МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное
учреждение высшего образования
«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
им. В.П. Астафьева»
ИНСТИТУТ ФИЗИЧЕСКОЙ КУЛЬТУРЫ, СПОРТА и ЗДОРОВЬЯ им. Я.С.Ярыгина

КАФЕДРА МЕДИКО-БИОЛОГИЧЕСКИХ ОСНОВ ФИЗИЧЕСКОЙ КУЛЬТУРЫ И БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

44.03.05 Педагогическое образование (с двумя профилями) направленность (профиль) образовательной программы
Физическая культура и Безопасность жизнедеятельности

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Красноярск-2018

Рабочая программа дисциплины «Информационная безопасность» составлена к.б.н., доцентом кафедры медико-биологических основ и безопасности жизнедеятельности Кужугет А.А.

РПД обсуждена на заседании кафедры теории и методики медико-биологических основ и безопасности жизнедеятельности «07» июня 2017 г., протокол № 9

Заведующий кафедрой _____ _____ Т. В. Колпакова

Одобрено научно-методическим советом

Института физической культуры, спорта и здоровья им. И. Ярыгина ФГБОУ ВПО «КГПУ им. В.П. Астафье

«08» июня 2017 г.) М.И. Бордуков

РПД актуализирована на заседании кафедры медико-биологических основ физической культуры и безопасности жизнедеятельности
«14» июня 2018 г., протокол № 11

И. о. зав. кафедрой ___ Н.Н. Казакевич

Одобрено научно-методическим советом специальности (направления подготовки) института физической культуры, спорта и здоровья им. И. С. Ярыгина
« 21» июня 2018 г. протокол № 10
Председатель НМСС (Н) М.И. Бордуков

РПД актуализирована на 2019-20 учебный год на заседании кафедры медико-биологических основ физической культуры и безопасности жизнедеятельности «30» апреля 2019 г протокол № 8

и. о. заведующий кафедрой Н. Н. Казакевич

Одобрено научно-методическим советом
Института физической культуры, спорта и здоровья им. И. Ярыгина
ФГБОУ ВПО «КГПУ им. В.П. Астафьева»

«_23_» мая 2019 г., протокол №__8_____ ___М.И. Бордуков

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Информационная безопасность» является ознакомление студентов с основами информационной безопасности. Изучаются информационные угрозы, их нейтрализация, вопросы организации мер защиты информационных ресурсов, нормативные документы, регламентирующие информационную деятельность, криптография, другие вопросы, связанные с обеспечением безопасности компьютерных сетей.

Задачи курса:

1.познакомить студентов с определением, классификацией и характеристиками информационной безопасности;

2.познакомить с организационными и экономическими аспектами работы с информационными ресурсами и методами оценки эффективности их безопасности;

3.дать представление об особенностях информационной безопасности, сегментах и участниках информационного рынка, особенностях формирования безопасности информации;

4.рассмотреть основные технологические принципы безопасности мировых информационных ресурсов на основе глобальной сети Internet;

5.рассмотреть возможности применения безопасности ресурсов Internet .

Данная программа составлена в полном соответствии с государственным образовательным стандартом и согласована с комплексом других программ для данной программы.. Обучение студентов по данной программе организуется в форме лекционных и семинарские занятий. Самостоятельная работа студентов заключается в изучении соответствующих учебных пособий и выполнении индивидуальных заданий с последующим контролем преподавателя. Предполагается, что реализацию заданий студенты должны выполнять на персональных компьютерах.

2. ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

1. Требования к исходному уровню подготовки: для усвоения материала курса необходимо, чтобы студенты имели базовые навыки написания программ на одном из алгоритмических языков; имели представление об информационных технологиях и системах.

2. Требования к знаниям, умениям и навыкам, приобретенным в результате изучения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Общекультурные компетенции (ОК):

- способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве (ОК-3);

Обучение по дисциплине «Информационная безопасность» формирует следующие **профессиональные и профессионально-прикладным компетенции (ПК и ППК):**

- готовностью реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов (ПК-1);
- способностью использовать современные методы и технологии обучения и диагностики (ПК-2).

В результате изучения дисциплины студент должен:

Знать:

- содержание основных понятий обеспечения информационной безопасности;
- источники угроз безопасности информации;
- методы оценки уязвимости информации;
- методы создания, организации и обеспечения функционирования систем комплексной защиты информации;
- методы пресечения разглашения конфиденциальной информации;
- виды и признаки компьютерных преступлений

Уметь:

- отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	Всего часов
Аудиторные занятия	28
Лекции	10
Практические занятия (семинары)	–
Лабораторные работы	18
Самостоятельная работа	179
Вид итогового контроля: экзамен	9
Общая трудоемкость	216

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. РАЗДЕЛЫ ДИСЦИПЛИНЫ И ВИДЫ ЗАНЯТИЙ

	Разделы дисциплины	Лекции	Практические занятия, семинары	Лабораторные работы
1	Международные стандарты информационного обмена.	1	–	2
2	Информационная безопасность в условиях функционирования в России глобальных сетей.	1	–	2
3	Виды возможных нарушений информационной системы.	2	–	2
4	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	1	–	2
5	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	1	–	2
6	Концепция информационной безопасности.	1	–	2
7	Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.	1	–	4
8	Анализ способов нарушений информационной безопасности. Методы криптографии. Криптографические методы защиты информации. Использование защищенных компьютерных систем.	2	–	2
	Всего часов	10	–	18

4.2. СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ

Тема 1. Международные стандарты информационного обмена. Понятие угрозы.

Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем.

Тема 2 Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».

Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).

Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности.

Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.

Тема 3. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Основные положения теории информационной безопасности информационных систем. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Тема 4. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации.

Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами).Использование криптографических средств для решения задач идентификация и аутентификация.

Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы. Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

Т**ема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.**

Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы

влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.

Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей.

Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.

Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.

Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.

Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

Тема 6. Концепция информационной безопасности.

Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

Тема 7. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.

Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности.

Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем.

Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.

Тема 8 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ

«Информационная безопасность»

для студентов образовательной программы

44.03.01 – Безопасность жизнедеятельности

по заочной форме обучения

Модуль	Трудоемкость		№№ раздела, темы	Лекционный курс		Занятия (номера)		Индивидуальные занятия		Формы контроля
	В кредитах	В часах		Вопросы, изучаемые на лекции	Часы	Семинарские	Лабораторно-практические	Содержание	Часы	
1		300	1	Международные стандарты информационного обмена.	2	–	–	–	–	Конспекты лекций. Групповая работа на ЛПЗ. Доклады. Ответы на вопросы. Тестовые задания. Написание рефератов
			2	Информационная безопасность в условиях функционирования в России глобальных сетей.	2	–	–	–	–	
			3	Виды возможных нарушений информационной системы.	2	–	2	–	–	
			4	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	2	–	2	–	–	
			5	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	2	–	–	–	–	

			6	Концепция информационной безопасности.	2	–	2	–	–	Групповая работа на ЛПЗ. Доклады. Ответы на вопросы. Тестовые задания. Написание рефератов. Экзамен
			7	Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.	4	–	2	–	–	
			8	Анализ способов нарушений информационной безопасности. Методы криптографии. Криптографические методы защиты информации. Использование защищенных компьютерных систем.	4	–	2	–	–	
Всего часов		30	–	–	20		10	–	–	

КАРТА МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ ДИСЦИПЛИНЫ

«Информационная безопасность

Наименование№ п/п	Вид	Форма доступа	Рекомендуемое использование	Потребность	Альтернатив. замены	Отв.	Стоимость
1Рабочая учебная программа	Печатный. Электронный (Word).	Информационный центр института физической культуры, спорта и здоровья им. И.С. Ярыгина.	Очная, заочная формы обучения. Электронный.				
2.Конспект лекций	Печатный. Электронный (Word).	Информационный центр института физической культуры, спорта и здоровья им. И.С. Ярыгина.	Очная, заочная формы обучения. Электронный.				
3.Методические разработки по проведению лабораторно-практических занятий	Печатный. Электронный (Word).	Информационный центр института физической культуры, спорта и здоровья им. И.С. Ярыгина.	Очная, заочная формы обучения. Электронный.				
4.Видеофильмы	Видеокассеты, CD, DVD	Информационный центр института физической культуры, спорта и здоровья им. И.С. Ярыгина.	Очная, заочная формы обучения. Электронный.				
5.Дополнительные материалы для проведения лабораторно-практических занятий	Печатный. Электронный (Word).	Информационный центр института физической культуры, спорта и здоровья им. И.С. Ярыгина.	Очная, заочная формы обучения. Электронный.				

Наименование№ п/п	Вид	Форма доступа	Рекомендуемое использование	Потребность	Альтернатив. замены	Отв.	Стоимость
6.Учебно-методический комплекс дисциплины	Печатный. Электронный (Word).	Информационный центр института физической культуры, спорта и здоровья им. И.С. Ярыгина.	Очная, заочная формы обучения. Электронный.				

КАРТА ОБЕСПЕЧЕННОСТИ ОБОРУДОВАНИЕМ ДИСЦИПЛИНЫ

«Информационная безопасность»

/п	Наименование	Кол-во	Форма использования	Ответствен-ный
Лаборатория физиологии двигательной деятельности				
	Видеокомплекс (видеомагнитофон, телевизор)	1	Демонстрация материалов лабораторно-практических занятий, учебных и научных видеофильмов	
	Персональные компьютеры	2	Доступ к образовательным и научным ресурсам, работа с мультимедийными материалами на практических занятиях, расчет результатов проведения лабораторных работ	
	Цветной принтер	1	Тиражирование методических разработок и дополнительных материалов для проведения лабораторно-практических занятий	
	Ксерокс	1	Тиражирование результатов проведения лабораторных работ для их оформления в тетрадях для практических занятий	
Информационный центр института физической культуры, спорта и здоровья им. И.С. Ярыгина				
	Персональные компьютеры	5	Доступ к образовательным и научным ресурсам: абонемент учебной литературы КГПУ, читальный зал КГПУ, Интернет	
Лекционная аудитория № 1-53				
	Видеопроектор	1	Демонстрация материалов лекций, учебных и научных видеоматериалов	

КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА ПО ДИСЦИПЛИНЕ
«Информационная безопасность»
для студентов образовательной программы
44.03.01 – Безопасность жизнедеятельности

по заочной форме обучения

Модуль	Номер раздела, темы	Самостоятельная работа студентов			Формы контроля
		Содержание работы, формы работы	Сроки выполнения	Общая трудоемкость	
1	1	Какие физические процессы лежат в основе появления побочных электромагнитных излучений и наводок? Охарактеризуйте особенности угроз безопасности информации, связанных с несанкционированной модификацией структур КС. Назовите особенности такого вида угроз как вредительские программы..	к занятию по данной теме	5	Ответы на семинарски их занятиях.
	2	Вида возможных нарушений информационной системы. Защита информационных систем. Критерии оценки процессов проектирования и правовой базы. Требований безопасности, отображенных в краткой спецификации в составе задания по безопасности. Модель разработки ОО Оценка создания более безопасных продуктов ИТ по направлениям.	к занятию по данной теме	5	Ответы на семинарски их занятиях.
	3	Что понимается под угрозой безопасности информации? Перечислите и охарактеризуйте случайные угрозы. Дайте общую характеристику преднамеренных угроз. В чем состоит особенность определения несанкционированного доступа к информации?	к занятию по данной теме	5	Ответы на семинарски их занятиях.
	4	Понятия о видах вирусов. Свойство вирусов. Вредительские программы Способы защита от вирусов технические . Способы защита от вирусов программные.	к занятию по данной теме	5	Ответы на семинарски их занятиях.
	5	Вида возможных нарушений информационной системы. Защита информационных систем. Основные нормативные руководящие документы, касающиеся государственной тайны. Нормативно-справочные документы. Системы с закрытым и открытым ключом.	к занятию по данной теме	5	Ответы на семинарски их занятиях.

