МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра информатики и прикладной математики

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ Е.И. Луковникова
«_____» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Б1.В.ДВ.08.01

НАПРАВЛЕНИЕ ПОДГОТОВКИ

05.03.06 Экология и природопользование

ПРОФИЛЬ ПОДГОТОВКИ

Экология

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

СОДЕРЖАНИЕ ПРОГРАММЫ **Стр.**

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся к производственно-технологическому и научно-исследовательскому видам профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Формирование у обучающихся знаний и умений, которые образуют теоретический и практический фундамент в области основ информационной безопасности, навыков практического обеспечения защиты информации и безопасного использования информационно-телекоммуникационных систем.

Задачи дисциплины

Изучение организационно-правовых основ защиты информации в информационно-коммуникационных системах; ознакомление обучающихся с основными угрозами информационной безопасности и правилами их выявления; приобретении практических навыков применения современных средств и способов обеспечения информационной безопасности.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ОПК-9	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**знать:** – сущность и понятие информационной безопасности, характеристику ее составляющих; – основные методы и средства защиты информации; – технологию организации обеспечения информационной безопасности; **уметь:** – выбирать эффективные способы и средства защиты; **владеть:** – навыками работы с программными и техническими средствами защиты информации.
ПК-4	способность прогнозировать техногенные катастрофы и их последствия, планировать мероприятия по профилактике и ликвидации последствий экологических катастроф, принимать профилактические меры для снижения уровня опасностей различного вида и их последствий	**знать:** – нормативно-правовую базу, регламентирующую основные положения в области информационной безопасности; **уметь:** – проводить анализ потенциально возможных угроз информации и информационным технологиям; **владеть:** – навыками использования в повседневной деятельности персональных средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ.08.01 «Основы информационной безопасности» относится к элективной части.

Дисциплина «Основы информационной безопасности» базируется на знаниях, полученных при изучении таких учебных дисциплин, как «Информатика», «Программное обеспечение ЭВМ», «Компьютерный практикум».

Основываясь на изучении перечисленных дисциплин, «Основы информационной безопасности» представляют основу для преддипломной практики и подготовки к государственной итоговой аттестации.

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	*Курс*	*Семестр*	*Трудоемкость дисциплины в часах*						*Курсовая работа (проект), контрольная работа, реферат, РГР*	*Вид промежуточной аттестации*
			Всего часов (с экз.)	*Аудиторных часов*	*Лекции*	*Лабораторные работы*	*Практические занятия*	*Самостоятельная работа*		
1	2	3	4	5	6	7	8	9	10	11
Очная	4	8	72	26	13	–	13	46	–	зачет
Заочная	–	–	–	–	–	–	–	–	–	–
Заочная (ускоренное обучение)	–	–	–	–	–	–	–	–	–	–
Очно-заочная	–	–	–	–	–	–	–	–	–	–

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	*Трудоемкость (час.)*	*в т.ч. в интерактивной, активной, инновационной формах, (час.)*	*Распределение по семестрам, (час.)*
			8
1	2	3	4
I. Контактная работа обучающихся с преподавателем (всего)	26	–	26
Лекции (Лк)	13	–	13
Практические занятия (ПЗ)	13	–	13
Групповые (индивидуальные) консультации	+	–	+
II.Самостоятельная работа обучающихся (СР)	46	–	46
Подготовка к практическим занятиям	26	–	26
Подготовка к зачету	20	–	20
III. Промежуточная аттестация зачет	+	–	+
Общая трудоемкость дисциплины час.	72	–	72
зач. ед.	2	–	2

