МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
Р.Ю. Демина
«08» июня 2023 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой
информационной безопасности ИБ
Р.Ю. Демина
от «08» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование)

Составитель(-и)	**Гурская Т.Г., к.т.н., доцент кафедры ИБ**
Направление подготовки / специальность	**10.03.01 Информационная безопасность**
Направленность (профиль) ОПОП	**Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий)**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приема	**2023**
Курс	**3**
Семестр	**5**

Астрахань – 2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целью освоения дисциплины (модуля) «Гуманитарные аспекты информационной безопасности» является формирование у обучаемого базовых знаний в области информационной безопасности и мотивировки к действиям в условиях информационного противоборства.

1.2. Задачи освоения дисциплины (модуля):

- формирование знаний, связанных с обеспечением информационно-психологической безопасности личности, общества и государства;
- рассмотрение основных видов информационно-психологических воздействий деструктивного характера, понятия манипулирования как средства скрытого управления личностью и обществом;
- изучение особенностей реализации информационных воздействий деструктивного характера в различных коммуникативных ситуациях, в том числе в сети Интернет;
- формирование умений применять простейшие способы обеспечения собственной информационно-психологической безопасности в различных коммуникативных ситуациях, в том числе при работе в сети Интернет.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина «Гуманитарные аспекты информационной безопасности» относится к обязательной (базовой) части учебного плана направления подготовки 10.03.01 Информационная безопасность 2023 года набора.

Изучение курса «Гуманитарные аспекты информационной безопасности» рассчитано на 1 семестр (5 семестр) и предусматривает сдачу студентами зачета.

Общая трудоемкость дисциплины – 108 часов/ 3 ЗЕ.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами:

1. Основы информационной безопасности

Знания: концептуальные основы информационной безопасности, основные положения, подходы и методы ее обеспечения, понимание того, что информационная безопасность является важнейшей частью обеспечения безопасности государства, предприятия, гражданина, основы комплексного обеспечения информационной безопасности, основы организационно-правовой защиты информации.

Умения: изучение и анализ опыта работы других специалистов, организаций и предприятий в области повышения эффективности защиты информации.

Навыки: сбор, изучение научно-технической информации, отечественного и зарубежного опыта специалистов в области информационной безопасности.

2. Организационное и правовое обеспечение информационной безопасности

Знания: основы права в области информационной безопасности и защиты информации

Умения: самостоятельно использовать знания правовых основ в области организационно-правового обеспечения информационной безопасности объекта защиты;

Навыки: анализ нормативно-правовой базы в области информационной безопасности.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

1. Основы управленческой деятельности
2. Основы управления информационной безопасностью
3. Информационные технологии в управлении проектами

4. Управление персоналом при обеспечении информационной безопасности
5. Организация и управление службой информационной безопасности
6. Анализ и оценка рисков

Также дисциплина «Гуманитарные аспекты информационной безопасности» поможет студентам при реализации задач производственной, преддипломной практик и написанию бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

общепрофессиональных (ОПК): ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ИОПК-13.1. Знать: основные этапы и закономерности исторического развития России.	ИОПК-13.2. Уметь: анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории.	ИОПК-13.3. Владеть: навыками формирования гражданской позиции и развития патриотизма

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) 3 з.е., 108 часов, 54 часа выделено на контактную работу обучающихся с преподавателем (лекции – 18, лабораторные работы – 36), 54 часов– на самостоятельную работу обучающихся.

Таблица 2 - Структура и содержание дисциплины (модуля)

№ п/п	Наименование раздела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной
				Л	ПЗ	ЛР	КР	СР	

									аттестации *(по семестрам)*
1	Гуманитарная сущность информационной безопасности	5	1-2	2		4	-	9	Устный опрос Вводное тестирование Лабораторная работа 1
2	Нормативные документы в области информационной безопасности		3-5	2		8	-	9	Устный опрос Практическая работа 1, кейс, Письменная работа 1
3	Компьютерные правонарушения		6	2		4	-	9	Устный опрос Ситуационные задачи
4	Информационный суверенитет государств		7-9	2		4	-	9	Устный опрос Коллоквиум
5	Компьютерная этика и интеллектуальная собственность		10-12	4		8	-	9	Устный опрос Защита реферата
6	Обеспечение информационно-психологической безопасности личности и общества		13-18	6		8	-	9	Устный опрос Тестирование №2
ИТОГО				**18**		**36**		**54**	**ЗАЧЕТ**

Примечание: Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; КР – курсовая работа; СР – самостоятельная работа.

Таблица 3 – Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Раздел, тема дисциплины (модуля	Кол-во часов	Код компетенции	общее количество компетенций
		ОПК 13	
Гуманитарная сущность информационной безопасности	15	+	1
Нормативные документы в области информационной безопасности	19	+	1
Компьютерные правонарушения	15	+	1
Информационный суверенитет государств	15	+	1
Компьютерная этика и интеллектуальная собственность	21	+	1

Обеспечение информационно-психологической безопасности личности и общества	23	+	1

Краткое содержание каждой темы дисциплины (модуля)

Модуль 1. Гуманитарная сущность информационной безопасности

Тема 1. Проблемы реализации гуманитарной сущности информационной безопасности

Предмет и задачи курса. Становление и развитие гуманитарной сущности ИБ как научной дисциплины. Соотношение понятий «гуманитарный» и «безопасность». Источники для изучения курса. Взгляд на гуманитарные науки, начиная с мыслителей Древней Греции и заканчивая современностью.

Определение понятия «безопасность». Три группы определений данного понятия.

Основополагающие принципы обеспечения безопасности, в том числе информационной. Теоретические и методологические основы безопасности.

Гуманитарная сущность информации. Функциональная концепция информации. Классификация информации. Научно-технический прогресс и роль информации.

Тема 2. Место и роль проблем информационной безопасности в становлении современного информационного общества

Структура преобразования гуманитарного знания в области информационной безопасности.

Институционализация информационной безопасности – формирование системы специализированных учреждений, служб, подразделений в составе различных организаций, фирм и ведомств.

Профессионализация информационной безопасности – формирование профессионального сообщества и системы профессиональных коммуникаций кадров, определение основных каналов миграции специалистов из смежных отраслей, выработка основных квалификационных требований к профессии, поиска решений в области профессионального образования.

Технологизация информационной безопасности – формирование технологий и методов деятельности.

Социализация информационной безопасности – становление и признание значимости отрасли в глазах общественности (формирование высокого социального статуса), появление ученых, публицистов, которые путем пропаганды и популяризации доносят до внимания общественности актуальность вопросов отрасли.

Модуль 2. Законодательство в области информационной безопасности

Тема 3. Нормативные документы в области информационной безопасности

Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г.

ГОСТ Р 6.30-2003. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов

Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ В. В. Путиным 2016 г.

Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: 1992.

Федеральный закон «Об электронной подписи» от 06 апреля 2011 г. № 63-ФЗ (в ред. Федеральных законов от 01.07.2011 № 169-ФЗ, от 10.07.2012 № 108-ФЗ, от 05.04.2013 № 60-ФЗ, от 02.07.2013 № 171-ФЗ).

Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ (в ред. Федеральных законов от 02.02.2006 № 19-ФЗ, от 18.12.2006 № 231-ФЗ, от 24.07.2007 № 214-ФЗ, от 11.07.2011 № 200-ФЗ).

Федеральный закон «О государственной тайне» от 21 июля 1993 г. № 5485-1 (в ред. Федеральных законов от 06.10.1997 № 131-ФЗ, от 30.06.2003 № 86-ФЗ, от 11.11.2003 № 153-ФЗ, от 29.06.2004 № 58-ФЗ, от 22.08.2004 № 122-ФЗ, от 01.12.2007 № 294-ФЗ, от 01.12.2007 № 318-ФЗ, от 18.07.2009 № 180-ФЗ, от 15.11.2010 № 99-ФЗ, от 18.07.2011 № 242-ФЗ, от 19.07.2011 № 248-ФЗ, от 08.11.2011 № 309-ФЗ, с изм., внесенными Постановлением Конституционного Суда РФ от 27.03.1996 № 8-П, определениями Конституционного Суда РФ от 10.11.2002 № 293-О, от 10.11.2002 № 314-О).

Федеральный закон «О лицензировании отдельных видов деятельности» от 04 мая 2011 г. № 99-ФЗ.

Федеральный закон «О техническом регулировании» от 27 декабря 2002 № 184-ФЗ.

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», Госстандарт России.

ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью», Госстандарт России.

Тема 4. Структура и задачи органов, обеспечивающих информационную безопасность.

Анализ деятельности государственных органов законодательной и исполнительной власти, определяющих и ведущих политику Российской Федерации в области информационной безопасности.

Комитет Государственной думы по безопасности.

Совет безопасности России

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

Федеральная служба безопасности Российской Федерации (ФСБ России)

Федеральная служба охраны Российской Федерации (ФСО России) и Служба специальной связи и информации ("Спецсвязь России")

Служба внешней разведки Российской Федерации (СВР России)

Министерство обороны Российской Федерации (Минобороны России)

Министерство внутренних дел Российской Федерации (МВД России)

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Центральный банк Российской Федерации (Банк России)

Модуль 3. Компьютерные преступления

Тема 5. Виды компьютерных правонарушений

Понятия «преступление» и «правонарушение». Классификация противозаконных действий в области информационных технологий. Криминологические группы общественно-опасных деяний в информационной сфере, предусмотренные Уголовным кодексом. Характерные особенности компьютерного преступления. Характеристики субъектов компьютерных преступлений. Международное сотрудничество в сфере борьбы с компьютерными преступлениями.

