Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ЛЕСОСИБИРСКИЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ –
филиал Сибирского федерального университета

УТВЕРЖДАЮ
Директор ЛПИ – филиала СФУ
_____ Т.Ю. Храмова
30 09 2016г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Б1.В.ОД.11 Информационная безопасность и защита информации индекс и наименование дисциплины в соответствии с ФГОС ВО и учебным планом
Направление подготовки	09.03.02 Информационные системы и технологии код и наименование направления подготовки
Профиль	09.03.02.07 Информационно-управляющие системы код и наименование профиля

Лесосибирск 2016

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по укрупненной группе

09.00.00 Информатика и вычислительная техника
код и наименование укрупненной группы

Направление подготовки (профиля) 09.03.02 Информационные системы и технологии
код и наименование направления подготовки (профиля)

09.03.02.07 Информационно-управляющие системы
код и наименование направления подготовки (профиля)

Программу составили Н. И. Пак
инициалы, фамилия, подпись

Е. В. Киргизова
инициалы, фамилия, подпись

Заведующий кафедрой (разработчик) Н. Ф. Романцова
инициалы, фамилия, подпись

«10» 09 2016 г.

Рабочая программа обсуждена на заседании кафедры высшей математики, информатики и естествознания
«10» 09 2016 г. протокол № 1

Заведующий кафедрой Н. Ф. Романцова
инициалы, фамилия, подпись

Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины.

Цель изучения дисциплины является ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами РФ, по данному вопросу и правилами получения соответствующих лицензий.

1.2 Задачи изучения дисциплины.

- получения студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации;
- формирование навыков, необходимых студентам по защите информации и администраторам локальных сетей.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы высшего образования.

Компетенции выпускника ООП, формируемые в результате освоения дисциплины:

- владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, умение логически верно, аргументированно и ясно строить устную и письменную речь (ОК-1):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии оценки
Минимальный: - знать основные положения методологии научного исследования и уметь применять их при работе над выбранной темой исследования. **Базовый** - уметь воспринимать информацию, ставить цели и выбирать пути ее достижения, логически верно, аргументировано и ясно строить устную и письменную речь. **Продвинутый:** - владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

- готовность к кооперации с коллегами, работе в коллективе, знание принципов и методы организации и управления малыми коллективами (ОК-2):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии

		оценки
Минимальный: - знать принципы и методы организации и управления малыми коллективами. **Базовый** - уметь работать в коллективе. **Продвинутый:** - владеть готовностью к кооперации с коллегами, работе в коллективе.	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

- способность находить организационно-управленческие решения в нестандартных ситуациях и готовность нести за них ответственность (ОК-3):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии оценки
Минимальный: - знать подходы к принятию организационно-управленческих решений в нестандартных ситуациях. **Базовый** - уметь находить организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность. **Продвинутый:** - владеть способностью находить организационно-управленческие решения в нестандартных ситуациях.	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

- понимание социальной значимости своей будущей профессии, обладание высокой мотивацией к выполнению профессиональной деятельности (ОК-4):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии оценки
Минимальный: - знать социальную значимость своей будущей профессии. **Базовый** - уметь понимать социальную значимость своей будущей профессии. **Продвинутый:** - владеть пониманием социальной значимости своей будущей профессии, высокой мотивацией к выполнению профессиональной деятельности.	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

- способностью научно анализировать социально значимые проблемы и процессы, умение использовать на практике методы гуманитарных, экологических, социальных и экономических наук в различных видах профессиональной и социальной деятельности (ОК-5)

Уровни формируемых компетенций	Технологии	Средства и

	формирования	технологии оценки
Минимальный: - знать социально значимые проблемы и процессы, методы гуманитарных, экологических, социальных и экономических наук в различных видах профессиональной и социальной деятельности. **Базовый** - уметь научно анализировать социально значимые проблемы и процессы, использовать на практике методы гуманитарных, экологических, социальных и экономических наук в различных видах профессиональной и социальной деятельности. **Продвинутый:** - владеть способностью научно анализировать социально значимые проблемы и процессы.	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

- понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии оценки
Минимальный: - знать сущность и значения информации в развитии современного информационного общества, основные требования к информационной безопасности, в том числе защите государственной тайны. **Базовый** - уметь соблюдать основные требования к информационной безопасности, в том числе к защите государственной тайны. **Продвинутый:** - владеть пониманием сущности и значения информации в развитии современного информационного общества.	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

- способность использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению (ОПК-5):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии оценки
Минимальный: - знать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и	лекции, практические занятия.	устный опрос, подготовка доклада,

обоснования принятых идей и подходов к решению. **Базовый** - использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению. **Продвинутый:** - способностью использовать современные компьютерные технологии поиска информации для решения поставленной задачи, критического анализа этой информации и обоснования принятых идей и подходов к решению.		подготовка презентации, тестирование, экзамен.

