Министерство просвещения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ульяновский государственный педагогический университет имени И.Н. Ульянова»
(ФГБОУ ВО «УлГПУ им. И.Н. Ульянова»)

Факультет физической культуры и спорта
Кафедра теории и методики физической культуры и безопасности жизнедеятельности

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0233C9D60038B01A9E48C1A3FBB4A9D9F6
Владелец: Титов Сергей Николаевич
Действителен: с 07.07.2023 до 28.04.2038

УТВЕРЖДАЮ
Проректор по учебно-методической работе С.Н. Титов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Программа учебной дисциплины
Предметно-методический модуль по профилю "Безопасность жизнедеятельности"

основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки),

направленность (профиль) образовательной программы
Физическая культура. Безопасность жизнедеятельности

(очная форма обучения)

Составитель: Богданов В.В., к.б.н.
доцент кафедры теории и методики физической культуры и безопасности жизнедеятельности

Рассмотрено и одобрено на заседании ученого совета факультета физической культуры и спорта, протокол от «21» мая 2024 г. №9

Ульяновск, 2024

Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к дисциплинам обязательной части Блока 1 Дисциплины (модули) Предметно-методический модуль по профилю "Безопасность жизнедеятельности" учебного плана основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) направленность (профиль) образовательной программы «Физическая культура. Безопасность жизнедеятельности», очной формы обучения.

Изучаемая дисциплина базируется на теоретические знания, умения и виды деятельности, сформированные в процессе изучения школьного курса «Основы безопасности жизнедеятельности», дает возможность существенно расширить умения и навыки для успешной профессиональной работы в области обеспечения личной и общественной безопасности.

Результаты изучения дисциплины являются основой для изучения дисциплин и прохождения практик: Технологии цифрового образования, Безопасность жизнедеятельности, Социальные опасности, профилактика и защита от них, Ознакомительная практика по безопасности жизнедеятельности, Технологическая (проектно-технологическая) практика (социально-экологическое проектирование), Предметно-содержательная практика по безопасности жизнедеятельности, Педагогическая практика по безопасности жизнедеятельности.

1. Перечень планируемых результатов обучения (образовательных результатов) по дисциплине

Целью освоения дисциплины «Информационная безопасность» является: - формирование профессиональных навыков, умений, необходимых будущему учителю для успешного решения основных задач в области организации и обеспечения безопасности различного рода образовательных организаций.

Задачей освоения дисциплины является формирование у студента целостного представления об основных этапах становления современной системы обеспечения информационной безопасности, ее структуре, об основных категориях, понятиях и методах, о роли и месте обеспечения информационной безопасности в профессиональной подготовке учителя, сформировать готовность будущего учителя к эффективному преподаванию пропедевтического, базового и профильных курсов по предмету.

В результате освоения программы бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине «Информационная безопасность» (в таблице представлено соотнесение образовательных результатов обучения по дисциплине с индикаторами достижения компетенций):

Компетенция и индикаторы ее достижения в дисциплине	Образовательные результаты дисциплины (этапы формирования дисциплины)		
	знает	умеет	владеет
ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативно-правовыми актами в сфере образования и нормами профессиональной этики ОПК-1.1. Понимает и объясняет сущность приоритетных направлений развития образовательной системы РФ, законов и иных нормативно-правовых актов,	ОР-1 основные нормативно-правовые акты в сфере образования и нормы профессиональной этики;	ОР-2 применять законы и иные нормативно-правовые акты, регламентирующие образовательную деятельность в Российской	

регламентирующих образовательную деятельность в РФ, нормативных документов по вопросам обучения и воспитания детей и молодежи, федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального обучения, законодательства о правах ребенка, трудового законодательства.		Федерации, нормативные документы по вопросам обучения и воспитания детей и молодежи, федеральные государственные образовательные стандарты дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального обучения, законодательство о правах ребенка, трудовое законодательство и нормы профессиональной этики	
ОПК-1.2. Применяет в своей деятельности основные нормативно-правовые акты в сфере образования и нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности.	ОР-3 сущность приоритетных направлений развития образовательной системы Российской Федерации; основные нормативно-правовые акты в сфере образования и нормы профессиональной этики	ОР-4 применять законы и иные нормативно-правовые акты, регламентирующие образовательную деятельность в Российской Федерации, нормативные документы по вопросам обучения и воспитания детей и молодежи, законодательство о правах ребенка, трудовое законодательство и нормы профессиональной этики; анализировать судебную практику	
ПК-1 Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач			
ПК-1.1 Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).	ОР-5 структуру, состав и дидактические единицы содержания преподаваемого предмета; традиционные и современные методы, средства и формы организации учебного процесса;	ОР-6 осуществлять отбор учебного содержания для его реализации в соответствии с требованиями ФГОС ОО;	
ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.			
ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий,	ОР-7 роль и место предметной области (преподаваемого предмета)	ОР-8 дидактические возможности современных технологий обучения, в	

применять методы, приемы и технологии обучения, в том числе информационные.	в общей картине научного знания	том числе информационных	

2. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Номер семестра	Всего		Учебные занятия						Форма промежуточной аттестации
	Трудоемк.		Лекции, час.	Практические занятия, час.	в т. ч. практическая подготовка, час.	Лабораторные занятия, час.	в т. ч. практическая подготовка, час.	Самостоят. работа, час.	
	Зач. ед.	Часы							
1	3	108	18	30	2	-	-	33	экзамен (27)
Итого:	3	108	18	30	2	-	-	33	-

3. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

3.1. Указание тем (разделов) и отведенного на них количества академических часов и видов учебных занятий

Наименование раздела и тем	Количество часов по формам организации			
	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа
1 семестр				
Тема 1.Информационная безопасность, ее место в системе безопасности РФ. Концепция информационной безопасности.	2	2		3
Тема 2. Основы государственной политики обеспечения информационной безопасности. Законодательство РФ в области обеспечения информационной безопасности.	2	2		3
Тема 3. Сведения, отнесенные к государственной, служебной и коммерческой тайне. Обеспечение сохранения коммерческой тайны предприятия	2	2		3
Тема 4. Инженерно-техническая защита информации	2	2		3
Тема 5. Методы и средства защиты электронной информации	2	2		3
Тема 6. Аудит информационной безопасности предприятия	2	4		3
Тема 7. Защита интеллектуальной собственности	2	4		3
Тема 8. Международная деятельность по обеспечению информационной безопасности. Конфиденциальность при работе с зарубежными партнерами		4		4

Тема 9. Социально-политические манипуляции с личностью и механизмы защиты. Формы и методы информационной агрессии. Информационные войны.	2	4		4
Тема 10. Негативные последствия глобальной информатизации общества. Информационные технологии и здоровье.	2	4		4
ИТОГО:	18	30		33

3.2. Краткое описание содержания тем (разделов) дисциплины

Тема 1. **Информационная безопасность, ее место в системе безопасности РФ. Концепция информационной безопасности.**

Понятия и место информационной безопасности в системе безопасности РФ. Основные элементы организационной основы системы обеспечения информационной безопасности РФ. Основные концептуальные положения системы защиты информации. Действия, приводящие к неправомерному овладению конфиденциальной информацией.