Модуль 4. Информационный суверенитет государств

Тема 6. Информационный суверенитет как элемент государственного суверенитета. Информационная политика государств.

Понятие и принципы «информационно-психологической войны». Традиционный суверенитет государства. Концепция суверенитета. Составляющие информационного

суверенитета. Медийная инфраструктура для обеспечения информационного суверенитета. Электронный щит. Пути реализации информационной войны в современном мире.

Модуль 5. Компьютерная этика и интеллектуальная собственность

Тема 7. Информационная этика

Информационная этика. Этапы развития этики. Основные проблемы информационной этики. Требования, предъявляемые специалисту в области информационной безопасности с этической точки зрения.

Тема 8. Интеллектуальная собственность.

Понятие интеллектуальной собственности и правовой охраны результатов интеллектуальной деятельности. Понятие патент, полезная модель, промышленный образец. Нюансы оформления исключительных прав. Федеральный институт промышленной собственности. Гражданский кодекс как основной нормативно-правовой акт в области защиты авторских прав.

Модуль 6. Обеспечение информационно-психологической безопасности личности и общества

Тема 9. Угрозы информационно-психологической безопасности личности и их основные источники.

Безопасность личности как важный аспект деятельности государства. Основные источники угроз информационно-психологической безопасности личности. Манипулятивные возможности масс-медиа. Способы нейтрализующего воздействия на деструктивные угрозы.

Тема 10. Психологический портрет личности

Психологический портрет личности с точки зрения информационной безопасности. Способы и методы выявления психологических свойств личности. Социальная инженерия.

Тема 11. Психология манипуляций и способы обеспечения информационной безопасности личности

Методы профайлинга и социальной инженерии. Методы определения инсайдерских атак в организации или коллективе с помощью методов профайлинга.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным и практическим занятиям необходимо воспользоваться учебно-методической литературой из п.8. Лекции необходимо проводить с использованием презентаций, созданных в прикладном пакете Microsoft Office PowerPoint.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой (основной и дополнительной) и информационно-справочными ресурсами из п.8.

Тестирование допускается проводить в бумажном или электронном виде на специализированных образовательных площадках (Moodle, Master-Test).

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Таблица 4 – Содержание самостоятельной работы обучающихся

№ раз-дела	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
1	Классификация информации	9	Внеаудиторная, изучение учебных пособий
2	Терминологический словарь рл документу «Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»	9	Внеаудиторная, изучение учебных пособий
3	Криминологические группы общественно-опасных деяний в информационной сфере, предусмотренные Уголовным кодексом (анализ статей УК РФ)	9	Внеаудиторная, изучение учебных пособий
4	Понятие «информационной войны». Пути реализации информационной войны в современном мире	9	Внеаудиторная, изучение учебных пособий
5	Понятие интеллектуальной собственности и правовой охраны результатов интеллектуальной деятельности (по ГК РФ)	9	Внеаудиторная, изучение учебных пособий
6	Социальная инженерия	9	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно.

Примерные темы рефератов

1. Эволюция, этапы развития компьютерной этики.
2. Основные проблемы компьютерной этики.
3. Влияние информационных технологий на обращение с персональными данными.
4. Международные нормы приватности граждан.
5. Правовые гарантии приватности граждан в России.
6. Анонимность в сети Интернет с точки зрения этики. Проблемы и критика.
7. Противоправные действия в сети Интернет: обзор, примеры.
8. Сетевой этикет (нетикет).
9. Серьезные нарушения сетевого этикета (вымогательство, обман, подделка и т.д.)
10. Проблемы собственности на программное обеспечение
11. Последствия миграции интеллектуальной собственности в Интернет.
12. Проблемы плагиата в Сети и нарушения авторского права разработчиками веб-сайтов
13. Право на доступ к компьютерным ресурсам. Важность доступа к компьютерным ресурсам.
14. Кодексы профессиональной этики в области компьютерных технологий в России и за рубежом.
15. Проблема правовой охраны нетрадиционных объектов авторского права.

Правила оформления текста пояснительной записки реферата

На титульном листе прописываются: название университета, факультета, кафедры, название дисциплины, темы реферата, Ф.И.О. студента, номер группы, Ф.И.О. преподавателя и оставляется место для проставления оценки и подписи преподавателя . Внизу пишется город и год написания.

Текстовая часть

Изложение текста и оформление работы следует выполнять в соответствии с требованиями.

Текст ПЗ оформляется на одной стороне листа формата А4.

Основной текст набирается шрифтом *Times New Roman 12,* с выравниванием *по ширине*, абзацный отступ должен быть одинаковым по всему тексту и равен *1,25 см*; строки разделяются *полуторным интервалом*.

Поля страницы: верхнее -2,5см, нижнее – 2,5 см, левое – 3,5 см, правое – 1,0 см.

Структурные элементы пояснительной записки **СОДЕРЖАНИЕ, ВВЕДЕНИЕ, ЗАКЛЮЧЕНИЕ, СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ, ПРИЛОЖЕНИЕ** должны начинаться с нового листа.

Их заголовки оформляются ***прописными буквами, шрифтом 14 Ж***, располагаются *в середине строки без точки в конце*. Дополнительный *интервал после* заголовка - 12 *пт*.

Основную часть работы разделяют на разделы, подразделы и, при необходимости, на пункты.

Каждый раздел необходимо начинать с нового листа. Разделы нумеруют арабскими цифрами в пределах всего текста. После номера и в конце заголовка раздела *точка не ставится*.

Если заголовок состоит из двух предложений, их разделяют точкой. *Переносы слов в заголовках не допускаются.*

Заголовки разделов оформляются ***с прописной буквы, шрифтом 14 Ж,*** с абзацного отступа *1,25* см. Дополнительный *интервал после заголовка - 6 пт.*

(Если заголовок раздела занимает две и большее число строк, то интервал между этими строками – *полуторным*).

Подразделы нумеруются в пределах каждого раздела. Номер подраздела состоит из номера раздела и порядкового номера подраздела, разделенных точкой. После номера подраздела точку не ставят.

Заголовки подразделов печатаются с абзацного отступа, ***с прописной буквы шрифтом 12 Ж,*** без точки в конце заголовка.

Дополнительный *интервал перед* заголовком подраздела – *6 пт*, *после* заголовка - 6 *пт*.

Пункты нумеруются в пределах каждого подраздела. Номер пункта состоит из номеров раздела, подраздела и пункта, разделенных точкой. После номера пункта точку не ставят.

Нельзя писать заголовок в конце страницы, если на ней не умещаются, по крайней мере, две строки текста, идущего за заголовком.

Пример оформления заголовков текста:

1 Разработка аппаратных средств

1.1
1.2
1.3

Нумерация пунктов первого раздела отчета

2 Технические характеристики

2.1
2.2
2.3

Нумерация пунктов второго раздела отчета

В пояснительной записке после титульного листа помещается лист **СОДЕРЖАНИЕ**, в котором указываются номера и наименования разделов, подразделов и приложений ТД с указанием номеров страниц, где они начинаются.

Разделы, подразделы записываются в содержании в точном соответствии с их наименованиями без сокращений *строчными буквами кроме первой прописной.*

Перечисления

В тексте пояснительной записки перечисления производятся с абзацного отступа, каждое с новой строки с *дефисом***.**

Примеры написания:

- текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
- приложения;
- перечень терминов;
- перечень сокращений;
- перечень литературы.

При необходимости ссылки в тексте отчета на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

При необходимости дальнейшей детализации перечислений используются арабские цифры и строчные буквы русского алфавита, после которых ставятся скобки:

а)…;

б)…;

1)…;

2)…;

в).

Примеры написания:

1) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
2) приложения;
3) перечень терминов;
4) перечень сокращений;
5) перечень литературы.

Примеры написания:

а) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);

б) приложения;

в) перечень терминов;

г) перечень сокращений;
д) перечень литературы.

Сокращения слов

Сокращение слов в тексте, как правило, не допускается. Исключение составляют сокращения, общепринятые в русском языке: т. е. (то есть), и т. п. (и тому подобное), и т. д. (и так далее), и др. (и другие).

При необходимости применения специфических терминов или сокращений нужно дать их разъяснение при первом упоминании. Например «…создание систем автоматического проектирования (САПР)». В последующем тексте принятые сокращения пишутся без скобок.

Формулы

Составной частью текста пояснительной записки являются математические формулы и соотношения. Формулы создаются в редакторе формул.

Формулы располагают в середине строки и выделяют из текста свободными строками.

Пример оформления расчетов:

Количество населения в заданном пункте и подчиненных окрестностях с учетом среднего прироста населения определяется по формуле (3.1):

$$H_t = H_0 \left(1 + \frac{\Delta H}{100}\right)^t, \qquad ((3.1)$$

где H_0 – число жителей на время проведения переписи населения, тыс. чел.;

ΔH – средний годовой прирост населения в данной местности, % (принимается 2…3%);

t – период, определяемый как разность между назначенным годом перспективного проектирования и годом проведения переписи населения, год.

$$H_t = 32{,}6\left(1 + \frac{2}{100}\right)^8 = 38{,}2 \text{ тыс. чел.}$$

Расшифровка формулы, при необходимости, приводится непосредственно под формулой. В конце формулы ставится запятая, пояснение значений символов дают с новой строки в той последовательности, в какой они приведены в формуле.

Формулы нумеруются в пределах раздела. Номер формулы состоит из номера раздела и порядкового номера формулы в этом разделе. Номер формулы в круглых скобках помещается в крайнем правом положении на строке.

