МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Базовая кафедра экономики и менеджмента

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Б1.В.ДВ.06.01

НАПРАВЛЕНИЕ ПОДГОТОВКИ

27.03.05 Инноватика

ПРОФИЛЬ ПОДГОТОВКИ
Управление инновациями

Программа прикладного 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 проектно-конструкторскому виду профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Цель изучения дисциплины – приобретение студентами теоретических знаний и практических навыков защиты информации, представленной в электронном виде, прежде всего средствами криптографии, типичными криптосистемами и другими методами, лежащими в ее основе, с целью обеспечения информационной безопасности инновационной деятельности.

Задачи дисциплины

– изложение системы основных концепций и понятий, используемых в современных технологиях информационной безопасности;

– описание основных подходов, принятых в сфере информационной безопасности;

– ознакомление с основными инструментальными средствами защиты информации;

– приобретение навыков работы с аппаратными средствами защиты информации;

– развитие логического мышления, навыков исследования явлений и процессов, связанных с предметной деятельностью;

– формирование навыков самостоятельной работы, организации исследовательской работы.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ОК-4	способность использовать основы правовых знаний в различных сферах жизнедеятельности	**знать:** - правовые и организационные основы комплексного обеспечения информационной безопасности; **уметь:** - использовать основы правовых знаний для разработки политики безопасности; **владеть:** - методами правового обеспечения безопасности информации.
ОПК-1	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:** - информационно-коммуникационные технологии и основные требования информационной безопасности; **уметь:** - решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности **владеть:** - навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1	2	3
ПК-13	Способность использовать информационные технологии и инструментальные средства при разработке проектов	**знать:** - информационные технологии и инструментальные средства при разработке инновационных проектов с учетом требований информационной безопасности; **уметь:** - использовать методы информационной безопасности информационных технологий при разработке инновационных проектов; **владеть:** - навыками применения информационных технологий и инструментальных средств при разработке инновационных проектов с учетом основных требований информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ.06.01 Информационная безопасность инновационной деятельности относится к элективной части.

Дисциплина базируется на знаниях, полученных при изучении таких учебных дисциплин, как: Б1.Б.12 Информатика, Б1.Б.13 Информационные технологии, Б1.В.ДВ.1.1 Правоведение, Б1.В.2 Технологии нововведений, Б1.В.9 Управление инновационной деятельностью.

Дисциплина представляет основу для изучения дисциплин: Б1.В.17 Управление интеллектуальной собственностью, Б1.В.13 Стратегический менеджмент в инновационных организациях.

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*							*Вид промежуточной аттестации*
			Всего часов	*Аудиторных часов*	*Лекции*	*Лабораторные работы*	*Практические занятия*	*Самостоятельная работа*	*Курсовая работа (проект), контрольная работа, реферат, РГР*	
Очная	4	7	72	34	17	-	17	38	-	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*
			7
I. Контактная работа обучающихся с преподавателем (всего)	34	10	34
Лекции (Лк)	17	4	17
Практические занятия (ПЗ)	17	6	17
Групповые (индивидуальные) консультации	+	-	+
II.Самостоятельная работа обучающихся (СР)	38	-	38
Подготовка к практическим занятиям	18	–	18
Подготовка к зачету в течение семестра	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

- для очной формы обучения:

№ темы	*Наименование темы дисциплины*	*Трудоемкость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)*		
			учебные занятия		*самостоятельная работа обучающихся*
			лекции	*практические занятия*	
1.	**Введение в информационную безопасность**	**10**	**2**	**2**	**6**
2.	**Правовое обеспечение информационной безопасности**	**12**	**4**	**2**	**6**
3.	**Организационное обеспечение информационной безопасности**	**18**	**2**	**4**	**12**
4.	**Средства и методы защиты информации**	**32**	**9**	**9**	**14**
	ИТОГО	**72**	**17**	**17**	**38**

4.2. Содержание дисциплины, структурированное по разделам и темам

№ темы	*Наименование темы*	*Содержание лекционных занятий*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**2**	**3**	**4**
1.	Введение в информационную безопасность	Информация, информационные потоки, информационная среда. Информационная безопасность, ее сущность, основные понятия, цели и роль. Принципы информационной безопасности. Природа и многофункциональность информационной безопасности. Информационная безопасность в инновационной деятельности. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Методы и средства обеспечения информационной безопасности организации.	Лекция беседа (2 часа)
2.	Правовое обеспечение информационной безопасности	Право в области обеспечения информационной безопасности. Информационная безопасность как объект права. Нормы и источники правового обеспечения информационной безопасности в инновационной деятельности. Структура правового регулирования информационной безопасности инновационной деятельности. Государственная политика в области информационной безопасности инновационной деятельности. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.	-
3.	Организационное обеспечение информационной безопасности	Системный подход к организации информационной безопасности. Состав и структура системы информационной безопасности. Принципы организации системы информационной безопасности. Факторы, влияющие на структуру и организацию системы информационной безопасности. Функции структурного подразделения, обеспечивающего информационную безопасность. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.	Лекция беседа (2 часа)
4.	Средства и методы защиты информации	Технические средства и методы защиты информации. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Программно-аппаратные средства и методы обеспечения информационной безопасности. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Криптографические методы защиты информации. Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.	-

4.3. Лабораторные работы

Учебным планом не предусмотрено.