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий

№ раздела и темы	*Наименование раздела и тема дисциплины*	*Трудоемкость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость, (час.)*		
			учебные занятия		*самостоятельная работа обучающихся*
			лекции	*практические занятия*	
1	2	3	4	5	6
1.	**Основные понятия и положения информационной безопасности**	**6**	**2**	**–**	**4**
1.1.	Предмет и объект защиты информации	3	1	–	2
1.2.	Наиболее распространенные угрозы информационной безопасности	3	1	–	2
2.	**Методы и средства защиты информации**	**54**	**9**	**11**	**34**
2.1.	Нормативно-правовые основы информационной безопасности	15	1	4	10
2.2.	Административный и процедурный уровни информационной безопасности	3	1	–	2
2.3.	Основные программно-технические меры	9	1	2	6
2.4.	Сервисы обеспечения информационной безопасности	27	6	5	16
3.	**Построение и организация функционирования комплексных систем защиты информации**	**12**	**2**	**2**	**8**
3.1.	Построение комплексных систем защиты информации (КСЗИ)	10	2	2	6
3.2.	Организация функционирования КСЗИ	4	2	–	2
	ИТОГО	**72**	**13**	**13**	**46**

4.2. Содержание дисциплины, структурированное по разделам и темам

№ раздела и темы	*Наименование раздела и темы дисциплины*	*Содержание лекционных занятий*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	2	3	4
1.	**Основные понятия и положения информационной безопасности**		
1.1.	Предмет и объект защиты информации	Понятие информационной безопасности. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности.	–

1.2.	Наиболее распространенные угрозы информационной безопасности	Основные определения и критерии классификации угроз. Наиболее распространенные угрозы доступности. Некоторые примеры угроз доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности.	
2.	**Методы и средства защиты информации**		
2.1.	Нормативно-правовые основы информационной безопасности	Законодательный уровень информационной безопасности. Место информационной безопасности в системе национальной безопасности. Законодательство РФ в области информационной безопасности, защиты сведений, составляющих государственную тайну, и информации ограниченного доступа. Доктрина информационной безопасности Российской Федерации об основных угрозах и их источниках в информационной сфере. Компьютерные правонарушения. Правовое обеспечение безопасности информационных систем. Юридическая ответственность за правонарушения в информационной сфере. Стандарты и спецификации в области информационной безопасности	–
2.2.	Административный и процедурный уровни информационной безопасности	Административный уровень информационной безопасности. Основные понятия. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками. Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.	
2.3.	Основные программно-технические меры	Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.	
2.4.	Сервисы обеспечения информационной безопасности	Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности. Экранирование, анализ защищенности. Обеспечение высокой доступности. Туннелирование и управление.	
3.	**Построение и организация функционирования комплексных систем защиты информации**		
3.1.	Построение комплексных систем защиты информации (КСЗИ)	Этапы создания КСЗИ. Научно-исследовательская разработка КСЗИ. Моделирование КСЗИ. Подходы к оценке эффективности КСЗИ. Создание организационной структуры КСЗИ.	–
3.2.	Организация функционирования КСЗИ	Применение КСЗИ по назначению. Техническая эксплуатация КСЗИ.	

4.3. Лабораторные работы

Учебным планом не предусмотрены.

4.4. Практические занятия

№ п/п	*Номер раздела дисциплины*	*Наименование тем практических занятий*	*Объем, (час.)*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1.	**2.**	Стандарты и законодательные документы в области обеспечения информационной безопасности.	4	–
2.	**2.**	Методы и технологии борьбы с компьютерными вирусами.	2	–
3.	**2.**	Криптографическое закрытие информации. Основные алгоритмы шифрования.	5	–
4.	**3.**	Построение комплексной системы защиты информации	2	–
		ИТОГО	**13**	**–**

4.5. Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат

Учебным планом не предусмотрены.