Ссылка в тексте на формулу: «…в формуле (3.1)».

Таблицы

Цифровой материал оформляется в виде таблиц. Таблицу следует располагать непосредственно после ссылки на нее.

Размеры таблиц выбираются произвольно, в зависимости от представляемого материала. Высота строк таблицы должна быть не менее 8 мм

Таблица 2.1 – Наименование таблицы

Заголовки граф

Подзаголовки граф

Строки

					(горизонтальные ряды)

Заголовки граф и строк таблицы должны начинаться с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком. Если подзаголовки граф имеют самостоятельное значение, то их начинают с прописной буквы.

Заголовки указывают в единственном числе. В конце заголовков и подзаголовков таблицы точки не ставят.

Разделять заголовки боковика и граф диагональными линиями не допускается. Графу «Номер по порядку» в таблицу включать не допускается.

Таблицы нумеруются в пределах раздела. Номер таблицы состоит из номера раздела и порядкового номера таблицы в этом разделе. Номер и наименование таблицы следует помещать над таблицей слева через тире.

Пример оформления таблицы:

Таблица 3.1– Длина участков трассы

Протяженность участка проектируемой трассы, км	Тип кабеля
0,084	ДПС-04-24А06-7,0
0,167	ДПС-04-24А06-7,0
0,301	ДПС-04-24А06-7,0
0,779	ДПС-04-24А06-7,0
Общая длина кабеля: 1,331 км	ДПС-04-24А06-7,0

Таблицу с большим числом строк допускается переносить на другой лист. При этом в первой части таблицы нижнюю горизонтальную линию не проводят. Над второй частью слева пишут: «Продолжение Таблицы 2.1».

Продолжение Таблицы 2.1

Дата	Наименование	Стоимость

Рисунки

Графический материал располагают, возможно, ближе к тексту, в котором о нём упоминается.

Все рисунки нумеруются в пределах раздела и должны иметь наименование, Номер рисунка и его наименование располагают под рисунком следующим образом:

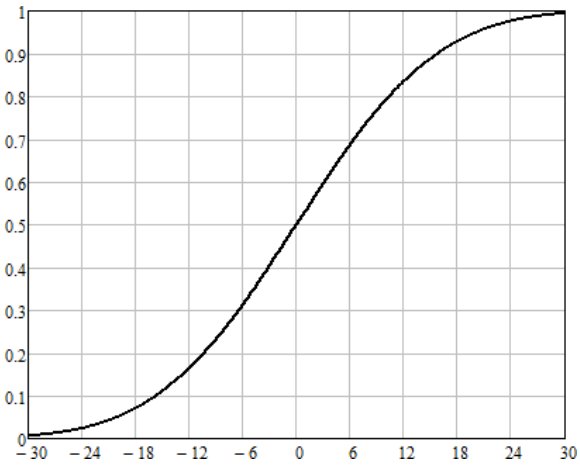


Рисунок 2.12 – Кривая коэффициента восприятия речи

Ссылка в тексте на рисунок: «…в соответствии с рисунком 4.3».
Если в разделе ВВЕДЕНИЕ есть рисунки, то они нумеруются как :
Рисунок В.1 – Название рисунка

Список использованных источников

Список использованных источников приводится в конце пояснительной записки. Список использованных учебников, справочников, статей, стандартов и др. следует располагать в порядке появления ссылок на источники в тексте работы и нумеровать арабскими цифрами без точки, печатать с абзацного отступа.

Список литературы должен быть составлен в алфавитном порядке. Список адресов серверов Internet указывается после литературных источников. При указании веб-адреса рекомендуется давать заголовок данного ресурса (заголовок веб-страницы).

При составлении списка литературы в алфавитном порядке следует придерживаться следующих правил:

1) законодательные акты и постановления правительства РФ;

2) специальная научная литература;

3) методические, справочные и нормативные материалы, статьи периодической печати.

Для многотиражной литературы при составлении списка указываются: полное название источника, фамилия и инициалы автора, издательство и год выпуска (для статьи – название издания и его номер). Полное название литературного источника приводится в начале книги на 2-3 странице.

Для законодательных актов необходимо указывать их полное название, принявший орган и дату принятия.

При указании адресов серверов Internet сначала указывается название организации, которой принадлежит сервер, а затем его полный адрес.

Примеры записей:

1 Глухов В. А. Исследование, разработка и построение системы электронной доставки документов в библиотеке: Автореф. дис. канд. техн. наук. – Новосибирск, 2000. – 18 с.

2 Экономика и политика России и государств ближнего зарубежья : аналит. обзор, апр. 2007, Рос. акад. наук, Ин-т мировой экономики и муждунар. отношений. – М. : ИМЭМО, 2007. – 39 с.

3 Фенухин В. И. Этнополитические конфликты в современной России: на примере Северо-Кавказкого региона : дис. … канд. полит. наук. – М., 2002. – с. 54–55.

4 Официальные периодические издания : электронный путеводитель / Рос. нац. б-ка, Центр правовой информации. [СПб], 200520076. URL: http://www.nlr.ru/lawcrnter/izd/index.html (дата обращения: 18.01.2007).

5 Логинова Л. Г. Сущность результата дополнительного образования детей // Образование: исследовано в мире: междунар. науч. пед. интернет-журн. 21.10.03. URL: http://www.oim.ru/reader.asp?nomer=366 (дата обращения: 17.04.07).

6 Рынок тренингов Новосибирска: своя игра [Электронный ресурс]. – Режим доступа: http://nsk.adme.ru/news/2006/07/03/2121.html (дата обращения: 17.10.08).

Оформление приложений

Нумерация приложений осуществляется русскими буквами, кроме букв Ё, Й, Ъ, Ь, Ы, О. В разделе СОДЕРЖАНИЕ название приложения оформляется следующим образом:

ПРИЛОЖЕНИЕ А – Диаграмма классов

В самом приложении слово **ПРИЛОЖЕНИЕ А** пишется жирным шрифтом по центру, на следующей строке пишется название приложения, по центру жирным шрифтом, например,

ПРИЛОЖЕНИЕ А
Диаграмма классов

Если приложение продолжается на следующей странице, то необходимо сверху по центру, нежирным шрифтом написать слова:

Продолжение Приложения А

Если в приложении, например, в приложении А есть таблицы, то они нумеруются как:

Таблица А.1– Название таблицы

Если в приложении есть рисунки, например, в приложении А, то они нумеруются как:

Рисунок А.1 – Название рисунка

Критерии оценки реферата:

– оценка «отлично» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент представил реферат в соответствии с методическими указаниями, информация в реферате сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не представил реферат или выполнил ее неверно, без использования методических указаний, обоснования неверные, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

Требования к оформлению презентации для защиты реферата

Выбрать одну из предложенных тем и подготовить презентацию.

Презентация включает в себя 15-20 слайдов (1 слайд — титульный (название темы, кто выполнил: №гр, ФИО), последний слайд — список литературы, ссылки на электронные ресурсы (не менее трех источников)).

Слайды должны быть пронумерованы (титульный слайд не нумеруется). Презентация должна включать в себя не только текст, но и картинки, схемы, таблицы с индивидуальным форматированием, диаграммы с данными и т.д, и соответствовать всем требованиям, предъявляемым к её оформлению.

Требования к оформлению презентации

В оформлении презентаций выделяют два блока правил, описывающих:

1) Представление информации
2) Оформление слайдов

Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к организации и оформлению данных блоков.

Презентация предполагает сочетание информации различных типов: текста, графических изображений, анимации и видеофрагментов. Поэтому необходимо учитывать специфику комбинирования фрагментов информации различных типов. Кроме того, оформление и демонстрация каждого из перечисленных типов информации также подчиняется определенным правилам. Так, например, для текстовой информации важен выбор шрифта, для графической — яркость и насыщенность цвета, для наилучшего их совместного восприятия необходимо оптимальное взаиморасположение на слайде.

Представление информации

Объем и форма представления информации:

- Рекомендуется сжатый, информационный способ изложения материала.
- Не стоит заполнять один слайд слишком большим объемом информации: человек в среднем может единовременно запомнить не более трех фактов, выводов, определений.
- Один слайд презентации в среднем рассчитывается на 0,5-1 минуту выступления.
- Для достижения наибольшей эффективности ключевые пункты отображаются по одному на каждом отдельном слайде.
- Желательно присутствие на слайде блоков с разнотипной информацией (текст, графики, диаграммы, таблицы, рисунки), дополняющей друг друга.
- Заголовки должны быть краткими и привлекать внимание аудитории.
- В текстовых блоках необходимо использовать короткие слова и предложения.
- Рекомендуется минимизировать количество предлогов, наречий, прилагательных.
- В таблицах рекомендуется использовать минимум строк и столбцов.
- Вся вербальная информация должна тщательно проверяться на отсутствие орфографических, грамматических и стилистических ошибок.
- При проектировании характера и последовательности предъявления материала должен соблюдаться принцип стадийности: информация может разделяться в пространстве (одновременное отображение в разных зонах одного слайда) или во времени (размещение информации на последовательно демонстрируемых слайдах).

Расположение информационных блоков на слайде

- Структура слайда должна быть одинаковой на всей презентации.

• Логика предъявления информации на слайдах и в презентации должна соответствовать логике ее изложения.

• Наиболее важная информация должна располагаться в центре экрана.

• Информационных блоков на слайде не должно быть слишком много (оптимально 3, максимум 5).

• Рекомендуется объединение семантически связанных информационных элементов в целостно воспринимающиеся группы;

• Рекомендуемый размер одного информационного блока — не более 1/2 размера слайда;

• Информационные блоки рекомендуется располагать горизонтально, связанные по смыслу блоки — слева направо.