4.4. Практические занятия

№ п/п	*Номер раздела дисциплины*	*Наименование практических занятий*	*Объем (час.)*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**1.**	Введение в информационную безопасность	**2**	Развивающий семинар (2 час.)
2	**2.**	Правовое обеспечение информационной безопасности	**2**	-
3	**3.**	Организационное обеспечение информационной безопасности	**4**	-
4	**4.**	Средства и методы защиты информации	**9**	Тренинг (4 часа)
		ИТОГО	**17**	**6**

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 тем дисциплины*	*Кол-во часов*	*Компетенции*			*Σ комп.*	$t_{ср}$, *час*	*Вид учебных занятий*	*Оценка результатов*
		ОК	*ОПК*	*ПК*				
		4	*1*	*13*				
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1. Введение в информационную безопасность	10	-	+	-	1	10	Лк, ПЗ, СР	тесты, зачет
2. Правовое обеспечение информационной безопасности	12	+	+	-	2	6	Лк, ПЗ, СР	тесты, зачет
3. Организационное обеспечение информационной безопасности	18	+	+	+	3	6	Лк, ПЗ, СР	тесты, зачет
4. Средства и методы защиты информации	32	-	+	+	2	16	Лк, ПЗ, СР	тесты, зачет
всего часов	**72**	**12**	**38**	**22**	**3**	**24**		

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

1. Иванов, М. Ю. Информационная безопасность: методические указания к выполнению лабораторных работ / М. Ю. Иванов. - Братск: БрГУ, 2014. - 44 с.

2. Баранова, Е. К. Криптографические методы защиты информации. Лабораторный практикум : учебное пособие для бакалавриата и магистратуры / Е. К. Баранова, А. В. Бабаш. - Москва : КноРус, 2017. - 200 с. + 1 эл. опт. диск.

3. Иванов, М. Ю. Защита информации и информационная безопасность в 2 ч. Ч.1-2 : методические указания к выполнению практических занятий / М. Ю. Иванов. - Братск : БрГУ, 2013 - . Ч.1. - 2013. - 23 с.

4. Иванов, М. Ю. Защита информации и информационная безопасность в 2 ч. Ч.1-2 : методические указания к выполнению практических занятий / М. Ю. Иванов. - Братск : БрГУ, 2013 - . Ч.2. - 2013. - 27 с.

5. Городов, О. А. Информационное право [Электронный ресурс] : учебник / О. А. Городов. - Москва : Кнорус, 2009. - 1 эл. опт. диск (CD-ROM).

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

№	*Наименование издания*	***Вид занятия*** (*Лк, ПЗ, СР*)	***Количество экземпляров в библиотеке,*** **шт.**	***Обеспеченность,*** **(экз./ чел.)**
1	**2**	**3**	**4**	**5**
	Основная литература			
1	Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд., перераб. и доп. - Москва : Форум; Инфра-М, 2014. - 432 с. - (Профессиональное образование).	Лк, ПЗ, СР	10	0,5
2	Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стереотип. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245	Лк, ПЗ, СР	1(ЭУ)	1
3	Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина ; Министерство образования и науки РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2017. - 86 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=467139	Лк, ПЗ, СР	1(ЭУ)	1
4	Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331	Лк, ПЗ, СР	1(ЭУ)	1

Дополнительная литература				
5	Галатенко, В.А. Стандарты информационной безопасности / В.А. Галатенко ; под ред. В.Б. Бетелина. - 2-е изд. - Москва : Интернет-Университет Информационных Технологий, 2006. - 264 с. - (Основы информационных технологий). - ISBN 5-9556-0053-1 ; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=233065	Лк, ПЗ, СР	1(ЭУ)	1
6	Иванов, М. Ю. Информационные технологии: методы криптографии : учебное пособие / М. Ю. Иванов. - Братск : БрГУ, 2010. - 100 с. - Б. ц.	Лк, ПЗ, СР	31	1
7	Краткий энциклопедический словарь по информационной безопасности : словарь / сост. В.Г. Дождиков, М.И. Салтан. - Москва : Энергия, 2010. - 240 с. - ISBN 978-5-98420-043-1; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=58393	Лк, ПЗ, СР	1(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. Электронно-библиотечная система «Издательство «Лань» http://e.lanbook.com .

5. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru .

6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru .

7. Университетская информационная система РОССИЯ (УИС РОССИЯ) https://uisrussia.msu.ru/ .

8. Национальная электронная библиотека НЭБ http://xn--90ax2c.xn--p1ai/how-to-search /.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

9.1. Методические указания для обучающихся по выполнению практических работ

Цель выполнения практических работ: выполнение практических заданий для приобретение теоретических знаний, умений и навыков в области информационной безопасности.

Порядок выполнения:

Изучить лекционный материал и источники, основную и дополнительную литературу по темам. Используя изученный материал, выполнить предложенные задания.

Форма отчетности:

Наличие выполненных заданий, оформленных в электронной форме.

Рекомендации по выполнению заданий и подготовке к практическому занятию

1. Подобрать источники по теме практического занятия.

2. Проработать основную и дополнительную литературу, термины, сведения, требующиеся для запоминания и являющиеся основополагающими в данной теме. Конспектирование прочитанных литературных источников.

3. Проработка материалов по изучаемому вопросу с использованием рекомендуемых библиотечных источников и ресурсов информационно-телекоммуникационной сети «Интернет».

4. На основании изученной литературы по теме выполнить задания для самостоятельной работы.

5. Ответить на контрольные вопросы для самопроверки.

Практическое занятие № 1. Тема: «Введение в информационную безопасность»

Задание 1: На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) написать эссе (не более 2 страниц) на тему « Принципы информационной безопасности».

Задание 2: На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) написать эссе (не более 2 страниц) на тему « Природа и многофункциональность информационной безопасности».

Задание 3: На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) написать эссе (не более 2 страниц) на тему «Модели информационной безопасности».