6	Модели безопасности и их применение. Методы защиты информации, с использованием голографии. Методы и средства шифрования и дешифровки. Кодирования и средства защиты при шифровании данных. Использование защищенных компьютерных систем.	к занятию по данной теме	5	Ответы на семинарски их занятиях.
7	Основные технологии построения защищенных ЭИС. Концепция информационной безопасности. Организация функционирования комплексных систем защиты информации	к занятию по данной теме	6	Ответы на семинарски их занятиях.
8	Национальная безопасность страны.	к занятию по данной теме	6	Ответы на семинарски их занятиях.

Карта литературного обеспечения дисциплины
«Информационная безопасность»
для студентов образовательной программы
44.03.01 – Безопасность жизнедеятельности

ПО ОЧНОЙ ФОРМЕ ОБУЧЕНИЯ

№ п/п	Наименование	Место хранения / электронный адрес	Кол-во экземпляров /точек доступа
	Основная литература		
1.	Гафнер, В. В. Информационная безопасность [Электронный ресурс] : учебное пособие. Ч. 1 / В. В. Гафнер ; Уральский гос. пед. ун-т. - Екатеринбург : [б. и.], 2009. - 155 с. - Библиогр.: с. 140-146. - Режим доступа: https://icdlib.nspu.ru/view/icdlib/5329/read.php	Межвузовская электронная библиотека	Индивидуальный неограниченный доступ
2.	Гафнер, В. В. Информационная безопасность [Электронный ресурс] : учебное пособие. Ч. 2 / В. В. Гафнер ; Уральский гос. пед. ун-т. - Екатеринбург : [б. и.], 2009. - 196 с. - Библиогр.: с. 160-166. - Режим доступа: https://icdlib.nspu.ru/view/icdlib/5330/read.php	Межвузовская электронная библиотека	Индивидуальный неограниченный доступ
3.	Башлы, П.Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. - Москва : Евразийский открытый институт, 2011. - 375 с. - ISBN 978-5-374-00301-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90539	ЭБС «Университетская библиотека онлайн»	Индивидуальный неограниченный доступ
	Дополнительная литература		
4.	Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 2-е изд., стер. - М. : Академия, 2007. - 336 с.	Научная библиотека	46
5.	Информационная безопасность [Электронный ресурс] : учебное пособие / [сост.: Е. Р. Кирколуп, Ю. Г. Скурыдин, Е. М. Скурыдина] ; Алтайский гос. пед. ун-т. - Барнаул: АлтГПУ, 2017. - 315 с. - Библиогр.: с. 313-315. - Режим доступа: https://icdlib.nspu.ru/view/icdlib/6506/read.php	Межвузовская электронная библиотека	Индивидуальный неограниченный доступ
6.	Сергеева, Ю.С. Защита информации: Конспект лекций : учебное пособие / Ю.С. Сергеева. - Москва : А-Приор, 2011. - 128 с. - (Конспект лекций). - ISBN 978-5-384-00397-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=72670	ЭБС «Университетская библиотека онлайн»	Индивидуальный неограниченный доступ

Информационные справочные системы и профессиональные базы данных			
7.	Межвузовская электронная библиотека (МЭБ)	https://icdlib.nspu.ru	Индивидуальный неограниченный доступ
8.	Elibrary.ru [Электронный ресурс]: электронная библиотечная система : база данных содержит сведения об отечественных книгах и периодических изданиях по науке, технологии, медицине и образованию / Рос. Информ. Портал. – Москва, 2000– . – Режим доступа: http://elibrary.ru	http://elibrary.ru	Индивидуальный неограниченный доступ
9.	East View: универсальные базы данных [Электронный ресурс] : периодика России, Украины и стран СНГ . – Электрон.дан. – ООО ИВИС. – 2011 - .	https://dlib.eastview.com/	Индивидуальный неограниченный доступ
10.	Межвузовская электронная библиотека (МЭБ)	https://icdlib.nspu.ru	Индивидуальный неограниченный доступ
11.	Гарант [Электронный ресурс]: информационно-правовое обеспечение: справочная правовая система. – Москва, 1992. -	http://www.garant.ru	Доступ из локальной сети вуза
12.	Электронный каталог КГПУ им. В.П. Астафьева [Электронный ресурс]: система автоматизации библиотек «ИРБИС 64»: база данных содержит сведения о книгах, брошюрах, диссертациях, компакт-дисках, статьях из научных и журналов. – Электрон. Дан. – Красноярск, 1992 – . – Режим доступа: http://library.kspu.ru	http://library.kspu.ru.	Свободный доступ

Согласовано:

главный библиотекарь  / Казанцева Е.Ю.

(должность структурного подразделения) (подпись) (Фамилия И.О.)

Фонд оценочных средств (контрольно-измерительные материалы)
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
им. В.П. Астафьева»

Кафедра-разработчик
Кафедра медико-биологических основ физической культуры и безопасности жизнедеятельности

УТВЕРЖДЕНО
на заседании кафедры
Протокол № 11
от «14» июня 2018 г.
И. о. зав. кафедрой Н.Н. Казакевич

ОДОБРЕНО
на заседании научно-методического совета специальности (направление подготовки) института физической культуры, спорта и здоровья им. И.С. Ярыгина
Протокол №10 от «21» июня 2018г.
Председатель: Бордуков М.И.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации обучающихся
по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

44.03.05 Педагогическое образование (с двумя профилями)
направленность (профиль) образовательной программы
Физическая культура и Безопасность жизнедеятельности

Квалификация (степень) выпускника:
БАКАЛАВР

Составитель _____ доц. каф. МБОФК и БЖ А.А. Кужугет

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ НА

Фонд оценочных средств дисциплины

(для проведения текущего контроля успеваемости и промежуточной аттестации) Информационная безопасность