• Поясняющая надпись должна располагаться под рисунком (фотографией, диаграммой, схемой).

Способы и правила выделения информации

Все информационные элементы (текст, изображения, диаграммы, элементы схем, таблицы) должны ясно и рельефно выделяться на фоне слайда, для этого используются:

• рамки, прорисовка границ (для оформления изображений, таблиц);

• тени (для отделения контура текста и объектов от фона);

• заливка, штриховка (для дизайна основ информационных блоков);

• стрелки (для оформления схем и логических блоков).

Ключевые слова в информационном блоке необходимо выделить (цветом, подчеркиванием, полужирным и курсивным начертанием, размером шрифта). Для иллюстрации наиболее важных фактов используются рисунки, диаграммы, схемы.

Единый стиль презентации

Вся презентация должна должны быть выдержана в едином стиле, на базе одного шаблона. Стиль включает в себя:

• общую схему шаблона: способ размещения информационных блоков;

• общую цветовую схему дизайна слайда;

• цвет фона или фоновый рисунок, декоративный элемент небольшого размера и др.;

• параметры шрифтов (гарнитура, цвет, размер) и их оформления (эффекты), используемых для различных типов текстовой информации (заголовки, основной текст, выделенный текст, гиперссылки, списки, подписи);

• способы оформления иллюстраций, схем, диаграмм, таблиц и др.

Необходимо обеспечить унификацию структуры и формы представления материала. Цветовая схема должна быть одинаковой на всех слайдах. Это создает у слушателей ощущение связности, преемственности, стильности, комфортности.

В стилевом оформлении презентации не рекомендуется использовать более 3 основных цветов и более 3 типов шрифта. Следует избегать излишне пёстрых стилей — оформление слайда не должно отвлекать внимание слушателей от содержательной части доносимой информации. При выборе элементов стиля (цветовых соотношений, размера текста, иллюстраций, таблиц) рекомендуется проводить проверку шаблона презентации на удобство чтения с экрана компьютера.

Правила использования цвета

Одним из основных компонентов дизайна презентации является учет физиологических особенностей восприятия цветов человеком. К наиболее значимым из них относят:

• стимулирующие (теплые) цвета способствуют возбуждению и действуют как раздражители (в порядке убывания интенсивности воздействия): красный, оранжевый, желтый;

• дезинтегрирующие (холодные) цвета успокаивают, вызывают сонное состояние (в том же порядке): фиолетовый, синий, голубой, сине-зеленый; зеленый;

• нейтральные цвета: светло-розовый, серо-голубой, желто-зеленый, коричневый;

• сочетание двух цветов — цвета знака и цвета фона — существенно влияет на зрительный комфорт, причем некоторые пары цветов не только утомляют зрение, но и могут привести к стрессу (например, зеленые буквы на красном фоне);

• наиболее хорошо воспринимаемые сочетания цветов шрифта и фона: белый на темно-синем, лимонно-желтый на пурпурном, черный на белом, желтый на синем.

Можно сформулировать следующие рекомендации по использованию цвета в презентации:

На одном слайде рекомендуется использовать не более трех базовых цветов: один для фона, один для заголовка, один для текста.

Составление цветовой схемы презентации начинается с выбора:

• трех базовых цветов: фона — текста — заголовка;

• трех главных функциональных цветов, которые используются для представления обычного текста, гиперссылок и посещенных ссылок.

Для фона и текста необходимо использовать контрастные цвета: текст должен хорошо читаться, но не резать глаза. Следует обратить внимание на цвет гиперссылок (до и после использования): их цвет должен заметно отличаться от цвета текста, но не контрастировать с ним.

Правила использования фона

• Фон является элементом заднего (второго) плана, должен выделять, оттенять, подчеркивать информацию, находящуюся на слайде, но не заслонять ее.

• Легкие пастельные тона лучше подходят для фона, чем белый цвет.

• Для фона предпочтительны холодные тона.

• Вместо того, чтобы использовать сплошной цвет лучше выбрать плавный градиентный переход гармонично сочетающихся цветов, мягкую (неконтрастную) текстуру или нейтральный фон.

• Любой активный фоновый рисунок повышает утомляемость глаз обучаемого и снижает эффективность восприятия материала.

• При планировании дизайна слайда следует всячески избегать проецирования текстовых блоков на области фона, содержащие изображения и декоративные элементы.

Правила использования текстовой информации

Не рекомендуется:

• перегружать слайд текстовой информацией;

• использовать блоки сплошного текста;

• в нумерованных и маркированных списках использовать уровень вложения глубже двух;

• использовать переносы слов;

• использовать наклонное и вертикальное расположение подписей и текстовых блоков;

• текст слайда не должен повторять текст, который преподаватель произносит вслух (зрители прочитают его быстрее, чем расскажет преподаватель, и потеряют интерес к его словам).

Рекомендуется:

• сжатость и краткость изложения, максимальная информативность текста: короткие тезисы, даты, имена, термины — главные моменты опорного конспекта;

• использование коротких слов и предложений, минимум предлогов, наречий, прилагательных;

• использование нумерованных и маркированных списков вместо сплошного текста;

• использование табличного (матричного) формата предъявления материала, который позволяет представить материал в компактной форме и наглядно показать связи между различными понятиями;

• выполнение общих правил оформления текста;

- тщательное выравнивание текста, буквиц, маркеров списков;
- горизонтальное расположение текстовой информации, в т.ч. и в таблицах;
- каждому положению, идее должен быть отведен отдельный абзац текста;
- основную идею абзаца располагать в самом начале — в первой строке абзаца (это связано с тем, что лучше всего запоминаются первая и последняя мысли абзаца);
- идеально, если на слайде только заголовок, изображение (фотография, рисунок, диаграмма, схема, таблица и т.п.) и подпись к ней.

Правила использования шрифтов

При выборе шрифтов для представления вербальной информации презентации следует учитывать следующие правила:

- Не рекомендуется смешивать разные типы шрифтов в одной презентации.
- Учитывая, что гладкие (плакатные) шрифты, т.е. шрифты без засечек (типа Arial, Tahoma, Verdana и т.п.) легче читать с большого расстояния, чем шрифты с засечками (типа Times), то:
- для основного текста предпочтительно использовать плакатные шрифты;
- для заголовка можно использовать декоративный шрифт, если он хорошо читаем и не контрастирует с основным шрифтом.
- Текст должен быть читабельным (его должно быть легко прочитать с самого дальнего места).
- Рекомендуемые размеры шрифтов:
- для заголовков — не менее 32 пунктов и не более 50, оптимально — 36 пункта;
- для основного текста — не менее 18 пунктов и не более 32, оптимально — 24 пункта;
- Не следует злоупотреблять прописными буквами (они читаются хуже строчных), поэтому их допустимо использовать только для смыслового выделения небольших фрагментов текста.
- Наиболее важный материал, требующий обязательного усвоения, желательно выделить ярче для включения ассоциативной зрительной памяти.
- Для выделения информации следует использовать цвет, жирный и/или курсивный шрифт.
- Выделение подчеркиванием обычно ассоциируется с гиперссылкой, поэтому использовать его для иных целей не рекомендуется.

Правила использования графической информации

Динамика взаимоотношений визуальных и вербальных элементов и их количество определяются функциональной направленностью учебного материала. Изображение информативнее, нагляднее, оно легче запоминается, чем текст. Поэтому, если можно заменить текст информативной иллюстрацией, то лучше это сделать.

При использовании графики в презентации следует выполнять следующие правила и рекомендации, обусловленные законами восприятия человеком зрительной информации:

- Графика (рисунки, фотографии, диаграммы, схемы) должна органично дополнять текстовую информацию или передавать ее в более наглядном виде.
- Каждое изображение должно нести смысл: желательно избегать в презентации рисунков, не несущих смысловой нагрузки, если они не являются частью стилевого оформления.
- Цвет графических изображений не должен резко контрастировать с общим стилевым оформлением слайда.
- Необходимо использовать изображения только хорошего качества. Для этого все изображения, помещаемые в презентацию, должны быть предварительно подготовлены в графическом редакторе.

Недопустимо:

- искажение пропорций;
- нарушение тонового и цветового баланса фотоизображений;

- использование изображений с пониженной резкостью;
- видимость пикселей на изображении;
- использование необработанных сканированных изображений; например — изображений с "грязным"(серым, желтым) фоном вместо белого, неконтрастных, размытых и т.п.
- При подготовке в графическом редакторе изображения для помещения его на слайд презентации важное значение имеет выбор для него оптимального размера и разрешения:
- Выбор размера изображения (в пикселах) осуществляется в графическом редакторе. Изображение уменьшается (ни в коем случае НЕ увеличивается!) до нужного размера относительно экрана (либо до немного большего, чем нужный, но не более чем в 1.5—2 раза, чтобы более точно отрегулировать его размер уже на слайде путем уменьшения масштаба от 100%).
- При масштабировании помещенного на слайд изображения его масштаб допустимо только уменьшать (от исходных 100%), и крайне нежелательно увеличивать масштаб свыше 100%, так как при этом теряется его качество — на слайде оно будет выглядеть размытым. Если на слайде в масштабе 100% изображение оказалось слишком маленьким, то его необходимо заново подготовить в графическом редакторе из исходного оригинала большого размера.
- Если презентацию предполагается демонстрировать на экране с большим разрешением, чем на том компьютере, на котором она создается (или если презентация предназначена еще и для распечатки), то при данном рабочем разрешении рекомендуется использовать соответственно большие размеры всех изображений, которые после помещения на слайд соответственно масштабируются (уменьшаются).
- Вместе с тем, не рекомендуется перегружать презентацию неоправданно большими размерами файлов изображений. Использование большого числа "тяжелых" файлов перегружает презентацию, что может привести к замедлению ее работы.
- Иллюстрации рекомендуется сопровождать пояснительным текстом, пояснительная надпись преимущественно располагается под рисунком.
- Изображения лучше помещать левее текста: поскольку мы читаем слева-на-право, то взгляд зрителя вначале обращается на левую сторону слайда.
- Сложный рисунок или схему следует выводить постепенно.
- Необходимо четко указать все связи в схемах и диаграммах.