Развивающий семинар « Информационная безопасность, ее сущность, основные понятия, цели и роль»

Цель: обеспечить студентам возможность овладеть достаточными теоретическими знаниями в области информационной безопасности и применение полученных знаний на практике.

Порядок проведения.

Для проведения семинара студентам предлагается разделиться на 2 группы и подготовить по данной теме перечень вопросов для студентов противоположной группы. Для более интересного проведения данного семинара предлагается каждой группе студентов сделать свои вопросы и соответствующие ответы на карточках одинакового цвета. Перед началом семинара можно разместить данные карточки на специально выделенных для каждой группы столах. И провести что-то вроде лотереи, т.е. студент из противоположной группы выходит и вытягивает карточку команды «противника» если правильно отвечает, то данная команда зарабатывает балл, если нет, то берет карточку соответствующего цвета и зачитывает ответ. Балл уходит к другой команде. По окончании семинара подсчитываются баллы каждой команды, и та группа, у которой баллов больше поощряется отличными оценками.

Предлагаемые вопросы для обсуждения

1.Что такое информация, информационная среда, информационные потоки?

2. Какие виды информации используются в инновационном менеджменте?

3. С помощью каких терминов можно описать сущность информационной безопасности?

4. Что такое информационная безопасность?

5. Определите цели информационной безопасности.

6. Какова роль информационной безопасности?

Задания для самостоятельной работы:

Задание 1. На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) написать эссе (не более 2 страниц) на тему «Информационная безопасность в инновационной деятельности».

Задание 2. На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) составить таблицу «Методы и средства обеспечения информационной безопасности».

Практическое занятие № 2. Тема: «Правовое обеспечение информационной безопасности»

Задание 1: С использованием лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) составить схему, отражающую нормы права и их источники в области информационной безопасности.

Задание 2: На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) написать эссе (не более 2 страниц) на тему «Информационная безопасность как объект права».

Задание 3: Провести дискуссию по вопросу «Право в области обеспечения информационной безопасности» с помощью вопросов:

1. Что такое информационное право?
2. Назовите основные источники информационного права.
3. Назовите нормы права в области обеспечения информационной безопасности?
4. Дайте характеристику структуры правового регулирования информационной безопасности.
5. Какие направления включает государственная политика в области информационной безопасности инновационной деятельности»?

Задания для самостоятельной работы:

Задание 1: На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) написать эссе (не более 2 страниц) на тему «Основные нормативно-правовые акты в области информационной безопасности».

Задание 2: Дать подробную характеристику правовых особенностей обеспечения безопасности конфиденциальной информации и государственной тайны. Привести примеры их использования.

Практическое занятие № 3. Тема: «Организационное обеспечение информационной безопасности»

Задание 1: С использованием лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) составить схему, отражающую состав и структура системы информационной безопасности.

Задание 2: На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) написать эссе (не более 2 страниц) на тему «Системный подход к организации информационной безопасности».

Задание 3: Провести дискуссию по вопросу «Факторы, влияющие на структуру и организацию системы информационной безопасности» с помощью вопросов:

1. Представьте классификацию факторов внешней среды, влияющей на информационную безопасность.
2. Представьте классификацию факторов внутренней среды, влияющей на информационную безопасность
3. Какие организационные факторы, влияют на информационную безопасность?
4. Перечислите факторы, связанные с деятельностью персонала в области информационной безопасности.
5. Какие технические факторы влияют на информационную безопасность.

6. Как влияет режим функционирования предприятия на информационную безопасность?

7. Какие экономические факторы влияют на информационную безопасность?

Задания для самостоятельной работы:

Задание 1. С использованием лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) составить таблицу, отражающую основные стандарты в области обеспечения информационной безопасности и их характеристика.

Задание 2. Описать пример политики предприятия в области информационной безопасности

Задание 3. На основе изучения лекционного материала и другой учебно-методической литературы (учебников, учебных пособий и т.п.) написать эссе (не более 3 страницы) на тему «Функции структурного подразделения, обеспечивающего информационную безопасность».

Практическое занятие № 4. Тема: « Средства и методы защиты информации»

Тренинг« Средства и методы защиты информации»

На основании данных, выданных преподавателем, с использованием компьютерных технологий выполняются следующие задания.

Задание 1: *Использование криптографических средств защиты информации*

Содержание задания:

Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание с использованием программы TrueCrypt. Используется компьютерные технология.

Задание выполняется в 2 этапа:

1. Создание скрытого тома:
   Выбор контейнера TrueCrypt
   Выбор алгоритма шифрования
   Выбор размера контейнера
   Выбор пароля.
2. Создание зашифрованного флеш-накопителя:
   Зашифровать не системный раздел
   Выбор устройства шифрования
   Выбор алгоритма шифрования
   Процесс выполнения шифрования
   введения пароля

Задание 2*:* *Реализация работы инфраструктуры открытых ключей*

Содержание задания:

Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание с использованием СКЗИ «КриптоПро CSP». Используется компьютерная технология.

Задание выполняется в 3 этапа:

1. Настройка СКЗИ «КриптоПро CSP» версии 3.6

2. Генерация закрытого ключа электронной подписи и запроса на издание сертификата ключа проверки электронной подписи

3. Установка сертификатов в систему

Задание 3: *Средства стеганографии для защиты информации (3 часа)*

Содержание задания:

Использование средств стеганографии для защиты файлов.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Практическое задание с использованием компьютерной стеганографии для решения задач информационной безопасности.

