МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РФ
федеральное государственное бюджетное образовательное учреждение высшего образования
«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.П. АСТАФЬЕВА»
(КГПУ им. В.П. Астафьева)

Кафедра информатики и информационных технологий в образовании

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль) образовательной программы: Математика и информатика

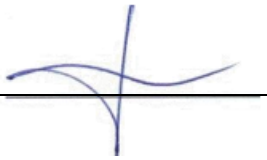
Квалификация (степень): Бакалавр

Красноярск 2021

Рабочая программа дисциплины «Защита информации» актуализирована *канд. пед. наук, доцентом кафедры информатики и информационных технологий в образовании П.С. Ломаско*.

Рабочая программа дисциплины обсуждена и одобрена на заседании кафедры информатики и информационных технологий в образовании

Протокол № 9 от «12» мая 2021 г.

Заведующий кафедрой  Пак Н.И.

Одобрено научно-методическим советом ИМФИ

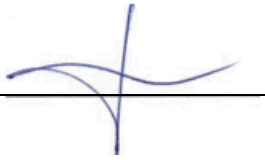
Протокол № 7 от «21» мая 2021 г.

Председатель  Бортновский С.В.

Рабочая программа дисциплины «Защита информации» актуализирована *канд. пед. наук, доцентом кафедры информатики и информационных технологий в образовании П.С. Ломаско.*

Рабочая программа дисциплины обсуждена и одобрена на заседании кафедры информатики и информационных технологий в образовании

Протокол № 11 от «20» мая 2020 г.

Заведующий кафедрой  Пак Н.И.

Одобрено научно-методическим советом ИМФИ

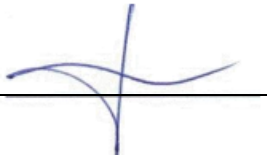
Протокол № 8 от «20» мая 2020 г.

Председатель  Бортновский С.В.

Рабочая программа дисциплины «Защита информации» актуализирована *канд. пед. наук, доцентом кафедры информатики и информационных технологий в образовании П.С. Ломаско.*

Рабочая программа дисциплины обсуждена и одобрена на заседании кафедры информатики и информационных технологий в образовании

Протокол № 9 от «08» мая 2019 г.

Заведующий кафедрой  Пак Н.И.

Одобрено научно-методическим советом ИМФИ

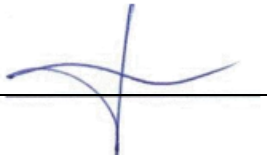
Протокол № 8 от «16» мая 2019 г.

Председатель  Бортновский С.В.

Рабочая программа дисциплины «Защита информации» актуализирована *канд. пед. наук, доцентом кафедры информатики и информационных технологий в образовании П.С. Ломаско.*

Рабочая программа дисциплины обсуждена на заседании кафедры информатики и информационных технологий в образовании

Протокол № 7 от «04» апреля 2018 г.

Заведующий кафедрой  Н.И. Пак

Одобрено научно-методическим советом ИМФИ

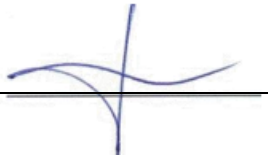
Протокол № 8 от «23» мая 2018 г.

Председатель  С.В. Бортновский

Рабочая программа дисциплины «Защита информации» разработана *канд. пед. наук, доцентом кафедры информатики и информационных технологий в образовании П.С. Ломаско.*

Рабочая программа дисциплины обсуждена и одобрена на заседании кафедры информатики и информационных технологий в образовании

Протокол № 10 от «03» мая 2017 г.

Заведующий кафедрой  Пак Н.И.

Одобрено научно-методическим советом ИМФИ

Протокол № 9 от «26» мая 2017 г.

Председатель  Бортновский С.В.

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Место дисциплины в структуре образовательной программы

Программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (уровень бакалавриата), утвержденным приказом Министерством образования и науки Российской федерации от 22 февраля 2018 г. № 125; Федеральным законом «Об образовании в РФ» от 29.12.2012 № 273-ФЗ; профессиональным стандартом «Педагог», утвержденным приказом Министерства труда и социальной защиты Российской Федерации от 18 октября 2013 г. № 544н.; нормативно-правовыми документами, регламентирующими образовательный процесс в КГПУ им. В.П. Астафьева по направленности (профилю) образовательной программы «Математика и информатика», очной формы обучения в институте математики физики и информатики КГПУ им. В.П. Астафьева с присвоением квалификации бакалавр.

Дисциплина относится к дисциплинам, формируемым участниками образовательных отношений, учебного плана основной образовательной программы, изучается в 9-м семестре, индекс дисциплины в учебном плане Б1.ОДП.05.01.02.06.

1.2. Общая трудоемкость дисциплины - в З.Е., часах и неделях.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа, из них на контактную работу с преподавателем – 28.25 час, часов самостоятельной работы – 43.75 час, формой промежуточной аттестации является зачет в 9-м семестре.

Текущий контроль образовательных результатов осуществляется на основании оценки практических и самостоятельных работ в системе электронного обучения.

Промежуточная аттестация производится в форме зачета, проводимого в форме предварительного тестирования и собеседования на основании перечня контрольных вопросов; текущих результатов обучающихся по дисциплине, достигнутых при выполнении практических заданий.

1.3. Основная цель дисциплины

Основная целью обучения дисциплине является формирование способности и готовности обучающихся к осуществлению учебной и будущей профессиональной деятельности с учетом рисков информационной безопасности и возможностей технологий защиты информации в контексте процессов интенсивной цифровизации сферы образования и с учетом реалий жизни в постиндустриальном обществе.

Рабочая программа дисциплины включает учебные задания, направленные на изучение и анализ тенденций изменений среды и условий осуществления задач будущей профессиональной деятельности с учетом перспектив развития средств защиты информации, необходимых для их решения.

Удельный вес занятий, проводимых в интерактивных формах, составляет не менее 60% от общего объема контактной работы с обучающимися. В курсе применяются следующие интерактивные методы и формы проведения учебных занятий: мозговой штурм; дискуссия; кейс-метод; профессиональные практико-ориентированные задания. Активно используются средства информационных технологий для проведения интерактивных опросов в аудитории, визуального и мультимедийного представления содержания учебных материалов, сетевого сопровождения и контроля самостоятельной работы через систему электронного обучения («Электронный университет»), средства для организации выполнения заданий курса обучающимися в режиме сетевой коллаборации.

1.4. Основные разделы содержания

Входной раздел. Актуализация опорных знаний из смежных предметных областей. Входное

экспресс-тестирование.
Основной раздел. Методы и средства защиты информации.
Тема 1. Информационное право и защищаемые объекты информационной сферы.
Тема 2. Угрозы и риски нарушения информационной безопасности.
Тема 3. Правовое обеспечение информационной безопасности в сфере образования.
Тема 4. Локальные акты и политика информационной безопасности.
Тема 5. Обеспечение целостности и доступности информационных ресурсов.
Тема 6. Классы конфиденциальности информационных ресурсов, грифы секретности и допуски.
Тема 7. Средства шифрования, электронная цифровая подпись и сертификаты безопасности.
Итоговый раздел. Контрольное тестирование по всем темам дисциплины. Выполнение итоговых заданий. Зачет.

1.5 Планируемые результаты обучения

Обучение дисциплине «Защита информации» направлено на формирование следующих образовательных результатов (таблица).