- способность поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества (ПК-30):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии оценки
Минимальный: - знать источники угроз безопасности информации, методы оценки уязвимости информации. . **Базовый** -уметь применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации. . **Продвинутый:** -владеть навыками освоения и внедрения средств защиты информации. .	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

- способностью обеспечивать безопасность и целостность данных информационных систем и технологий (ПК-31):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии оценки
Минимальный: - знать данные информационных систем и технологий. **Базовый** - уметь обеспечивать безопасность и целостность данных информационных систем и технологий. . **Продвинутый:** - владеть способностью обеспечивать безопасность и целостность данных информационных систем и	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

технологий.		

• способностью составлять инструкции по эксплуатации информационных систем (ПК-33):

Уровни формируемых компетенций	Технологии формирования	Средства и технологии оценки
Минимальный: - знать инстукции по эксплуатации информационных систем. **Базовый** -уметь составлять инструкции по эксплуатакции информационных систем. **Продвинутый:** -владеть способностью составлять инструкции по эксплуатакции информационных систем. .	лекции, практические занятия.	устный опрос, подготовка доклада, подготовка презентации, тестирование, экзамен.

1.4 Место дисциплины (модуля) в структуре образовательной программы высшего образования.

Дисциплина «Технологии обработки информации» относится к профессиональному циклу и входит в образовательный стандарт подготовки бакавлавров направления Информационные системы и технологии. Знания и навыки, полученные при изучении дисциплины «Технологии обработки информации» могут быть использованы при освоении, как теоретического материала, так и при решении практических задач при изучении специальных дисциплин («Системное программное обеспечение», «Информационные технологии», «Проектирование ИС», «Архитектура вычислительных систем» и пр.).

1.5 Особенности реализации дисциплины.

Дисциплина реализуется на русском языке.

2 Объем дисциплины (модуля)

Видучебнойработы	Всего, зачетных единиц (акад.часов)	Семестр
		8
Общая трудоемкость дисциплины	**5 (180)**	**5 (180)**
Контактная работа спреподавателем:	0,61 (22)	0,61 (22)
занятия лекционного типа	0,38 (14)	0,38 (14)
занятия семинарского типа	0,2 (8)	0,2 (8)
в том числе:семинары Практические занятия практикумы Лабораторные работы	0,2 (8)	0,2 (8)

другие виды контактной работы		
в том числе: курсовое проектирование Групповые консультации Индивидуальные консультации иные виды внеаудиторной контактной работы		
В том числе: в интерактивной форме	0,11 (4)	0,11 (4)
в электронной форме	0,11 (4)	0,11 (4)
Самостоятельная работа обучающихся:	**4,13 (149)**	**4,13 (149)**
изучение теоретического курса(ТО)	4,13 (149)	4,13 (149)
расчетно-графические задания, задачи(РГЗ)		
реферат, эссе(Р)		
курсовое проектирование(КР)		
Вид промежуточной аттестации (зачет,экзамен)	**Экзамен 0,25 (9)**	**Экзамен 0,25 (9)**

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий).

/п	Модули, темы (разделы) дисциплины	Занятия лекцион-ного (акад.час)	Занятия семинарского типа		Самостоятель-ная работа (акад.час)	Формируемые компетенции
			Семинары и/или практические занятия (акад.час)	Лабораторные работы и/или практи-кумы (акад. час)		
1	Информационные уязвимости объектов Угрозы информационной безопасности и их источники	10			70	ОК-1,2,3,4,5 ПК - 30,31,33
2	Средства обеспечения информационной безопасности	4		8	79	ОК-1,4,5 ОПК-4 ПК - 30

3.2 Занятия лекционного типа.