Интерактивная форма: «Групповое обсуждение».

Тема 2 **Основы государственной политики обеспечения информационной безопасности. Законодательство РФ в области обеспечения информационной безопасности.**

Доктрина информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз информационной безопасности РФ. Внутренние и внешние источники угроз информационной безопасности. Основные методы обеспечения информационной безопасности РФ. Особенности обеспечения информационной безопасности в различных сферах общественной жизни: в экономике, внутренней и внешней политике, в области науки и техники, в сфере духовной жизни. Основные направления обеспечения информационной безопасности РФ в общегосударственных и телекоммуникационных системах, в правоохранительных и судебных сферах. Основные положения государственной политики обеспечения информационной безопасности РФ. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ. Организационная основа системы обеспечения информационной безопасности РФ. Правовая защита информации Понятие права. Структура законодательства РФ в области защиты информации. Закон «Об информации, информатизации и защите информации». Закон «О правовой охране программ для ЭВМ и БД». Конфиденциальная информация. Основные понятия об информации с ограниченным доступом. Нормативно-правовые акты, разрабатываемые на предприятии. Взаимосвязь патентов и коммерческой тайны. Организационно-правовые формы защиты коммерческой тайны.

Интерактивная форма: «Групповое обсуждение».

Тема 3 **Сведения, отнесенные к государственной, служебной и коммерческой тайне. Обеспечение сохранения коммерческой тайны предприятия**

Характеристика сведений, отнесенных к государственной тайне. Определение и характеристики сведений, отнесенных к государственной тайне: в военной области, во внешнеполитической и внешнеэкономической деятельности. Сведения в области разведывательной, контрразведывательной оперативно-розыскной деятельности, отнесенные к государственной тайне. Сведения, отнесенные к служебной тайне. Характер сведений, отнесенных к служебной тайне. Меры, принимаемые к обеспечению сохранности сведений. Характеристика сведений, отнесенных к коммерческой тайне. Порядок определения сведений, относящихся к коммерческой тайне предприятия, и сроков ее действия. Порядок работы со сведениями, содержащими коммерческую тайну. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну предприятия. Порядок работы с документами с грифом «КТ». Обеспечение сохранности документов, дел и изданий. Обязанности лиц, допущенных к сведениям, составляющим

коммерческую тайну предприятия. Ответственность за разглашение, утрату документов, содержащих коммерческую тайну.

Интерактивная форма: «Дискуссия».

Тема 4. **Инженерно-техническая защита информации**

Определение основных мер, направленных на обеспечение информационной информации. Предупреждение, выявление, обнаружение и ликвидация угроз. Цели защиты информации. Защитные действия от неправомерного овладения конфиденциальной информацией. Мероприятия по защите информации. Организационные, организационно-технические и технические мероприятия по защите информации. Характеристика защитных действий. Классификация защитных действий. Модель информационного контакта. Каналы распространения информации. Способы пресечения разглашения. Понятие утечки информации. Физический путь от источника информации к злоумышленнику. Причины возникновения каналов утечки информации. Классификация технических каналов утечки информации. Структура канала утечки информации. Акустические каналы утечки информации. Визуально-оптические каналы утечки. Классификация электромагнитных каналов утечки информации. Источники электромагнитных каналов утечки. Материально-вещественные каналы утечки.

Интерактивная форма: «Дискуссия».

Тема 5. **Методы и средства защиты электронной информации**

Особенности защиты информации от утечки по техническим каналам. Организационные меры защиты информации от утечки за счет электромагнитного излучения. Защита от утечки за счет взаимного влияния поводов и линий связи. Защита от утечки в оптоволоконных линиях и системах связи. Защита информации от утечки по визуально-оптическим каналам. Средства и способы защиты информации от утечки по визуально-оптическим каналам. Защита информации от утечки по акустическим каналам. Основные мероприятия по защите. Средства и способы защиты. Защита информации по электромагнитным каналам. Электромагнитные каналы утечки и методы защиты. Конструкторские и технологические мероприятия по локализации возможности образования условий возникновения каналов утечки за счет побочных электромагнитных излучений и наводок. Защиты от утечки за счет микрофонного эффекта. Защита от утечки по линиям связи от утечки за счет электромагнитного излучения. Разработка информационных систем, технологий и средств их обеспечения. Требования к информационным системам. Порядок развития направлений информатизации и их финансирования. Аппаратные средства защиты. Требования к аппаратным средствам. Ограничение права на доступ к электронной информации. Защита от несанкционированного доступа и копирования электронных баз данных. Программные средства защиты.Основные направления использования программных средств защиты. Разновидности специальных программ. Обеспечение особого контроля доступа к файлам. Процедура идентификации посредством программных средств. Управление доступом. Защита от копирования и разрушения информации. Защита электронной почты. Вредоносное программное обеспечение. Механизмы распространения вредоносного программного обеспечения. Борьба со спамом и вирусами. Основные методы и средства защиты от атак на электронную переписку. Криптографические средства защиты. Краткие сведения о криптографии. Общая технология шифрования. Технология шифрования речи.

Интерактивная форма: «Круглый стол».

Тема **6. Аудит информационной безопасности предприятия.**

Проведение аудита информационной безопасности. Аудит информационной безопасности как проверка состояния степени защиты информации. Задачи аудита. Основные направления деятельности в области аудита безопасности информации. Аудит выделенных помещений. Этапы аудита помещений. Специальное оборудование и технические средства. Структура плана аудита помещений. Этапы непосредственного

проведения аудита. Особенности проверки телефонных каналов. Средства обнаружения несанкционированных средств съема информации в ПЭВМ. Подготовка акта по итогам проведения комплексной проверки помещений.