Задачи освоения дисциплины	**Планируемые результаты обучения по дисциплине** *(дескрипторы)*	**Код результата обучения** *(компетенция)*
обеспечение условий для формирования готовности к применению знаний в области правовых аспектов информационной деятельности, понятий предметной области информационного права, рисков и угроз информационной безопасности	**знать** – виды угроз информационной безопасности; – методы защиты интеллектуальной собственности (законодательные, административные, программные, технические)	ОПК-2 – способность участвовать в разработке основных и дополнительных образовательных программ, разрабатывать отдельные их компоненты (в том числе с использованием информационно-коммуникационных технологий)
	уметь – оценивать степень риска и возможный ущерб при нарушении информационной безопасности на различных уровнях – применять общие принципы защиты информации в компьютерных системах и телекоммуникационных сетях	
	владеть – методами минимизации рисков нарушения информационной безопасности на различных уровнях; – способами действий по использованию средств специального программного обеспечения (антивирусов, средств сетевого экранирования,	

	средств ограничения файлового доступа и шифрования, средств для восстановления информации) для обеспечения личной информационной безопасности, безопасности информационного пространства профессиональной деятельности	
формирование четкого понимания наличия ответственности при осуществлении любой информационной деятельности, способности ориентироваться в вопросах защиты информации в постиндустриальном обществе, в условиях интенсивной цифровизации образовательной деятельности	**знать** – основные виды правонарушений в сфере информационной деятельности, правовые статьи законодательства Российской Федерации, предусматривающие административную или уголовную ответственность за деяния, совершенные в сфере информационной деятельности; – особенности рисков нарушения информационной безопасности в образовательной деятельности (контентные, программные, технические, экономические, этические, психолого-педагогические аспекты)	ПК-1 – способность организовывать индивидуальную и совместную учебно-проектную деятельность обучающихся в соответствующей предметной области
	уметь – выделять конкретную проблему из ситуации, связанной с информационной безопасностью (инцидента); –производить криптографические преобразования информации («вручную» при помощи древних симметричных шифров, при помощи специальных программных средств)	
	владеть – средствами моделирования и анализа ситуаций нарушения информационной безопасности и прогнозирования возможных (негативных) последствий	
создание условий для овладения способами действий для оценки функциональных, количественных и качественных характеристик методов и средств защиты	**знать** – классификацию мер обеспечения состояния информационной безопасности (законодательного, административного, процедурного, программно-	ПК-2 – способность поддерживать образцы и ценности социального поведения, навыки поведения в мире виртуальной реальности и социальных сетях

информации с помощью программного обеспечения, теоретических обоснований алгоритмов шифрования, истории криптологии как науки	технического уровней); – теоретические обоснования основных методов защиты информации	
	уметь – обнаруживать вредоносное программное обеспечение и сетевые атаки; – устранять последствия воздействия вредоносного программного обеспечения и сетевых атак	
	владеть – способами действий по самостоятельному изучению, анализу и проектированию безопасной информационной деятельности на законодательном, административном, организационном и программно-техническом уровнях	
создание условий для углубления знаний в областях, смежных с информационной безопасностью, в области интернет-технологий и прикладных средств программного обеспечения	**знать** – о криптографических методах защиты и основных принципах функционирования симметричных и асимметричных криптосистем	ОПК-2 – способность участвовать в разработке основных и дополнительных образовательных программ, разрабатывать отдельные их компоненты (в том числе с использованием информационно-коммуникационных технологий); ПК-1 – способность организовывать индивидуальную и совместную учебно-проектную деятельность обучающихся в соответствующей предметной области; ПК-2 – способность поддерживать образцы и ценности социального поведения, навыки поведения в мире виртуальной реальности и
	уметь – применять методы ограничения доступа к информации на различных уровнях – самостоятельно найти и оценить способ минимизации рисков консольных и сетевых атак	
	владеть – способами действий по самостоятельному изучению, анализу и проектированию безопасной информационной деятельности при помощи интернет-технологий и прикладных средств программного обеспечения различных типов устройств, в том числе смартфонов, планшетов, бытового смарт-оборудования; устройств обеспечения коллективного и	

	индивидуального сетевого доступа	социальных сетях.

1.6 Контроль результатов освоения дисциплины.

Оценочные средства результатов освоения дисциплины, критерии оценки выполнения заданий представлены в разделе «Фонды оценочных средств для проведения промежуточной аттестации».

1.7 Перечень образовательных технологий, используемых при освоении дисциплины

Преподавание дисциплины осуществляется на русском языке. В процессе обучения применяются следующие образовательные технологии:

1. *Ubiquitous learning (u-learning)* – обучение с помощью информационно-коммуникационных технологий посредством электронной учебного курса, реализованного на платформе «Электронный университет» (LMS Moodle). Данный курс включает доступные повсеместно обучающимся через Интернет с любых устройств материалы лекций, практических заданий, средств организации самостоятельной работы, видео, мультикастов, тестов с автоматической проверкой результатов, интерактивных обучающих средств в виде тренажеров, аудио-опросов, ссылок на дополнительные материалы и информационные ресурсы в виде справочной литературы в цифровой форме. Данный курс обеспечен и средствами виртуальной коммуникации и сетевого взаимодействия с преподавателем.

2. *Проблемное обучение.* Создание в процессе организации учебно-познавательной деятельности проблемных ситуаций, разрешение которых предполагает активную самостоятельную работу обучающихся по их разрешению, в результате чего происходит творческое овладение знаниями, умениями, навыками, развиваются мыслительные способности.

3. Технологии формирования критического мышления. Суть данной технологии основывается на проектировании образовательных условий, в которых будущим учителям информатики приходится работать с различными источниками информации, творчески переосмысливать прочитанное и осуществлять критическое оценивание. Технология развития критического мышления, реализуемая с целью формирования у обучающихся умения мыслить качественно и непредвзято, осуществляется в рамках трех стадий:

1) стадия вызова, в ходе которой выполняется актуализация знаний и мотивация на выполнение информационного поиска;

2) стадия осмысления, в течение которой предусматривается непосредственная работу с информационными ресурсами (коллективно, в группах или индивидуально) с последующим установлением связей и поиском несоответствий;

3) стадия рефлексии, во время которой происходит закрепление предметных образовательных результатов и метапредметных умений.

Технология критического мышления основана на применении следующих педагогических методов и приемов: мозгового штурма, собирания «Корзины идей», составления эссе, интеллектуальных разминок, реализации ролевых проектов, содержательного группового изучения интерактивных видео, материалов сайтов с остановками, построению причинно-следственных связей и логических цепочек.

4. Кейс-технология. Базируется на принципе выделения в рамках дисциплины «Защита информации» отдельных практических ситуаций проблемного характера (кейсов), в ходе обсуждения которых преподавателя с обучающимися удается обеспечить формирование точечных и универсальных компетенций, равномерное распределение понятийного и

практического модуля знаний.

Реализация кейс-технологии осуществляется в рамках следующих этапов: Самостоятельная работа обучающихся, нацеленная на формулирование проблемы, поиск возможных путей ее преодоления. Взаимодействие студентов в малых группах (поиск преодоления учебного затруднения). Групповая экспертиза результатов.

2. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ

2.1. Технологическая карта обучения дисциплине «Защита информации»

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки),
направленность (профиль) образовательной программы: Математика и информатика,
квалификация (степень): Бакалавр
по **очной** форме обучения (общая трудоемкость 2,0 з.е.)

Наименование разделов и тем дисциплины	Всего часов	Контакт.	Лекций	Практич.	Лаб.	КРЗ	Сам. работы	КРЭ	Контроль
ВХОДНОЙ РАЗДЕЛ.	**5**	**0**	**0**	**0**	**0**	**0**	**5**	**0**	**0**
БАЗОВЫЙ РАЗДЕЛ. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ	**63**	**36**	**14**	**0**	**14**	**0**	**35**	**0**	**0**
Тема 1. Информационное право и защищаемые объекты информационной сферы	9	4	2	0	2	0	5	0	0
Тема 2. Угрозы и риски нарушения информационной безопасности	9	4	2	0	2	0	5	0	0
Тема 3. Правовое обеспечение информационной безопасности в сфере образования	9	4	2	0	2	0	5	0	0
Тема 4. Локальные акты и политика информационной безопасности	9	4	2	0	2	0	5	0	0
Тема 5. Обеспечение целостности и доступности информационных ресурсов	9	4	2	0	2	0	5	0	0
Тема 6. Классы конфиденциальности информационных ресурсов, грифы секретности и допуски	9	4	2	0	2	0	5	0	0
Тема 7. Средства шифрования, электронная цифровая подпись и сертификаты безопасности	9	4	2	0	2	0	5	0	0
ИТОГОВЫЙ РАЗДЕЛ. Форма промежуточной аттестации по учебному плану - ЗАЧЕТ	**4**	**0,25**	**0**	**0**	**0**	**0,25**	**3,75**	**0**	**0**
ИТОГО	**72**	**28,25**	**14**	**0**	**14**	**0,25**	**43,75**	**0**	**0**

2.2. Содержание основных разделов и тем дисциплины

ВХОДНОЙ РАЗДЕЛ. Актуализация опорных знаний из смежных предметных областей. Входное тестирование. Понятие информации, информационных процессов. Математические методы обработки информации, кодирование информации, измерение количества информации. Программное обеспечение компьютерных систем, операционные системы и утилиты. Архитектура компьютера. Интернет-технологии: адресация, сетевое оборудование, протоколы, хостинг, облачные технологии, контент, брандмауэр. Цифровизация и понятие информационно-образовательной среды. Социальные сети и сервисы. Экономические понятия: блага, ущерб. Общеметодологические понятия: безопасность, критичность, достоверность, риски, угрозы. Основы права: административная и уголовная ответственность, Конституция РФ, информационные отношения, информационная сфера.

ОСНОВНОЙ РАЗДЕЛ. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.

Тема 1. Информационное право и защищаемые объекты информационной сферы. Общие вопросы информационной безопасности. Информационная модель постиндустриального общества. Ключевые документы в области информационной безопасности РФ. Уровни информационной безопасности. Классификация мер обеспечения состояния информационной безопасности (законодательный, административный, процедурный, программно-технический уровни). Информационная безопасность государства, общества, личности.

Тема 2. Угрозы и риски нарушения информационной безопасности. Классификации угроз информационной безопасности. Экономические, политические, программно-технические, контентные, этические, психологические и психолого-педагогические риски нарушения информационной безопасности. Целостность, доступность и конфиденциальность защищаемых объектов.

Тема 3. Правовое обеспечение информационной безопасности в сфере образования. Юридические определения объектов защиты информации и поддерживающей инфраструктуры. Обзор российской и мировой законодательной практики. Судебные прецеденты и ответственность за нарушение законов. Вопросы информационной безопасности в Гражданском кодексе РФ. Интеллектуальная собственность и авторские права. Creative Commons. Вопросы информационной безопасности в Уголовном кодексе РФ. Незаконное распространение информации, защита детей от информации и возрастные ограничения на контент. Вопросы информационной безопасности в образовательном законодательстве. Информационная открытость деятельности образовательных организаций. Сайт образовательной организации. Защита персональных данных в сфере образования.

Тема 4. Локальные акты и политика информационной безопасности. Понятие политики информационной безопасности. Информационно-образовательная среда образовательных организаций: содержательные, организационные и программно-технические компоненты. Допуски и грифы. Должностные инструкции, приказы и распоряжения для организации защиты информации. Легальное использование программного обеспечения, цифровых образовательных ресурсов. Регулирование вопросов использования локальной сети в организации, учетные записи пользователей, политика ограничения доступа. Внутренняя и внешняя информационная политика образовательной организации. Контент-фильтрация, договоры с провайдерами, вопросы обслуживания сайтов образовательных организаций: доменные имена, хостинг, требования к безопасности сетевых ресурсов образовательной организации.

Тема 5. Обеспечение целостности и доступности информационных ресурсов. Формальные и неформальные методы защиты. Статическая и динамическая целостность. Поддерживающая инфраструктура. Средства резервного копирования и ограничения доступа к информационным ресурсам. Модели управления доступом в информационных

системах: ролевая, мандатная, дискреционная. Ограничения доступа средствами операционных систем. Защита документов. Атаки, нарушающие целостность и доступность объектов защиты. Вредоносные программы: вирусы, черви, троянские программы, эксплойты, ботнеты. Сетевые атаки на доступность и методы защиты от них.

Тема 6. Классы конфиденциальности информационных ресурсов, грифы секретности и допуски. Конфиденциальность с точки зрения законодательства, тайны. Классы конфиденциальности. Несанкционированный доступ к информации и модели нарушителя. Спуффинг, сниффинг, кибесквоттинг, XSS, консольные атаки на конфиденциальность. Стеганография: классическая и компьютерная. Допуски и грифы служебной информации. Вопросы конфиденциальной информации в сфере образования: усыновление, персональные данные, сведения о здоровье обучающихся. Механизмы и сервисы ограничения доступа к защищаемой информации. Идентификация, аутентификация, авторизация. Правила обращения с секретными сведениями. Стойкость паролей. Журналирование доступа к объектам защиты.

Тема 7. Средства шифрования, электронная цифровая подпись и сертификаты безопасности. Понятие криптосистемы. Основы криптографии: ключ, шифрование, функции криптопреобразования. Принципы Кирхгоффа. Симметричная и асимметричная криптография. Проблемы распределения ключей. Открытые и закрытые ключи. Хеширование. Хранение паролей в информационных системах. Контрольные суммы для проверки файлов. Электронная цифровая подпись. Цифровые сертификаты безопасности. Безопасность сетевых протоколов. Методы и средства защиты информации при сетевом взаимодействии. Программные средства для шифрования защищаемой информации. Защита информации как комплекс и система. Аппаратные средства защиты информации. Криптомаршрутизаторы и аппаратное шифрование данных на носителях.

ИТОГОВЫЙ РАЗДЕЛ. Контрольное тестирование по всем темам дисциплины. Выполнение итоговых (кейсовых) заданий. Зачет.

2.3. Методические рекомендации по освоению дисциплины «Защита информации» для обучающихся образовательной программы

Уважаемые обучающиеся!

Преподавание учебной дисциплины «Защита информации» предусматривает использование не только традиционные формы обучения (чтение лекций, проведение групповых практических занятий), но и использование новых информационных и образовательных технологий.

