофонов. Универсальные поисковые приборы. Программно-аппаратные поисковые комплексы. Нелинейные локаторы. Технические средства контроля двухпроводных линий

Тема 5. Защита информации от утечки по техническим каналам (6 час.)

Методы и средства защиты информации, обрабатываемой ТСПИ. Методы и средства защиты речевой информации в помещении. Методы и средства защиты телефонных линий.

Тема 6. Защита компьютерной информации от несанкционированного доступа (6 час.)

Угрозы безопасности информации в компьютерных системах. Программы-шпионы. Парольная защита операционных систем. Аппаратно-программные средства защиты информации от НСД. Проблемы обеспечения безопасности в глобальных сетях. Построение комплексных систем защиты информации

Тема 7. Стандарты и рекомендации в области информационной безопасности (6 час.)

Оранжевая книга (TCSEC). Радужная серия. Гармонизированные критерии Европейских стандартов (ITSEC). Рекомендации X.800. Концепция защиты СВТ и АС от НСД к информации

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы (18 час.)

Занятие 1. Законодательство РФ в области информационной безопасности (2 час.)

Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации. Федеральные законы в области информации и информационной безопасности. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности. Правовые режимы защиты информации. Правовые вопросы защиты информации с использованием технических средств.

Занятие 2. Закон РФ "О персональных данных" (2 час.)

Работа с перечнем законодательных документов Российской Федерации по защите персональных данных. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные Постановлением Правительства Российской Федерации от 01.11.2012 N 1119. Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 N 687, п.7.

Занятие 3. GnuPG (GNU Privacy Guard) - открытая реализация PGP (2 час.)

Установка необходимых программ. Создание открытых и закрытых ключей. Публикация открытого ключа. Использование при подписании и шифровании текстовых файлов. Использование при подписании и шифровании бинарных файлов.

Занятие 4. Настройка защищённого веб-сервера Apache (4 час.)

Использование самоподписанных сертификатов. Создание ключа и ssl-сертификата. Использование сертификатов центра сертификации. Извлечение сертификата из Хранилища Windows. Конвертация сертификата Windows для использования Apache. Размещение сертификата. Проверка защищённости веб-сервера.

Занятие 5. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации (4 час.)

Система сертификации средств защиты информации по требованиям безопасности информации. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации. Виды и схемы сертификации средств защиты информации. Функции ФСТЭК в области сертификации средств защиты информации. Функции органов сертификации средств защиты информации. Функции испытательных лабораторий (центров). Функции заявителей. Порядок проведения сертификации и контроля. Перечень средств защиты информации, подлежащих сертификации.

Занятие 6. Система сертификации средств криптографической защиты информации (4 час.)

Система сертификации средств криптографической защиты информации. Виды и схемы сертификации средств криптографической защиты информации. Функции органов, лабораторий и заявителей в системе сертификации криптографической защиты информации. Особенности подготовки и проведения сертификации криптографических средств защиты информации. Контроль и надзор за проведением сертификации криптографических средств защиты информации и стабильностью характеристик сертифицированной продукции.

Занятие 7. Антивирусная защита компьютерных систем (3 час.)

Установка и предварительная настройка. Обновление антивирусных баз. Настройки уведомлений. Настройки правил межсетевого экранирования. Настройки правил контентной фильтрации.

Занятие 8. Электронная цифровая подпись" (3 час.)

Получение электронной цифровой подписи в Центре сертификации. Публикация сертификата электронной цифровой подписи в глобальный

список адресов. Отправка и получение электронных писем с ЭЦП. Отправка и получение зашифрованных электронных писем.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Защита информации» представлено в разделе VIII и включает в себя: план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию; характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению; требования к представлению и оформлению результатов самостоятельной работы; критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы/темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Тема 1. Основные понятия информационной безопасности	ПК-11 ОПК-7	Знает	ПР1 тест	Зачет, часть 1, вопросы № 1
	Тема 2. Концепция информационной безопасности	ПК-11 ОПК-7	Знает	ПР1 тест	Зачет, часть 1, вопросы № 2-5
	Тема 3. Направления обеспечения информационной безопасности	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 1, вопросы № 6-14
			Умеет Владеет	ПР11 разноуровневые задания	
	Тема 4. Выявление технических каналов утечки информации	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 1, вопросы № 15-23
			Умеет Владеет	ПР11 разноуровневые задания	
	Тема 5. Защита информации от утечки по техническим каналам	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 2 вопросы № 1-13
			Умеет Владеет	ПР11 разноуровневые задания	
	Тема 6. Защита компьютерной	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 2 вопросы № 14-22

	информации от несанкционированного доступа		Умеет Владеет	ПР11 разноуровневые задания	
	Тема 7. Стандарты и рекомендации в области информационной безопасности	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 2 вопросы № 23-25
			Умеет Владеет	ПР11 разноуровневые задания	
2	Практические занятия 1-8	ПК-11 ОПК-7	Умеет Владеет	ПР11 разноуровневые задания	Зачет

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в разделе IX.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Информационная безопасность: учебник для вузов по гуманитарным и социально-экономическим специальностям / В. И. Ярочкин; [отв. ред. Л. И. Филиппенко]. Москва: Академический проект, 2006. – 543 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:350791&theme=FEFU
2. Комплексная защита информации в корпоративных системах : учебное пособие для вузов / В. Ф. Шаньгин.- Изд.: Форум Инфра-М., 2010. – 591 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:294516&theme=FEFU
3. Хорев П.Б. Программно-аппаратная защита информации: Учебное пособие. – Изд.: Форум, 2009. – 351 с. https://lib.dvfu.ru:8443/lib/item?id=chamo:294891&theme=FEFU
4. Методы и средства защиты информации в компьютерных системах: Учебное пособие / П.Б. Хорев. – М: Академия, - 2006. – 255 с. https://lib.dvfu.ru:8443/lib/item?id=chamo:385659&theme=FEFU
5. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. http://znanium.com/catalog.php?bookinfo=432654
6. Афанасьев А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс]: учебное пособие/ Афанасьев А.А., Веденьев Л.Т., Воронцов А А.—

Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 550 c. http://www.iprbookshop.ru/11978
7. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 c. http://www.iprbookshop.ru/7943
8. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – ДМК Пресс. 2012.- 592с. http://e.lanbook.com/books/element.php?pl1_id=3032