Для проведения занятия применяются следующие программные продукты:

Наименование	**Возможности**	**Принцип работы**	**Преимущества**	**Недостатки**	**Операционная система**
1	**2**	**3**	**4**	**5**	**6**
OutGuess	Сокрытие данных в JPEG изображениях	Сокрытие данных в младших битах, отличных от нуля квантованных коэффициентов блоков изображения	Возможность контроля вносимых “статистических искажений”, большая стойкость к атакам	Нестойкость к атакам пассивных противников, возможность автоматического детектирования наличия скрытого сообщения	Написано для работы в UNIX-подобных операционных системах
JSTEG					Ориентировано на операционную систему MS-DOS
JPHS					
Gifshuffle	Сокрытие данных в графических файлах в формате GIF	Сокрытие информации посредством изменения порядка цветов в палитре	Возможность предварительного сжатия или шифрования скрываемого сообщения	Малый объем скрываемого сообщения, не зависящий от размера контейнера	Написано для работы в UNIX-подобных операционных системах.
Hide-and-Seek		Сокрытие информации путем замены младших битов цветовых индексов точек изображения	Использует алгоритм шифрования “Blowfish”, осуществляет случайный выбор точек хранения		Ориентировано на операционную систему MS-DOS.
Steganos	Сокрытие в графических файлах BMP, DIB,VOC, WAV, ASCII	Сокрытие информации путем замены младших битов элементов изображения	Заполнение неиспользованного пространства контейнера шумоподобным сигналом	Использование устаревших форматов контейнеров	Ориентировано на операционную систему MS-DOS и Windows
Steghide	Сокрытие данных в графических BMP- и звуковых WAV- и AU- файлах	Сокрытие информации путем замены младших бит элементов контейнера	Возможность предварительного шифрования скрываемого сообщения		Ориентировано на операционную систему MS-DOS
DC-Stegano	Сокрытие данных в графических файлах в формате PCX	Сокрытие посредством замены младших битов цветовых индексов точек изображения		Отсутствие стегоключа, строго заданный размер изображения-контейнера	

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

- Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
- Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 license No Level
- Антивирусное программное обеспечение Kaspersky Security.

• Adobe Reader
• doPDF;
• 7-Zip
• ИСС «Кодекс». Информационно-справочная система
• Справочно-правовая система «Консультант Плюс»

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

Вид занятия	***Наименование аудитории***	***Перечень основного оборудования***	***№ ЛР или ПЗ*** *(согласно р. 4.3,4.4 РПД)*
1	**2**	**3**	**4**
Лк	Лекционная аудитория (мультимедийный класс)	Персональный компьютер AMD FX-4100, интерактивная доска ActivBoard 595 Pro, интерактивный планшет Wacom PL-720, колонки акустические	
ПЗ	Дисплейный класс	Оборудование-10 шт. ПК P4-640 (монитор TFT 17 LG L1753S-SF); проектор EPSON Multi Media Projector EB-S62	ПЗ № 1-4
СР	Читальный зал №1	Оборудование 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	Тема	ФОС
ОК-4	способность использовать основы правовых знаний в различных сферах жизнедеятельности	**2.** Правовое обеспечение информационной безопасности **3.** Организационное обеспечение информационной безопасности	Тест Вопросы к зачету (6-15)
ОПК-1	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.** Введение в информационную безопасность **2.** Правовое обеспечение информационной безопасности **3.** Организационное обеспечение информационной безопасности **4.** Средства и методы защиты информации	Тест Вопросы к зачету (1-21)
ПК-13	способность использовать информационные технологии и инструментальные средства при разработке проектов	**3.** Организационное обеспечение информационной безопасности **4.** Средства и методы защиты информации	Тест Вопросы к зачету (11-21)

2. Вопросы к зачету

№ п/п	Компетенции		ВОПРОСЫ К ЗАЧЕТУ	№ и наименование темы
	Код	Определение		
1	2	3	4	5
1.	ОК-4	способность использовать основы правовых знаний в различных сферах жизнедеятельности	6. Право в области обеспечения информационной безопасности	**2.** Правовое обеспечение информационной безопасности **3.** Организационное обеспечение информационной безопасности
			7. Нормы и источники правового обеспечения информационной безопасности в инновационной деятельности	
			8. Структура правового регулирования информационной безопасности инновационной деятельности.	
			9. Основные нормативно-правовые акты в области информационной безопасности.	
			10. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны	
			11.Системный подход к организации информационной безопасности. Состав и структура системы информационной безопасности.	
			12.Принципы организации системы информационной безопасности.	
			13.Факторы, влияющие на структуру и организацию системы информационной безопасности.	
			14. Функции структурного подразделения, обеспечивающего информационную безопасность.	
			15. Основные стандарты в области обеспечения информационной безопасности.	