Преподавателями будут максимально использоваться те формы обучения, которые потребуют от вас активности, самостоятельности и ответственности.

При изучении лекционного материала вам необходимо будет использовать как выложенные в электронном курсе опорные презентации и сопроводительные материалы, так и дополнительные статьи из периодических изданий и зарубежных источников. Освоение данной дисциплины требует также активного использования возможностей Интернет-ресурсов, что позволяет значительно обогатить используемый в практике материал, а также способствует развитию вашей профессиональной компетентности в области использования возможностей информационных систем в будущей деятельности.

В ходе занятий необходимо быть готовыми использовать новые информационные технологии, в частности, использовать средства мультимедийных аудиторий. Лекционный материал будет сопровождаться использованием в ходе занятий средств повышения наглядности представляемых материалов (наглядных пособий, аудиовизуальных средств обучения, интерактивных заданий и упражнений), чтобы сформировать у вас понимание, умения и навыки их применения в практической деятельности.

Особое внимание необходимо уделять изучению понятийного аппарата

дисциплины. Лекции ориентированы на систематизированное представление знаний, раскрытие сущности наиболее трудных для освоения учебных вопросов (материалов). При посещении лекции нужно учитывать, что затем будет проводиться практическое, следует делать краткие записи в виде конспекта, задавать преподавателю вопросы относительно дальнейшего применения лекционного материала на практических занятиях и промежуточной аттестации (контрольной работе, тестировании, зачете, экзамене) по каждой теме.

Практические занятия проводятся в виде: группового обсуждения студентами проблем по предлагаемым темам в рамках определенного раздела изучаемой дисциплины; анализа, проведения, обработки и интерпретации результатов изучения различных информационных источников; изучения характеристик и возможностей средств различных научных отраслей; практической отработки навыков применения теоретических знаний на практике; обсуждения выполненных в ходе занятия работ (заданий).

В качестве текущего контроля успеваемости на занятиях используются проблемные практические задания, которые потребуют от вас решения конкретных задач и проблем, моделирования поведения в ситуациях, принятия решений и активных действий согласно собственному плану. При текущем контроле преподаватель будет в первую очередь обращать внимание на проявление у вас признаков информационной культуры, сформированность исследовательских навыков, способность аргументировать свою позицию, развитие навыков обоснования выполненных действий, способность действовать самостоятельно.

Преподаватель в течение всего семестра будет оценивать вашу активность и качество выполнения всех заданий, при этом активно помогая тем, кто испытывает определенные затруднения при изучении материалов учебной дисциплины, при помощи консультаций, дополнительных пояснений или специальных дополнительных материалов и заданий.

Итоговой формой контроля работы по дисциплине является зачет. Критериями допуска к зачету являются:

а) успешное выполнение и сдача не менее 75% промежуточных заданий в текущем семестре;

б) успешное прохождение итогового тестирования по дисциплине (на положительную оценку в 61% и более баллов);

в) успешная защита кейсового задания;

г) наличие посещаемости большей части (60% и более) очных занятий и/или активности в электронном курсе (изучение не менее 70% ресурсов).

К итоговому тестированию необходимо будет подготовиться, опираясь на список заданий и лекции. В качестве источников для ответов на тестовые задания можно использовать рекомендованные данной программой учебники и учебные пособия, материалы занятий, ресурсы электронного курса, а также самостоятельно обнаруженные цифровые ресурсы образовательного характера.

3. КОМПОНЕНТЫ МОНИТОРИНГА УЧЕБНЫХ ДОСТИЖЕНИЙ ОБУЧАЮЩИХСЯ

3.1 Технологическая карта рейтинга дисциплины «Защита информации»

Наименование дисциплины/курса	Направление подготовки и уровень образования (бакалавриат, магистратура) Наименование программы/ профиля	Количество зачетных единиц/кредитов
Защита информации	44.03.05 Педагогическое образование (с двумя профилями подготовки), направленность (профиль) образовательной программы: Математика и информатика, квалификация (степень): Бакалавр	**2**

ВХОДНОЙ РАЗДЕЛ			
	Форма работы	Количество баллов 5 %	
		min	max
Текущая работа	Заполнение индивидуального глоссария по опорным понятия курса	0,5	1
Промежуточный рейтинг-контроль	Входное тестирование	1	4
Итого		**1,5**	**5**
БАЗОВЫЙ РАЗДЕЛ			
	Форма работы	Количество баллов 70 %	
		min	max
Промежуточный рейтинг-контроль	Контрольная работа № 1	6	10
Промежуточный рейтинг-контроль	Контрольная работа № 2	6	10
Промежуточный рейтинг-контроль	Контрольная работа № 3	6	10
Промежуточный рейтинг-контроль	Контрольная работа № 4	6	10
Рубежный рейтинг-контроль	Выполнение кейсового задания	16	30
Итого		**40**	**70**

ИТОГОВЫЙ РАЗДЕЛ			
Содержание	Форма работы	Количество баллов 25 %	
		min	max
Итоговый контроль	Тестирование	17	25
Итого		**17**	**25**

ДОПОЛНИТЕЛЬНЫЙ РАЗДЕЛ		
Форма работы	Количество баллов	
	min	max
Проектирование кейса по темам курса	5	20
Защита спроектированного кейсового задания	5	20
Итого	**10**	**40**
Общее количество баллов по дисциплине (по итогам изучения всех модулей, без учета дополнительного модуля)	min	max
	60	**100**

3.2. Фонд оценочных средств (контрольно-измерительные материалы)

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РФ
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Красноярский государственный педагогический университет им. В.П. Астафьева» (КГПУ им. В.П. Астафьева)

Институт математики, физики и информатики
(наименование института/факультета)

Кафедра информатики и информационных технологий в образовании
(наименование кафедры-разработчика)

УТВЕРЖДЕНО
на заседании кафедры
протокол № 9 от «12» мая 2021 г.
Заведующий кафедрой ИИТвО

_____Пак Н.И.

ОДОБРЕНО
На заседании научно-методического
совета специальности (направления подготовки) ИСГТ
«21» мая 2021 г. Протокол № 7
Председатель НМСИ(Н)

_____Бортновский С.В.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине
«Защита информации»
(наименование дисциплины/модуля/вида практики)

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль) образовательной программы: Математика и информатика

Квалификация (степень): Бакалавр

Составитель:

канд. пед. наук, доцент кафедры ИИТвО Ломаско П.С.

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ НА ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Представленный фонд оценочных средств для текущей и промежуточной аттестации соответствует требованиям ФГОС ВО и профессиональным стандартам Педагог (профессиональная деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель), утвержденным приказом Минтруда России от 18.10.2013 N 544н.

Предлагаемые формы и средства аттестации адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), направленность (профиль) образовательной программы: «Математика и информатика», квалификация (степень): бакалавр.

Оценочные средства и критерии оценивания представлены в полном объеме. Формы оценочных средств, включенных в представленный фонд, отвечают основным принципам формирования ФОС, установленных в Положении о формировании фонда оценочных средств для текущего контроля успеваемости, промежуточной и итоговой (государственной 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», утвержденного приказом ректора № 297 (п) от 28.04.2018.