Дополнительная литература

1. Безопасность глобальных сетевых технологий / В.М. Зима, А.А, Молдовян, Н.А. Молдовян. – СПб.: БХВ-Петербург, 2003. – 368 с. https://lib.dvfu.ru:8443/lib/item?id=chamo:395097&theme=FEFU
2. Обнаружение хакерских атак / Дж. Чирилло. – СПб.: Питер, 2002. – 864 с. https://lib.dvfu.ru:8443/lib/item?id=chamo:144708&theme=FEFU
3. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин. - Екатеринбург: Изд-во Уральского университета, 2003.- 327 с. https://lib.dvfu.ru:8443/lib/item?id=chamo:250511&theme=FEFU.
4. Стохастические методы и средства защиты информации в компьютерных системах и сетях / М. А. Иванов, А. В. Ковалев, Н. А. Мацук [и др.] ; под ред. И. Ю. Жукова. Москва: Кудиц-Пресс, 2009. – 510 с. https://lib.dvfu.ru:8443/lib/item?id=chamo:288892&theme=FEFU
5. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: http://znanium.com/go.php?id=489084
6. Защита информации. Словарь базовых терминов и определений / Алексенцев А.И. – Изд. Российского гуманитарного университета. – 2000. – 17 с. https://lib.dvfu.ru:8443/lib/item?id=chamo:12148&theme=FEFU

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://e.lanbook.com/books/element.php?pl1_id=3032 Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – ДМК Пресс. 2012.- 592с.
2. http://www.iprbookshop.ru/7943 Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 c.— Режим доступа: ЭБС «IPRbooks», по паролю
3. http://www.iprbookshop.ru/17926 Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения

конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— СПб.: Российский государственный гидрометеорологический университет, 2010.— 104 с.— Режим доступа: ЭБС «IPRbooks», по паролю

4. http://www.iprbookshop.ru/11978 Афанасьев А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс]: учебное пособие/ Афанасьев А.А., Веденьев Л.Т., Воронцов А А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 550 с.— Режим доступа: ЭБС «IPRbooks», по паролю
5. http://www.studentlibrary.ru/book/ISBN9785987045138.html Правовое обеспечение национальных интересов Российской Федерации в информационной сфере / Н.Н. Куняев. - М.: Логос, 2010. - 348 с.
6. http://www.consultant.ru/document/cons_doc_LAW_61798/ Закон РФ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 г. № 149-ФЗ.
7. http://www.consultant.ru/document/cons_doc_LAW_48699/ Закон РФ "О коммерческой тайне" от 29.07.2004 г. №98-ФЗ.

Нормативно-правовые материалы

Код или обозначение документа	Наименование документа	Вид документа (Бумажный носитель/ электронная форма)
BS ISO/IEC 17799:2000	**Information technology - Code of practice for information security management (IDT)**	-
BS ISO/IEC 27001:2005	**Information technology - Security techniques - Information security management systems - Requirements**	-
BS 7799-3:2006	**Information Security Management Systems - Guidelines for Information Security Risk Management**	-
ФЕДЕРАЛЬНЫЙ ЗАКОН от 27.07.2006 N 149-ФЗ	ФЕДЕРАЛЬНЫЙ ЗАКОН от 27.07.2006 N 149-ФЗ **"ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ"** (принят ГД ФС РФ	ИПС «Консультант Плюс»

	08.07.2006)	
Доктрина ИБ РФ	**"ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ"** (утв. Президентом РФ 09.09.2000 N Пр-1895)	ИПС «Консультант Плюс»
ЗАКОН РФ от 21.07.1993 N 5485-1	ЗАКОН РФ от 21.07.1993 N 5485-1 (ред. от 22.08.2004) **"О ГОСУДАРСТВЕННОЙ ТАЙНЕ"**	ИПС «Консультант Плюс»
УКАЗ Президента РФ от 30.11.1995 N 1203	УКАЗ Президента РФ от 30.11.1995 N 1203 (ред. от 11.02.2006) **"ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ СВЕДЕНИЙ, ОТНЕСЕННЫХ К ГОСУДАРСТВЕННОЙ ТАЙНЕ"**	ИПС «Консультант Плюс»
ФЕДЕРАЛЬНЫЙ ЗАКОН от 29.07.2004 N 98-ФЗ	ФЕДЕРАЛЬНЫЙ ЗАКОН от 29.07.2004 N 98-ФЗ (ред. от 02.02.2006, с изм. от 18.12.2006) **"О КОММЕРЧЕСКОЙ ТАЙНЕ"** (принят ГД ФС РФ 09.07.2004)	ИПС «Консультант Плюс»
УКАЗ Президента РФ от 06.03.1997 N 188	УКАЗ Президента РФ от 06.03.1997 N 188 (ред. от 23.09.2005) **"ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА"**	ИПС «Консультант Плюс»
ФЕДЕРАЛЬНЫЙ ЗАКОН от 27.07.2006 N 152-ФЗ	ФЕДЕРАЛЬНЫЙ ЗАКОН от 27.07.2006 N 152-ФЗ **"О ПЕРСОНАЛЬНЫХ ДАННЫХ"** (принят ГД ФС РФ 08.07.2006)	ИПС «Консультант Плюс»
ФЕДЕРАЛЬНЫЙ ЗАКОН от 10.01.2002 N 1-ФЗ	ФЕДЕРАЛЬНЫЙ ЗАКОН от 10.01.2002 N 1-ФЗ **"ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ"** (принят ГД ФС РФ 13.12.2001)	ИПС «Консультант Плюс»
ПРИКАЗ ФСБ РФ от 09.02.2005 N 66	ПРИКАЗ ФСБ РФ от 09.02.2005 N 66 **"ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О РАЗРАБОТКЕ, ПРОИЗВОДСТВЕ, РЕАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ (ПОЛОЖЕНИЕ ПКЗ-2005)"** (Зарегистрировано в Минюсте РФ 03.03.2005 N 6382)	ИПС «Консультант Плюс»
ФЕДЕРАЛЬНЫЙ ЗАКОН от	ФЕДЕРАЛЬНЫЙ ЗАКОН от 08.08.2001 N	ИПС