Интерактивная форма: «Case-study (анализ конкретных ситуаций)».

Тема 7. **Защита интеллектуальной собственности.**

Понятие интеллектуальной собственности. Характеристика объектов и информации, подпадающих под определение интеллектуальной собственности. Законодательство в области авторского права. Мероприятия по защите интеллектуальной собственности. Организационные и технические мероприятия по защите интеллектуальной собственности.

Интерактивная форма: «Круглый стол».

Тема 8. **Международная деятельность по обеспечению информационной безопасности. Конфиденциальность при работе с зарубежными партнерами**

Направления взаимодействия с зарубежными партнерами. Научно-техническое сотрудничество с зарубежными партнерами. Возможные экономические потери при заключении контрактов и причины потерь. Составление соглашений (договоров) о сотрудничестве. Отражение вопросов защиты интеллектуальной собственности. Интеллектуальная собственность в договорах подряда. Распределение прав на результаты работ. Научно-техническое сотрудничество, технологический обмен и его регулирование. Результаты научно-технической деятельности как специфический товар. Особенности рынка технологий. Пути технологического обмена информацией. Коммерческий и некоммерческий варианты обмена информацией. Особенности коммерческих международных операций. Характеристики основных коммерческих операций. Операции по торговле научно-техническими знаниями (опытом). Операции по торговле техническими услугами (инжиниринг). Виды инжиниринга. Конфиденциальность при заключении договоров. Научно-техническая документация – источник конфиденциальной информации. Виды научно-технической документации. Критерии оценки. Возможные условия разглашения сведений, составляющих коммерческую тайну. Экспертиза ценности передаваемой научно-технической документации. Организация работы с зарубежными партнерами. Оценка потенциальных партнеров. Прием иностранных представителей и проведение коммерческих переговоров. Планирование переговоров. Подготовка и ведение переговоров. Информация, представляющая интерес при проведении переговоров. Особенности при проведении переговоров при продаже «ноу-хау». Особенности передачи информации зарубежному партнеру. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами

Интерактивная форма: «Case-study (анализ конкретных ситуаций)».

Тема 9. **Социально-политические манипуляции с личностью и механизмы защиты. Формы и методы информационной агрессии. Информационные войны.**

Манипуляции как средство воздействия на население. Виды манипуляций. Манипуляция сознанием и поведением. Манипуляции массовым сознанием для достижения поставленных задач с помощью информационных воздействий. Механизмы защиты личности. Человеческий фактор в обеспечении информационной безопасности. Организационно-психологические способы воздействия информацией. Деструктивные религиозные организации и защита от них. Криминальные угрозы и технология защиты. История возникновения информационных войн. Формы и методы ведения информационных войн. Примеры из прошлого и современности. Роль СМИ в информационных войнах.

Интерактивная форма: «Case-study (анализ конкретных ситуаций)».

Тема 10. **Негативные последствия глобальной информатизации общества. Информационные технологии и здоровье.**

Средства массовой информации как инструмент влияния на формирование мировоззрения подрастающего поколения. СМИ, основные характеристики. Способы

воздействия на читателей, слушателей и зрителей через печатные и электронные СМИ. Распространение через интернет информации негативного характера. «Желтая пресса» и ее разлагающая роль в воспитании молодежи. Молодежь как наиболее благоприятный объект информационного воздействия. Примеры негативного влияния СМИ на подрастающее поколения. Использование рекламы для коммерческого продвижения товаров и услуг. Расширение рекламы товаров и услуг. Неблаговидная роль СМИ в продвижении товаров, не имеющих соответствующих сертификатов безопасности. Дестабилизирующее воздействие на человека потока рекламы в электронных СМИ.

Интерактивная форма: «Case-study (анализ конкретных ситуаций)».

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Общий объем самостоятельной работы студентов по дисциплине включает аудиторную и внеаудиторную самостоятельную работу студентов в течение семестра.

Аудиторная самостоятельная работа осуществляется в форме выполнения тестовых заданий по дисциплине. Аудиторная самостоятельная работа обеспечена базой тестовых материалов.

Внеаудиторная самостоятельная работа осуществляется в формах:

- подготовки к устным докладам (мини-выступлениям);
- подготовка к защите реферата;
- подготовка к защите индивидуальных практических работ.

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов является особой формой организации учебного процесса, представляющая собой планируемую, познавательно, организационно и методически направляемую деятельность студентов, ориентированную на достижение конкретного результата, осуществляемую без прямой помощи преподавателя. Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, а также выполнение учебных заданий, подготовку к предстоящим занятиям и экзамену. Она предусматривает, как правило, разработку рефератов, написание докладов, выполнение творческих, индивидуальных заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Тема для такого выступления может быть предложена преподавателем или избрана самим студентом, но материал выступления не должен дублировать лекционный материал. Реферативный материал служит дополнительной информацией для работы на практических занятиях. Основная цель данного вида работы состоит в обучении студентов методам самостоятельной работы с учебным материалом. Для полноты усвоения тем, вынесенных в практические занятия, требуется работа с первоисточниками. Курс предусматривает самостоятельную работу студентов со специальной литературой. Следует отметить, что самостоятельная работа студентов результативна лишь тогда, когда она выполняется систематически, планомерно и целенаправленно.

Задания для самостоятельной работы предусматривают использование необходимых терминов и понятий по проблематике курса. Они нацеливают на практическую работу по применению изучаемого материала, поиск библиографического материала и электронных источников информации, иллюстративных материалов. Задания по самостоятельной работе даются по темам, которые требуют дополнительной проработки.

Общий объем самостоятельной работы студентов по дисциплине включает аудиторную и внеаудиторную самостоятельную работу студентов в течение семестра.

Аудиторная самостоятельная работа осуществляется в форме выполнения тестовых заданий, кейс-задач, письменных проверочных работ по дисциплине. Аудиторная

самостоятельная работа обеспечена базой тестовых материалов, кейс-задач по разделам дисциплины.