1	2	3	4	5
2.	ОПК-1	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. Информационная безопасность, ее сущность, основные понятия, цели и роль.	**1.** Введение в информационную безопасность **2.** Правовое обеспечение информационной безопасности **3.** Организационное обеспечение информационной безопасности **4.** Средства и методы защиты информации
			2. Принципы информационной безопасности.	
			3.Информационная безопасность в инновационной деятельности.	
			4.Модели информационной безопасности.	
			5.Методы и средства обеспечения информационной безопасности организации	
			6. Право в области обеспечения информационной безопасности	
			7. Нормы и источники правового обеспечения информационной безопасности в инновационной деятельности	
			8. Структура правового регулирования информационной безопасности инновационной деятельности.	
			9. Основные нормативно-правовые акты в области информационной безопасности.	
			10. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны	
			11.Системный подход к организации информационной безопасности. Состав и структура системы информационной безопасности.	
			12.Принципы организации системы информационной безопасности.	
			13.Факторы, влияющие на структуру и организацию системы информационной безопасности.	
			14.Функции структурного подразделения, обеспечивающего информационную безопасность.	
			15.Основные стандарты в области обеспечения информационной безопасности.	
			16.Технические средства и методы защиты информации.	
			17.Программно-аппаратные средства и методы обеспечения информационной безопасности.	
			18.Основные виды сетевых и компьютерных угроз, средства и методы защиты.	
			19.Симметричные и ассиметричные системы шифрования.	
			20.Цифровые подписи (Электронные подписи).	
			21.Криптографические протоколы.	
3.	ПК-13	способность использовать информационные технологии и инструментальные средства при разработке проектов	11.Системный подход к организации информационной безопасности. Состав и структура системы информационной безопасности.	**3.** Организационное обеспечение информационной безопасности **4.** Средства и методы защиты информации
			12.Принципы организации системы информационной безопасности.	
			13.Факторы, влияющие на структуру и организацию системы информационной безопасности.	
			14.Функции структурного подразделения, обеспечивающего информационную безопасность.	
			15.Основные стандарты в области обеспечения информационной безопасности.	
			16.Технические средства и методы защиты информации.	
			17.Программно-аппаратные средства и методы обеспечения информационной безопасности.	
			18.Основные виды сетевых и компьютерных угроз, средства и методы защиты.	
			19.Симметричные и ассиметричные системы шифрования.	
			21.Криптографические протоколы.	

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать (ОК-4): - правовые и организационные основы комплексного обеспечения информационной безопасности; (ОПК-1): - информационно-коммуникационные технологии и основные требования информационной безопасности; (ПК-13): - информационные технологии и инструментальные средства при разработке инновационных проектов с учетом требований информационной безопасности **;** **Уметь** (ОК-4): - использовать основы правовых знаний для разрабоки политики безопасности; (ОПК-1): - решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности (ПК-13): - использовать методы информационной безопасности информационных технологий при разработке инновационных проектов; **Владеть** (ОК-4): - методами правового обеспечения безопасности информации; (ОПК-1): - навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; (ПК-13): - навыками применения информационных технологий и инструментальных средств при разработке инновационных проектов с учетом основных требований информационной безопасности.	**зачтено**	Оценка «зачтено» ставится при: - *всестороннем систематическом знании:* - правовых и организационных основ комплексного обеспечения информационной безопасности; - информационно-коммуникационные технологии и основные требования информационной безопасности; - информационные технологии и инструментальные средства при разработке инновационных проектов с учетом требований информационной безопасности - *умении:* - использовать основы правовых знаний для разработки политики безопасности; - решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности - использовать методы информационной безопасности информационных технологий при разработке инновационных проектов; - *владении:* - методами правового обеспечения безопасности информации; - навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; - навыками применения информационных технологий и инструментальных средств при разработке инновационных проектов с учетом основных требований информационной безопасности.
	не зачтено	Оценка «не зачтено» ставится при: - *отсутствии знаний:* - правовых и организационных основ комплексного обеспечения информационной безопасности; - информационно-коммуникационные технологии и основные требования информационной безопасности; - информационные технологии и инструментальные средства при разработке инновационных проектов с учетом требований информационной безопасности - *неумении:* - использовать основы правовых знаний для разработки политики безопасности; - решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности - использовать методы информационной безопасности информационных технологий при разработке инновационных проектов; - *неудовлетворительном владении:* - методами правового обеспечения безопасности информации; - навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; - навыками применения информационных технологий и инструментальных средств при разработке инновационных проектов с учетом основных требований информационной безопасности.

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

Текущая самостоятельная работа по курсу «Информационная безопасность инновационной деятельности» направлена на углубление и закрепление знаний, на развитие практических умений и включает такие виды работ, как:

- работа с лекционным материалом;
- работа с рекомендованной литературой при подготовке к практическим занятиям;
- подготовка к зачету.

Лекционные занятия желательно проводить в режиме презентаций с демонстрацией применения основного материала, излагаемого в теме. Это существенно улучшает динамику лекций.

Целесообразно обеспечивать студентов на 1-2 лекции вперед раздаточным материалом в электронном виде (сложные схемы, графики, аналитические исследования и опорный конспект). Основное время лекции лучше тратить на подробные аналитические комментарии и особенности применения рассматриваемого материала в профессиональной деятельности студента.

Практические занятия следует проводить в компьютерном классе либо в аудитории с мультимедийным оборудованием, используя оригинальную методику и профессиональные программы. Можно рекомендовать установку оригинальных программ на ПК студентов и выполнять ряд задач дома. В этом случае в классе основное внимание концентрируется на методике использования названных программ и анализе полученных результатов.

Текущий контроль (ТК) - это проверка знаний студентов по разделу программы. Формы: Опрос по теории согласно списку вопросов для самостоятельной оценки усвоения материала.

Цель ТК: побудить студентов отчитаться за усвоение раздела дисциплины накопительным образом, т.е. сначала за первый, затем за второй, затем за третий разделы и т.д. В конечном итоге многие студенты могут получить итоговые оценки по дисциплине «автоматом».

Промежуточная аттестация по дисциплине (ПА) - это проверка уровня учебных достижений студентов по всей дисциплине за семестр. Форма ПА: зачет. Цель промежуточной аттестации: проверка базовых знаний дисциплины, полученных при изучении модуля, достаточных для последующего обучения.

Самостоятельную работу необходимо начинать с проработки конспекта лекций, обобщения, систематизации, углубления и конкретизации полученных теоретических знаний с использованием основной и дополнительной литературы, а также рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет».

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и Интернете.