Разработанный и представленный для экспертизы фонд оценочных средств **рекомендуется к использованию в процессе подготовки по указанной программе.**

Эксперт:
учитель информатики высшей категории,
заместитель директора по учебно-воспитательной работе
МБОУ «СОШ № 10 с углубленным изучением отдельных
предметов имени академика Ю.А. Овчинникова»
г. Красноярска

МБОУ СОШ № 10 МП

Г.С. Карпенко

Муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная школа № 10 с углубленным изучением отдельных предметов имени академика Ю.А. Овчинникова»
Адрес: 660017, г. Красноярск, ул. Ленина, 114.
Телефон: (391) 211-32-59 Эл. почта: school10_krs@mail.ru, официальный сайт: http://school10.org

1. **Назначение фонда оценочных средств**

1.1. **Целью** создания ФОС дисциплины «Защита информации» является установление соответствия учебных достижений запланированным результатам обучения и требованиям основной профессиональной образовательной программы, рабочей программы дисциплины.

1.2. ФОС по дисциплине решает **задачи**:

1. Осуществления педагогического менеджмента процесса приобретения обучающимися необходимых составляющих компетенций, определенных в образовательных стандартах по соответствующему направлению подготовки (специальности).

2. Непосредственного управления процессом достижения реализации образовательных программ, определенных в виде набора компетенций выпускников.

3. Педагогической диагностики достижений обучающихся в процессе изучения дисциплины с определением положительных/отрицательных результатов и планирование предупреждающих/корректирующих мероприятий.

4. Обеспечения соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс.

5. Обеспечения процессов самоподготовки и самоконтроля обучающихся.

1.3. ФОС разработан на основании нормативных **документов**:

- федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), бакалавриат

(код и наименование направления подготовки, уровень подготовки)

- образовательной программы высшего образования по направлению подготовки Направленность (профиль) образовательной программы: «Математика и информатика»

(код и наименование направления подготовки, уровень подготовки)

- 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 магистратуре в федеральном государственном бюджетном образовательном учреждении высшего образования «Красноярский государственный педагогический университет им. В.П. Астафьева» и его филиалах.

1.3. Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей. Оценочными средствами для студентов с ограниченными возможностями здоровья в рамках изучения дисциплины являются:

– для студентов с нарушением слуха: контрольные вопросы, подразумевающие письменные ответы и проверку в системе электронного обучения;

– для студентов с нарушением контрольные вопросы, подразумевающие устные ответы, в том числе в режиме аудио- и видеосвязи, организованного с помощью средств ИКТ и через систему электронного обучения (запись подкастов с ответами);

– для студентов с нарушением опорно-двигательного аппарата контрольные вопросы, подразумевающие устные или письменные (на выбор) ответы, в том числе в режиме аудио- и видеосвязи, организованного с помощью средств ИКТ и через систему электронного обучения в дистанционном режиме (запись подкастов с ответами, собеседование по видеоконференцсвязи).

2. Перечень компетенций с указанием этапов их формирования в процессе изучения дисциплины/модуля/прохождения практики:

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

2.2. Оценочные средства

Компетенция	Дисциплины, практики, участвующие в формировании данной компетенции	Тип контроля	Оценочное средство/КИМ	
			Номер	Форма
ОПК-2 – способность участвовать в разработке основных и дополнительных образовательных программ, разрабатывать отдельные их компоненты (в том числе с использованием информационно-коммуникационных технологий);	Модуль 2 «Коммуникативный» Информационно-коммуникационные технологии в образовании и социальной сфере	Текущий контроль успеваемости	1-4	Кейсовые задания
	Проектирование урока по требованию ФГОС Методика работы с классным коллективом Дисциплины предметной подготовки, ориентированные на достижение результатов обучения Основы предметно-профильной подготовки Алгебра Теория вероятностей и математическая статистика Теоретические основы информатики Языки и методы программирования Современные направления развития научной отрасли (по профилю подготовки) Основы теории функций комплексного переменного Теория функций действительного переменного История информатики Защита информации Архитектура компьютера и операционные системы Дисциплины методической подготовки, ориентированные на достижение результатов обучения Методика обучения и воспитания (по профилю подготовки Математика) Технологии современного образования (по профилю подготовки Математика) Модуль 11 «Предметно-практический» Физика	Промежуточная аттестация	1	Зачет

Компетенция	Дисциплины, практики, участвующие в формировании данной компетенции	Тип контроля	Оценочное средство/КИМ	
			Номер	Форма
	Модуль 7 «Педагогическая интернатура» Модуль 9 «Предметно-методический» Производственная практика: педагогическая практика интерна Междисциплинарный практикум Педагогическая практика Подготовка к сдаче и сдача государственного экзамена Выполнение и защита выпускной квалификационной работы			
ПК-1 – способность организовывать индивидуальную и совместную учебно-проектную деятельность обучающихся в соответствующей предметной области;	Модуль 1 «Мировоззренческий» Культурология Естественнонаучная картина мира Модуль 2 «Коммуникативный» Иностранный язык Русский язык и культура речи Информационно-коммуникационные технологии в образовании и социальной сфере Педагогическая риторика Модуль 3 «Здоровьесберегающий» Основы ЗОЖ и гигиена Анатомия и возрастная физиология Безопасность жизнедеятельности Физическая культура и спорт «Физическая культура и спорт: Элективная дисциплина с по общей физической подготовке/Элективная дисциплина по подвижным и спортивным играм/Элективная дисциплина по физической культуре для обучающихся с ОВЗ и инвалидов)» Модуль 4 «Теория и практика инклюзивного образования» Современные технологии инклюзивного образования Проектирование индивидуальных образовательных	Текущий контроль успеваемости	1-4	Кейсовые задания
		Промежуточная аттестация	1	Зачет

Компетенция	Дисциплины, практики, участвующие в формировании данной компетенции	Тип контроля	Оценочное средство/КИМ	
			Номер	Форма
	маршрутов детей с ОВЗ Основы математической обработки информации Основы учебно-исследовательской работы (профильное исследование) Теория обучения и воспитания Проектирование урока по требованию ФГОС Дисциплины предметной подготовки ориентированные на достижение результатов обучения Основы предметно-профильной подготовки Теория вероятностей и математическая статистика Теоретические основы информатики Языки и методы программирования Современные направления развития научной отрасли (по профилю подготовки) Теория функций действительного переменного История информатики Цифровые технологии в оценивании образовательных результатов Защита информации Архитектура компьютера и операционные системы Дисциплины методической подготовки ориентированные на достижение результатов обучения Методика обучения и воспитания (по профилю подготовки Математика) Школьный практикум по дисциплинам (математика) Школьный практикум по дисциплинам (информатика) Технологии современного образования (по профилю подготовки Информатика) Методика обучения и воспитания (по профилю подготовки Информатика) Модуль 10 «Предметно-теоретический»			

Компетенция	Дисциплины, практики, участвующие в формировании данной компетенции	Тип контроля	Оценочное средство/КИМ	
			Номер	Форма
	Геометрия Числовые системы Программирование вычислительных алгоритмов Компьютерное моделирование Информационные системы и сети Основы искусственного интеллекта Системы искусственного интеллекта в образовании Информатика Компьютерная графика и анимация Модуль 11 «Предметно-практический» Физика История математики математического образования в России Социальная информатика Модуль 5 «Учебно-исследовательский» Модуль 6 «Теоретические основы профессиональной деятельности» Модуль 7 «Педагогическая интернатура» Модуль 8 «Основы вожатской деятельности» Модуль 9 «Предметно-методический» Учебная практика: ознакомительная практика Учебная практика: научно-исследовательская работа (получение первичных навыков научно-исследовательской работы) Производственная практика: преддипломная практика Учебная практика: введение в профессию Учебная практика: технологическая (проектно-технологическая) практика Производственная практика: педагогическая практика интерна Учебная практика: общественно-педагогическая практика			