44.03.05 Педагогическое образование (с двумя профилями) направленность (профиль) образовательной программы Физическая культура и Безопасность жизнедеятельности

Квалификация и степень выпускника - бакалавр

Фонд оценочных средств разработан в соответствии с положением утвержденным приказом ректора № 297 (п) от 28.04.2018 и ориентирован на решение следующих задач: управление процессами приобретения, обучающимися необходимых знаний, умений, навыков и формирования компетенций, определённых в образовательном стандарте по направлению подготовки 44.03.05 Педагогическое образование, достижения результатов освоения образовательной программы, определённой в виде набора компетенций выпускников, оценку достижений обучающихся в процессе изучения дисциплины «Информационная безопасность» с определением положительных результатов обучения задачам будущей профессиональной деятельности через совершенствование комплекса традиционных и инновационных методов обучения.

Фонд оценочных средств включает перечень компетенций с указанием этапов их формирования в процессе изучения основ научной деятельности студента, этапы формирования и оценивания компетенций, учебно-методическое и информационное обеспечение фондов оценочных средств, выступление на семинаре, выполнение заданий практической работы, собеседование.

Перечисленные выше задания позволяют автору ФОС выявлять уровень освоения формируемых компетенций, таких как способностью использовать естественнонаучные и математические

знания для ориентирования в современном информационном пространстве, готовностью реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов. Задания способствуют пониманию и освоению теоретического содержания, направлены на получение практического опыта.

В целом фонд оценочных средств по курсу «Информационная безопасность» соответствует требованиям, предъявляемым к данному типу учебно-методических материалов и может быть использован при организации образовательного процесса по направлению подготовки 44.03.05 Педагогическое образование.

Заместитель директора по
учебно- воспитательной работе
МБОУ «СОШ № 10 с углубленным
изучением отдельных предметов имени
академика Ю. А. Овчинникова»
Васильева Т.И.

1. Назначение фонда оценочных средств

1.1. Целью создания фонда оценочных средств по дисциплине «Информационная безопасность» является установление соответствия учебных достижений запланированным результатом обучения и требования основной профессиональной программы дисциплины.

1.2. ФОС по дисциплине решает задачи:

- контроль и управление процессом приобретения студентами необходимых знаний, умений, навыков и уровня сформированности компетенции, определѐнных в ФГОС ВО по направлению подготовки 44.03.01 – Педагогическое образование;
- контроль (с помощью набора оценочных средств) и управление (с помощью элементов обратной связи) достижением целей реализации ОП, определенных в виде набора компетенций выпускников;
- обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс Университета.

1.3. Фонд оценочных средств разработан в соответствии с нормативными документами:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями образования) (уровень бакалавриата).
- Образовательной программы высшего образования по направлению подготовки 44.03.05 Педагогическое образование по профилям физическая культура и безопасность жизнедеятельности, уровень бакалавриата.
- Положения о формировании фонда оценочных средств для текущего контроля успеваемости, промежуточной и итоговой аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, программам подготовки научно-педагогических кадров в аспирантуре в федеральном государственном бюджетном образовательном учреждении высшего образования «Красноярский государственный педагогический университет им. В.П. Астафьева» и его филиалах.
- Федеральный закон от 29.12.2012 № 273–ФЗ «Об образовании в Российской Федерации».
- Приказ Минтруда России № 544н от 18 октября 2013 г. «Об утверждении профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального

общего, основного общего, среднего общего образования) (воспитатель, учитель)».

2. Перечень компетенций с указанием этапов их формирования в процессе изучения дисциплины.

2.1. **Перечень компетенций,** формируемых в процессе изучения дисциплины:

- способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве (ОК-3);
- готовностью реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов (ПК-1).
- способностью использовать современные методы и технологии обучения и диагностики (ПК-2).

2.2. Этапы формирования и оценивания компетенций.

Компетенции	Этап формирования компетенции	Дисциплины, участвующие в формировании компетенции	Тип контроля	Оценочное средство/КИМы	
				№	Форма
ОК-3 способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	ориентировочный	Безопасность жизнедеятельности, Теоретические основы безопасности человека, Основы обороны государства	Текущий контроль	1	Опрос
	когнитивный	Безопасность жизнедеятельности, Теоретические основы безопасности человека, Основы обороны государства	Текущий контроль	2	Опрос Доклады

	праксиологический	Безопасность жизнедеятельности, Теоретические основы безопасности человека, Основы обороны государства	Промежуточная аттестация	3	Устные сообщения Защита рефератов
	рефлексивно-оценочный	Безопасность жизнедеятельности, Теоретические основы безопасности человека, Основы обороны государства	Промежуточная аттестация	4	Устные сообщения Защита рефератов
ПК-1 – готовность реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов.	ориентировочный	Теория и методика обучения ФК, Теория и методика обучения БЖ.	Текущий контроль	1	Опрос
	когнитивный	Теория и методика обучения ФК, Теория и методика обучения БЖ.	Текущий контроль	2	Опрос Доклады
	праксиологический	Теория и методика обучения ФК, Теория и методика обучения БЖ, Педагогическая практика	Промежуточная аттестация	3	Устные сообщения Защита рефератов
	рефлексивно-оценочный	Теория и методика обучения ФК, Теория и методика обучения БЖ, Педагогическая практика	Промежуточная аттестация	4	Устные сообщения Защита рефератов
ПК2 способностью использовать	ориентировочный	Теория и методика обучения ФК, Теория и	Текущий контроль	1	Опрос

современные методы и технологии обучения и диагностики		методика обучения БЖ.			
	когнитивный	Теория и методика обучения ФК, Теория и методика обучения БЖ.	Текущий контроль	2	Опрос Доклады
	праксиологический	Теория и методика обучения ФК, Теория и методика обучения БЖ, Педагогическая практика	Промежуточная аттестация	3	Устные сообщения Защита рефератов
	рефлексивно-оценочный	Теория и методика обучения ФК, Теория и методика обучения БЖ, Педагогическая практика	Промежуточная аттестация	4	Устные сообщения Защита рефератов