08.08.2001 N 128-ФЗ	128-ФЗ (ред. от 05.02.2007) **"О ЛИЦЕНЗИРОВАНИИ ОТДЕЛЬНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ"** (принят ГД ФС РФ 13.07.2001)	«Консультант Плюс»
ФЕДЕРАЛЬНЫЙ ЗАКОН от 27.12.2002 N 184-ФЗ	ФЕДЕРАЛЬНЫЙ ЗАКОН от 27.12.2002 N 184-ФЗ (ред. от 01.05.2007) **"О ТЕХНИЧЕСКОМ РЕГУЛИРОВАНИИ"** (принят ГД ФС РФ 15.12.2002)	ИПС «Консультант Плюс»
УКАЗ Президента РФ от 16.08.2004 N 1085	УКАЗ Президента РФ от 16.08.2004 N 1085 (ред. от 30.11.2006) **"ВОПРОСЫ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ"**	ИПС «Консультант Плюс»
ПОСТАНОВЛЕНИЕ Правительства РФ от 15.08.2006 N 504	ПОСТАНОВЛЕНИЕ Правительства РФ от 15.08.2006 N 504 **"О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ"**	ИПС «Консультант Плюс»
ПОСТАНОВЛЕНИЕ Правительства РФ от 26.01.2006 N 45	ПОСТАНОВЛЕНИЕ Правительства РФ от 26.01.2006 N 45 **"ОБ ОРГАНИЗАЦИИ ЛИЦЕНЗИРОВАНИЯ ОТДЕЛЬНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ"**	ИПС «Консультант Плюс»
УКАЗ Президента РФ от 03.04.1995 N 334	УКАЗ Президента РФ от 03.04.1995 N 334 (ред. от 25.07.2000) **"О МЕРАХ ПО СОБЛЮДЕНИЮ ЗАКОННОСТИ В ОБЛАСТИ РАЗРАБОТКИ, ПРОИЗВОДСТВА, РЕАЛИЗАЦИИ И ЭКСПЛУАТАЦИИ ШИФРОВАЛЬНЫХ СРЕДСТВ, А ТАКЖЕ ПРЕДОСТАВЛЕНИЯ УСЛУГ В ОБЛАСТИ ШИФРОВАНИЯ ИНФОРМАЦИИ"**	ИПС «Консультант Плюс»
ПОСТАНОВЛЕНИЕ Правительства РФ от 26.06.1995 N 608	ПОСТАНОВЛЕНИЕ Правительства РФ от 26.06.1995 N 608 (ред. от 17.12.2004) **"О СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ"**	ИПС «Консультант Плюс»
ПОСТАНОВЛЕНИЕ Правительства РФ от 31.08.2006 N 532	ПОСТАНОВЛЕНИЕ Правительства РФ от 31.08.2006 N 532 **"О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО РАЗРАБОТКЕ**	ИПС «Консультант Плюс»

	И (ИЛИ) ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ"	
ЗАКОН РФ от 09.07.1993 N 5351-1	ЗАКОН РФ от 09.07.1993 N 5351-1 (ред. от 20.07.2004) **"ОБ АВТОРСКОМ ПРАВЕ И СМЕЖНЫХ ПРАВАХ"**	ИПС «Консультант Плюс»
РД Гостехкомиссии РФ. СТР-К	РД Гостехкомиссии РФ **"Специальные требования и рекомендации по технической защите конфиденциальной информации"**	Бумажный носитель
Положение по аттестации объектов информатизации по требованиям безопасности информации	**Положение по аттестации объектов информатизации по требованиям безопасности информации** (Утверждено председателем Гостехкомиссии России от 25 ноября 1994 года)	электронная форма
Положение о сертификации средств защиты информации по требованиям безопасности информации	**Положение о сертификации средств защиты информации по требованиям безопасности информации** (Утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199)	электронная форма
Положение о государственном лицензировании деятельности в области защиты информации	**Положение о государственном лицензировании деятельности в области защиты информации** (Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 27 апреля 1994 г. №10) (с изменениями и дополнениями от 24 июня 1997 г. №60)	электронная форма
РД Гостехкомиссии РФ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации	Руководящий документ. **Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации** (Решение председателя Гостехкомиссии России от 30 марта 1992 года)	электронная форма
РД Гостехкомиссии РФ. Защита от несанкционированного доступа к информации.	Руководящий документ. **Защита от несанкционированного доступа к информации. Термины и определения** (Решение председателя Гостехкомиссии	электронная форма

Термины и определения	России от 30 марта 1992 года)	
РД Гостехкомиссии РФ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации	**Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации** (Решение председателя Гостехкомиссии России от 30 марта 1992 года)	электронная форма
РД Гостехкомиссии РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации	Руководящий документ. **Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации** (Решение председателя Гостехкомиссии России от 30 марта 1992 года)	электронная форма
РД Гостехкомиссии РФ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники	Руководящий документ. **Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники** (Решение председателя Гостехкомиссии России от 30 марта 1992 года)	электронная форма
РД Гостехкомиссии РФ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации	Руководящий документ. **Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации** (Решение председателя Гостехкомиссии России от 25 июля 1997 года)	электронная форма
РД Гостехкомиссии РФ. Защита информации. Специальные защитные знаки. Классификация и общие требования	Руководящий документ. Защита информации. **Специальные защитные знаки. Классификация и общие требования** (Решение председателя Гостехкомиссии России от 25 июля 1997 года)	электронная форма
РД Гостехкомиссии РФ. Защита от несанкционированного	Руководящий документ. **Защита от несанкционированного доступа к**	электронная

доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей	**информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей** (Приказ председателя Гостехкомиссии России от 4 июня 1999 года № 114)	форма
РД Гостехкомиссии РФ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий	Руководящий документ. **Безопасность информационных технологий. Критерии оценки безопасности информационных технологий** (Приказ председателя Гостехкомиссии России от 19 июня 2002 года № 187)	электронная форма
РД Гостехкомиссии РФ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности	Руководящий документ. **Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности** (Гостехкомиссия России, 2003 год)	электронная форма
РД Гостехкомиссии РФ. Безопасность информационных технологий. Руководство по регистрации профилей защиты	Руководящий документ. **Безопасность информационных технологий. Руководство по регистрации профилей защиты** (Гостехкомиссия России, 2003 год)	электронная форма
РД Гостехкомиссии РФ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты	Руководящий документ. **Безопасность информационных технологий. Руководство по формированию семейств профилей защиты** (Гостехкомиссия России, 2003 год)	электронная форма
РД Гостехкомиссии РФ. Руководство по разработке профилей защиты и заданий по безопасности	**Руководство по разработке профилей защиты и заданий по безопасности** (Гостехкомиссия России, 2003 год)	электронная форма
ГОСТ Р 52069.0-2003	**Защита информации. Система стандартов. Основные положения**	Бумажный носитель, ИПС «Консультант Плюс»
ГОСТ Р ИСО/МЭК 17799-2005	**Информационная технология. Практические правила управления информационной безопасностью**	Бумажный носитель
ГОСТ Р ИСО МЭК 15408-1-2002	**Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1.**	Бумажный носитель