Внеаудиторная самостоятельная работа осуществляется в формах:
- подготовки к устным докладам (выступлениям по теме реферата);
- подготовки и защиты итоговой практической работы;

Тематика рефератов

1. Обучение персонала в системе обеспечения информационной безопасности образовательного учреждения.
2. Вопросы защиты информации в Конституции РФ и Уголовном кодексе РФ Закон «Об информации, информатизации и защите информации»
3. Понятие о конфиденциальной информации и коммерческой тайне. Угрозы, действия, приводящие к неправомерному овладению конфиденциальной информацией
4. Инженерно-техническая защита информации
5. Вредоносное программное обеспечение и борьба с ним
6. Типовая схема действий разведывательных органов в отношении дестабилизации хозяйствующего субъекта
7. Основные черты и методы ведения информационной войны, роль СМИ, «Активные мероприятия».
8. Защита интеллектуальной собственности в России, понятие и виды, авторское, смежное и патентное право.

Содержание и защита итоговой практической работы

Каждый студент после выполнения и защиты текущих практических работ готовит фрагмент учебной мультимедийной презентации по заданной теме объемом не менее 10 слайдов – итоговая работа.

а) структура мультимедийной презентации:

- титульный лист;
- оглавление;
- содержание (изложение учебного материала) в виде текстовой, графической информации, аудио и видеоматериалов;
- система самоконтроля и самопроверки;
- словарь терминов;
- использованные источники с краткой аннотацией.

б) критерии оценивания

Студент должен продемонстрировать умения и навыки работы с прикладным программным обеспечением общего и специального назначения.

Примерный перечень тем индивидуальных практических работ:

1. Инженерно-техническая защита информации
2. Физические средства защиты информации
3. Средства контроля доступа
4. Аппаратные средства защита информации
5. Аппаратные средства электронной информации
6. Программные средства защиты электронной информации
7. Средства защиты электронной информации от несанкционированного доступа
8. Защита от копирования и разрушения электронной информации
9. Защита электронной почты
10. Вредоносное программное обеспечение и борьба с ним
11. Основные методы и средства защиты от атак на электронную переписку
12. Криптографические средства защиты

Вопросы для самостоятельного изучения обучающимися (темы мини-выступлений)

1. Защита интеллектуальной собственности

2. Понятие и виды интеллектуальной собственности
3. Авторское право интеллектуальной собственности
4. Смежное право применительно к интеллектуальной собственности
5. Патентное право
6. Защита интеллектуальной собственности в России
7. Национальные интересы РФ в международной сфере
8. Направления взаимодействия с зарубежными партнерами
9. Договора о сотрудничестве в зарубежными партнерами
10. Рынок технологий
11. Особенности коммерческих международных операций
12. Возможные условия разглашения сведений, составляющих коммерческую тайну.
13. Работа с иностранными партнерами в организациях
14. Прием иностранных представителей и проведение коммерческих переговоров
15. Формы работы с зарубежными партнерами

Для самостоятельной подготовки к занятиям по дисциплине рекомендуется использовать учебно-методические материалы:

1. Крылова Ю.А., Морозова М.М. Безопасность жизнедеятельности: сборник тестов и ситуационных задач по подготовке к зачету и итоговому контролю. Учебно - методическое пособие для подготовки бакалавров направления 050100.62 Педагогическое образование. – Ульяновск: ФГБОУ ВО «УлГПУ им. И.Н. Ульянова», 2016 – 100 с.

5. Примерные оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Организация и проведение аттестации студента

ФГОС ВО ориентированы на выработку у бакалавра компетенций – динамического набора знаний, умений, навыков и личностных качеств, которые позволят выпускнику стать конкурентоспособным на рынке труда и успешно профессионально реализовываться.

В процессе оценки бакалавров необходимо используются как традиционные, так и инновационные типы, виды и формы контроля. При этом постепенно традиционные средства совершенствуются в русле компетентностного подхода, а инновационные средства адаптированы для повсеместного применения в российской вузовской практике.

Цель проведения аттестации – проверка освоения образовательной программы дисциплины-практикума через сформированность образовательных результатов.

Промежуточная аттестация осуществляется в конце семестра и завершает изучение дисциплины; помогает оценить крупные совокупности знаний и умений, формирование определенных компетенций.

Оценочными средствами текущего оценивания являются: доклад, тесты по теоретическим вопросам дисциплины, защита практических работ и т.п. Контроль усвоения материала ведется регулярно в течение всего семестра на практических (семинарских, лабораторных) занятиях.

№ п/п	**СРЕДСТВА ОЦЕНИВАНИЯ,** используемые для текущего оценивания показателя формирования компетенции	Образовательные результаты дисциплины
	Оценочные средства для текущей аттестации ОС-1 Устные доклады (мини-выступления) ОС-2 Контрольная работа (тест	ОР-1 основные нормативно-правовые акты в сфере образования и нормы профессиональной этики; ОР-2 применять законы и иные нормативно-правовые акты, регламентирующие образовательную деятельность в Российской Федерации, нормативные

	из 32 вопросов) ОС-3 Отчет о выполнении индивидуального задания ОС-4 Защита реферата	документы по вопросам обучения и воспитания детей и молодежи, федеральные государственные образовательные стандарты дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального обучения, законодательство о правах ребенка, трудовое законодательство и нормы профессиональной этики; ОР-3 сущность приоритетных направлений развития образовательной системы Российской Федерации; основные нормативно-правовые акты в сфере образования и нормы профессиональной этики; ОР-4 применять законы и иные нормативно-правовые акты, регламентирующие образовательную деятельность в Российской Федерации, нормативные документы по вопросам обучения и воспитания детей и молодежи, законодательство о правах ребенка, трудовое законодательство и нормы профессиональной этики; анализировать судебную практику; ОР-5 структуру, состав и дидактические единицы содержания преподаваемого предмета; традиционные и современные методы, средства и формы организации учебного процесса; ОР-6 осуществлять отбор учебного содержания для его реализации в соответствии с требованиями ФГОС ОО; ОР-7 роль и место предметной области (преподаваемого предмета) в общей картине научного знания; ОР-8 дидактические возможности современных технологий обучения, в том числе информационных
	Оценочные средства для промежуточной аттестации зачет (экзамен) ОС-5 Экзамен в форме устного собеседования	

Описание оценочных средств и необходимого оборудования (демонстрационного материала), а так же процедуры и критерии оценивания индикаторов достижения компетенций на различных этапах их формирования в процессе освоения образовательной программы представлены в Фонде оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Информационная безопасность».