Анимационные эффекты

Возможности анимации позволяют акцентировать внимание учащихся на наиболее важных моментах урока, позволяют понять логику построения логических цепочек, схем, таблиц.

Рекомендуется использовать возможности компьютерной анимации для представления информации на слайде. Однако не стоит чрезмерно насыщать презентацию такими эффектами, иначе это вызовет негативную реакцию аудитории.

- Анимация должна быть сдержанна, хорошо продумана и допустима:
- для демонстрации динамичных процессов;
- для привлечения внимания слушателей и создания определенной атмосферы презентации.
- Не стоит злоупотреблять различными анимационными эффектами, они не должны отвлекать внимание от содержания информации на слайде.
- Анимация не должна быть слишком активной. Особенно нежелательные такие эффекты, как вылет, вращение, волна, побуквенное появление текста и т.д. В учебных презентациях для детей и подростков такие эффекты, как движущиеся строки по горизонтали и вертикали, запрещены нормативными документами.
- Большое влияние на подсознание человека оказывает мультипликация. Ее воздействие гораздо сильнее, чем действие обычного видео. Четкие, яркие, быстро

сменяющиеся картинки легко "впечатываются" в подсознание. Причем, чем короче воздействие, тем оно сильнее.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Гуманитарная сущность информационной безопасности	Обзорная лекция	Фронтальный опрос	Устный опрос. Вводное тестирование, выполнение лабораторной работы
Нормативные документы в области информационной безопасности	Лекция - презентация	Фронтальный опрос. Решение кейсов	Устный опрос. выполнение письменной, практической работы 1, кейса
Компьютерные правонарушения	Лекция - презентация	Фронтальный опрос	Устный опрос. Решение ситуационных задач
Информационный суверенитет государств	Обзорная лекция	Тематические дискуссии	Устный опрос Коллоквиум
Компьютерная этика и интеллектуальная собственность	Лекция - презентация	Фронтальный опрос	Устный опрос Защита реферата
Обеспечение информационно-психологической безопасности личности и общества	Лекция - презентация	Фронтальный опрос	Устный опрос Тестирование №2

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

6.2. Информационные технологии

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Цифровое обучение») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Гуманитарные аспекты информационной безопасности» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной

программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие изучаемых разделов, результатов обучения и оценочных средств

№ п/п	Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1	Гуманитарная сущность информационной безопасности	ОПК-13	Вопросы для обсуждения. Вводное тестирование Лабораторная работа 1
2	Нормативные документы в области информационной безопасности	ОПК-13	Вопросы для обсуждения. Практическая работа 1, кейс, Письменная работа 1
3	Компьютерные правонарушения	ОПК-13	Вопросы для обсуждения. Ситуационные задачи
4	Информационный суверенитет государств	ОПК-13	Вопросы для обсуждения. Коллоквиум
5	Компьютерная этика и интеллектуальная собственность	ОПК-13	Вопросы для обсуждения. Защита реферата
6	Обеспечение информационно-психологической безопасности личности и общества	ОПК-13	Вопросы для обсуждения. Тестирование №2

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания,

	умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетво рительно»	не способен правильно выполнить задание

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	2	3	4
1	Ситуационные задачи	Совместная деятельность группы обучающихся и преподавателя под управлением преподавателя с целью решения учебных и профессионально-ориентированных задач путем моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема), концепция, роли и ожидаемый результат по каждой игре
2	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект контрольных заданий по вариантам
3	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов
4	Лабораторная работа	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может выполняться в индивидуальном порядке или группой обучающихся.	Задания для лабораторных работ
5	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий

6	Коллоквиум	Промежуточный зачет, имеющий целью уменьшить список тем, выносимых на основной зачет, и оценить текущий уровень знаний студентов.	Перечень вопросов к коллоквиуму

7.3. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

Образцы оценочных средств представляются в виде контрольных вопросов, заданий, комплексных заданий, образцов тестов для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины, а также для контроля самостоятельной работы обучающегося по отдельным разделам дисциплины.

Модуль № 1: Гуманитарная сущность информационной безопасности

1. Вопросы для обсуждения

Предмет и задачи курса. Становление и развитие гуманитарной сущности ИБ как научной дисциплины. Соотношение понятий «гуманитарный» и «безопасность». Источники для изучения курса. Взгляд на гуманитарные науки, начиная с мыслителей Древней Греции и заканчивая современностью.

Определение понятия «безопасность». Три группы определений данного понятия.

Основополагающие принципы обеспечения безопасности, в том числе информационной. Теоретические и методологические основы безопасности.

Гуманитарная сущность информации. Функциональная концепция информации. Классификация информации. Научно-технический прогресс и роль информации.

Структура преобразования гуманитарного знания в области информационной безопасности.

Институционализация информационной безопасности – формирование системы специализированных учреждений, служб, подразделений в составе различных организаций, фирм и ведомств.

Профессионализация информационной безопасности – формирование профессионального сообщества и системы профессиональных коммуникаций кадров, определение основных каналов миграции специалистов из смежных отраслей, выработка основных квалификационных требований к профессии, поиска решений в области профессионального образования.

Технологизация информационной безопасности – формирование технологий и методов деятельности.

Социализация информационной безопасности – становление и признание значимости отрасли в глазах общественности (формирование высокого социального статуса), появление ученых, публицистов, которые путем пропаганды и популяризации доносят до внимания общественности актуальность вопросов отрасли.

2. Входное тестирование на определение сознательности студентов в вопросах информационной безопасности

Вопрос №1: Что вы обычно делаете с напечатанными документами? Выберите один ответ:

1. выбрасываю в мусорку
2. ничего не делаю, они сами куда-то деваются
3. пускаю в шредер (измельчитель)
4. рву на несколько частей и выбрасываю в мусорку
5. перечеркиваю чертой и использую для черновиков
6. сминаю и выбрасываю в мусорку

Вопрос №2: Вам позвонили из налоговой службы и просят сообщить данные о вашем коллеге. Ваши действия? Выберите один ответ:

1. Бросите трубку: это мошенники
2. Скажете, что у вас нет такой информации
3. Предложите им сделать запрос на официальном бланке ФНС и отправить по почте или через ТКС
4. Попросите, чтобы они приехали лично и взяли ее самостоятельно у коллеги

Вопрос №3: За распространение конфиденциальной информации законодательством РФ не предусмотрено. Выберите один или несколько ответов:

1. дисциплинарное взыскание
2. смертная казнь
3. конфискация имущества
4. административный штраф
5. лишение свободы

Вопрос №4: Вам нужно отойти «на пару минут» – налить кофе или перекусить. Что вы точно сделаете, прежде чем уйти? Выберите один ответ:

1. Спрошу, не принести ли что-нибудь коллегам
2. Закрою, сохранив все документы, над которыми работал
3. Напишу в общем чате коллегам, что отлучился, чтобы они проследили, чтобы никто не подходил к моему компьютеру
4. Заблокирую компьютер

Вопрос №5: На рабочий компьютер нужно установить программу. Ваши действия? Выберите один ответ:

1. Напишу заявку. Если одобрят, установлю сам
2. Скачаю бесплатную версию из Интернета
3. Если уже что-то подобное устанавливал, то сделаю все сам. Если нужно что-то новенькое, обращусь к сисадминам.
4. Напишу заявку. Если одобрят, то попрошу установить сисадмина

Вопрос №6: Вы отправили на печать список с информацией о клиентах. Принтер стоит в коридоре, но вас отвлек коллега со срочной задачей. Как поступите? Выберите один ответ:

1. Выслушаю коллегу, потом заберу документы
2. Попрошу коллегу подождать, а сам сначала заберу бумаги
3. Если задача действительно срочная, попрошу коллегу забрать бумаги, пока я выполняю задачу

Вопрос №7: Допускается ли использование почтовых ящиков в рабочих целях на общедоступных почтовых серверах? Например, mail.ru, yandex, google и т.д. Выберите один ответ:

1. Только для отправки срочных писем
2. Деловые письма - только с рабочей почты
3. Если в письме нет конфиденциальной информации
4. Да, предварительно заархивировав и запаролив архив

Вопрос №8: Вам нужно поработать из дома, но для этого нужно «взять» с собой некоторые конфиденциальные документы. Как вы поступите? Выберите один ответ:

1. Возьму с собой, всегда так делаю.
2. Составлю акт о перемещении конфиденциальных документов и заберу домой

3. Спрошу у коллег, если они не против - возьму
4. Это запрещено, но работу-то надо закончить, поэтому все равно возьму
5. Лучше задержусь в офисе и доделаю работу

3. Лабораторная работа 1

Крылатые выражения для монологического высказывания

Учащимся по вариантам предлагается 2 цитаты, афоризма или крылатых выражения. Необходимо подготовить устное монологическое высказывание по обоим цитатам, в котором требуется согласиться или не согласиться с автором.