1. **Фонд оценочных средств для промежуточной аттестации**
   3.1. Фонды оценочных средств включают: вопросы к экзамену.
   3.2. Оценочные средства
   3.2.1. Критерии оценивания по оценочному средству **1** – **вопросы к зачету**, разработчик

Формируемые компетенции	Высокий уровень сформированности компетенций	Продвинутый уровень сформированности компетенций	Базовый уровень сформированности компетенций
	(87-100 баллов) отлично/зачтено	(73-86 баллов) хорошо/зачтено	(60-72 баллов) удовлетворительно/зачтено
ОК-3 способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	Обучающийся знает этиология возникновения данной проблемы, и результат, содержащий полный правильный ответ, полностью соответствующий требованиям критерия.	Обучающийся знает основные положения организации информационной безопасности. Способен использовать нормативно-правовые документы в своей профессиональн	Обучающийся знает основные положения организации информационной безопасности.

	Обучающийся владеет терминами науки, излагается литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента	ой деятельности.	
ПК-1 – готовность реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов.	Обучающийся на высоком уровне готов использовать знания по дисциплине для реализации образовательной программу по ОБЖ в соответствии с требованиями образовательных стандартов.	Обучающийся на среднем уровне готов использовать знания по дисциплине для реализации образовательной программу по ОБЖ в соответствии с требованиями образовательных стандартов.	Обучающийся на удовлетворительном уровне готов использовать знания по дисциплине для реализации образовательной программу по ОБЖ в соответствии с требованиями образовательных стандартов.

*Менее 60 баллов компетенция не сформирована.

4. Фонды оценочных средств для текущего контроля успеваемости

4.1. Фонд оценочных средств включают: устный опрос, тесты, доклады. Разработчик

4.2.1. Критерии оценивания по оценочному средству **1** – **устный опрос.**

Критерии оценивания	Количество баллов (вклад в рейтинг)
Посещение занятий	1
Знает теоретическое содержание разделов предмета	2
Четко, последовательно излагает учебный материал	1
Отвечает на заданные вопросы	1
Максимальный балл	5

4.2.2. Критерии оценивания по оценочному средству **2** – **тесты**

Критерии оценивания	Количество баллов (вклад в рейтинг)
Посещение занятий	1
Правильных ответов 90-100%	5
Правильных ответов 70-89%	4
Правильных ответов 60-69%	3
Правильных ответов менее 60%	1-2
Максимальный балл	6

4.2.3. Критерии оценивания по оценочному средству **3** – доклад.

Критерии оценивания	Количество баллов (вклад в рейтинг)
Полный ответ в соответствии с темой	2
Отвечает на заданные вопросы	2
Максимальный балл	4

5. **Учебно-методическое и информационное обеспечение фонда оценочных средств** (литература; методические указания, рекомендации, программное обеспечение и другие материалы, использованные для разработки ФОС).

5.1. Литература:

1. Анин Б.Ю. Защита компьютерной информации. –СПб.: БХВ - Петербург, 2000.-384 с.
2. Шкерина Л.В. Измерение и оценивание уровня сформированности профессиональных компетенций студентов – будущих учителей математики: учебное пособие; Краснояр. гос. пед. ун-т им. В. П. Астафьева. Красноярск, 2014. – 136 с.
3. Цирлов В.Л. Основы информационной безопасности автоматизированных систем -Феникс 2008 г
4. Мэйволд Эрик Безопасность сетей Конспект лекций (www.intuit.ru)

6. **Оценочные средства (контрольно-измерительные материалы) для промежуточной аттестации**

Вопросы к экзамену

1. Правовое регулирование в области безопасности информации:

2. законодательная база информатизации общества; структура государственных органов, обеспечивающих безопасность информационных технологий.
3. Информационная безопасность. Основные определения
4. Угрозы информационной безопасности. Модель системы зашиты.
5. Организационные меры и меры обеспечения физической безопасности.
6. Идентификация и аутентификация. Методы аутентификации.
7. Особенности парольных систем аутентификации: рекомендации по практической реализации парольных систем, оценка стойкости парольных систем, методы хранения паролей.
8. Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности информации.
9. Методы зашиты внешнего периметра.
10. Протоколирование и аудит.
11. Построение систем защиты от угроз нарушения целостности: типовая структура такой системы.
12. Криптографические методы обеспечения целостности информации: реализация механизма цифровой подписи, криптографические хэш-функции и ее преимущества, коды проверки подлинности.
13. Структура системы защиты от угроз нарушения доступности: поясните основные составляющие.
14. Формальные модели управления доступом: модель Харрисона - Руззо-Ульмана, модель Беллл-ЛаПалулы.
15. Критерии оценки безопасности информационных технологий. Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002.
16. Структура профиля защиты в соответствии с ГОСТ Р ИСО/МЭК 15408-2002
17. Основные положения ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"
18. Основные положения ГОСТ Р ИСО/МЭК 270012006 "Информационная технология. Методы и средства обеспечения безопасности.
19. Методика анализа рисков в сфере информационной безопасности CRAMM.
20. Методика анализа рисков в сфере информационной безопасности FRAP.
21. Методика анализа рисков в сфере информационной безопасности OCTAVE
22. Проведение оценки рисков в соответствии с методикой Microsoft.