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Компетенции / *№, наименование разделов дисциплины*	*Кол-во часов*	*Компетенции*		*Σ комп.*	*tср, час*	*Вид учебных занятий*	*Оценка результатов*
		ОПК	*ПК*				
		9	*4*				
1	2	3	4	5	6	7	8
1. Основные понятия и положения информационной безопасности	6	+	+	2	3	Лк, СР	зачет
2. Методы и средства защиты информации	54	+	+	2	27	Лк, ПЗ, СР	зачет
3. Построение и организация функционирования комплексных систем защиты информации	12	+	+	2	6	Лк, ПЗ, СР	зачет
всего часов	**72**	**36**	**36**	**2**	**36**		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Цирлов В.Л. Основы информационной безопасности: краткий курс / В.Л. Цирлов. – Ростов-на-Дону: Феникс, 2008. – 253 с.

2. Степанов Е.А. Информационная безопасность и защита информации: учебное пособие / Е.А. Степанов, И.К. Корнеев. – Москва: Инфра-М, 2001. – 304 с.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	*Наименование издания*	*Вид занятия*	*Количество экземпляров в библиотеке*, шт.	*Обеспеченность*, (экз./чел.)
1	2	3	4	5
Основная литература				
1.	Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. – Москва; Берлин: Директ-Медиа, 2015. – 253 с. URL: http://biblioclub.ru/index.php?page=book&id =276557	Лк, ПЗ, СР	ЭУ	1
2.	Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие/ Ю.Н. Загинайлов. – Москва; Берлин: Директ-Медиа, 2015. – 105 с.: ил. – Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book&id= 362895	Лк, ПЗ, СР	ЭУ	1
Дополнительная литература				
3.	Правовое обеспечение информационной безопасности: учебное пособие для вузов / Под ред. С.Я. Казанцева. – 2-е изд., испр. и доп. – Москва: Академия, 2007. – 240 с.	Лк, ПЗ, СР	15	1
4.	Малюк А.А. Введение в защиту информации в автоматизированных системах: учебное пособие / А.А Малюк. − 4-е изд., стереотип. − Москва: Горячая линия-Телеком, 2011. − 146 с.	Лк, ПЗ, СР	5	0,3
5.	Олифер В.Г. Безопасность компьютерных сетей: учебник / В.Г. Олифер, Н.А. Олифер. − Москва: Горячая линия-Телеком, 2014. − 644 с.	Лк, СР	10	0,6
6.	Технические средства и методы защиты информации: Учебное пособие/ А.П.Зайцев и др. – М.: Горячая линия-Телеком, 2012.− 616 с.	Лк, СР	30 (включая аналоги)	1
7.	Смарт Н. Криптография: учебное пособие / Н. Смарт; Пер. с англ. – Москва: Техносфера, 2006. 528 с.	Лк, ПЗ, СР	7	0,4
8.	Гультяева Т.А. Основы теории информации и криптографии: конспект лекций / Т.А. Гультяева; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск: НГТУ, 2010. – 88 с. URL: http://biblioclub.ru/index.php?page=book&id =228963	Лк, ПЗ, СР	ЭУ	1

9.	Торокин А.А. Инженерно-техническая защита информации: учебное пособие / А.А. Торокин. – Москва: Гелиос АРВ, 2005. – 960 с.	Лк, ПЗ, СР	10	0,6
10.	Долозов Н.Л. Программные средства защиты информации: конспект лекций / Н.Л. Долозов, Т.А. Гультяева; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск: НГТУ, 2015. – 63 с. URL: http://biblioclub.ru/index.php?page=book&id=438307	Лк, ПЗ, СР	ЭУ	1

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.Электронный каталог библиотеки БрГУ http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.

2. Электронная библиотека БрГУ http://ecat.brstu.ru/catalog .

3. Электронно-библиотечная система «Университетская библиотека online» http://biblioclub.ru .

4. Информационная система «Единое окно доступа к образовательным ресурсам» http://window.edu.ru/.

5. Научная электронная библиотека «eLIBRARY.ru» http://elibrary.ru/.

6. Федеральная университетская компьютерная сеть России http://www.runnet.ru/.

7. Каталог учебников, оборудования, электронных ресурсов http://ndce.edu.ru/.