В процессе консультации с преподавателем обучающийся может уточнить отдельные положения по изучаемым вопросам по дисциплине.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Информационная безопасность инновационной деятельности

1. Цель и задачи дисциплины

Цель изучения дисциплины – приобретение студентами теоретических знаний и практических навыков защиты информации, представленной в электронном виде, прежде всего средствами криптографии, типичными криптосистемами и другими методами, лежащими в ее основе, с целью обеспечения информационной безопасности инновационной деятельности.

Задачи изучения дисциплины

– изложение системы основных концепций и понятий, используемых в современных технологиях информационной безопасности;

– описание основных подходов, принятых в сфере информационной безопасности;

– ознакомление с основными инструментальными средствами защиты информации;

– приобретение навыков работы с аппаратными средствами защиты информации;

– развитие логического мышления, навыков исследования явлений и процессов, связанных с предметной деятельностью;

– формирование навыков самостоятельной работы, организации исследовательской работы.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: лекции – 17 часов, практические занятия – 17 часа, самостоятельная работа – 38 часа.

Общая трудоемкость дисциплины составляет 72 часа, 2 зачетных единицы

2.2 Основные разделы дисциплины:

1. Введение в информационную безопасность
2. Правовое обеспечение информационной безопасности
3. Организационное обеспечение информационной безопасности
4. Средства и методы защиты информации

Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОК-4: способность использовать основы правовых знаний в различных сферах жизнедеятельности

ОПК-1: 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-13: способность использовать информационные технологии и инструментальные средства при разработке проектов

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 №____ от «___» _____ 20 ____ г.,
(разработчик)

Заведующий кафедрой _____ _____
(подпись) *(Ф.И.О.)*

Приложение 4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Тема	ФОС
ОК-4	способность использовать основы правовых знаний в различных сферах жизнедеятельности	**1.** Введение в информационную безопасность **2.** Правовое обеспечение информационной безопасности **3.** Организационное обеспечение информационной безопасности **4.** Средства и методы защиты информации	*Тест*
ОПК-1	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		*Тест*
ПК-13	способность использовать информационные технологии и инструментальные средства при разработке проектов		*Тест*

2. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать (ОК-4): - правовые и организационные основы комплексного обеспечения информационной безопасности; (ОПК-1): - информационно-коммуникационные технологии и основные требования информационной безопасности; (ПК-13): - информационные технологии и инструментальные средства при разработке инновационных проектов с учетом требований информационной безопасности; **Уметь** (ОК-4): - использовать основы правовых знаний для разработки политики безопасности; (ОПК-1): - решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности (ПК-13): - использовать методы информационной безопасности информационных технологий при разработке инновационных проектов; **Владеть** (ОК-4): - методами правового обеспечения безопасности информации; (ОПК-1): - навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; (ПК-13): - навыками применения информационных технологий и инструментальных средств при разработке инновационных проектов с учетом основных требований информационной безопасности.	**зачтено**	Правильные ответы на зачетный тест составляют 80 % и более от общего числа заданий в тесте.
	не зачтено	Правильные ответы на зачетный тест не превышают 79 % от общего числа заданий в тесте.

3. Фонд тестовых заданий

1. Какие законы существуют в России в области компьютерного права?
Выберите несколько из 6 вариантов ответа:
1) О государственной тайне
2) об авторском праве и смежных правах
3) о гражданском долге
4) о правовой охране программ для ЭВМ и БД
5) о правовой ответственности
6) об информации, информатизации, защищенности информации

2. Какие существуют основные уровни обеспечения защиты информации?
Выберите несколько из 7 вариантов ответа:
1) законодательный
2) административный
3) программно-технический
4) физический
5) вероятностный
6) процедурный
7) распределительный

3. Физические средства защиты информации
Выберите один из 4 вариантов ответа:
1) средства, которые реализуются в виде автономных устройств и систем
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
3) это программы, предназначенные для выполнения функций, связанных с защитой информации
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

4. В чем заключается основная причина потерь информации, связанной с ПК?
Выберите один из 3 вариантов ответа:
1) с глобальным хищением информации
2) с появлением интернета
3) с недостаточной образованностью в области безопасности

5. Технические средства защиты информации
Выберите один из 4 вариантов ответа:
1) средства, которые реализуются в виде автономных устройств и систем
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
3) это программы, предназначенные для выполнения функций, связанных с защитой информации
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

6. К аспектам ИБ относятся
Выберите несколько из 5 вариантов ответа:
1) дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность

7. Что такое криптология?
Выберите один из 3 вариантов ответа:
1) защищенная информация
2) область доступной информации
3) тайная область связи

8. Что такое несанкционированный доступ (НСД)?
Выберите один из 5 вариантов ответа:
1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2) Создание резервных копий в организации
3) Правила и положения, выработанные в организации для обхода парольной защиты
4) Вход в систему без согласования с руководителем организации
5) Удаление не нужной информации

9. Что является основой для формирования государственной политики в сфере информации? (Ответьте 1 словом)

10. Что такое целостность информации?
Выберите один из 4 вариантов ответа:
1) Свойство информации, заключающееся в возможности ее изменения любым субъектом
2) Свойство информации, заключающееся в возможности изменения только единственным пользователем
3) Свойство информации, заключающееся в ее существовании в виде единого набора файлов
4) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

11. Кто является знаковой фигурой в сфере информационной безопасности
Выберите один из 4 вариантов ответа:
1) Митник
2) Шеннон
3) Паскаль
4) Беббидж

12. В чем состоит задача криптографа?
Выберите один из 2 вариантов ответа:
1) взломать систему защиты
2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