Вар	Цитата №1	Цитата №2
1	Безопасные корабли - это вытащенные на берег корабли. /Анахарсис Скифский/	Кто держит в поле зрения все, не замечает ничего. Марк Клейман
2	В жизни нет гарантий, существуют одни вероятности. /Том Клэнси/	Информация сама по себе — не сила, иначе самыми могущественными людьми на свете были бы библиотекари. Брюс Стерлинг
3	Муха, которая не желает быть прихлопнутой, безопасней чувствует себя на самой хлопушке. /Георг Лихтенберг/	Мы тонем в информации и задыхаемся от нехватки знаний. Джон Нейзбитт
4	Никогда не ставь свою безопасность в зависимость от благородства другого человека. /Уилла Кадер/	Не информация убеждает, а интонация. Сильвия Чиз
5	Главной опасностью в жизни является то, что вы предпринимаете слишком много мер предосторожности. /Альфред Адлер/	Информация – ключ ко всему. Вы должны узнать сильные стороны ваших врагов и понять, кто из друзей вам вовсе не друг. (Лорд Варис Игра престолов)
6	Того, кто не задумывается о далеких трудностях, поджидают близкие неприятности /Конфуций/	— За эти сведения наш агент отдал жизнь. — Это говорит не о важности сведений, а о его промахе. Шерлок (Sherlock)
7	Ощущение полной безопасности наиболее опасно. /И. Шевелев/	Недостоверная информация опасней пули. Мстители (The Avengers)
8	Осмотрительность так же подобает воину, как и храбрость. /Ф. Купер/	Чем совершеннее техника передачи информации, тем более заурядным, пошлым, серым становится ее содержание. Артур Кларк
9	Страх опасности в тысячу раз страшнее самой опасности /Д. Дефо/	До девяноста пяти процентов всей информации, которую воспринимают твои глаза и уши каждый день, заранее отобраны по чьей-то воле и оплачены из чьего-то кармана. Харуки Мураками

10	Возможность украсть создает вора. /Ф. Бэкон/	Информация в чистом виде - это не знание. Настоящий источник знания - это опыт. • Альберт Эйнштейн
11	С теми, кто воспринимает несчастный случай как личное оскорбление, несчастный случай не происходит." /Марио Пьюзо "Крестный отец"/	Средства массовой информации не меннее опасны, чем средства массового уничтожения. • Сергей П. Капица
12	Безопасность — это процесс, а не результат /Bruce Schneier/	Если вы увеличиваете процент потребления общедоступной информации, результат вашей мыслительной деятельности едва ли сможет претендовать на оригинальность. • Павел Дуров
13	„Друг мой, вспомни, что молчать хорошо, безопасно и красиво.“ — Ф М Достоевский	Дайте мне средства массовой информации и я из любого народа сделаю стадо свиней. © Пауль Йозеф Геббельс

Модуль № 2: Нормативные документы в области информационной безопасности

1. Вопросы для обсуждения

1. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г.
2. ГОСТ Р 6.30-2003. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов
3. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ В. В. Путиным 2016 г.
4. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: 1992.
5. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ.
6. Федеральный закон «Об электронной подписи» от 06 апреля 2011 г. № 63-ФЗ
7. Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ
8. Федеральный закон «О государственной тайне» от 21 июля 1993 г. № 5485-1 Федеральный закон «О лицензировании отдельных видов деятельности» от 04 мая 2011 г. № 99-ФЗ.
9. Федеральный закон «О техническом регулировании» от 27 декабря 2002 № 184-ФЗ.
10. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», Госстандарт России.
11. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью», Госстандарт России.
12. Анализ деятельности государственных органов законодательной и исполнительной власти, определяющих и ведущих политику Российской Федерации в области информационной безопасности :
    - Комитет Государственной думы по безопасности.
    - Совет безопасности России

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России)
- Федеральная служба безопасности Российской Федерации (ФСБ России)
- Федеральная служба охраны Российской Федерации (ФСО России) и Служба специальной связи и информации ("Спецсвязь России")
- Служба внешней разведки Российской Федерации (СВР России)
- Министерство обороны Российской Федерации (Минобороны России)
- Министерство внутренних дел Российской Федерации (МВД России)
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
- Центральный банк Российской Федерации (Банк России)

2. Самостоятельная работа 1 (по органам власти)

Государственные органы власти Российской Федерации в области информационной безопасности

В самостоятельной работе необходимо привести анализ деятельности государственных органов законодательной и исполнительной власти, определяющих и ведущих политику Российской Федерации в области информационной безопасности. Результат практической самостоятельной работы следует представить в виде доклада с презентацией.

Органы власти для доклада распределяются среди студентов преподавателем. Время на устный ответ: 5-6 минут. Презентация оформляется в формате программы MS Office Power Point согласно требованиям кафедры.

В докладе необходимо отразить следующую информацию:

- Цели и задачи изучаемого органа власти, его функции, миссия.
- Место органа власти в структуре государственной власти.
- Организационная структура с разделением функционала.
- Краткая историческая справка о деятельности органа власти (год основания, преобразования, реорганизация и т.д.).
- Обзор основных видов деятельности за последние 2 года (отчеты о работе органа исполнительной власти, отчет о законах и законопроектах для органов законодательной власти и т.д.).

Для крупных многопрофильных организаций необходимо рассматривать и описывать только тот функционал и те отделы, которые относятся к вопросам обеспечения информационной безопасности. Такие организации распределяются среди группы студентов (по два или три человека).

Данная практическая работа оценивается по устному выступлению и презентации. Презентация к выступлению выкладывается на учебный портал в течение 3 дней с момента очного выступления. Работа считается выполненной при соблюдении следующих условий: успешный устный доклад по теме на практическом занятии, презентация по требованиям кафедры опубликована на учебном портале в разделе «Практическая работа ко второй лекции».

Перечень органов власти представлен в таблице:

Наименование	**Кол-во студентов**

Комитет Государственной думы по безопасности;	1
Совет безопасности России	2
Федеральная служба по техническому и экспортному контролю (ФСТЭК России)	1
Федеральная служба безопасности Российской Федерации (ФСБ России)	3
Федеральная служба охраны Российской Федерации (ФСО России) и Служба специальной связи и информации ("Спецсвязь России")	1
Служба внешней разведки Российской Федерации (СВР России)	1
Министерство обороны Российской Федерации (Минобороны России)	1
Министерство внутренних дел Российской Федерации (МВД России)	1
Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)	1
Центральный банк Российской Федерации (Банк России)	1

3. Кейс

Задание: разработайте собственный раздел для договора кредитования, который бы решил проблему. Используйте терминологию, соответствующую предметной области и формальному юридическому языку.

В 2012 г. Ярославский областной суд вынес апелляционное определение по жалобам коммерческого банка «Юниаструм Банк» и коллекторского агентства «Морган энд Страут» на решение Фрунзенского районного суда г. Ярославля. Суд первой инстанции признал незаконным действия банка по передаче персональных данных гражданина «Григорьева» коллекторскому агентству «Морган энд Стаут», обязал коллектора уничтожить персональные данные истца, взыскал с банка и коллектора денежные средства в целях возмещения морального ущерба, нанесенного гражданину «Григорьеву». В апелляционной жалобе «Юниаструм банк» поставил вопрос об отмене решения районного суда и направлении дела на новое рассмотрение.

Ярославский областной суд, рассмотрев апелляционные жалобы банка и коллекторского агентства на решение Фрунзенского районного суда г. Ярославля, в удовлетворении жалобы отказал. Областной суд исходил из того, что банк предоставил «Григорьеву» потребительский кредит на основании соответствующего договора. В связи с тем, что клиент перестал регулярно выполнять свои обязательства по кредитному договору, банк передал его персональные данные в коллекторское агентство для организации взыскания задолженности. При этом в кредитном договоре не было прописано условие о передаче персональных данных заемщика третьему лицу в случае ненадлежащего исполнения им своих обязанностей по данному договору. Банк также не запросил согласие «Григорьева» на передачу его персональных данных, а осуществил передачу самостоятельно. При этом судом также установлено, что передача прав требования от банка «Морган энд Страут» не было оформлено в порядке, предусмотренном законодательством. Ярославский областной суд. Апелляционное определение от 05.03.2012 г. по делу No 33-939/2012.

Вопрос: каким образом, по вашему мнению, банк мог избежать нарушения законодательства?

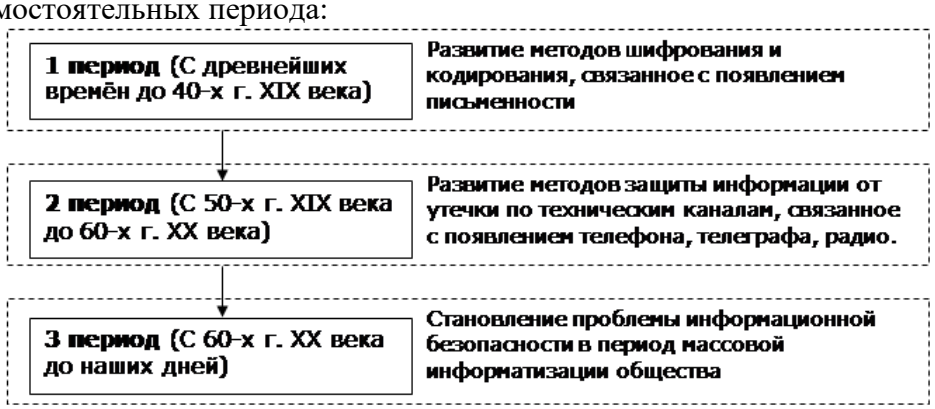
4. Письменная работа 1

«Обеспечение информационной безопасности в зарубежных странах»

Цель: ознакомление с основными принципами обеспечения информационной безопасности в зарубежных странах.