Материалы, используемые для текущего контроля успеваемости обучающихся по дисциплине

Пример контрольной работы (тест из 32 вопросов).
Критерии оценивания: за каждый правильный ответ - 1 балл.

1. Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы: ***Выберите несколько из 6 вариантов ответа:***
1) конфиденциальность
2) целостность
3) доступность
4) учет
5) неотрекаемость
6) мобильность

2. Сопоставьте понятия и их определения. ***Укажите соответствие для всех 5 вариантов ответа:***

1) возможность ознакомиться с информацией имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями.
2) возможность внести изменение в информацию должны иметь только те лица, кто на это уполномочен.
3) возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.
4) все значимые действия лица, выполняемые им в рамках, контролирумых системой безопасности, должны быть зафиксированы и проанализированы.
5) лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения.

__ конфиденциальность
__ целостность
__ доступность
__ учет
__ неотрекаемость

3. ... - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности. *Выберите один из 5 вариантов ответа:*
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

4. ... - распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности. *Выберите один из 5 вариантов ответа:*
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

5. ... - обеспечение уверенности в том, что участник процесса обмена информацией определен верно, т.е. действительно является тем, чей идентификатор он предъявил. *Выберите один из 5 вариантов ответа:*
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

6. ... - создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа. *Выберите один из 5 вариантов ответа:*
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

7. ... - формирование профиля прав для конкретного участника процесса информационного обмена из набора правил контроля доступа. ***Выберите один из 5 вариантов ответа:***
1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

8. ... - обеспечение соответствия возможных потерь от нарушения информационной безопасности затратам на их построение. *Выберите один из 5 вариантов ответа:*
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

9. ... - поддержание среды информационного обмена в минимально допустимом работоспособном состоянии и соответствии требованиям информационной безопасности в условиях деструктивны внешних или внутренних воздействий.
Выберите один из 5 вариантов ответа:
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

10. ... - совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности.
Выберите один из 5 вариантов ответа:
1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

11. Перечислите основные направления информационной безопасности. ***Выберите несколько из 4 вариантов ответа:***
1) Физическая безопасность
2) Компьютерная безопасность
3) Визуальная безопасность
4) Сензитивная безопасность

12. Перечислите состав службы информационной безопасности. ***Выберите несколько из 6 вариантов ответа:***
1) Руководитель службы
2) Операционный отдел
3) Исследовательский отдел
4) Методический отдел
5) Отдел общения с прессой
6) Отдел бухгалтерии

13. Составление списка объектов, которые будут подлежать защите, и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы, - это ... ***Запишите ответ:***

_____

14. Критериями определения уровня безопасности систем являются: В*ыберите несколько из 5 вариантов ответа:*
1) Оранжевая книга
2) Красная книга
3) Зеленая книга
4) Серо-буромалиновая книга
5) Белая книга

15... - выпущенные Министерством обороны США критерии оценки уровня безопасности компьютерных систем. *Выберите один из 5 вариантов ответа:*
1) Оранжевая книга
2) Красная книга
3) Белая книга
4) Зеленая книга
5) Открытая книга

16. ... - выпущенные Министерством обороны США расширение критериев оценки уровня безопасности компьютерных систем для случаев использования компьютерных систем в информационной сети. *Выберите один из 5 вариантов ответа:*
1) Оранжевая книга
2) Красная книга
3) Белая книга
4) Зеленая книга
5) Открытая книга

17. Перечислите модели классификации информационных объектов. ***Выберите несколько из 5 вариантов ответа:***
1) По наличию
2) По несанкционированной модификации (целостность)
3) По разглашению
4) По принадлежности
5) По аппелируемости

18. Какой считается информация, по классификации информационных объектов, если без нее можно работать, но очень короткое время. ***Выберите один из 6 вариантов ответа:***
1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

19.Какой считается информация, по классификации информационных объектов, если без нее можно работать, но ее использование экономит ресурсы. ***Выберите один из 6 вариантов ответа:***
1) критической
2) очень важной
3) важной

4) полезной
5) несущественной
6) вредной

20. Какой считается по классификации информационных объектов устаревшая или неиспользуемая информация, не влияющая на работу субъекта. ***Выберите один из 6 вариантов ответа:***
1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

21.Какой считается информация, по классификации информационных объектов, разглашение которой может принести моральный ущерб в очень редких случаях. ***Выберите один из 6 вариантов ответа:***
1) критической
2) очень важной
3) важной
4) значимой
5) малозначимой
6) незначимой

22. Какой считается информация, по классификации информационных объектов, если ее несанкционированное изменение скажется через некоторое время, но не приведет к сбою в работе субъекта, последствия модификации необратимы. ***Выберите один из 6 вариантов ответа:***
1) критической
2) очень важной
3) важной
4) значимой
5) малозначимой
6) незначимой

23. Жизненный цикл информации состоит из следующих стадий: ***Выберите несколько из 4 вариантов ответа:***
1) Информация используется в операционном режиме
2) Информация используется в архивном режиме
3) Информация хранится в архивном режиме
4) Информация хранится в операционном режиме

24. Какие существуют основные классы атак? ***Выберите несколько из 5 вариантов ответа:***
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Атака фрикера
5) Распределенная атака

25. ... - это случай, когда злоумышленник оказался непосредственно перед клавиатурой данного компьютера. ***Выберите один из 5 вариантов ответа:***
1) Локальная атака
2) Удаленная атака

3) Атака на поток данных
4) Распределенная атака
5) Атака фрикера

26. ... - это вариант атаки, когда злоумышленник не видит ту рабочую станцию, с которой он работает. ***Выберите один из 5 вариантов ответа:***
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Рейдерская атака
5) Социальная инженерия

27. ... - это вариант атаки, когда атакуемый компьютер активно отправляет, принимает или обменивается с данными с другими компьютерами сети, локальной или глобальной, а местом приложения атакующего воздействия является сегмент сети или сетевой узел между этими системами. ***Выберите один из 5 вариантов ответа:***
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Рейдерская атака
5) Социальная инженерия

28. ... - идейный борец за свободу информации, вторгающийся в чужие системы в основном из интереса, без прямой материальной заинтересованности. ***Выберите один из 5 вариантов ответа:***
1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

29. ... - тот, кто взламывает чужие системы, преследуя собственный финансовый интерес. ***Выберите один из 5 вариантов ответа:***
1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