13. Под ИБ понимают
Выберите один из 3 вариантов ответа:
1) защиту от несанкционированного доступа
2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера
3) защиту информации от компьютерных вирусов

14. Что такое аутентификация?
Выберите один из 5 вариантов ответа:
1) Проверка количества переданной и принятой информации
2) Нахождение файлов, которые изменены в информационной системе несанкционированно
3) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

4) Определение файлов, из которых удалена служебная информация
5) Определение файлов, из которых удалена служебная информация

15. "Маскарад"- это
Выберите один из 2 вариантов ответа:
1) осуществление специально разработанными программами перехвата имени и пароля
2) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями

16. Верификация -
Выберите один из 3 вариантов ответа:
1) это проверка принадлежности субъекту доступа предъявленного им идентификатора.
2) проверка целостности и подлинности инф, программы, документа
3) это присвоение имени субъекту или объекту

17. Кодирование информации -
Выберите один из 2 вариантов ответа:
1) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.
2) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

18. Утечка информации
Выберите один из 3 вариантов ответа:
1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
2) ознакомление постороннего лица с содержанием секретной информации
3) потеря, хищение, разрушение или неполучение переданных данных

19. Под изоляцией и разделением (требование к обеспечению ИБ) понимают
Выберите один из 2 вариантов ответа:
1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)
2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

20. К аспектам ИБ относятся
Выберите несколько из 5 вариантов ответа:
1) дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность

21. Линейное шифрование –
Выберите один из 3 вариантов ответа:
1) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
3) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами

22. Прочность защиты в АС
Выберите один из 3 вариантов ответа:
1) вероятность не преодоления защиты нарушителем за установленный промежуток времени
2) способность системы защиты информации обеспечить достаточный уровень своей безопасности
3) группа показателей защиты, соответствующая определенному классу защиты

23. Уровень секретности - это
Выберите один из 2 вариантов ответа:
1) ответственность за модификацию и НСД информации
2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

24. Угроза – это
Выберите один из 2 вариантов ответа:
1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов
2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

25. Под ИБ понимают
Выберите один из 3 вариантов ответа:
1) защиту от несанкционированного доступа
2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера
3) защиту информации от компьютерных вирусов

26. Что такое криптография?
Выберите один из 3 вариантов ответа:
1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
2) область доступной информации
3) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом

27. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется
Выберите один из 4 вариантов ответа:
1) кодируемой
2) шифруемой
3) недостоверной
4) защищаемой

28. Продолжите фразу: "Административная и законодательная мера, соответствующая мере ответственности лица за потерю конкретной секретной информации, регламентирующаяся специальным документом с учетом государственных и военно-стратегических, коммерческих или частных интересов - это..."
Запишите ответ:
_____

29. Продолжите фразу: " Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой - это..."
Запишите ответ:
_____

30. Способ представления информации в вычислительных системах
Запишите ответ:
_____

31. Вставьте пропущенное слово:
Информация может быть защищена без аппаратных и программных средств защиты с помощью _____ преобразований.
Запишите ответ:
_____

32. Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это
Выберите один из 4 вариантов ответа:
1) текст
2) данные
3) информация
4) пароль

33. Какие атаки предпринимают хакеры на программном уровне?
Выберите несколько из 4 вариантов ответа:
1) атаки на уровне ОС
2) атаки на уровне сетевого ПО
3) атаки на уровне пакетов прикладных программ
4) атаки на уровне СУБД

34. Организационные угрозы подразделяются на
Выберите несколько из 4 вариантов ответа:
1) угрозы воздействия на персонал
2) физические угрозы
3) действия персонала
4) несанкционированный доступ

35. Виды технической разведки (по месту размещения аппаратуры)
Выберите несколько из 7 вариантов ответа:
1) космическая
2) оптическая
3) наземная
4) фотографическая
5) морская
6) воздушная
7) магнитометрическая

36. Основные группы технических средств ведения разведки
Выберите несколько из 5 вариантов ответа:
1) радиомикрофоны
2) фотоаппараты
3) электронные "уши"
4) дистанционное прослушивание разговоров

5) системы определения местоположения контролируемого объекта

37. Разновидности угроз безопасности
Выберите несколько из 6 вариантов ответа:
1) техническая разведка
2) программные
3) программно-математические
4) организационные
5) технические
6) физические

38. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется
Выберите один из 4 вариантов ответа:
1) угрозой;
2) опасностью;
3) намерением;
4) предостережением.

39. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?
Запишите ответ:
_____

40. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?
Выберите один из 4 вариантов ответа:
1) операционной системы, сетевого программного обеспечения
2) операционной системы, сетевого программного обеспечения и системы управления базами данных;
3) операционной системы, системы управления базами данных;
4) сетевого программного обеспечения и системы управления базами данных.

41. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется
Выберите один из 4 вариантов ответа:
1) системой угроз;
2) системой защиты;
3) системой безопасности;
4) системой уничтожения.