8. Научная электронная библиотека «КИБЕРЛЕНИНКА» http://cyberleninka.ru/.

9. Университетская информационная система РОССИЯ (УИС РОССИЯ) http://uisrussia.msu.ru/

10. Национальный Открытый университет – Интуит (Интернет-университет информационных технологий) https://www.intuit.ru/

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебных занятий	Организация деятельности обучающихся
Лекции	Написание конспекта лекций: краткое, последовательное изложение основных положений, формулировок, выводов, обобщений; техническое оформление записей (подчеркивание, выделение ключевых слов и терминов). Активная работа на лекции.
Практические занятия	Выполнение заданий с использованием методических указаний и рекомендаций по выполнению работ, оформление отчетов.
Самостоятельная работа обучающихся	*Подготовка к практическим занятиям.* Проработка материалов по теме практической работы с использованием рекомендуемой литературы, конспекта лекций, ресурсов информационно-телекоммуникационной сети Интернет; выполнение заданий; оформление отчетов. *Подготовка к зачету.* Систематическая работа с конспектом лекций: чтение записей; проверка терминов с помощью энциклопедий, словарей и справочников; обозначение вопросов, материал, которых вызывает трудности; попытка найти ответ в рекомендуемых источниках; подготовка вопросов преподавателю, если не удается самостоятельно разобраться в материале.

9.1. Методические указания для обучающихся по выполнению практических работ

Практическая работа № 1. Стандарты и законодательные документы в области обеспечения информационной безопасности.

Цель работы: изучение нормативно-правовой базы, регламентирующей основные положения в области информационной безопасности.

Задание

Изучить предлагаемый список стандартов, законодательных и нормативно-методических документов в области обеспечения информационной безопасности. Ответить на поставленные вопросы по каждому документу.

Порядок выполнения

Список документов: Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон № 63-ФЗ «Об электронной подписи»; Федеральный закон № 152-ФЗ «О персональных данных»; Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» (с изменениями); закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями); «Об основах государственной политики в сфере информатизации» от 20.01.94 г. № 170 (с изменениями); «Об утверждении перечня сведений конфиденциального характера» от 06.03.97 г. № 188 (с изменениями); Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (с изменениями); «Доктрина информационной безопасности Российской Федерации», утверждена Президентом РФ 9 сентября 2000 г. № ПР.-1895; ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности. Основные термины и определения; ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий; ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью; ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

Список вопросов (фрагмент):

1. Перечислите сферы действия закона.
2. Что такое электронное сообщение?
3. Что такое информационные технологии?
4. Что такое информационная система?
5. Кто может быть обладателем информации?
6. На какие виды можно подразделить информацию?
7. Дать определение обладателя информации.
8. Кто и при каких условиях может стать обладателем информации?
9. Права и обязанности обладателя информации.
10. Какую информацию запрещено относить к информации с ограниченным доступом?
11. Кто и при каких условиях может осуществлять сбор, хранение, использование и распространение информации о частной жизни?
12. Какую информацию запрещено распространять?
13. Дать определение государственных информационных систем.
14. Кто устанавливает особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям?
15. В чём заключается защита информации?
16. Ответственность за нарушение данного закона.
17. Что понимается под информационной безопасностью РФ?
18. В чём заключаются интересы личности в информационной сфере?
19. В чём заключаются интересы государства в информационной сфере?
20. 4 основные составляющие национальных интересов РФ в информационной сфере.
21. Что является угрозой безопасности информационных и телекоммуникационных средств и систем?

22. Какие задачи необходимо решить в области обеспечения информационной безопасности РФ?

23. Общие методы обеспечения информационной безопасности РФ. Охарактеризовать более подробно организационно-технические.

24. Что является основными направлениями обеспечения информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах?

25. Как в настоящее время определены первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ?

26. Что является основными элементами организационной основы системы обеспечения информационной безопасности РФ? В чём состоит роль Совета Безопасности РФ при обеспечении информационной безопасности РФ?