30. ... - злоумышленник, использующий в собственных интересах уязвимости в телефонных системах. ***Выберите один из 5 вариантов ответа:***
1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

31. ... - это набор мероприятий по сбору сведений об информационной системе, напрямую не связанный с техническими подробностями реализации системы, основанный на человеческом факторе. ***Запишите ответ:***

_____

32. ... в аппаратном обеспечении -это устройство, которое выполняет некоторые недокументированные функции, обычно в ущерб пользователю данной информационной системы. ***Запишите ответ:***

_____

Материалы, используемые для промежуточного контроля успеваемости обучающихся по дисциплине

ОС-5 Экзамен в форме устного собеседования
Примерные вопросы к экзамену

1. Информационная безопасность, ее место в системе безопасности РФ
2. Угрозы информационной безопасности
3. Концепция информационной безопасности
4. Направления обеспечения информационной безопасности
5. Концептуальная модель информационной безопасности
6. Угрозы конфиденциальной информации (КИ)
7. Действия, приводящие к неправомерному овладению КИ
8. Государственная политика в области информационной безопасности
9. Доктрина информационной безопасности РФ –4 составляющие
10. Организационные основы системы обеспечения информационной безопасности
11. Политика информационной безопасности предприятия
12. Законодательный уровень обеспечения информационной безопасности
13. Правовая защита информации
14. Структура законодательства России в области ИБ
15. Вопросы защиты информации в Конституции РФ и Уголовном кодексе РФ
16. Закон «Об информации, информатизации и защите информации»
17. Понятие о конфиденциальной информации и коммерческой тайне
18. Нормативно-правовые документы предприятия по информационной безопасности
19. Система мер, направленных на обеспечение ИБ и их характеристики
20. Организационные мероприятия по защите информации
21. Организационно-технические мероприятия по защите информации
22. Технические мероприятия по защите конфиденциальной информации
23. Особенности защиты информации в ПЭВМ и информационных системах
24. Организационная защита информации
25. Функции службы безопасности предприятия по защите деловой информации и сведений, составляющих служебную, коммерческую и государственную тайну
26. Инженерно-техническая защита информации
27. Физические средства защиты информации
28. Средства контроля доступа
29. Аппаратные средства защита информации
30. Аппаратные средства электронной информации
31. Программные средства защиты электронной информации
32. Средства защиты электронной информации от несанкционированного доступа
33. Защита от копирования и разрушения электронной информации
34. Защита электронной почты
35. Вредоносное программное обеспечение и борьба с ним
36. Основные методы и средства защиты от атак на электронную переписку
37. Криптографические средства защиты
38. Защита интеллектуальной собственности
39. Понятие и виды интеллектуальной собственности
40. Авторское право интеллектуальной собственности
41. Смежное право применительно к интеллектуальной собственности
42. Патентное право
43. Защита интеллектуальной собственности в России
44. Национальные интересы РФ в международной сфере
45. Направления взаимодействия с зарубежными партнерами
46. Договора о сотрудничестве в зарубежными партнерами
47. Рынок технологий

48. Особенности коммерческих международных операций
49. Возможные условия разглашения сведений, составляющих коммерческую тайну.
50. Работа с иностранными партнерами в организациях
51. Прием иностранных представителей и проведение коммерческих переговоров
52. Формы работы с зарубежными партнерами
53. Основные черты и методы ведения информационной войны
54. «Активные мероприятия», их цели и методы ведения
55. Типовая схема действий разведывательных органов в отношении дестабилизации хозяйствующего субъекта
56. Роль СМИ в информационных войнах
57. Использование Интернета для ведения информационных войн
58. Способы подачи материалов «активных мероприятий»
59. Мошенничество в Интернете
60. Реклама и ее негативное влияние на психику человека

В конце изучения дисциплины подводятся итоги работы студентов на лекционных и практических занятиях путем суммирования заработанных баллов в течение семестра.

Критерии оценивания знаний обучающихся по дисциплине

Формирование балльно-рейтинговой оценки работы обучающихся

		Посещение лекций	Посещение практических занятий	Работа на практических занятиях	Экзамен
1 семестр	Разбалловка по видам работ	9 х 1=9 баллов	15 х 1=15 баллов	212 баллов	64 балла
	Суммарный макс. балл	9 баллов max	24 балла max	236 баллов max	300 баллов max

Критерии оценивания работы обучающегося по итогам 1 семестра

Оценка	**Баллы (3 ЗЕ)**
«отлично»	271-300
«хорошо»	211-270
«удовлетворительно»	151-210
«неудовлетворительно»	150 и менее

6. Методические указания для обучающихся по освоению дисциплины

Успешное изучение курса требует от обучающихся посещения лекций, активной работы на практических занятиях, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

Запись **лекции** – одна из форм активной самостоятельной работы обучающихся, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. В конце лекции преподаватель оставляет время (5 минут) для того, чтобы обучающиеся имели возможность задать уточняющие вопросы по изучаемому материалу. Из-за недостаточного количества аудиторных часов некоторые темы не удается осветить в полном объеме, поэтому преподаватель, по своему усмотрению, некоторые вопросы выносит на самостоятельную работу студентов, рекомендуя ту или иную литературу. Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. В случае необходимости обращаться к преподавателю за консультацией.

Подготовка к практическим занятиям.

При подготовке к практическим занятиям студент должен изучить теоретический материал по теме занятия (использовать конспект лекций, изучить основную литературу, ознакомиться с дополнительной литературой, при необходимости дополнить конспект, делая в нем соответствующие записи из литературных источников). В случае затруднений, возникающих при освоении теоретического материала, студенту следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале практического занятия преподаватель знакомит студентов с темой, оглашает план проведения занятия, выдает задания. В течение отведенного времени на выполнение работы студент может обратиться к преподавателю за консультацией или разъяснениями. В конце занятия проводится прием выполненных заданий, собеседование со студентом.

Результаты выполнения практических зданий оцениваются в баллах, в соответствии с балльно-рейтинговой системой университета.

Планы практических занятий (1 семестр)

Практическая работа № 1. **Информационная безопасность, ее место в системе безопасности РФ. Концепция информационной безопасности.**

Цель работы: выполнив предложенные задания, ознакомиться с общими вопросами информационной безопасности, ее местом в системе безопасности РФ, концепции информационной безопасности.