	Введение и общая модель	
ГОСТ Р ИСО МЭК 15408-2-2002	**Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности**	Бумажный носитель, ИПС «Консультант Плюс»
ГОСТ Р ИСО МЭК 15408-3-2002	**Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности**	Бумажный носитель
ГОСТ Р 50922-96	**Защита информации. Основные термины и определения**	Бумажный носитель
Р 50.1.053-2005	**Информационные технологии. Основные термины и определения в области технической защиты информации**	Бумажный носитель
ГОСТ Р 51275-99	**Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения**	Бумажный носитель
РД 50-34.698-90	**АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ДОКУМЕНТОВ**	Бумажный носитель
ГОСТ Р 52447-2005	**Защита информации. Техника защиты информации. Номенклатура показателей качества**	Бумажный носитель
ГОСТ Р 50739-95	**Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования**	Бумажный носитель
ГОСТ Р 51188-98	**Защита информации. Испытания программных средств на наличие компьютерных вирусов**	Бумажный носитель
ГОСТ Р 51898-2002	**Аспекты безопасности. Правила включения в стандарты**	-
ГОСТ Р ИСО 9000-2001	**СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА. ОСНОВНЫЕ**	ИПС «Консультант

	ПОЛОЖЕНИЯ И СЛОВАРЬ	Плюс»
ГОСТ 1.1-2002	**МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ. МЕЖГОСУДАРСТВЕННАЯ СИСТЕМА СТАНДАРТИЗАЦИИ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**	ИПС «Консультант Плюс»
ГОСТ Р 51897-2002	**МЕНЕДЖМЕНТ РИСКА. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**	ИПС «Консультант Плюс»
ГОСТ 34.003-90	**Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения**	-
ГОСТ 15971-90	**Системы обработки информации. Термины и определения**	-
ГОСТ Р 52292-2004	**ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. ЭЛЕКТРОННЫЙ ОБМЕН ИНФОРМАЦИЕЙ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**	ИПС «Консультант Плюс»
ГОСТ Р 34.10-2001	**ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ**	ИПС «Консультант Плюс»
ГОСТ Р 34.11-94	**ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ФУНКЦИЯ ХЭШИРОВАНИЯ**	ИПС «Консультант Плюс»
ГОСТ Р 51624-2000	**Защита информации. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**	-
ГОСТ Р 51583-2000	**Защита информации. ПОРЯДОК СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**	-

Перечень информационных технологий и программного обеспечения

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используется следующее программное обеспечение:

1. Microsoft Office (PowerPoint, Word и Visio).
2. Open Office.
3. Skype.

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используются следующие информационно-справочные системы:

1. Научная электронная библиотека eLIBRARY.
2. Электронно-библиотечная система издательства «Лань».
3. Электронная библиотека "Консультант студента".
4. Электронно-библиотечная система IPRbooks.
5. Информационная система "ЕДИНОЕ ОКНО доступа к образовательным ресурсам".
6. Доступ к электронному заказу книг в библиотеке ДВФУ, доступ к нормативным документам ДВФУ, расписанию, рассылке писем.

Лекции проводятся с использованием проектора и мультимедийного комплекса для проведения лекций внутренней системы портала ДВФУ. Лабораторные занятия проводятся в специализированном компьютерном классе.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Дисциплина «Защита информации» изучается в следующих организационных формах: лекционное занятие; практические занятия; самостоятельное изучение теоретического материала; самостоятельное выполнение индивидуального проекта; индивидуальные и групповые консультации.

Основной формой самостоятельной работы студента является изучение конспекта лекций, их дополнение рекомендованной литературой, выполнение проекта, а также активная работа на практических занятиях.

К прослушиванию лекции следует готовиться, для этого необходимо знать программу курса и рекомендованную литературу. Тогда в процессе лекции легче отделить главное от второстепенного, легче сориентироваться: что

записать, что самостоятельно проработать, что является трудным для понимания, а что легко усвоить.

Контроль за выполнением самостоятельной работы студента производится в виде контроля каждого этапа работы, отраженного в документации и защиты проекта.

Студент должен планировать график самостоятельной работы по дисциплине и придерживаться его.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Лекции проводятся с использованием проектора и внутренней системы портала ДВФУ. Лабораторные занятия проходят в аудиториях, оборудованных компьютерами типа Lenovo C360G-i34164G500UDK с лицензионными программами Microsoft Office 2013 и аудиовизуальными средствами проектор Panasonic DLPProjectorPT-D2110XE, плазма LG FLATRON M4716CCBAM4716CJ. Для выполнения самостоятельной работы студенты в жилых корпусах ДВФУ обеспечены Wi-Fi.

VIII. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Формулировка задачи	Примерные нормы времени на выполнение	Форма контроля
	7 семестр			
1.	1 неделя	Закон РФ "Об электронной цифровой подписи"	3	собеседование
2.	1-3 неделя	Угрозы конфиденциальной информации	3	собеседование
3.	4 неделя	Охрана объектов информатизации	3	собеседование
4.	5 неделя	Физические средства защиты	3	собеседование
5.	6 неделя	Аппаратные средства защиты	3	собеседование
6.	7-9 неделя	Программные средства защиты	3	собеседование
7.	10 неделя	Криптографические средства защиты	3	собеседование
8.	11 неделя	Защита от утечки за счет микрофонного эффекта	3	собеседование
9.	12 неделя	Защита от утечки за счет электромагнитного излучения	3	собеседование
10.	13 неделя	Защита от утечки за счет паразитной генерации	3	собеседование
11.	14 неделя	Защита от утечки по цепям питания	3	собеседование
12.	15 неделя	Защита от утечки по цепям заземления	3	собеседование
13.	16-18 неделя	Противодействие подслушиванию посредством микрофонных схем	3	собеседование
14.	19 неделя	Противодействие радиосистемам акустического подслушивания	3	собеседование
15.	20 неделя	Обеспечение безопасности телефонных переговоров	3	собеседование
16.	21 неделя	Противодействие лазерному подслушиванию	2	собеседование
17.	22 неделя	Защита операционных систем	2	собеседование
18.	23неделя	Защита баз данных	2	собеседование
19.	24 неделя	Защита отдельных файлов	1	собеседование
20.	25-27 неделя	Общие вопросы IP-безопасности	1	собеседование
21.	28-30 неделя	Проблемы реализации комплексных систем защиты информации	1	собеседование
		Итого	54 час	

Рекомендации по самостоятельной работе студентов

Самостоятельная работа студентов состоит из подготовки к практическим занятиям, работы над рекомендованной литературой, написания докладов по теме практического занятия.