№ п/п	№ раздела дисциплины	Наименование занятий[1]	Объем в акад.часах		
			всего	в томчисле в инновационной форме	в том числе в электронной форме
1	1	Тема №1. Актуальность информационной безопасности в современных условиях.	2	2	2

2	1	Тема №2. Угрозы информационной безопасности (Угрозы безопасности информации. Информационная безопасность в условиях функционирования в России глобальных сетей)	2		
3	1	Тема №3. Дискреционная и мандатная модели политики безопасности (Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обусловливающие их существование. Анализ способов нарушений информационной безопасности удаленная атака. Использование защищенных компьютерных систем.	2		
4	2	Тема №4. Традиционные и современные криптосистемы (Введение. Понятия криптологии, криптографии и криптоанализа. Основные определения. Методы шифрования данных. Основные криптографические алгоритмы. Абонентское и пакетное шифрование. Системы аутентификации электронных данных. Обеспечение целостности информации на основе электронной цифровой подписи	4		
5	2	Тема №5. Нормы и требования российского законодательства в области лицензирования и сертификации. (Лицензирование и сертификация в области защиты информации. Правила построения и функционирования	2		

		системы лицензирования ФАПСИ (федеральное агентство правительственной связи и информации).Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы)			
6	2	Тема №6. Угрозы безопасности БД: общие и специфические (Угрозы ИБ баз данных. Функции администратора БД. Методы защиты БД.. Правовая охрана баз данных	2		

3.3 Занятия практического типа.

Планом не предусмотрены.

3.4 Лабораторные занятия.

№ п/п	№ раздела дисциплины	Наименование занятий[1]	Объем в акад.часах		
			всего	в том числе в инновационной форме	в том числе в электронной форме
1	2	Тема №1. Изучение программных средств защиты от несанкционированного доступа	2	2	2
2	2	Тема №2. Средства безопасности Windows. Обеспечение безопасности хранения данных в ОС Windows	2		
3	2	Тема №3. Шифр Цезаря. Шифр Гронсфельда. Шифры перестановки (маршрутное шифрование)	2		
4	2	Тема №4. Защита баз данных на примере MS	2		

		ACCESS.			

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

1. Киргизова, Е.В. Теория информации: учебное пособие. – Красноярск, 2008.

2. Симонович, С.В. Специальная информатика: учебное пособие / С.В. Симонович, Г.А. Евсеев, А.Г. Алексеев. – Москва: АСТ ПРЕСС: Инфорком-Пресс, 2008.

5 Фонд оценочных средств для проведения промежуточной аттестации

Вопросы к зачету к экзамену (Приложение 1).

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

Таблица 1- Рекомендованные оценочные средства для студентов с ограниченными возможностями здоровья

Категория студентов	Виды оценочных средств	Форма контроля и оценки результатов обучения
С нарушением слуха	Тесты, рефераты, контрольные вопросы	Преимущественно письменная проверка
С нарушением зрения	Контрольные вопросы	Преимущественно устная проверка (индивидуально)
С нарушением опорно-двигательного аппарата	Решение тестов, контрольные вопросы дистанционно	Организация контроля с помощью электронной оболочки MOODLE, письменная проверка

6 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины(модуля)

Основная:

1. Жук, А.П. Защита информации: Учеб.пособие / А.П. Жук, Е.П. Жук, О.А. Лепешкин, А.И. Тимошкин. – Москва: РИОР; ИНФРА–М, 2013. – 392 с. – (Высшее образование: Бакалавриат; Магистратура).

2. Мельников, В.П. Защита информации: учебник для студ. учреждений высш. обрразования / В.П. Мельников, А.И. Куприянов, А.Г. Схиртладзе: под. ред. проф. В.П. Мельникова. – Москва: Издательски йцентр «Академия», 2014. – 304 с.

3. Тушко, Т.А. Информатика: учебное пособие для студентов вузов

направления подготовки бакалавров 230400.62 «Информационные системы и технологии» / Т. А. Тушко, Н. В. Молокова, С. А. Виденин. - Красноярск : СФУ, 2012. - 188 с. [Электронный ресурс]. – Режим доступа: Полный текст (pdf, 2,9 Мб). Доступ в сети СФУ

Дополнительная литература:

1. Баженова, И.Ю. Языки программирования : Учебник для студентов учреждений высш. проф. образования, обуч. по направлениям «Фундаментальная информатика и информационные технологии» и «Информационная безопасность» / под ред. И. Ю. Баженова; В. А. Сухомлина. - Москва: Академия, 2012.

2. Новожилов, О. П. Информатика : учебное пособие для студ. высш. учеб. заведений, обуч. по спец. «Экономика и управление» и «Информатика и вычислительная техника»: доп. УМО вузов по унив. политехнич. образованию / О. П. Новожилов ; Московский. гос. индустриальный университет. - 2-е изд., испр. и доп. - Москва : Юрайт, 2014. - 584 с.

3. Гаврилов, М. В. Информатика и информационные технологии: учебник для прикладного бакалавриата / М. В. Гаврилов, В. А. Климов ; Саратовская гос. юридическая академия . - 4-е изд., перераб. и доп. - Москва : Юрайт, 2015. - 382 с.

4.