Компетенция	Дисциплины, практики, участвующие в формировании данной компетенции	Тип контроля	Оценочное средство/КИМ	
			Номер	Форма
	Производственная практика: вожатская практика Междисциплинарный практикум Педагогическая практика Учебная практика Учебная практика Подготовка к сдаче и сдача государственного экзамена Выполнение и защита выпускной квалификационной работы			
ПК-2 – способность поддерживать образцы и ценности социального поведения, навыки поведения в мире виртуальной реальности и социальных сетях.	Модуль 1 «Мировоззренческий» История (история России, всеобщая история) Философия Основы права и политологии Экономика знаний Социология Модуль 2 «Коммуникативный» Информационно-коммуникационные технологии в образовании и социальной сфере Модуль 4 «Теория и практика инклюзивного образования» Психологические особенности детей с ОВЗ Современные технологии инклюзивного образования Проектирование индивидуальных образовательных маршрутов детей с ОВЗ История образования и педагогической мысли Психологические основы педагогической деятельности Педагогическая конфликтология Методика работы с классным коллективом Дисциплины предметной подготовки ориентированные на достижение результатов обучения Современные направления развития научной отрасли (по профилю подготовки) Основы теории функций комплексного переменного	Текущий контроль успеваемости	1-4	Кейсовые задания
		Промежуточная аттестация	1	Зачет

Компетенция	Дисциплины, практики, участвующие в формировании данной компетенции	Тип контроля	Оценочное средство/КИМ	
			Номер	Форма
	Защита информации Дисциплины методической подготовки, ориентированные на достижение результатов обучения Методика обучения и воспитания (по профилю подготовки Математика) Технологии современного образования (по профилю подготовки Математика) Школьный практикум по дисциплинам (математика) Школьный практикум по дисциплинам (информатика) Технологии современного образования (по профилю подготовки Информатика) Методика обучения и воспитания (по профилю подготовки Информатика) Модуль 11 «Предметно-практический» Физика Социальная информатика Модуль 6 «Теоретические основы профессиональной деятельности» Модуль 7 «Педагогическая интернатура» Модуль 9 «Предметно-методический» Учебная практика:технологическая (проектно-технологическая) практика Производственная практика: педагогическая практика интерна Междисциплинарный практикум Педагогическая практика Учебная практика Учебная практика Подготовка к сдаче и сдача государственного экзамена Выполнение и защита выпускной квалификационной работы			

3. Фонд оценочных средств для промежуточной аттестации

3.1. Фонды оценочных средств для промежуточной аттестации включают: вопросы к экзамену.

3.2. Оценочные средства

3.2.1. Оценочное средство вопросы для проведения устного собеседования

ВОПРОСЫ К ЗАЧЕТУ ПО ДИСЦИПЛИНЕ
«ЗАЩИТА ИНФОРМАЦИИ»
Направление подготовки: 44.03.05 Педагогическое образование
(с двумя профилями подготовки)
Направленность (профиль) образовательной программы:
Математика и информатика
Квалификация (степень): Бакалавр
по **очной** форме обучения

Задания для устного собеседования

1. Назовите и охарактеризуйте основные понятия предметной области информационной безопасности. Приведите примеры, раскрывающие понятия: воздействия, угрозы, уязвимости, риски, атаки.
2. Опишите текущую ситуацию в цифровом обществе с позиции кибербезопасности. Укажите, каковы наиболее часто встречающиеся инциденты кибербезопасности в нашей стране и мире. Дайте определение кибертерроризму. Назовите и приведите примеры угроз кибербезопасности.
3. На примере объектов персональной защиты раскройте понятие информационных ценностей и покажите, как определить ценность информационных активов. Определите понятие и виды ущерба. Перечислите основные группы информационных ценностей.
4. Перечислите и раскройте смысл составляющих информационной безопасности. Опишите типовые ситуации, нарушающие данные составляющие и дайте название каждому типу.
5. Опишите основные виды средств формальной и неформальной защиты информации, приведите конкретные примеры на каждый вид. Приведите схему, показывающую, что защита информации должна быть комплексной и системной.
6. Приведите не менее 4 примеров основных инцидентов, связанных с информационной безопасностью и защитой информации персональных ценностей. Предложите меры по их предотвращению и устранению последствий.
7. Дайте определение общему понятию атаки и назовите ее ключевые признаки. Приведите 3-4 примера известных вам атак, связанных с кибербезопасностью.
8. Перечислите и охарактеризуйте основные фазы жизненного цикла атаки: общую схему любой атаки и фазы таргетированной атаки. Приведите примеры таргетированной и нетаргетированной атаки.
9. Назовите и охарактеризуйте основные виды кибератак. Приведите по 1-2 примера на каждый вид. Предложите контрмеры для избегания таких случаев и устранения последствий каждого вида атак.
10. Дайте определение консольным атакам. Приведите примеры 4-5 возможных инцидентов, связанных с консольными атаками на настольные ПК, ноутбуки, смартфоны и планшеты.
11. Перечислите и поясните 4-5 основных возможных инцидентов при атаках на браузеры, сервисы быстрых сообщений и электронной почты. Как определить фальсификацию сообщений электронной почты и социальный «спуффинг»?
12. Приведите примеры использования социальной инженерии при реализации сетевых атак: «маскарад» и использование беспечных пользователей. Предложите контрмеры для избегания и устранения последствий каждого вида атак.