7. Оценочные средства для текущего контроля успеваемости

Контрольные задания

Вариант №1

1. Свойства информации в форме сообщения:
(укажите правильный вариант)

a. идеальность
b. субъективность
c. информационная неуничтожаемость
d. динамичность
e. материальность
f. накапливаемость

2. Свойства информации в форме сведений: (укажите правильный вариант)

a. материальность
b. измеримость
c. сложность
d. проблемная ориентированность
e. накапливаемость

3. Информационная сфера – это … , … , … , … .
4. Первая классификация национальных интересов:
   a. интересы …
   b. интересы …
   c. интересы …
5. Общие методы обеспечения информационной безопасности:
   a. …
   b. …
   c. …
6. Информация – наиболее ценный … современного общества.
7. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?
   a. Документы
   b. Персонал
   c. Организационные единицы
   d. Промышленные образцы
   e. Научный инструментарий
8. Поставьте в порядке важности национальные интересы:
   a. **Информационное обеспечение государственной политики Российской Федерации.**
   b. **Развитие современных информационных технологий, отечественной индустрии информации.**
   c. **Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.**
   d. **Защита информационных ресурсов от несанкционированного доступа.**

9. Допишите различные подходы к понятию информации:
   a. информация …
   b. информация …
   c. … информация
10. Составляющие национальной безопасности:
    a. …
    b. …
    c. …
    d. …
    e. …
    f. …
    g. …
    h. …
11. Общие методы обеспечения национальной безопасности:
    a. …
    b. …
    c. …
12. Основные объекты воздействия в информационной войне?
    a. …
    b. …

c. …
d. …
e. …

13. Перечислите информационное оружие:
    a. …
    b. … средства
    c. … генераторы
    d. средства …
    e. средства …
14. Война, есть продолжение … другими, насильственными средствами.
15. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов … , … , … .

Вариант №2

1. Допишите различные подходы к понятию информации:
    a. информация …
    b. информация …
    c. … информация
2. Составляющие национальной безопасности:
    a. … b. … c. … d. …
    e. … f. … g. …
3. Информация – наиболее ценный … современного общества.
4. Поставьте в порядке важности национальные интересы:
    a. Информационное обеспечение государственной политики Российской Федерации.
    b. Развитие современных информационных технологий, отечественной индустрии информации.
    c. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.
    d. Защита информационных ресурсов от несанкционированного доступа
5. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?
    a. Документы
    b. Персонал
    c. Организационные единицы
    d. Промышленные образцы
    e. Научный инструментарий
6. Война, есть продолжение … другими, насильственными средствами.
7. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов … , … , … .
8. Перечислите информационное оружие:
    a. …
    b. … средства
    c. … генераторы
    d. средства …
    e. средства …
9. Информационная сфера – это … , … , … , … .
10. Первая классификация национальных интересов:
    a. интересы …
    b. интересы …
    c. интересы …

11. Общие методы обеспечения информационной безопасности:

d. … b. … c. …

12. Общие методы обеспечения национальной безопасности:

a. …
b. …
c. …

13. Основные объекты воздействия в информационной войне?

a. … b. … c. … d. … e. …

14. Свойства информации в форме сведений: (укажите правильный вариант)

a. материальность
b. измеримость
c. сложность
d. проблемная ориентированность
e. накапливаемость

15. Свойства информации в форме сообщения:
(укажите правильный вариант)

g. субъективность
h. информационная неуничтожаемость
i. динамичность
j. материальность
k. накапливаемость

Вариант №3

1. Какой метод обеспечения информационной безопасности отсутствует в перечне :

a. Организационный b. Правовой c. Технический
d. Экономический e. Идеологический

2. Совокупность информации, информационной инфраструктуры, субъектов и системы регулирования общественных отношений являются составляющими частями … … .

3. Автономная информация – информация , существующая … от какого-либо субъекта.

4. Информационная сфера – являясь системообразующим фактором жизни общества, активно влияет на сосояние … , … , … и др. составляющих безопасности Российской Федерации.

5. Информация взаимодействия - … одного субъекта на другого, имеющее целью …, моделей внешней среды двух субъектов или коллектива.

6. Информация воздействия - … знания, … модели окружающего мира.

7. Информационная безопасность - … защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью … интересов личности, общества и государства.

8. Составляющие национальной безопасности:

a. соблюдение … Российской Федерации.
b. Правовое … всех участников процесса информационного взаимодействия.
c. Соблюдение … прав и свобод человека и гражданина в области получения информации и пользования ею.
d. Приоритетное … отечественных современных информационных и телекоммуникационных технологий

9. Общая схема национальной безопасности:

a. Формулировка …

b. Формирование перчня …
c. Оценка … и …
d. Разработка …
e. Принятие …

10. Для информационной войны обычно четко определена … … .

11. Вторая классификация национальных интересов:

a. по принадлежности интересов
b. по важности интересов
c. по национальным признакам
d. по экономическим признакам

12. Классификация информации как объекта исследования:

f. … информация
g. информация…
h. информация…

13. Программные продукты являются следующей составляющей информационных ресурсов (выберите правильный вариант):

a. документы
b. персонал
c. организационные интересы
d. промышленные образцы
e. научный инструментарий

14. Свойства информации в форме сообщения:
(укажите правильный вариант)

a. идеальность
c. динамичность
f. информационная неуничтожаемость
b. субъективность
d. накапливаемость
g. измеримость

15. Свойства информации в форме сведений: (укажите правильный вариант)

a. материальность
b. динамичность
c. проблемная ориентированность
a. измеримость
e. сложность

Вариант №4

1. Информация – наиболее ценный … современного общества.
2. Поставьте в порядке важности национальные интересы:
   a. Информационное обеспечение государственной политики Российской Федерации.
   b. Развитие современных информационных технологий, отечественной индустрии информации.
   c. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.
   d. Защита информационных ресурсов от несанкционированного доступа
3. Допишите различные подходы к понятию информации:
   a. информация …
   b. информация …
   c. … информация
4. Составляющие национальной безопасности:
   a. … b. … c. … d. …
   e. … f. … g. …
5. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?
   a. Документы

b. Персонал
c. Организационные единицы
d. Промышленные образцы
e. Научный инструментарий

6. Перечислите информационное оружие:
a. …
b. … средства
c. … генераторы
d. средства …
e. средства …