и др.

Вопросы из списка, подлежащие раскрытию в отчете по практической работе, назначаются преподавателем.

Форма отчетности: отчет по практической работе должен включать титульный лист установленного образца; цель работы; задание; результаты выполнения задания (ответы на поставленные вопросы).

Рекомендации по выполнению заданий и подготовке к практической работе: при подготовке и выполнении задания практической работы рекомендуется использовать материалы лекций соответствующих разделов; источники, указанные в разделе 6 данной программы, основную и дополнительную литературу [1-3]; электронные ресурсы, предложенные для освоения дисциплины.

Практическая работа № 2. Методы и технологии борьбы с компьютерными вирусами.

Цель работы: изучение возможностей и настройка антивирусных программ

Задание

1) Изучите и сделайте сравнение функциональных возможностей антивирусных программ Dr Web, Kaspersky, NOD-32.

2) Сделайте подробное описание функционала одной из программ (на выбор).

3) Выполните настройку программы.

Порядок выполнения

Настройка программы:

– Защита компьютера, в том числе защита файловой системы в режиме реального времени; контроль устройств; игровой режим и др.

– Защита Интернета, в том числе защита доступа в Интернет, защита почтового клиента, защита от фишинга и др.

Форма отчетности: отчет по практической работе должен включать титульный лист установленного образца; цель работы; задание; результаты выполнения задания (с соответствующим иллюстративным материалом).

Рекомендации по выполнению задания и подготовке к практической работе: при подготовке и выполнении задания практической работы рекомендуется использовать материалы лекций соответствующих разделов; источники, указанные в разделе 6 данной программы, основную и дополнительную литературу [1, 2, 4, 10]; электронные ресурсы, предложенные для освоения дисциплины.

Контрольные вопросы:

1. Назовите признаки классификации компьютерных вирусов.

2. Поясните принцип действия «стелс»-вирусов, полиморфных вирусов, файловых вирусов, макровирусов и загрузочных вирусов.

3. Дайте характеристику методов обнаружения вирусов.

4. Перечислите профилактические меры предотвращения заражения вирусами КС.
5. Приведите порядок действий пользователя при заражении ЭВМ вирусами.
6. Виды антивирусных программ.

Практическая работа № 3. Криптографическое закрытие информации. Основные алгоритмы шифрования.

Цель работы: получить практические шифрования и дешифрования информации.

Задание
Выполнить кодирование и декодирование предложенного текста.

Порядок выполнения:
При выполнении кодирования и декодирования предлагаемого текста используются:
– Шифрование методами перестановок.
– Шифрование методами замены.
– Аналитические методы шифрования.

Форма отчетности: отчет по практической работе должен включать титульный лист установленного образца; цель работы; задание; результаты выполнения задания (с соответствующим иллюстративным материалом).

Рекомендации по выполнению задания и подготовке к практической работе: при подготовке и выполнении задания практической работы рекомендуется использовать материалы лекций соответствующих разделов; источники, указанные в разделе 6 данной программы, основную и дополнительную литературу [1, 2, 4, 7, 8]; электронные ресурсы, предложенные для освоения дисциплины.

Контрольные вопросы:
1. Дайте определение криптографической защиты информации.
2. Приведите классификацию методов криптографического преобразования информации и поясните сущность методов.
3. Назовите и охарактеризуйте методы шифрования.
4. Сравните наиболее распространенные стандарты шифрования.
5. Каковы перспективы криптозащиты информации в КС?

Практическая работа № 4. Построение комплексной системы защиты информации.

Цель работы: получить практические навыки выполнения отдельных работ по разработке КСЗИ.

Задание
Разработать модель КСЗИ (на концептуальном уровне) для предлагаемой организации.

Порядок выполнения
1) Сделайте анализ важности информации об указанных объектах предметной области и анализ угроз этой информации. Постройте модель угроз.
2) Определите требования к защищенности информации.
3) Создайте модель КСЗИ.
4) Сделайте вывод, оцените степень надежности системы.