13. Дайте определение и приведите примеры атак: сетевого спуффинга, сниффинга, фладинга, боминга. Охарактеризуйте следующие типы злоумышленников: хакер, кардер, пранкер, кибербуллер, крэкер, шпион, вандал, спаммер.
14. Охарактеризуйте атаки на средства аутентификации, используя слова: «стойкость паролей», «брутфорс», «атака по словарю». Приведите примеры консольных и сетевых атак на пароли.
15. Опишите, каковы целевые назначения систем защиты информации и каковы минимальные требования к обеспечению информационной безопасности. Охарактеризуйте каждый уровень защиты информации с позиции системного подхода.
16. Дайте определение политике информационной безопасности организации. Приведите основные характеристики и принципы по ее реализации с точки зрения различных уровней: организационного, программного, технического.
17. Раскройте через примеры основные способы защиты информационных ценностей: препятствие, управление, маскировка, регламентация, побуждение и принуждение. Приведите схему, раскрывающую модель комплексной системы защиты информации.
18. Перечислите и дайте определение основным механизмам защиты информации. Приведите примеры реализации каждого механизма.
19. Опишите особенности построения моделей комплексной защиты информации через модель угроз и модель нарушителя. Приведите примеры угроз и потенциальных инцидентов.
20. Приведите основные виды программных угроз информационной безопасности. Охарактеризуйте каждый вид с позиции возможных инцидентов и ущерба от них. Опишите основные виды вредоносного программного обеспечения.
21. Охарактеризуйте основные методы оценки рисков информационной безопасности и пути их применения. Перечислите и поясните основные стратегии управления рисками. Опишите, как должно осуществляться реагирование на реализацию рисков в системах защиты информации.
22. Дайте определение криптологии как области знаний. Перечислите и охарактеризуйте основные составляющие. Приведите примеры, раскрывающие применение в защите информации ее основных разделов.
23. Приведите в ретроспективе процесс развития стеганографии с древних времен до современного этапа. Проиллюстрируйте применение современной стеганографии для защиты информации.
24. Раскройте определение криптоанализа и его роли при построении систем защиты информации. Перечислите и поясните на примерах основные методы криптоанализа.
25. Раскройте определение криптографии и ее роли при построении систем защиты информации. Приведите в ретроспективе процесс развития криптографии с древних времен до современного этапа и возможные перспективы в будущем.
26. Приведите схему, раскрывающую основные виды криптоалгоритмов. Укажите определение криптосистемы и основных понятий, с ней связанных. Объясните, для чего применяются бесключевые криптоалгоритмы.
27. Опишите принцип работы симметричного шифрования. Продемонстрируйте процесс шифрования и расшифрования при помощи любого известного вам метода (шифра).
28. Раскройте основные направления и особенности применения симметричных криптосистем, приведите примеры и их названия. Объясните, в чем основной недостаток применения симметричных шифров на текущем этапе развития цифрового общества.
29. Опишите различия потоковых и блочных шифров. Поясните их на примере простого шифрования. Объясните, какой вклад внес в развитие криптографии Хорст Фейстель и в чем его суть.
30. Объясните, каким образом определяется стойкость криптоалгоритма. Укажите, какой вклад в данную область внес Огюст Керкгоффс и какие шифры сегодня считаются

абсолютно стойкими и достаточно стойкими.

31. Опишите принцип работы асимметричного шифрования. Раскройте основные направления и особенности применения асимметричных криптосистем, приведите примеры и их названия.
32. Объясните, в чем суть проблемы распределения ключей шифрования. Приведите пример такой проблемы между двумя сторонами, возможные варианты ее решения. Укажите, какой способ решения предложили Уитфилд Диффи и Мартин Хеллман.
33. Раскройте суть правового обеспечения информационной безопасности через понятие информационного права, основные объекты защиты. Приведите основные законы РФ, связанные с областью информационной безопасности.

3.2.2. Критерии оценивания по оценочному средству п. 3.2.1

Формируемые компетенции	Высокий уровень сформированности компетенций	Продвинутый уровень сформированности компетенций	Базовый уровень сформированности компетенций
	(87 - 100 баллов) отлично	(73 - 86 баллов) хорошо	(60 - 72 баллов) * удовлетворительно
ОПК-2	Обучающийся способен назвать все основные понятий и категорий, ситуаций, связанных с корректным использованием средств защиты информации, привести подробные примеры, строить аналогии и перспективы адекватного использования ИКТ	Обучающийся способен назвать большинство основных понятий и категорий, ситуаций, связанных с корректным использованием средств защиты информации, привести примеры	Обучающийся способен назвать несколько основных понятий и категорий, ситуаций, связанных с корректным использованием средств защиты информации
	Обучающийся готов продемонстрировать умение осуществлять выбор всех изученных средств информационных технологий в соответствии с задачами защиты информации с приведением различных примеров	Обучающийся готов продемонстрировать умение осуществлять выбор большинства изученных средств информационных технологий в соответствии с задачами защиты информации с приведением конкретных примеров	Обучающийся готов продемонстрировать умение осуществлять выбор основных изученных средств информационных технологий в соответствии с задачами защиты информации без приведения конкретных примеров
	Обучающийся демонстрирует владение всеми	Обучающийся демонстрирует владение основными	Обучающийся демонстрирует владение основными методами

	изученными методами получения научного знания в области защиты информации, приводит примеры изученных материалов научных исследований и ссылается на личный опыт	методами получения научного знания в области защиты информации, приводит примеры из личного опыта или изученных материалов научных исследований	получения научного знания в области защиты информации, приводит частично корректные примеры из личного опыта или изученных материалов научных исследований
ПК-1	Обучающийся способен назвать и привести примеры всех изученных направлений использования защиты информации в психолого-педагогической деятельности, ссылаясь на личный опыт, привести конкретные примеры	Обучающийся способен назвать и привести примеры большинства изученных направлений использования защиты информации в психолого-педагогической деятельности, привести примеры	Обучающийся способен назвать и привести примеры нескольких изученных направлений использования средств защиты информации без приведения примеров
	Обучающийся полностью готов продемонстрировать умение организовывать пространство собственной психолого-педагогической деятельности средствами защиты информации, описывая его вербально и в виде схемы и показывая средства и технологии, которые используются	Обучающийся в большей степени готов продемонстрировать умение организовывать пространство собственной психолого-педагогической деятельности средствами защиты информации, описывая его вербально и/или в виде схемы и, показывая средства и технологии, которые используются	Обучающийся посредственно готов продемонстрировать умение организовывать пространство собственной психолого-педагогической деятельности средствами защиты информации, описывая его вербально или в виде схемы и, показывая средства и технологии, которые используются
	Обучающийся демонстрирует владение всеми освоенными способами использования средств защиты информации	Обучающийся демонстрирует владение большинством освоенных способов использования средств защиты информации	Обучающийся демонстрирует владение некоторыми способами использования средств защиты информации

ПК-2	Обучающийся способен назвать и привести примеры всех изученных принципов выбора средств информационных технологий для решения задач защиты информации и критерии их оценки;	Обучающийся способен назвать и привести примеры большинства изученных принципов выбора средств информационных технологий для решения задач защиты информации и критерии их оценки;	Обучающийся способен назвать и привести примеры некоторых изученных принципов выбора средств информационных технологий для решения задач защиты информации и критерии их оценки;
	Обучающийся полностью готов продемонстрировать умение организовывать и проводить защиту информации с использованием информационных технологий на конкретном примере	Обучающийся в большей степени готов продемонстрировать умение организовывать и проводить защиту информации с использованием информационных технологий на конкретном примере	Обучающийся в посредственно готов продемонстрировать умение организовывать и проводить защиту информации с использованием информационных технологий на конкретном примере
	Обучающийся демонстрирует владение всеми освоенными способами защиты информации в будущей профессиональной деятельности	Обучающийся демонстрирует владение большинством освоенных способов защиты информации в будущей профессиональной деятельности	Обучающийся демонстрирует владение некоторыми способами использования средств защиты информации