При организации самостоятельной работы **преподаватель** должен учитывать уровень подготовки каждого студента и предвидеть трудности, которые могут возникнуть при выполнении самостоятельной работы. Преподаватель дает каждому студенту индивидуальные и дифференцированные задания. Некоторые из них могут осуществляться в группе (например, подготовку доклада по одной теме могут делать несколько студентов с разделением своих обязанностей – один готовит научно-теоретическую часть, а второй проводит анализ практики).

IX. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
ОПК-7. Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой	Знает	основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий.
	Умеет	применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ.
	Владеет	Имеет навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач
ПК-11. Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	Знает	концепции и атрибуты качества ПО
	Умеет	определять атрибуты качества ПО
	Владеет	Имеет навыки в использовании методов, инструментов и технологий обеспечения качества ПО

№ п/п	Контролируемые разделы/темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Тема 1. Основные понятия информационной безопасности	ПК-11 ОПК-7	Знает	ПР1 тест	Зачет, часть 1, вопросы № 1
	Тема 2. Концепция информационной безопасности	ПК-11 ОПК-7	Знает	ПР1 тест	Зачет, часть 1, вопросы № 2-5

	Тема 3. Направления обеспечения информационной безопасности	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 1, вопросы № 6-14
			Умеет Владеет	ПР11 разноуровневые задания	
	Тема 4. Выявление технических каналов утечки информации	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 1, вопросы № 15-23
			Умеет Владеет	ПР11 разноуровневые задания	
	Тема 5. Защита информации от утечки по техническим каналам	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 2 вопросы № 1-13
			Умеет Владеет	ПР11 разноуровневые задания	
	Тема 6. Защита компьютерной информации от несанкционированного доступа	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 2 вопросы № 14-22
			Умеет Владеет	ПР11 разноуровневые задания	
	Тема 7. Стандарты и рекомендации в области информационной безопасности	ПК-11 ОПК-7	Знает	ПР1 тест,	Зачет, часть 2 вопросы № 23-25
			Умеет Владеет	ПР11 разноуровневые задания	
2	Практические занятия 1-8	ПК-11 ОПК-7	Умеет Владеет	ПР11 разноуровневые задания	Зачет

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ОПК-7. Способен применять в практической деятельности и основные концепции, принципы, теории и	знает (пороговый уровень)	Методы обеспечения информационной безопасности Математические методы защиты информации от компьютерных вирусов	Знание методологии создания систем защиты информации, методы и средства обеспечения информационной безопасности	Способность дать ответы на вопросы

факты, связанные с информатикой			компьютерных систем Знание классов средств защиты информации от компьютерных вирусов	
	умеет (продвинутый)	Использовать методы обеспечения информационной безопасности при работе с информационными технологиями Использовать антивирусные программы	Умение выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации Умение выбрать необходимые средства защиты и умение выполнить их установку на компьютер	Способность привести аргументы выбора средств защиты информации Способность пояснить процесс установки и обосновать выбор
	владеет (высокий)	Методами обеспечения информационной безопасности при поиске информации Методами обновления антивирусных баз	Владеет методами защищенного поиска современной научно-технической информации по проблемам защиты информации Владение методами проверки актуальности установленных средств защиты и обновления их	Способность пояснить, какие источники информации являются безопасными и почему Способность привести критерии, при выполнении которых требуется обновление
ПК-11. Владение концепциями и атрибутами качества программного обеспечения	знает (пороговый уровень)	основы интеллектуальных прав для выявления, учета, обеспечения правовой охраны результатов интеллектуальной деятельности и распоряжения ими, в том числе в целях	особенности зашиты информации для разных классов операционных систем	Способность дать ответы на вопросы

(надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества		практического применения		
	умеет (продвинутый)	решает задачи, связанные с выбором способов использования прав на результаты интеллектуальной деятельности, и осуществляет распоряжение такими правами, включая введение таких прав в гражданский оборот	Использовать средства защиты информации при проектировании информационных систем	Сделать и обосновать выбор средства защиты информации при проектировании информационных систем
	владеет (высокий)	навыками предварительного проведения патентных исследований и патентного поиска	Методами программирования компьютерных подсистем защиты информации в программных средствах	Способность применить методы программирования компьютерных подсистем защиты информации в программных средствах

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная аттестация студентов. Промежуточная аттестация студентов по дисциплине «Защита информации» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Промежуточная аттестация по дисциплине предусмотрена в виде зачета в устной форме (устный опрос в форме ответов на вопросы)

Оценочные средства для промежуточной аттестации

Вопросы к зачету (часть 1)

1. Понятие национальной безопасности. Информационная безопасность в системе национальной безопасности РФ
2. Основные концептуальные положения системы защиты информации
3. Концептуальная модель информационной безопасности
4. Угрозы конфиденциальной информации
5. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
6. Правовая защита

7. Закон РФ "О государственной тайне"
8. Закон РФ "Об информации, информатизации и о технической защите информации"
9. Закон РФ "О коммерческой тайне"
10. Закон РФ "О персональных данных"
11. Закон РФ "Об электронной цифровой подписи"
12. Доктрина Информационной безопасности
13. Организационная защита
14. Инженерно-техническая защита
15. Основные способы защиты информации
16. Пресечение разглашения конфиденциальной информации
17. Индикаторы поля, интерсепторы и измерители частоты
18. Специальные сканирующие радиоприемники
19. Обнаружители диктофонов
20. Универсальные поисковые приборы
21. Программно-аппаратные поисковые комплексы
22. Нелинейные локаторы
23. Технические средства контроля двухпроводных линий

Вопросы к зачету (часть 2)

1. Защита информации от утечки по визуально-оптическим каналам
2. Защита информации от утечки по акустическим каналам
3. Защита информации от утечки по электромагнитным каналам
4. Защита информации от утечки по материально-вещественным каналам
5. Защита от утечки за счет электромагнитного излучения
6. Защита от утечки за счет паразитной генерации
7. Защита от утечки по цепям питания
8. Защита от утечки по цепям заземления
9. Способы несанкционированного доступа
10. Защита от наблюдения и фотографирования
11. Защита от подслушивания
12. Противодействие незаконному подключению к линиям связи
13. Защита от перехвата
14. Защита в локальных сетях
15. Защита в глобальных сетях
16. Противодействие подслушиванию посредством микрофонных схем
17. Противодействие радиосистемам акустического подслушивания
18. Обеспечение безопасности телефонных переговоров
19. Противодействие лазерному подслушиванию

20. Стандарты и рекомендации в области информационной безопасности

21. Основные методы защиты операционных систем

22. Межсетевые экраны

23. Стандарты и рекомендации в области информационной безопасности

24. Оранжевая книга (TCSEC). Радужная серия. Гармонизированные критерии Европейских стандартов (ITSEC).