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.
2. Повторить лекционный материал по теме «Информационная безопасность, ее место в системе безопасности РФ. Концепция информационной безопасности», ответить на контрольные вопросы.

Вопросы для группового обсуждения:

1. Понятия и место информационной безопасности в системе безопасности РФ.
2. Основные концептуальные положения системы защиты информации.
3. Действия, приводящие к неправомерному овладению конфиденциальной информацией.

Форма представления отчета:

Студент должен представить решение предложенных задач в устной или письменной форме.

Практическая работа № 2. **Основы государственной политики обеспечения информационной безопасности. Законодательство РФ в области обеспечения информационной безопасности.**

Цель работы: выполнив предложенные задания, ознакомиться с системой государственных и общественных мероприятий в области обеспечения информационной безопасности.

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.
2. Повторить лекционный материал по теме «Основы государственной политики обеспечения информационной безопасности. Законодательство РФ в области обеспечения информационной безопасности», ответить на контрольные вопросы.

Вопросы для дискуссии:

1. Доктрина информационной безопасности.
2. Национальные интересы РФ в информационной сфере и их обеспечение.
3. Виды угроз информационной безопасности РФ (внутренние и внешние источники угроз).
4. Особенности обеспечения информационной безопасности в различных сферах общественной жизни: в экономике, внутренней и внешней политике, в области науки и техники, в сфере духовной жизни.

5. Основные направления и методы обеспечения информационной безопасности РФ в общегосударственных и телекоммуникационных системах, в правоохранительных и судебных сферах.

7. Правовая защита информации – структура законодательства РФ в области защиты информации.

8. Закон «Об информации, информатизации и защите информации».

9. Закон «О правовой охране программ для ЭВМ и БД».

10. Конфиденциальная информация.

11. Нормативно-правовые акты, разрабатываемые на предприятии в области защиты информации.

12. Организационно-правовые формы защиты коммерческой тайны.

Форма представления отчета:

Студент должен представить решение предложенных задач в устной или письменной форме.

Практическая работа № 3. **Сведения, отнесенные к государственной, служебной и коммерческой тайне. Обеспечение сохранения коммерческой тайны предприятия.**

Цель работы: выполнив предложенные задания, ознакомиться с общими сведениями, отнесенными к государственной, служебной и коммерческой тайне. Обеспечение сохранения коммерческой тайны предприятия.

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.

2. Повторить лекционный материал по теме «Сведения, отнесенные к государственной, служебной и коммерческой тайне. Обеспечение сохранения коммерческой тайны предприятия», ответить на контрольные вопросы.

Вопросы для круглого стола:

1. Определение и характеристики сведений, отнесенных к государственной тайне: в военной области, во внешнеполитической и внешнеэкономической деятельности.

2. Сведения в области разведывательной, контрразведывательной оперативно-розыскной деятельности, отнесенные к государственной тайне.

3. Порядок определения сведений, относящихся к служебной и к коммерческой тайне предприятия, характеристика сведений.

4. Порядок работы со сведениями, содержащими коммерческую тайну с документами с грифом «КТ».

5. Система допуска сотрудников, командированных и частных лиц к сведениям, составляющим коммерческую тайну предприятия.

6. Обязанности лиц, допущенных к сведениям, составляющим коммерческую тайну предприятия.

7. Ответственность за разглашение, утрату документов, содержащих коммерческую тайну.

Форма представления отчета:

Студент должен представить решение предложенных задач в устной или письменной форме.

Практическая работа № 4. **Инженерно-техническая защита информации**

Цель работы: выполнив предложенные задания, ознакомиться с принципами, методами, способами и средствами обеспечения инженерно-технической защиты информации.

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.

2. Повторить лекционный материал по теме «Инженерно-техническая защита информации», ответить на контрольные вопросы.

Вопросы для группового обсуждения:

1. Понятие утечки информации и причины возникновения каналов утечки информации.

2. Классификация и структура технических каналов утечки информации.

3. Акустические, визуально-оптические, материально-вещественные и электромагнитные каналы утечки информации.

4. Особенности защиты информации от утечки по техническим каналам, основные мероприятия по защите.

5. Средства и способы защиты.

6. Конструкторские и технологические мероприятия по локализации возможности образования условий возникновения каналов утечки.

Форма представления отчета:

Студент должен представить решение предложенных задач в устной или письменной форме.

Практическая работа № 5. **Методы и средства защиты электронной информации**

Цель работы: выполнив предложенные задания, ознакомиться с методами и средствами защиты электронной информации

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.

2. Повторить лекционный материал по теме «Методы и средства защиты электронной информации», ответить на контрольные вопросы.

Вопросы для дискуссии:

1. Разработка информационных систем, технологий и средств их обеспечения.

2. Порядок развития направлений информатизации и их финансирования.

3. Аппаратные средства защиты

4. Ограничение права на доступ к электронной информации.

5. Защита от несанкционированного доступа и копирования электронных баз данных.

6. Основные направления использования программных средств защиты.

7. Процедура идентификации посредством программных средств.

8. Защита от копирования и разрушения информации.

9. Защита электронной почты, борьба со спамом и вирусами, основные методы и средства защиты от атак на электронную переписку.

10. Вредоносное программное обеспечение. Механизмы распространения вредоносного программного обеспечения.

11. Криптографические средства защиты.

Форма представления отчета:

Студент должен представить решение предложенных задач в устной или письменной форме.

Практическая работа № 6. **Аудит информационной безопасности предприятия**

Цель работы: выполнив предложенные задания, ознакомиться с системой аудита информационной безопасности предприятия

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.

2. Повторить лекционный материал по теме «Аудит информационной безопасности предприятия», ответить на контрольные вопросы.

Вопросы для круглого стола:

1. Определить задачи проведения аудита информационной безопасности, как проверки состояния степени защиты информации

2. Обозначить основные направления деятельности в области аудита безопасности информации.

3. Произвести планирование аудита выделенных помещений, специального оборудования и технических средств.

4. Предложить средства обнаружения несанкционированных средств съема информации в ПЭВМ.

Форма представления отчета:

Студент должен представить решение предложенных задач в устной или письменной форме.

Практическая работа № 7. **Защита интеллектуальной собственности**

Цель работы: выполнив предложенные задания, ознакомиться с системой защиты интеллектуальной собственности

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.
2. Повторить лекционный материал по теме «Защита интеллектуальной собственности», ответить на контрольные вопросы.