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины(модуля)

1. Крупнейшая техническая библиотека [Электронный ресурс].– Режим доступа: www.citforum.ru;
2. Бесплатное дистанционное обучение в Национальном Открытом Университете «ИНТУИТ» [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/
3. Сайт для студентов«Студопедия» [Электронный ресурс].– Режим доступа: http://studopedia.net

Электронно-библиотечныесистемы:

1. ЭБС «Лань» [Электронный ресурс]. – Режим доступа: http://e.lanbook.com/;
2. ЭБС «ИНФРА-М» [Электронный ресурс]. – Режим доступа: http://www.znanium.com/;
3. ЭБС «Национальный цифровой ресурс «Руконт»» [Электронный ресурс]. – Режим доступа:: http://rucont.ru.
4. ЭБС СФУ: http://bik.sfu-kras.ru/
5. ЭБС ЛПИ - филиал СФУ http://95.188.107.8/

8 Методические указания для обучающихся по освоению дисциплины(модуля)

Самостоятельная работа включает изучение теоретического материала

и решение задач. Теоретические вопросы, вынесенные на самостоятельное изучение, оглашаются на лекции и входят в список вопросов к экзамену.

Задачи выдаются в виде заданий (в каждом от 4 до 10 задач в зависимости от сложности темы), в порядке изучения разделов дисциплины. Решение задач оформляется в тетради и сдается на проверку.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации в зависимости от нозологии:

Для лиц с нарушениями зрения:

– в форме электронного документа.

Для лиц с нарушением слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

9 **Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)**

9.1 Перечень необходимого программного обеспечения

1. Операционная система Microsoft Windows 7.
2. Пакет программ Microsoft Office Professional Plus 2007.
3. Kaspersky Endpoint Security 10.
4. Программа-архиватор: WinRAR.
5. Microsoft Visual Studio.
6. Radmin 3.

9.2 Перечень необходимых информационных справочных систем

В качестве информационных справочных систем для реализации дисциплины используются Yandex, Google и ЭБС ЛПИ-филиалаСФУ.

10 **Материально-техническая база, необходимой для осуществления образовательного процесса по дисциплине(модулю)**

В перечень материально-технического обеспечения входит:

- мультимедийная лекционная аудитория, оснащенная проектором, обеспечивающим воспроизводство слайдов и текстов с экрана монитора компьютера лектора, устройства мизатемнения;
- компьютерный класс с необходимым программным обеспечением.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными или электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Приложение 1

Вопросы к экзамену

1. Информационная безопасность в системе национальной безопасности
2. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
3. Виды национальной безопасности и их краткая характеристика.
4. Системные связи информационной безопасности с другими видами национальной безопасности.
5. Информационные уязвимости объектов.
6. Антропогенные информационные уязвимости.
7. Техногенные информационные уязвимости.
8. Организационно-правовые информационные уязвимости.
9. Комбинированные информационные уязвимости
10. Угрозы информационной безопасности и их источники.
11. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.
12. Эндогенные и экзогенные, угрозы информационной безопасности, их классификация.
13. Антропогенные и техногенные угрозы информационной безопасности, их

классификация.

14. Системная классификация угроз информационной безопасности.
15. Угрозы конфиденциальности, целостности и доступности

информации.

16.Информационная война как высшая форма угрозы информационной безопасности.

17. Категорирование информации.

18.Допуск к информационным ресурсам.

19.Основные принципы защиты информации от несанкционированного доступа.

20.Средства обеспечения информационной безопасности.

21. Аппаратные средства обеспечения информационной безопасности.

22.Программные средства обеспечения информационной безопасности.

23.Криптографические средства обеспечения информационной безопасности.

24.Стеганографические средства обеспечения информационной безопасности.

25.Организационно-правовые средства обеспечения информационной безопасности,

26.Государственная политика в области информационной безопасности.

27.Государственные органы обеспечения информационной безопасности.

28.Приоритетные направления обеспечения информационной безопасности в условиях информационного общества.

29.Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества.

30.Технические каналы утечки конфиденциальной информации.

31.Пассивные средства противодействия техническим разведкам.

32.Активные средства противодействия техническим разведкам.

33.Базовые стратегии организации защиты информации.

34.Полное множество функций защиты информации.

35.Задачи защиты информации. Репрезентативное множество задач защиты.

36.Формирование политики обеспечения информационной безопасности объекта.

37.Проектирование оптимальных систем защиты информации.

38.Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения.

39.Риски информационной безопасности

40.Статистика инцидентов информационной безопасности.

41.Основные макропроцессы управления функционированием комплексной системы защиты информации.