7. Война, есть продолжение … другими, насильственными средствами.
8. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов … , … , … .
9. Информационная сфера – это … , … , … , … .
10. Первая классификация национальных интересов:
a. интересы …
b. интересы …
c. интересы …

11. Общие методы обеспечения информационной безопасности:
a. … b. … c. …

12. Свойства информации в форме сообщения:
(укажите правильный вариант)
l. субъективность
m. информационная неуничтожаемость
n. динамичность
o. материальность
p. накапливаемость

13. Общие методы обеспечения национальной безопасности:
d. …
e. …
f. …

14. Основные объекты воздействия в информационной войне?
a. … b. … c. … d. … e. …

15. Свойства информации в форме сведений: (укажите правильный вариант)
a. материальность
b. измеримость
c. сложность
d. проблемная ориентированность
e. накапливаемость

Вариант №5

1. Информационная сфера – это … , … , … , … .
2. Первая классификация национальных интересов:
a. интересы …
b. интересы …
c. интересы …

3. Общие методы обеспечения информационной безопасности:
a. … b. … c. …

4. Свойства информации в форме сообщения: (укажите правильный вариант)
q. субъективность

r. информационная неуничтожаемость
s. динамичность
t. материальность
u. накапливаемость

5. Свойства информации в форме сведений: (укажите правильный вариант)
   a. материальность
   b. измеримость
   c. сложность
   d. проблемная ориентированность
   e. накапливаемость

6. Информация – наиболее ценный … современного общества.

7. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?
   a. Документы
   b. Персонал
   c. Организационные единицы
   d. Промышленные образцы
   e. Научный инструментарий

8. Перечислите информационное оружие:
   a. …
   b. … средства
   c. … генераторы
   d. средства …
   e. средства …

9. Война, есть продолжение … другими, насильственными средствами.

10. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов … , … , … .

11. Поставьте в порядке важности национальные интересы:
   a. Информационное обеспечение государственной политики Российской Федерации.
   b. Развитие современных информационных технологий, отечественной индустрии информации.
   c. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.
   d. Защита информационных ресурсов от несанкционированного доступа

12. Допишите различные подходы к понятию информации:
   a. информация …
   b. информация …
   c. … информация

13. Составляющие национальной безопасности:
   a. … b. … c. … d. …
   e. … f. … g. …

14. Общие методы обеспечения национальной безопасности:
   a. …
   b. …
   c. …

15. Основные объекты воздействия в информационной войне?
   a. … b. … c. … d. … e. …

Вариант №6

1. Составляющие национальной безопасности:
   a. соблюдение … Российской Федерации.
   b. Правовое … всех участников процесса информационного взаимодействия.
   c. Соблюдение … прав и свобод человека и гражданина в области получения информации и пользования ею.
   d. Приоритетное … отечественных современных информационных и телекоммуникационных технологий

2. Для информационной войны обычно четко определена … … .

3. Какой метод обеспечения информационной безопасности отсутствует в перечне :

1 Организационный 3 Правовой 5 Технический
2 Экономический 4 Идеологический

4. Информация воздействия - … знания, … модели окружающего мира.

5. Совокупность информации, информационной инфраструктуры, субъектов и системы регулирования общественных отношений являются составляющими частями … … .

6. Автономная информация – информация , существующая … от какого-либо субъекта.

7. Информационная сфера – являясь системообразующим фактором жизни общества, активно влияет на сосояние … , … , … и др. составляющих безопасности Российской Федерации.

8. Информация взаимодействия - … одного субъекта на другого, имеющее целью …, моделей внешней среды двух субъектов или коллектива.

9. Информационная безопасность - … защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью … интересов личности, общества и государства.

10. Общая схема национальной безопасности:
   a. Формулировка …
   b. Формирование перечня …
   c. Оценка … и …
   d. Разработка …
   e. Принятие …

11. Вторая классификация национальных интересов:

1. по принадлежности интересов 2. по важности интересов
3. по национальным признакам 4. по экономическим признакам

12. Классификация информации как объекта исследования:
   a. … информация
   b. информация…
   c. информация…

13. Программные продукты являются следующей составляющей информационных ресурсов (выберите правильный вариант):

1. документы 2. персонал 3. организационные интересы
4. промышленные образцы 5. научный инструментарий

14. Свойства информации в форме сообщения:
(укажите правильный вариант)

1. идеальность 2. динамичность 3. информационная неуничтожаемость
4. субъективность 5. накапливаемость 6. измеримость

15. Свойства информации в форме сведений: (укажите правильный вариант)

1. материальность
2. динамичность
3. с. проблемная ориентированность
4. измеримость
5. е. сложность

7.1. Тематика докладов

1. Формы психологической защиты человека от информационной перегрузки.
2. Социально вредная информация в СМИ.
3. Вредная и опасная информация в Интернет.
4. Формы и методы недобросовестной рекламной деятельности.
5. Формы обмана и мошенничества в Интернет.
6. Атаки на информационные системы путем перегрузки каналов связи и входных буферов памяти. Использование «протоколов вежливости» для реализации сетевых атак.
7. Способы подделки компьютерной информации (денег, документов, доказательств) и программный инструментарий.
8. Компьютерное «пиратство» и его формы. Перспективы противодействия незаконному копированию компьютерной информации.
9. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.
10. Формы и методы диверсионно-террористической деятельности с использованием современных информационных технологий.
11. Виды и формы применения информационно-технологического оружия.
12. Доктрина информационной безопасности России и реальности ее осуществления.
13. Анализ способов информационного воздействия и форм информационной защиты, отраженных в сказках, сказаниях, былинах и мифах.
14. Государственная система защиты граждан и общества от опасной информации (законодательство и практика).
15. Вопросы информационной безопасности в теории военного искусства.
16. Вопросы информационной безопасности в политике и дипломатии.
17. Формы и методы выживания биологических особей и возможности их применения при защите информации.
18. Стратегия пассивной информационной защиты.
19. Стратегия уничтожения источника угроз в сфере информационной защиты.
20. Стратегия обмана и ее использование в сфере информационной защиты.
21. Модель комплексной информационной защиты и ее элементы.
22. Модель информационной защиты каналов связи.
23. Угрозы скрытого информационного воздействия на пользователей Интернет.
24. Формы и методы защиты признаковой информации.
25. Информация как ценность и объект преступных посягательств.
26. Угрозы конфиденциальности и формы их реализации.
27. Модель информационного нарушителя, посягающего на конфиденциальную информацию методами несанкционированного доступа.
29. Задачи информационной защиты в финансовой сфере.