25. Рекомендации X.800. Концепция защиты СВТ и АС от НСД к информации.

Критерии выставления оценки студенту на зачете по дисциплине «Защита информации»

Баллы (рейтинговой оценки)	**Оценка зачета/ экзамена** (стандартная)	**Требования к сформированным компетенциям**
86-100	«зачтено»/ «отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
76-85	«зачтено»/ «хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
61-75	«зачтено»/ «удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

0-60	«не зачтено»/ «неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Текущий контроль

Текущая аттестация студентов. Текущая аттестация студентов по дисциплине «Защита информации» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация по дисциплине «Защита информации» проводится в форме тестирования.

Объектами оценивания выступают:

- учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);
- степень усвоения теоретических знаний - оценивается в форме собеседования, тестирования;
- уровень овладения практическими умениями и навыками;
- результаты самостоятельной работы.

Тесты для подготовки к контрольным мероприятиям

Задание 1

Вопрос 1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

1) политическая разведка;
2) промышленный шпионаж;
3) добросовестная конкуренция;
4) конфиденциальная информация;
5) правильного ответа нет.

Вопрос 2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности ?

1) любая информация;
2) только открытая информация;
3) запатентованная информация;
4) закрываемая собственником информация;
5) коммерческая тайна.

Вопрос 3. Кто может быть владельцем защищаемой информации?

1) только государство и его структуры;
2) предприятия акционерные общества, фирмы;
3) общественные организации;
4) только вышеперечисленные;
5) кто угодно.

Вопрос 4. Какие сведения на территории РФ могут составлять коммерческую тайну?

1) учредительные документы и устав предприятия;
2) сведенья о численности работающих, их заработной плате и условиях труда;
3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
4) другие;
5) любые.

Вопрос 5. Какие секретные сведения входят в понятие «коммерческая тайна»?

1) связанные с производством;
2) связанные с планированием производства и сбытом продукции;
3) технические и технологические решения предприятия;
4) только 1 и 2 вариант ответа;
5) три первых варианта ответа.

Задание 2

Вопрос 1. Что называют источником конфиденциальной информации?

1) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;

2) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;
3) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;
4) это защищаемые предприятием сведения в области производства и коммерческой деятельности;
5) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

Вопрос 2. Как называют процессы обмена информацией с помощью официальных, деловых документов?
1) непосредственные**;**
2) межличностные;
3) формальные**;**
4) неформальные**;**
5) конфиденциальные.

Вопрос 3. Какое наиболее распространенное действие владельца конфиденциальной информации, приводит к неправомерному овладению ею при минимальных усилиях со стороны злоумышленника?
1) хищение носителей информации;
2) использование технических средств для перехвата электромагнитных ПЭВМ;
3) разглашение;
4) копирование программой информации с носителей;
5) другое.

Вопрос 4. Каким образом происходит разглашение конфиденциальной информации?
1) утеря документов и других материалов, или пересылка их посредством почты, посыльного, курьера;
2) опубликование материалов в печати;
3) сообщение, передача, предоставление в ходе информационного обмена;
4) все вышеперечисленные способы;
5) правильного варианта ответа нет.

Задание 3

Вопрос 1. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

1) получить, изменить, а затем передать ее конкурентам;
2) размножить или уничтожить ее;
3) получить, изменить или уничтожить;
4) изменить и уничтожить ее;
5) изменить, повредить или ее уничтожить.

Вопрос 2. Какой самый прямой и эффективный способ склонения к сотрудничеству?

1) психическое давление;
2) подкуп;
3) преследование;
4) шантаж;
5) угрозы.

Вопрос 3. Наиболее сложный и дорогостоящий процесс несанкционированного доступа к источникам конфиденциальной информации?

1) инициативное сотрудничество;
2) выпытывание;
3) наблюдение;
4) хищение;
5) копирование.

Вопрос 4. Какое из утверждений неверно?

1) подкуп — сложный процесс, требует долгой и кропотливой работы;
2) выпытывание — это стремление путем внешне наивных вопросов получить определенные сведения;
3) процесс наблюдения не сложен, так как не требует затрат сил и средств;
4) под незаконным подключением понимают контактное или бесконтактное подсоединение к линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них;
5) негласное ознакомление — способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать.

Вопрос 5. Завершающим этапом любого сбора конфиденциальной информации является

1) копирование;
2) подделка;
3) аналитическая обработка;
4) фотографирование;
5) наблюдение.

Задание 4

Вопрос 1. Как называются реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации?

1) ненадежность;
2) угроза;
3) несчастный случай;
4) авария;
5) правильного ответа среди перечисленных нет.

Вопрос 2. Что в скором времени будет являться главной причиной информационных потерь?

1) материальный ущерб, связанный с несчастными случаями;
2) кража и преднамеренная порча материальных средств;
3) информационные инфекции;
4) аварии и выход из строя аппаратуры, программ и баз данных;
5) ошибки эксплуатации.

Вопрос 3. В каком варианте ответа инфекции расположены от более простого к более сложному, по возрастанию?

1) логические бомбы, троянский конь, червь, вирус;
2) червь, вирус логические бомбы, троянский конь;
3) червь логические бомбы вирус, троянский конь;
4) логические бомбы, вирус, троянский конь червь;
5) вирус, логические бомбы, троянский конь червь.

Вопрос 4. Причины, связанные с информационным обменом и приносящие наибольшие убытки?

1) остановка или выход из строя информационных систем;
2) потери информации;
3) неискренность;
4) проникновение в информационную систему;

5) перехват информации.

Вопрос 5. Какие цели преследуются при активном вторжении в линии связи?

1) анализ информации(содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
2) воздействие на поток сообщений(модификация, удаление и посылка ложных сообщений) или восприпятствие передаче сообщений;
3) инициализация ложных соединений;
4) варианты 1 и 2;
5) варианты 2 и 3.