Вопросы для группового обсуждения:

1. Дать характеристику объектов и информации, подпадающих под определение интеллектуальной собственности.
2. Проанализировать законодательство в области авторского права.
3. Предложить организационные и технические мероприятия по защите интеллектуальной собственности.

Форма представления отчета:

Студент должен представить решение предложенных задач в устной или письменной форме.

Практическая работа № 8. **Международная деятельность по обеспечению информационной безопасности. Конфиденциальность при работе с зарубежными партнерами.**

Цель работы: выполнив предложенные задания, ознакомиться с международной деятельностью по обеспечению информационной безопасности. Конфиденциальность при работе с зарубежными партнерами

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.
2. Повторить лекционный материал по теме «Международная деятельность по обеспечению информационной безопасности. Конфиденциальность при работе с зарубежными партнерами», ответить на контрольные вопросы.

Задачи:

1. Предположить возможные экономические потери при заключении контрактов и причины потерь.
2. Выяснить отражение вопросов защиты интеллектуальной собственности.
3. Оценить научно-техническое сотрудничество, технологический обмен и его регулирование, пути технологического обмена информацией.
4. Установить возможные условия разглашения сведений, составляющих коммерческую тайну.
5. Предложить организацию приема иностранных представителей, планирование и проведение коммерческих переговоров.
6. Проанализировать порядок защиты конфиденциальной информации при работе с зарубежными партнерами, особенности передачи информации зарубежному партнеру.

Форма представления отчета:

Студент должен представить решение предложенных задач в устной или письменной форме.

Практическая работа № 9. **Социально-политические манипуляции с личностью и механизмы защиты. Формы и методы информационной агрессии. Информационные войны.**

Цель работы: выполнив предложенные задания, ознакомиться с системой социально-политических манипуляций с личностью и механизмы защиты. Формы и методы информационной агрессии. Информационные войны

Рекомендации к самостоятельной работе:

1. Проработать материал по теме практической работы.

2. Повторить лекционный материал по теме «Социально-политические манипуляции с личностью и механизмы защиты. Формы и методы информационной агрессии. Информационные войны», ответить на контрольные вопросы.

Задачи:

1. Предположить современные формы и методы ведения информационных войн.
2. Проанализировать роль СМИ в информационных войнах.
3. Привести исторические примеры манипуляции массовым сознанием для достижения поставленных задач с помощью информационных воздействий.
4. Предположить механизмы защиты личности от воздействия деструктивных религиозных организаций и криминальных угроз.
5. Проанализировать влияние СМИ на формирование мировоззрения подрастающего поколения.
6. Примеры распространения через интернет информации негативного характера.
7. «Желтая пресса» и ее разлагающая роль в воспитании молодежи.
8. Дать характеристику дестабилизирующего воздействия на человека потока рекламы в электронных СМИ.

Подготовка к **устному докладу.**

Доклады делаются по каждой теме с целью проверки теоретических знаний обучающегося, его способности самостоятельно приобретать новые знания, работать с информационными ресурсами и извлекать нужную информацию.

Доклады заслушиваются в начале практического занятия после изучения соответствующей темы. Продолжительность доклада не должна превышать 7 минут. Тему доклада студент выбирает по желанию из предложенного списка.

При подготовке доклада студент должен изучить теоретический материал, используя основную и дополнительную литературу, обязательно составить план доклада (перечень рассматриваемых им вопросов, отражающих структуру и последовательность материала), подготовить раздаточный материал или презентацию. План доклада необходимо предварительно согласовать с преподавателем.

Выступление должно строиться свободно, убедительно и аргументировано. Преподаватель следит, чтобы выступление не сводилось к простому воспроизведению текста, не допускается простое чтение составленного конспекта доклада. Выступающий также должен быть готовым к вопросам аудитории и дискуссии.

Выполнение итоговой **практической работы.**

Для закрепления практических навыков по использованию информационных технологий студенты выполняют итоговое задание - самостоятельно или работая в малых группах по 2 человека, под руководством преподавателя.

Текущая проверка разделов работы осуществляется в ходе выполнения работы на занятиях и на консультациях. Защита итоговой работы проводится на последнем занятии или на консультации преподавателя. Для оказания помощи в самостоятельной работе проводятся индивидуальные консультации.

Подготовка к **тесту.**

При подготовке к тесту необходимо изучить теоретический материал по дисциплине. С целью оказания помощи студентам при подготовке к тесту преподавателем проводится групповая консультация с целью разъяснения наиболее сложных вопросов теоретического материала.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. - Москва ; Вологда : Инфра-Инженерия, 2022. - 104 с. - ISBN 978-5-9729-0864-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902587.

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное

пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657.

Дополнительная литература

1. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988.

2. Поликарпов, В. С. Философские проблемы информационного противоборства : учебное пособие для бакалавров, студентов, магистрантов и аспирантов / В. С. Поликарпов [и др.] ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университет, 2018. - 210 с. - ISBN 978-5-9275-2716-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1021754

3. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189328

Лист согласования рабочей программы
учебной дисциплины (практики)

Направление подготовки: 44.03.05 Педагогическое образование
Профиль: Физическая культура. Безопасность жизнедеятельности
Рабочая программа Информационная безопасность
Составитель: В.В. Богданов – Ульяновск: УлГПУ, 2024.

Программа составлена с учетом федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.03.05 Педагогическое образование, утверждённого Министерством образования и науки Российской Федерации, и в соответствии с учебным планом.

Составители _____ В.В. Богданов
(подпись)

Рабочая программа учебной дисциплины (практики) одобрена на заседании кафедры теории и методики физической культуры и безопасности жизнедеятельности "14" 05 2024 г., протокол № 9

Заведующий кафедрой

_____	Л.И. Костюнина	14.05.24
личная подпись	*расшифровка подписи*	*дата*

Рабочая программа учебной дисциплины (практики) согласована с библиотекой

Сотрудник библиотеки

_____	Ю.Б. Марсакова	14.05.24.
личная подпись	*расшифровка подписи*	*дата*

Программа рассмотрена и одобрена на заседании ученого совета факультета физической культуры и спорта "21" 05 2024 г., протокол № 9

Председатель ученого совета факультета физической культуры и спорта

_____	А.Н. Илькин	21.05.24
личная подпись	*расшифровка подписи*	*дата*