Обеспечение защиты информации волновало человечество всегда. В процессе эволюции цивилизации менялись виды информации, для её защиты применялись различные методы и средства.

Процесс развития средств и методов защиты информации можно разделить на три относительно самостоятельных периода:



Наблюдаемые в последние годы тенденции в развитии информационных технологий могут уже в недалеком будущем привести к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне, которые могут принимать форму информационной войны, а сама информационная война станет одним из основных инструментов внешней политики, включая защиту государственных интересов и реализацию любых форм агрессии. Это является одной из причин, почему полезно ознакомиться с основными принципами обеспечения ИБ в ведущих зарубежных странах.

Другая причина заключается в том, что большинство применяемых на территории РФ средств и методов обеспечения ИБ основаны на импортных методиках и строятся из импортных компонентов, которые были разработаны в соответствии с нормами и требованиями по обеспечению ИБ стран-изготовителей. В связи с этим прежде чем приступить к изучению непосредственно технологий и средств обеспечения ИБ, следует познакомиться с политикой ИБ ведущих зарубежных стран.

Задание

1. Подготовить доклад, используя любые доступные источники информации, о системе обеспечения информационной безопасности в одной из стран (распределяется преподавателем).
2. Заполнить таблицу "Системы обеспечения ИБ в зарубежных странах» на основе подготовленного материала, а также докладов других студентов.
3. Провести анализ собранной информации и сделать выводы.
4. Отчет сдается **только** в печатном виде. Уникальность сдаваемого реферата не ниже 40%. Рефераты с более низким показателем не оцениваются. Объем реферата – не менее 5 страниц и не более 20 страниц. Титульный лист и содержание не учитываются в общем объеме.

Индивидуальное задание

Государство	**Основные принципы обеспечения ИБ**	**Основные документы в области обеспечения ИБ**	**Структура государственных органов обеспечения национальной ИБ**

США			
Великобритания			
Швеция			
Франция			
Германия			
Китай			
Япония			
Швейцария			
Евросоюз			
Австралия			
Болгария			
Италия			
Казахстан			

Модуль № 3: Компьютерные правонарушения

1. Вопросы для обсуждения

1. Понятия «преступление» и «правонарушение».
2. Классификация противозаконных действий в области информационных технологий.
3. Криминологические группы общественно-опасных деяний в информационной сфере, предусмотренные Уголовным кодексом.
4. Характерные особенности компьютерного преступления.
5. Характеристики субъектов компьютерных преступлений.
6. Международное сотрудничество в сфере борьбы с компьютерными преступлениями.

2. Ситуационные задачи по компьютерным преступлениям

Задача №1

Используя свой ноутбук, товарищ Шевцов «на спор» подключился к внутренней сети Росгидромета и для доказательства того, что ему это удалось, отредактировал информацию о параметрах метеоусловий в центральных районах страны и изменил пароль для доступа к этой информации работниками Росгидромета.

Имеются ли основания рассматривать совершенное Шевцовым деяние как преступление в сфере компьютерной деятельности. Дайте юридическую оценку его действиям.

Задача №2

Дударов приобрел в магазине диск с игрой и, проверив ее на наличие «вирусов» (они обнаружены не были), установил на свой персональный компьютер.

Спустя некоторое время работа компьютера была полностью заблокирована. Придя к выводу, что причиной тому новейший «вирус», которым поражена купленная им игра, Дударов продал диск с ней своему знакомому, утаив от него нюанс, связанный с вирусом.

Имеются ли основания рассматривать совершенное Дударовым общественно опасное деяние как преступление в сфере компьютерной информации? Как следует квалифицировать действия Дударова?

Задача №3

Служащий банка «Южный» Игрунков приобрел на рынке диск с компьютерной игрой. На следующий день Игрунков установил игру на своем рабочем компьютере, связанном по сети с другими компьютерами банка. В результате распространения вируса, записанного на диске, компьютерная система банка была выведена из строя и не могла нормально функционировать более суток, из-за чего банк понес существенные убытки.

Как квалифицировать действия Игрункова?

Модуль № 4: Информационный суверенитет государств

1. Вопросы для обсуждения

1. Понятие и принципы «информационно-психологической войны».
2. Традиционный суверенитет государства.
3. Концепция суверенитета.
4. Составляющие информационного суверенитета.
5. Медийная инфраструктура для обеспечения информационного суверенитета.
6. Электронный щит.
7. Пути реализации информационной войны в современном мире.

2. Коллоквиум

Перечень вопросов к коллоквиуму

1. Гуманитарная сущность безопасности. Основные нормативно-правовые акты России по вопросам безопасности.
2. Гуманитарная сущность информации. Технократический и гуманитарный подходы к информации.
3. Гуманитарная сущность информационной безопасности.
4. Место и роль проблем информационной безопасности в становлении современного информационного общества.
5. Основные положения Доктрины информационной безопасности РФ.
6. Основные источники информационных угроз безопасности (согласно Доктрины ИБ РФ)
7. Стадии формирования информационной безопасности (ИБ). Институционализация отрасли ИБ.
8. Стадии формирования информационной безопасности (ИБ). Профессионализация отрасли ИБ.
9. Стадии формирования информационной безопасности (ИБ). Технологизация отрасли ИБ.
10. Стадии формирования информационной безопасности (ИБ). Социализация отрасли ИБ.
11. Государственные службы, занимающиеся вопросами информационной безопасности.
12. Международные и отечественные стандарты информационной безопасности.
13. Основные законодательные акты в вопросах ИБ в России.
14. Основные виды правонарушений в области ИБ в России.

Модуль № 5: Компьютерная этика и интеллектуальная собственность

1. Вопросы для обсуждения

1. Информационная этика.
2. Этапы развития этики.
3. Основные проблемы информационной этики.
4. Требования, предъявляемые специалисту в области информационной безопасности с этической точки зрения.
5. Понятие интеллектуальной собственности и правовой охраны результатов интеллектуальной деятельности.
6. Понятие патент, полезная модель, промышленный образец.
7. Нюансы оформления исключительных прав.
8. Федеральный институт промышленной собственности.
9. Гражданский кодекс как основной нормативно-правовой акт в области защиты авторских прав.

2. Реферат

Темы рефератов

1. Эволюция, этапы развития компьютерной этики.
2. Основные проблемы компьютерной этики.
3. Влияние информационных технологий на обращение с персональными данными.
4. Международные нормы приватности граждан.
5. Правовые гарантии приватности граждан в России.
6. Анонимность в сети Интернет с точки зрения этики. Проблемы и критика.
7. Противоправные действия в сети Интернет: обзор, примеры.
8. Сетевой этикет (нетикет).
9. Серьезные нарушения сетевого этикета (вымогательство, обман, подделка и т.д.)
10. Проблемы собственности на программное обеспечение
11. Последствия миграции интеллектуальной собственности в Интернет.
12. Проблемы плагиата в Сети и нарушения авторского права разработчиками веб-сайтов
13. Право на доступ к компьютерным ресурсам. Важность доступа к компьютерным ресурсам.
14. Кодексы профессиональной этики в области компьютерных технологий в России и за рубежом.
15. Проблема правовой охраны нетрадиционных объектов авторского права.

Модуль № 6: Обеспечение информационно-психологической безопасности личности и общества

1. Вопросы для обсуждения

1. Безопасность личности как важный аспект деятельности государства.
2. Основные источники угроз информационно-психологической безопасности личности.
3. Манипулятивные возможности масс-медиа.
4. Способы нейтрализующего воздействия на деструктивные угрозы.
5. Психологический портрет личности с точки зрения информационной безопасности.
6. Способы и методы выявления психологических свойств личности.
7. Социальная инженерия.
8. Психология манипуляций и способы обеспечения информационной безопасности личности
9. Методы профайлинга и социальной инженерии.
10. Методы определения инсайдерских атак в организации или коллективе с помощью методов профайлинга.

2. Тестирование № 2

1. Выберите правильный вариант ответа. Какой проблемы реализации гуманитарной сущности информационной безопасности не существует?

- Институционализация
- Коммерциализация
- Профессионализация
- Технологизация

2. Какого правового уровня институционализации информационной безопасности не существует?

- Международно-правовой
- Объектно-правовой
- Личностно-правовой
- Национально-правовой

3. Выберите правильный вариант ответа. Какой документ из перечисленных был принят ООН в декабре 2002 года?

- Доктрина информационной безопасности РФ
- Резолюция по созданию глобальной культуры кибербезопасности
- Пакт по профессиональному стандарту специалиста по ЗИ
- Закон «Об информации, информационных технологиях и о защите информации»

4 Выберите правильный вариант ответа. Какого элемента институционализации проблемы информационной безопасности не существует?

- гуманитарный
- когнитивный
- самоорганизационный
- правовой

5. Выберите правильный вариант ответа. Как называются нормативные акты, регламентирующие технологии защиты информации?

- федеральный закон
- международные резолюции
- приказы Роскомнадзора и ФСТЭК
- государственные стандарты
- постановления правительства

6. Выберите правильные варианты ответа. Что из перечисленного характеризует социализацию проблемы информационной безопасности?