Задание 5

Вопрос 1. Что определяет модель нарушителя?

1) категории лиц, в числе которых может оказаться нарушитель;
2) возможные цели нарушителя и их градации по степени важности и опасности;
3) предположения о его квалификации и оценка его технической вооруженности;
4) ограничения и предположения о характере его действий;
5) все выше перечисленные.

Вопрос 2. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.

1) ознакомление с информационной системой или вычислительной сетью;
2) похитить программу или иную информацию;
3) оставить записку, выполнить, уничтожить или изменить программу;
4) вариант 2 и 3;
5) вариант 1, 2 и 3.

Вопрос 3. Какое из утверждений неверно?

1) наблюдается тенденция к стремительному росту попыток получить несанкционированный доступ к информационным системам или вычислительным сетям;

2) недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования;
3) считается, что компьютерные преступления, более легкий путь добывания денег, чем ограбление банков;
4) очень малое число фирм могут пострадать от хакеров;
5) к категории хакеров-профессионалов обычно относят: преступные группировки, преследующие политические цели.

Вопрос 4. Какое из утверждений неверно?
1) хакеры могут почерпнуть много полезной информации изгазети других периодических изданий;
2) хакерами часто используется завязывание знакомств для получения информации о вычислительной системе или выявления служебных паролей;
3) один из наиболее эффективных и наименее рискованных путей получения конфиденциальной информации и доступа к ЭВМ — просто изучая черновые распечатки;
4) о перехвате сообщений в каналах связиречь может идти лишь в связи с деятельностью военных или секретных служб;
5) после получения необходимого объема предварительной информации, компьютерный хакер-профессионал осуществляет непосредственное вторжение в систему.

Вопрос 5. Какое из утверждений неверно?
1) наибольшие убытки (в среднем) приносит саботаж в нематериальной сфере;
2) убытки, связанные с забастовками не превышают убытков связанных с аварией оборудования;
3) уход ведущих специалистов опасен для малых центров;
4) хищения, в первую очередь осуществляются сотрудниками предприятия или пользователями;
5) аварии оборудования или основных элементов системы являются мало распространенными и определяются надежностью аппаратуры.

Задание 6

Вопрос 1. Метод скрытие — это...
1) максимальное ограничение числа секретов, из-за допускаемых к ним лиц;
2) максимального ограничения числа лиц, допускаемых к секретам;
3) уменьшение числа секретов неизвестных большинству сотрудников;
4) выбор правильного места, для утаивания секретов от конкурентов;

5) поиск максимального числа лиц, допущенных к секретам.

Вопрос 2. Что включает в себя ранжирование как метод защиты информации?

1) регламентацию допуска и разграничение доступа к защищаемой информации**;**
2) деление засекречиваемой информации по степени секретности;
3) наделять полномочиями назначать вышестоящими нижестоящих на соответствующие посты;
4) вариант ответа 1 и 2;
5) вариант ответа 1, 2 и 3.

Вопрос 3. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?

1) скрытие;
2) дезинформация;
3) дробление;
4) кодирование;
5) шифрование.

Вопрос 4. Что в себя морально-нравственные методы защиты информации?

1) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений;
2) контроль работы сотрудников, допущенных к работе с секретной информацией;
3) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
4) вариант ответа 1 и 3;
5) вариант ответа 1, 2 и 3.

Вопрос 5. Какое из выражений неверно?

1) страхование — как метод защиты информации пока еще не получил признания;
2) кодирование — это метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации;
3) шифрование может быть предварительное и линейное;

4) дирекция очень часто не может понять необходимость финансирования безопасности;
5) безопасность предприятия — не стабильное состояние предприятия, не поддающееся прогнозированию во времени.

Задание 7

Вопрос 1. Какой должна быть защита информации с позиции системного подхода?
1) безопасной для сотрудников;
2) активной;
3) универсальной;
4) надежной;
5) непрерывной.

Вопрос 2. Что такое «служба безопасности»?
1) система внештатных формирований, предназначенных для обеспечения безопасности объекта;
2) структурное подразделение, предназначенное для охраны помещений и территорий предприятия;
3) система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации;
4) структурное подразделение, предназначенное для хранения и выдачи документов, носителей конфиденциальной информации;
5) структурное подразделение, задача которого: подбор персонала и работа с сотрудниками.

Вопрос 3. Кому подчиняется служба безопасности?
1) владельцу предприятия;
2) владельцу предприятия и лицу которому тот подчиняется;
3) руководителю предприятия, либо лицу, которому тот делегировал свои права по руководству ее деятельностью;
4) заместителю руководителя предприятия по организационным вопросам;
5) только начальнику службы безопасности.

Вопрос 4. Какие задачи не входят в круг обязанностей службы безопасности?

1) внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической безопасности предприятия;
2) определение участков сосредоточения сведений, составляющих коммерческую тайну;
3) определение на предприятии технологического оборудования, выход из строя которого может привести к большим экономическим потерям;
4) ограничение круга сторонних предприятий, работающих с данным предприятием, на которых возможен выход из-под контроля сведений составляющих коммерческую тайну предприятия;
5) определение круга сведений, составляющих коммерческую тайну.

Вопрос 5. Какие средства использует инженерно-техническая защита (по функциональному назначению)?
1) программные, аппаратные, криптографические, технические;
2) программные, физические, шифровальные, криптографические;
3) программные, аппаратные, криптографические физические;
4) физические, аппаратные, материальные, криптографические;
5) аппаратные, физические, программные, материальные.

Задание 8

Вопрос 1. В каком нормативном акте говорится о формировании и защите информационных ресурсов как национального достояния?
1) в Конституции РФ;
2) в Законе об оперативно розыскной деятельности;
3) в Законе об частной охране и детективной деятельности;
4) в Законе об информации, информатизации и защите информации;
5) в Указе Президента РФ № 170 от 20 января 1994 г. «Об основах государственной политики в сфере информатизации».

Вопрос 2. На какую структуру возложены организационные, коммерческие и технические вопросы использования информационных ресурсов страны
1) Министерство Информатики РФ;
2) Комитет по Использованию Информации при Госдуме;
3) Росинформресурс;
4) все выше перечисленные;
5) правильного ответа нет.

Вопрос 3. На каком уровне защиты информации создаются комплексные системы защиты информации?