Прежде всего производится анализ конфиденциальности и важности информации, которая должна обрабатываться, храниться и передаваться в КС. На основе анализа делается вывод о целесообразности создания КСЗИ. Если информация не является конфиденциальной и легко может быть восстановлена, то создавать КСЗИ нет необходимости. Не имеет смысла также создавать КСЗИ в КС, если потеря целостности и конфиденциальности информации связана с незначительными потерями. В этих случаях достаточно использовать штатные средства КС и, возможно, страхование от утраты информации.

При анализе информации определяются потоки конфиденциальной информации, элементы КС, в которых она обрабатывается и хранится. На этом этапе рассматриваются также вопросы разграничения доступа к информации отдельных пользователей и целых сегментов КС. На основе анализа информации определяются требования к ее защищенности. Требования задаются путем присвоения определенного грифа конфиденциальности, установления правил разграничения доступа.

Анализ угроз безопасности является одним из обязательных условий построения КСЗИ. По результатам проведенного анализа строится модель угроз безопасности информации в КС. Модель угроз безопасности информации в КС содержит систематизированные данные о случайных и преднамеренных угрозах безопасности информации в конкретной КС. Систематизация данных модели предполагает наличие сведений обо всех возможных угрозах, их опасности, временных рамках действия, вероятности реализации.

Моделирование КСЗИ заключается в построении образа (модели) системы, с определенной точностью воспроизводящего процессы, происходящие в реальной системе. Реализация модели позволяет получать и исследовать характеристики реальной системы.

Форма отчетности: отчет по практической работе должен включать титульный лист установленного образца; цель работы; задание; результаты выполнения задания.

Рекомендации по выполнению задания и подготовке к практической работе: при подготовке и выполнении задания практической работы рекомендуется использовать материалы лекций соответствующих разделов; источники, указанные в разделе 6 данной программы; основную и дополнительную литературу [1, 2, 4, 9]; электронные ресурсы, предложенные для освоения дисциплины.

Контрольные вопросы:

1. Назовите основные принципы построения защищенных КС.
2. Дайте краткую характеристику этапов создания КСЗИ.
3. Последовательность и содержание этапов научно-исследовательской разработки КСЗИ
4. Подходы к оценке эффективности КСЗИ.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

- Авторские комплекты слайдов, используемых при проведении лекционных занятий.
- ОС Windows 7 Professional.
- Microsoft Office 2007 Russian Academic OPEN No Level.
- Антивирусное программное обеспечение Kaspersky Security.
- Adobe Reader.
- Chrome.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Вид занятия	***Наименование аудитории***	***Перечень основного оборудования***	***№ ПЗ***
Лк	Мультимедийный класс	Интерактивная доска SMART Board 680I со встроенным проектором UX60. ПК: AMD Athlon™7550 Dual-Core Processor 250 GHz/RAM 2Gb/HDD. Монитор Samsung 943N MY19LS	–
ПЗ	Дисплейный класс	Интерактивная доска SMART Board 680I со встроенным XGA проектором Unifi 35 (77"/195,6 см). 18-ПК: CPU 5000/RAM 2Gb/HDD. Монитор TFT 19 LG1953S-SF. Принтер: HP LaserJet Pro 400M 401dne. Сканер: Canon LiDE 220.	1-4
СР	Читальный зал №1	10 ПК i5-2500/H67/4Gb. Монитор TFT19 Samsung. Принтер HP LaserJet P2055D.	–