30.Задачи информационной защиты в сфере предоставление услуг связи.

31.Организационно-распорядительные меры информационной защиты.

32.Традиционные направления информационной защиты и пути их интеграции.

5.2. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Международные стандарты информационного обмена.
2. Понятие угрозы.
3. Информационная безопасность в условиях функционирования в России глобальных сетей.
4. Виды противников или «нарушителей».
5. Понятия о видах вирусов.
6. Три вида возможных нарушений информационной системы. Защита.
7. Основные нормативные руководящие документы. Стандарт шифрования данных ГОСТ 28147-89
8. Системы с открытым ключом
9. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
10. Основные положения теории информационной безопасности информационных систем.
11. Модели безопасности и их применение.
12. Методы защиты информации с использованием голографии являются актуальным и развивающимся направлением
13. Анализ способов нарушений информационной безопасности.
14. Криптографические методы
15. Использование защищенных компьютерных систем.
16. Методы криптографии.
17. Основные технологии построения защищенных ЭИС.
18. Концепция информационной безопасности

5.3. ПРИМЕРНАЯ ТЕМАТИКА РЕФЕРАТОВ, КУРСОВЫХ РАБОТ

1. Формы психологической защиты человека от информационной перегрузки.

2. Социально вредная информация в СМИ.

3. Вредная и опасная информация в Интернет.

4. Формы и методы недобросовестной рекламной деятельности.

5. Формы обмана и мошенничества в Интернет.

6. Атаки на информационные системы путем перегрузки каналов связи и входных буферов памяти. Использование «протоколов вежливости» для реализации сетевых атак.

7. Способы подделки компьютерной информации (денег, документов, доказательств) и программный инструментарий.

8. Компьютерное «пиратство» и его формы. Перспективы противодействия незаконному копированию компьютерной информации.

9. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.

10.Формы и методы диверсионно-террористической деятельности с использованием современных информационных технологий.

11.Виды и формы применения информационно-технологического оружия.

12.Доктрина информационной безопасности России и реальности ее осуществления.

13.Анализ способов информационного воздействия и форм информационной защиты, отраженных в сказках, сказаниях, былинах и мифах.

14.Государственная система защиты граждан и общества от опасной информации (законодательство и практика).

15.Вопросы информационной безопасности в теории военного искусства.

16.Вопросы информационной безопасности в политике и дипломатии.

17.Формы и методы выживания биологических особей и возможности их применения при защите информации.

18.Стратегия пассивной информационной защиты.

19.Стратегия уничтожения источника угроз в сфере информационной защиты.

20.Стратегия обмана и ее использование в сфере информационной защиты.

21.Модель комплексной информационной защиты и ее элементы.

22.Модель информационной защиты каналов связи.

23.Угрозы скрытого информационного воздействия на пользователей Интернет.

24.Формы и методы защиты признаковой информации.

25.Информация как ценность и объект преступных посягательств.

26.Угрозы конфиденциальности и формы их реализации.

27.Модель информационного нарушителя, посягающего на конфиденциальную информацию методами несанкционированного доступа.

28.Модель компьютерного вирмейкера.

29.Задачи информационной защиты в финансовой сфере.

30.Задачи информационной защиты в сфере предоставление услуг связи.

31.Организационно-распорядительные меры информационной защиты.

32.Традиционные направления информационной защиты и пути их интеграции.

Требования к оформлению рефератов:

форматирование:

- Word for Windows и выше;
- формат А4;
- шрифт Times New Roman;
- кегль –14;
- сноски, подрисуночные надписи, названия таблиц – кегль 12;
- межстрочный интервал – полуторный;
- встроенные в текст рисунки, графики схемы – черно-белые;
- список литературы размещается после текста, в алфавитном порядке, а в тексте дается ссылка на порядковый номер источника и страницу цитирования (пример: [*3*,121]);
- поля – 2,5 см со всех сторон;
- ориентация – книжная.

Структура:

- название (по центру, буквы – прописные, кегль – 14, полужирный, без переносов и подчеркиваний, без точки в конце названия);
- справа через один интервал прописными буквами фамилия и инициалы автора;
- иллюстративный материал должен быть встроен в текст (функция «объект»).

Лист внесения изменений

Дополнения и изменения рабочей программы на 2018/2019 учебный год

В рабочую программу вносятся следующие изменения:

1. На титульном листе РПД и ФОС изменено название ведомственной принадлежности «Министерство науки и высшего образования» на основании приказа «о внесении изменений в сведения о КГПУ им. В.П. Астафьева» от 15.07.2018 № 457 (п).

2. Обновлен перечень лицензионного программного обеспечения

3. В фонд оценочных средств внесены изменения в соответствии приказом «Об утверждении Положения о фонде оценочных средств для текущего контроля успеваемости, промежуточной и итоговой (государственной итоговой) аттестации» от 28.04.2018 №297 (п)

4. На титульном листе РПД и ФОС изменено название кафедры приказ ректора ФГБОУ ВО «КГПУ им. В. П. Астафьева» №672 (п) от 07. 11.2018г

Учебная программа пересмотрена и одобрена на заседании кафедры

«30» апреля 2019г., протокол № 8

Внесенные изменения утверждаю

Заведующий кафедрой  Н.Н. Казакевич