42. К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?
Запишите ответ:
_____

43. К видам защиты информации относятся:
Выберите несколько из 4 вариантов ответа:
1) правовые и законодательные:
2) морально-этические;
3) юридические;
4) административно-организационные;

44. Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации называется
Запишите ответ:
_____

45. К методам защиты от НСД относятся
Выберите несколько из 5 вариантов ответа:
1) разделение доступа;
2) разграничение доступа;
3) увеличение доступа;
4) ограничение доступа.
5) аутентификация и идентификация

46. Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы
Запишите ответ:
_____

47. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется
Выберите один из 4 вариантов ответа:
1) политикой информации
2) защитой информации
3) политикой безопасности
4) организацией безопасности

48. Выделите группы, на которые делятся средства защиты информации:
Выберите один из 3 вариантов ответа:
1) физические, аппаратные, программные, криптографические, комбинированные;
2) химические, аппаратные, программные, криптографические, комбинированные;
3) физические, аппаратные, программные, этнографические, комбинированные;

49. Техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации- все это есть
Запишите ответ:
_____

50. Что такое компьютерный вирус?
Выберите один из 4 вариантов ответа:
1) Разновидность программ, которые способны к размножению
2) Разновидность программ, которые самоуничтожаются
3) Разновидность программ, которые не работают
4) Разновидность программ, которые плохо работают

51. Как подразделяются вирусы в зависимости от деструктивных возможностей?
Выберите один из 4 вариантов ответа:
1) Сетевые, файловые, загрузочные, комбинированные
2) Безвредные, неопасные, опасные, очень опасные
3) Резидентные, нерезидентные

4) Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

52. Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется
Запишите ответ:
_____

53. Установите соответствие
Укажите соответствие для всех 4 вариантов ответа:
1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей
4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии
__ защита информации от утечки по акустическому каналу
__ Защита информации от утечки по визуально-оптическому каналу
__ Защита информации от утечки по электромагнитным каналам
__ Защита информации от утечки по материально-вещественному каналу

54. Надежным средством отвода наведенных сигналов на землю служит
Запишите ответ:
_____

55. Установите соответствие
Укажите соответствие для всех 2 вариантов ответа:
1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи
2) наука скрывающая содержимое секретного сообщения
__ стеганография
__ криптография

Верные ответы:
1) (1 б.) Верные ответы: 1; 2; 4; 6;
2) (1 б.) Верные ответы: 1; 2; 3; 6;
3) (1 б.) Верные ответы: 1;
4) (1 б.) Верные ответы: 3;
5) (1 б.) Верные ответы: 4;
6) (1 б.) Верные ответы: 2; 3; 5;
7) (1 б.) Верные ответы: 3;
8) (1 б.) Верные ответы: 1;
9) (1 б.) Верный ответ: "доктрина".
10) (1 б.) Верные ответы: 4;
11) (1 б.) Верные ответы: 1;
12) (1 б.) Верные ответы: 2;
13) (1 б.) Верные ответы: 2;

14) (1 б.) Верные ответы: 3;
15) (1 б.) Верные ответы: 2;
16) (1 б.) Верные ответы: 2;
17) (1 б.) Верные ответы: 1;
18) (1 б.) Верные ответы: 2;
19) (1 б.) Верные ответы: 2;
20) (1 б.) Верные ответы: 2; 3; 5;
21) (1 б.) Верные ответы: 2;
22) (1 б.) Верные ответы: 1;
23) (1 б.) Верные ответы: 2;
24) (1 б.) Верные ответы: 1;
25) (1 б.) Верные ответы: 2;
26) (1 б.) Верные ответы: 1;
27) (1 б.) Верные ответы: 4;
28) (1 б.) Верный ответ: "уровень секретности".
29) (1 б.) Верный ответ: "пароль".
30) (1 б.) Верный ответ: "двоичный код".
31) (1 б.) Верный ответ: "криптографических".
32) (1 б.) Верные ответы: 3;
33) (1 б.) Верные ответы: 1; 2; 4;
34) (1 б.) Верные ответы: 1; 3;
35) (1 б.) Верные ответы: 1; 3; 5; 6;
36) (1 б.) Верные ответы: 1; 3; 5;
37) (1 б.) Верные ответы: 1; 3; 4;
38) (1 б.) Верные ответы: 1;
39) (1 б.) Верный ответ: "Техническая".
40) (1 б.) Верные ответы: 2;
41) (1 б.) Верные ответы: 2;
42) (1 б.) Верный ответ: "организационного".
43) (1 б.) Верные ответы: 1; 2; 4;
44) (1 б.) Верный ответ: "несанкционированным доступом".
45) (1 б.) Верные ответы: 1; 2; 4; 5;
46) (1 б.) Верный ответ: "аутентификации".
47) (1 б.) Верные ответы: 3;
48) (1 б.) Верные ответы: 1;
49) (1 б.) Верный ответ: "средство защиты информации".
50) (1 б.) Верные ответы: 1;
51) (1 б.) Верные ответы: 2;
52) (1 б.) Верный ответ: "каналом утечки информации".
53) (1 б.) Верные ответы:
3;
4;
1;
2;
54) (1 б.) Верный ответ: "заземление".
55) (1 б.) Верные ответы:
1;
2.

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 27.03.05 Инноватика от «11» августа 2016 г. № 1006

для набора 2015 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «03» июля 2018 г. № 413;

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» октября 2016 г. № 684;

для набора 2017 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» марта 2017 г. № 125.

Программу составил:

Кобзов А.Ю., доцент базовой кафедры ЭиМ _____

Рабочая программа рассмотрена и утверждена на заседании базовой кафедры ЭиМ

от «20» __декабря___ 2018 г., протокол № 8

Заведующий базовой кафедрой ЭиМ _____ М.И.Черутова

СОГЛАСОВАНО:

Заведующий выпускающей базовой кафедрой ЭиМ _____ М.И.Черутова

Директор библиотеки _____ Т.Ф.Сотник

Рабочая программа одобрена методической комиссией факультета ЭиУ

от «28» __декабря_____ 2018 г., протокол № 4

Председатель методической комиссии факультета ЭиУ _____ Е.В.Трапезникова

СОГЛАСОВАНО:

Начальник
учебно-методического управления _____ Г.П.Нежевец

Регистрационный №_____