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ОПК-9	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**1.** Основные понятия и положения информационной безопасности	1.1. Предмет и объект защиты информации.	Вопросы к зачету
			1.2. Наиболее распространенные угрозы информационной безопасности.	
		2. Методы и средства защиты информации	2.1. Нормативно-правовые основы информационной безопасности.	
			2.2. Административный и процедурный уровни информационной безопасности.	
ПК-4	способность прогнозировать техногенные катастрофы и их последствия, планировать мероприятия по профилактике и ликвидации последствий экологических катастроф, принимать профилактические меры для снижения уровня опасностей различного вида и их последствий		2.3. Основные программно-технические меры.	
			2.4. Сервисы обеспечения информационной безопасности.	
		3. Построение и организация функционирования комплексных систем защиты информации	3.1. Построение комплексных систем защиты информации (КСЗИ).	
			3.2. Организация функционирования КСЗИ	

2. Вопросы к зачету

№ п/п	Компетенции		ВОПРОСЫ К ЗАЧЕТУ	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1.	ОПК-9	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**1.** Предмет и объект защиты информации.	**1.** Основные понятия и положения информационной безопасности
			2. Классификация угроз информационной безопасности.	
			3. Основные угрозы доступности, целостности и конфиденциальности информации.	
			4. Вредоносное программное обеспечение.	
			1. Законодательный уровень информационной безопасности. Место информационной безопасности в системе национальной безопасности.	**2.** Методы и средства защиты информации
			2. Компьютерные правонарушения. Юридическая ответственность за правонарушения в информационной сфере.	
			3. Стандарты и спецификации в области информационной безопасности.	

2.	ПК-4	способность прогнозировать техногенные катастрофы и их последствия, планировать мероприятия по профилактике и ликвидации последствий экологических катастроф, принимать профилактические меры для снижения уровня опасностей различного вида и их последствий	**4.** Административный уровень информационной безопасности.	
			5. Процедурный уровень информационной безопасности.	
			6. Основные понятия программно-технического уровня информационной безопасности.	
			7. Идентификация и аутентификация, управление доступом.	
			8. Протоколирование и аудит.	
			9. Криптографические методы защиты.	
			10. Методы защиты межсетевого обмена.	
			1. Построение комплексных систем защиты информации (КСЗИ).	**3.** Построение и организация функционирования комплексных систем защиты информации
			2. Организация функционирования КСЗИ	

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать: ОПК-9: – сущность и понятие информационной безопасности, характеристику ее составляющих; – основные методы и средства защиты информации; – технологию организации обеспечения информационной безопасности; ПК-4: – нормативно-правовую базу, регламентирующую основные положения в области информационной безопасности; **Уметь**: ОПК-9: – выбирать эффективные способы и средства защиты; ПК-4: – проводить анализ потенциально возможных угроз информации и информационным технологиям; **Владеть:** ОПК-9: – навыками работы с программными и техническими средствами защиты информации; ПК-4: – навыками использования в повседневной деятельности персональных средств защиты информации.	**зачтено**	Обучающийся демонстрирует твердое знание программного материала на достаточном уровне. Четко и последовательно излагает материал. Отдельные несущественные ошибки в ответе самостоятельно исправляет по требованию преподавателя.
	незачтено	Обучающийся демонстрирует отсутствие знания значительной части программного материала. При изложении материала допускает принципиальные ошибки.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Дисциплина «Основы информационной безопасности» направлена на формирование у обучающихся знаний и умений, которые образуют теоретический и практический фундамент в области основ информационной безопасности, навыков практического обеспечения защиты информации и безопасного использования информационно-телекоммуникационных систем.

Освоение дисциплины предусматривает следующие виды занятий и работ: лекции, практические занятия и самостоятельную работу обучающихся в объемах часов, соответствующих учебному плану направления.

Лекционные занятия проводятся в режиме презентаций с демонстрацией применения основного материала, излагаемого в теме. Это существенно улучшает динамику лекций. Обучающиеся заранее (на 1-2 лекции вперед) обеспечиваются раздаточным материалом в электронном виде (опорный конспект). Основное время лекции выделяется на пояснения, аналитические комментарии, рассмотрение примеров и особенностей применения излагаемых сведений в профессиональной деятельности обучающегося.