- признание феномена информационной безопасности как важнейшего инструмента управления организацией, достижения ею конкурентных преимуществ;
- формирование представления о профессиональном специалисте по защите информации как специалисте, способном справиться с управлением информацией, с защитой информационных интересов как государства, так и отдельного хозяйствующего субъекта;
- формирование рынка ИБ и слоя реальных и потенциальных клиентов, профессиональных потребителей услуг по ИБ в организации;
- формирование представления о ИБ как необходимом компоненте культуры управления, предпринимательской деятельности, инструменте современного менеджмента, составной части корпоративной культуры и т. п.
- Все вышеперечисленное верно
- Нет правильного ответа

7. Выберите правильные варианты ответа. Что из перечисленного легло в основу национальных интересов согласно Доктрине ИБ РФ?

- Соблюдение конституционных прав и свобод человека и гражданина в области информации, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.
- Информационное противоборство угрозам российского гражданского общества
- Информационное обеспечение государственной политики Российской Федерации.
- Развитие отечественной информационной индустрии.
- Защита информационных ресурсов.
- Все вышеперечисленное верно

- Нет правильного ответа

8. Дайте определение понятию «информационный суверенитет государства».

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;
- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.
- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.
- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже, чем «удовлетворительно»;
- оценка «не зачтено», если тест оценен ниже, чем «удовлетворительно».

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма				
1.	Задание закрытого типа	Действия против средств электронных коммуникаций, радиосвязи, радаров, компьютерных сетей – 1. Электронная война 2. Психологическая война 3. Экономическая информационная война 4. Кибервойна	1	2
2.		Диверсионные действия против гражданских объектов противника, такие, как тотальный паралич сетей, перебои связи, введение случайных ошибок в пересылку данных, тайный мониторинг сетей, несанкционированный доступ к закрытым данным 1. Электронная война 2. Психологическая война 3. Экономическая информационная война 4. Кибервойна	4	2
3.		Защита информации, предусматривающая возмещение убытков от её уничтожения или модификации путем получения страховых выплат, - это 1. страховая защита 2. моральная защита 3. этическая защита	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
4.		Какие понятия относятся к самоорганизационному компоненту проблемы институционализации информационной безопасности? 1. гражданское общество 2. личность 3. Совет Федерации 4. общественные фонды 5. национальные союзы 6. мировые суды	1, 4, 5	2
5.		Какое определение информационной безопасности дает Доктрина ИБ РФ? 1. отсутствие опасностей 2. определенная деятельность по обеспечению или по предупреждению каких-либо угроз, опасностей (т. е. это деятельностный подход, связанный с уровнем развития общественного производства, благодаря которому и создаются те или иные защитные (предупреждающие) действия 3. состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства; 4. состояние защищенности субъекта, выражающееся в безопасности информации субъекта и его информационно-психологической безопасности, достигаемое посредством рефлексивного определения и контролирования единства его естественного существования и развития в ходе реализации информационных процессов как на содержательном, так и на представительном уровнях информации	3	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
6.	Задание открытого типа	Дать определение «Информационное и информационно-психологическое воздействие»	воздействие, которое осуществляется с применением информационного оружия, т. е. таких средств, которые позволяют осуществлять с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия. Информационно-психологическое воздействие представляет собой целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние (положительное или отрицательное) на функционирование и развитие информационно-психологической среды общества, психику и поведение населения, руководство страны, военнослужащих.	2
7.		Дать определение «Информационная война»	это открытые и скрытые целенаправленные информационные воздействия социальных, политических, этнических и иных систем друг на друга с целью получения определенного выигрыша в материальной сфере. Информационную войну также можно определить как комплекс мероприятий и операций, проводимых вооруженными силами государств и другими (как правительственными, так и частными) организациями, направленных на обеспечение информационного превосходства над противником и нанесения ему материального, идеологического или иного ущерба. В информационной войне информация является одновременно оружием, ресурсом и целью.	2
8.		Основными формами информационной войны являются	Командно-управленческая война – война, нацеленная	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			на каналы связи между командованием и исполнителями. Разведывательная война – сбор важной в военном отношении информации (как нападение) и защита собственной. Электронная война – действия против средств электронных коммуникаций, радиосвязи, радаров, компьютерных сетей. Сюда же входит и кибервойна. Оружием в этой войне являются компьютерные вирусы и др. программное обеспечение. Психологическая война – пропаганда, «промывание мозгов», информационная обработка населения. Эта форма войны имеет три составляющие — подрыв гражданского духа, деморализация вооруженных сил, дезориентация командования. Экономическая информационная война – нанесение ущерба экономической (производственной, финансовой, коммерческой и т.д.) сфере противника, создание предпосылок для кризисных ситуаций.	
9.		Что понимается под информационным оружием	В широком смысле под информационным оружием понимаются способы целенаправленного информационного воздействия на противника, рефлексивного управления им с целью изменения его замысла на проведение стратегических или тактических действий в нужном направлении. В более узком смысле под информационным оружием понимается комплекс способов, методов, технических средств и технологий, предназначенных для получения контроля над информационными	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			ресурсами потенциального противника и вмешательства в работу его информационных систем для выведения их из строя, нарушения процесса нормального функционирования, получения или модификации содержащихся в них данных, а также целенаправленного продвижения выгодной информации (или дезинформации). При этом сама информация, попадание которой к противнику может нанести ему заметный материальный или иной ущерб, также нередко совершенно справедливо и обоснованно рассматривается в качестве одного из видов информационного оружия.	
10.		Дать определение шпионажа по Уголовному кодексу РФ	передача, собирание, похищение или хранение в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности РФ, если эти деяния совершены иностранным гражданином или лицом без гражданства	2

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Методические рекомендации по выполнению лабораторных работ, проведению зачета

Отчет по самостоятельным и практическим письменным работам

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие целей и задач лабораторной работы,
- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

Зачет и коллоквиум

К зачету допускаются студенты, сдавшие до зачетной недели все лабораторные и контрольные работы, тестирования, а также получивший зачет по вопросам коллоквиума и итогового проекта.

Оценивание студентов на зачете осуществляется в соответствие с требованиями и критериями зачетной системы (зачет или незачет). Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе зачета.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных и тематических контрольных работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях.

На зачете осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины. Теоретические и практические знания оцениваются путем компьютерного тестирования и на основании письменных ответов студентов по нескольким теоретическим вопросам.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Реферат*	1/5	5	По расписанию
2.	*Выполнение практической работы*	1/8	8	
3.	*Выполнение письменной работы*	1/8	8	
4.	*Тест*	2/5	10	
5.	*Ответ на занятии*	18/3	54	
6.	*Коллоквиум*	1/5	5	
Всего			**90**	-
Блок бонусов				
7.	*Посещение занятий без пропусков*	1	3	
8.	*Своевременное выполнение всех заданий*	1	3	
9.	*Активность студента на занятии*	1	4	
Всего			**10**	-

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

Киреева О.Ф., Коммуникационный консалтинг как средство обеспечения информационной безопасности в современном обществе [Электронный ресурс] / Киреева О.Ф. - М. : Дашков и К, 2018. - 138 с. - ISBN 978-5-394-02993-6 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785394029936.html

Костин В.Н., Методы и средства защиты компьютетной информации: законодательные и нормативные акты по защите информации [Электронный ресурс]: учеб. пособие / В.Н. Костин - М. : МИСиС, 2017. - 26 с. - ISBN 978-5-906846-87-7 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785906846877.html

Куняев Н.Н., Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс] / Н.Н. Куняев - М. : Логос, 2015. - 348 с. - ISBN 978-5-98704-513-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785987045138.html

Судариков С.А., Право интеллектуальной собственности: учебник [Электронный ресурс] / С.А. Судариков. - М. : Проспект, 2014. - 368 с. - ISBN 978-5-392-16752-4 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392167524.html

Чусавитина Г.Н., Информационная безопасность и вопросы профилактики кибер-экстремизма среди молодежи [Электронный ресурс] / Чусавитина Г.Н. - М. : ФЛИНТА, 2014. - 161 с. - ISBN 978-5-9765-2038-7 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785976520387.html

б) Дополнительная литература:

Информационное право: учебник для бакалавров / Городов О.А. - М. : Проспект, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785392196982.html (ЭБС «Консультант студента»).

Ищенко Е.П., Виртуальный криминал [Электронный ресурс] : учебное пособие / Е.П. Ищенко. - М. : Проспект, 2014. - 232 с. - ISBN 978-5-392-12256-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392122561.html

Кин Э., Ничего личного: Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные [Электронный ресурс] / Эндрю Кин; Пер. с англ. - М. : Альпина Паблишер, 2016. - 224 с. - ISBN 978-5-9614-5128-3 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785961451283.html

Кузнецов П.У., Основы информационного права [Электронный ресурс] : учебник для бакалавров / П.У. Кузнецов. - М. : Проспект, 2015. - 312 с. - ISBN 978-5-392-16692-3 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392166923.html ЭБС «Консультант студента».

Малюк А.А., Защита информации в информационном обществе [Электронный ресурс]: Учебное пособие для вузов. / А.А. Малюк - М. : Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204811.html ЭБС «Консультант студента»

Шарков Ф.И., Правовые основы коммуникации: в рекламе, связях с общественностью, журналистике: учебное пособие [Электронный ресурс] / Шарков Ф.И., Захарова В.И. - М. : Проспект, 2016. - 224 с. - ISBN 978-5-392-19922-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392199228.html ЭБС «Консультант студента»

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

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для проведения лабораторных занятий необходима компьютерная аудитория, в которой организован доступ к сети Интернет и установлено программное обеспечение. Для проведения публичной защиты проектов и рефератов необходима мультимедийная аудитория с проектором.

Учебные аудитории, библиотеки АГУ, центр мониторинга и аудита качества образования, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).