1) на организационно-правовом;
2) на социально политическом;
3) на тактическом*;*
4) на инженерно-техническом;
5) на всех вышеперечисленных.

Вопрос 4. Какие существуют наиболее общие задачи защиты информации на предприятии?

1) снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной*;*
2) предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;
3) документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;
4) создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;
5) все вышеперечисленные.

Вопрос 5. Какие меры и методы защиты секретной или конфиденциальной информации в памяти людей не являются основными?

1) воспитание понимания важности сохранения в тайне доверенных им секретных или конфиденциальных сведений;
2) подбор людей, допускаемых к секретным работам;
3) обучение лиц, допущенных к секретам, правилам их сохранения;
4) добровольное согласие на запрет работы по совместительству у конкурентов;
5) стимулирование заинтересованности работы с засекреченной информацией и сохранения этих сведений в тайне.

Задание 9

Вопрос 1. В каком документе содержаться основные требования к безопасности информационных систем в США?

1) в красной книге;
2) в желтой прессе;
3) в оранжевой книге;
4) в черном списке;
5) в красном блокноте.

Вопрос 2. Какое определение соответствует термину «Аутентификация»?
1) набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации в данной организации;
2) распознавание имени объекта;
3) подтверждение того, что предъявленное имя соответствует объекту;
4) регистрация событий, позволяющая восстановить и доказать факт происшествия событий;
5) правильного определения нет.

Вопрос 3. Какое требование относится к термину «Подотчетность»?
1) субъекты индивидуально должны быть идентифицированы;
2) гарантированно защищенные механизмы, реализующие указанные базовые требования, должны быть постоянно защищены от "взламывания";
3) необходимо иметь явную и хорошо определенную политику обеспечения безопасности;
4) аудиторская информация должна храниться и защищаться так, чтобы имелась возможность отслеживать действия, влияющие на безопасность;
5) метки, управляющие доступом, должны быть установлены и связаны с объектами.

Вопрос 4. Какой уровень безопасности системы соответствует низшему?
1) A;
2) B;
3) C;
4) D;
5) E.

Вопрос 5. Какой класс присваивается системам, которые не прошли испытания?
1) A1;
2) B2:
3) B3;

4) C4;
5) D.

Задание 10

Вопрос 1. Что включают в себя технические мероприятия по защите информации?
1) поиск и уничтожение технических средств разведки;
2) кодирование информации или передаваемого сигнала;
3) подавление технических средств постановкой помехи;
4) применение детекторов лжи;
5) все вышеперечисленное.

Вопрос 2. Какие устройства поиска технических средств разведки не относятся к устройствам поиска пассивного типа?
1) металлоискатели;
2) тепловизоры;
3) устройства и системы поиска по электромагнитному излучению;
4) аккустические корреляторы;
5) детекторы записывающей аппаратуры.

Вопрос 3 Какие устройства не относятся к устройствам поиска по электромагнитному излучению?
1) частотомер;
2) шумомер;
3) сканер;
4) нелинейный локатор;
5) анализатор спектра.

Вопрос 4. Какова цена самого дешевого японского компактного приемника-сканера?
1) 200 US$.
2) 300 US$.
3) 500 US$.
4) 700 US$.
5) 900 US$.

Вопрос 5. Какова дальность обнаружения звукозаписывающей аппаратуры?

1) 1 м.
2) более 1 м.
3) менее 1 м.
4) 3 м.
5) 5 м.

Задание 11

Вопрос 1. Какова скорость перемешивания частотных интервалов при частотном скремблировании?
1) 1 цикл в сек.
2) 20 циклов в сек.
3) От 20 до 30 циклов в сек.
4) От 2 до 16 циклов в сек.
5) От 30 до 40 циклов в сек.

Вопрос 2. С какого расстояния можно считать информацию с монитора компьютера?
1) 200 м.
2) менее 200 м.
3) 500 м.
4) 750 м.
5) 1 км.

Вопрос 3. Какие материалы не применяются при экранировании помещения?
1) листовая сталь;
2) медная сетка;
3) алюминиевая фольга;
4) все вышеперечисленные;
5) фтористая сетка.

Вопрос 4. Какое устройство позволяет обеспечивать защищенность от разного рода сигналов генерируемых устройствами, которые могут служить источником утечки информации?
1) приемник-сканер;
2) телефонный адаптер;
3) скремблер;
4) сетевой фильтр;

5) все вышеперечисленные.

Вопрос 5. Какие существуют основные типы детекторов лжи?
1) полиграф;
2) сигнализатор психологического стресса;
3) анализатор стресса по голосу;
4) все вышеперечисленные;
5) правильного ответа нет.

Задание 12

Вопрос 1. Какие основные направления в защите персональных компьютеров от несанкционированного доступа Вы знаете?
1) недопущение нарушителя к вычислительной среде;
2) защита вычислительной среды;
3) использование специальных средств защиты информации ПК от несанкционированного доступа;
4) все вышеперечисленные;
5) правильного ответа нет.

Вопрос 2. По скольким образцам почерка определяются параметры при опознавании пользователей ПК по почерку?
1) 1-3;
2) 3-5;
3) 5-10;
4) 10-15;
5) 15-18.

Вопрос 3. Какие средства защиты информации в ПК наиболее распространены?
1) применение различных методов шифрования, не зависящих от контекста информации;
2) средства защиты от копирования коммерческих программных продуктов;
3) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
4) защита от компьютерных вирусов и создание архивов;
5) все вышеперечисленные.

Вопрос 4. Какой программный продукт предназначен для защиты жесткого диска от несанкционированного доступа?

1) MAWR, ver. 5.01;
2) PROTEST.COM, ver. 3.0:
3) PASSW, ver. 1.0;
4) ADM, ver. 1.03;
5) Все вышеперечисленные.

Вопрос 5. Какое утверждение неверно?

1) чтобы уменьшить потери по эксплуатационным причинам, следует иметь архивные копии используемых файлов и систематически обновлять копии изменяемых файлов;
2) программы-архиваторы позволяют не только сэкономить место на архивных дискетах, но и объединять группы совместно используемых файлов в один архивный файл, что заметно облегчает ведение архивов:
3) информация на жестком диске может разрушиться только вследствие действия компьютерного вируса или злого умысла вашего недоброжелателя;
4) единственно надежным способом уберечь информацию от любых разрушительных случайностей является четкая, неукоснительно соблюдаемая система резервного копирования;
5) одним из основных симптомов, возникновения серьезных дефектов на диске, является замедление работы дисковода.