Практические занятия проводятся в компьютерном классе. Рекомендуется установка оригинальных программ на компьютеры обучающихся для программного и информационного обеспечения самостоятельной работы в домашних условиях. В этом случае во время аудиторных занятий основное внимание можно акцентировать на методике использования программ и анализе полученных результатов.

Система оценивания уровня освоения дисциплины предусматривает текущий и итоговый виды контроля.

Текущий контроль основан на проверке выполнения практических работ. При этом оценивается: правильность выполнения заданий, соблюдение требований к содержанию и оформлению отчетов, соблюдение сроков выполнения работ, уровень ответов при защите работ.

Основная цель текущего контроля – своевременная оценка успеваемости обучающихся, побуждающая их работать равномерно, исключая малые загрузки или перегрузки в течение семестра.

Итоговый контроль (промежуточная аттестация) по дисциплине – это проверка уровня учебных достижений обучающихся по всей дисциплине за семестр. Проводится в форме зачета (устного собеседования). Для оценивания знаний, умений, навыков используется ФОС по дисциплине, содержащий вопросы к зачету.

К зачету допускаются обучающиеся, которые выполнили, оформили и защитили все практические работы, предусмотренные рабочей программой дисциплины.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
«Основы информационной безопасности»

1. Цель и задачи дисциплины

Целью изучения дисциплины является формирование у обучающихся знаний и умений, которые образуют теоретический и практический фундамент в области основ информационной безопасности, навыков практического обеспечения защиты информации и безопасного использования информационно-телекоммуникационных систем.

Задачами изучения дисциплины являются: изучение организационно-правовых основ защиты информации в информационно-коммуникационных системах; ознакомление обучающихся с основными угрозами информационной безопасности и правилами их выявления; приобретении практических навыков применения современных средств и способов обеспечения информационной безопасности.

.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: лекции – 13 часов, практические занятия – 13 часов; самостоятельная работа обучающихся (всего) – 46 часов.

Общая трудоемкость дисциплины составляет 72 часа, 2 зачетных единицы.

2.2 Основные разделы дисциплины:

1 − Основные понятия и положения информационной безопасности.

2 − Методы и средства защиты информации.

3 − Построение и организация функционирования комплексных систем защиты информации.

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-9 – способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

– ПК-4 – способность прогнозировать техногенные катастрофы и их последствия, планировать мероприятия по профилактике и ликвидации последствий экологических катастроф, принимать профилактические меры для снижения уровня опасностей различного вида и их последствий.

4. Вид промежуточной аттестации: зачет.

Приложение 3

Протокол о дополнениях и изменениях в рабочей программе
на 20__-20__ учебный год

1. В рабочую программу по дисциплине вносятся следующие дополнения:
_____
_____

2. В рабочую программу по дисциплине вносятся следующие изменения:
_____
_____

Протокол заседания кафедры ИиПМ №____ от «___» _____ 20 __ __ г.,

И.о. заведующего кафедрой ИиПМ _____ А.С. Толстиков

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 05.03.06 Экология и природопользование от 11 августа 2016 г. № 998

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от 06.10.2016 г. № 684.

Программу составил:
Васильева Л.В., старший преподаватель кафедры ИиПМ _____

Рабочая программа рассмотрена и утверждена на заседании кафедры ИиПМ
от «___» _____ 201___ г., протокол № ____.

И.о. заведующего кафедрой ИиПМ _____ А.С. Толстиков

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой ЭБЖиХ _____ М.Р. Ерофеева

Директор библиотеки _____ Т.Ф. Сотник

Рабочая программа одобрена методической комиссией ЕНФ
от «___» _____ 201___ г., протокол №_____

Председатель методической комиссии ЕНФ _____ М.А. Варданян

СОГЛАСОВАНО:

Начальник
учебно-методического управления _____ Г.П. Нежевец

Регистрационный №_____