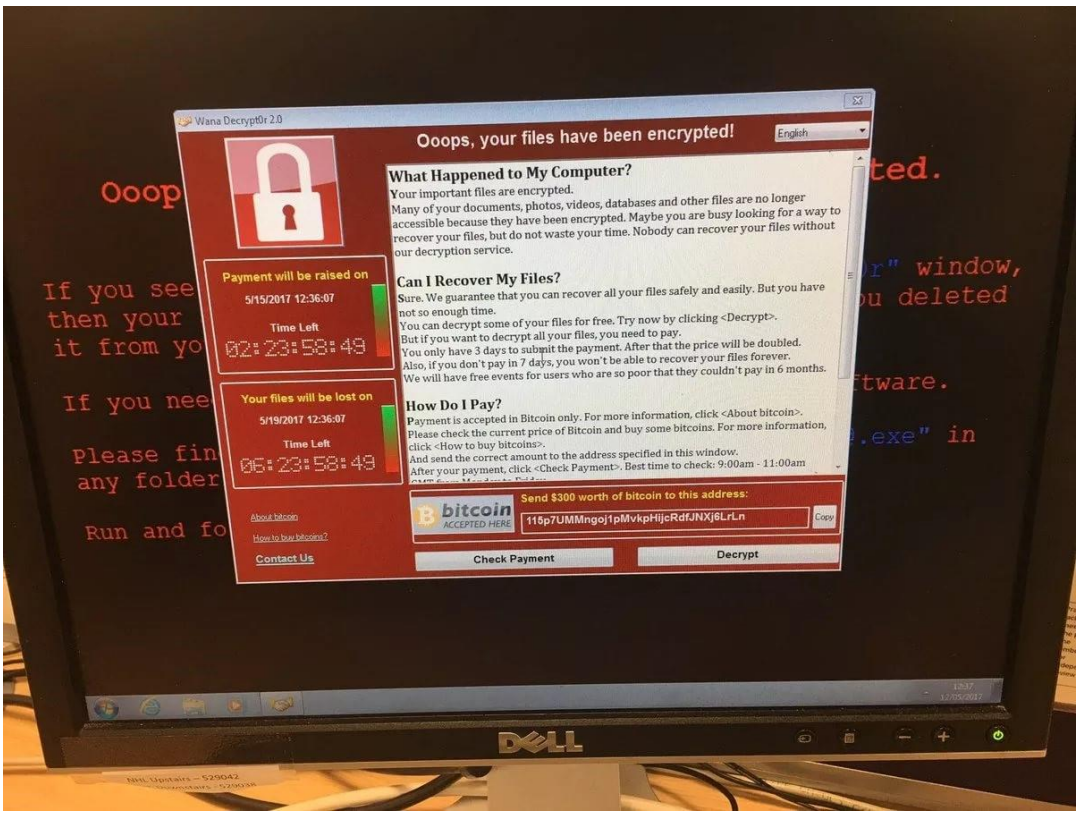
*Менее 60 баллов – компетенция не сформирована

3.2.3. Оценочное средство тестовые задания для проведения итогового тестирования

ИТОГОВОЕ ТЕСТИРОВАНИЕ
«ЗАЩИТА ИНФОРМАЦИИ»

1) Сетевая атака, которая характеризуется отказом сервера принимать входящие соединения в результате многочисленных распределенных (то есть происходящих с разных точек интернет-доступа) запросов, называется
a) Фладдинг
b) DDOS
c) Бомбинг
d) Фишинг

2)



На скриншоте демонстрируется атака вируса:
a) Cry for me
b) Never cry
c) No cry
d) Wanna Cry

3) Внедрение вредоносного исполняемого кода (скриптов) в поддерживаемые сайтам html-блоки (форумы, комментарии) - это тип атаки, который называется
a) XSS
b) Spooffing
c) DDOS
d) SSL

4) В списке указаны криптосистемы:
- **RSA** (Rivest-Shamir-Adleman)
- **DSA** (Digital Signature Algorithm)
- **Elgamal** (Шифросистема Эль-Гамаля)
- **Diffie-Hellman** (Обмен ключами Диффи — Хелмана)
- **ECC** (Elliptic Curve Cryptography, криптография эллиптической кривой)
- **ГОСТ Р 34.10-2001**

Они являются представителями классов (a):
a) бесключевых
b) одноключевых
c) двухключевых
d) трехключевых

5) Произведённое действие или его попытка, которое нарушило состояние информационной безопасности - это
a) атака
b) уязвимость
c) угроза
d) риск

6)

Электронный ключ, изображенный на иллюстрации, называется:
a) SmartLock
b) iButton
c) USB-Locker
d) eToken

7) Ситуация, когда вирус-вымогатель блокирует операционную систему от запуска каких-либо программ, иллюстрирует нарушение:
a) конфиденциальности
b) целостности и доступности
c) целостности
d) доступности
e) целостности и конфиденциальности

8) Недобросоветный системный администратор школьного сервера, продающий логины и пароли от электронной почты учителей родителям, может быть классифицирован как

a) спаммер
b) хакер
c) инсайдер
d) пранкер

9) Секретная информация, используемая криптографическим алгоритмом при шифровании/расшифровке сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности - это
a) пароль
b) хэш
c) логин
d) ключ

10) Ситуация, в которой у вас несанкционированно скопировали и распространили ваши личные фотографии является нарушением:
a) тайны частной жизни
b) целостности
c) доступности
d) конфиденциальности

11) Отметьте атаки, относящиеся к локальным (консольным):
a) Блокирование доступа пользователя к документам через подмену флеш-карты планшета
b) Удаление файлов пользователя через вход в систему с использованием пустых или простых паролей на рабочем месте
c) Редактирование контактов адресной книги пользователя через подключение смартфона к компьютеру
d) Копирование документов путем загрузки операционной системы с флеш-диска

12) Минимально достаточные требования информационной безопасности включают наличие мер на следующих уровнях:
a) Административный
b) Программный
c) Процедурный
d) Технический
e) Этический
f) Моральный

13) Комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в различных системах - это
a) стратегия минимизации рисков
b) информационная политика
c) защита информации
d) аудит информационных ценностей

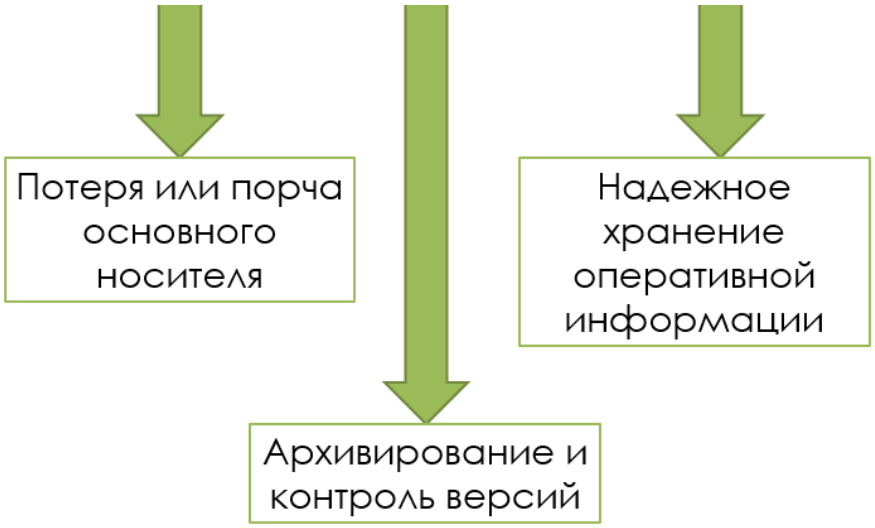
14) Обучение, аттестация и выдача специальных разрешений (допусков) на работу с информационной системой - это меры какого уровня?
a) морально-этического
b) процедурного
c) организационного

d) программного
e) административного

15) Набор формальных (официально утвержденных либо традиционно сложившихся) правил, которые регламентируют функционирование механизмов информационной безопасности - это
a) механизм ИБ
b) сервис ИБ
c) протокол ИБ
d) политика ИБ

16) Вероятность того, что конкретные действия, нарушающие информационную безопасность, будут осуществлены с использованием конкретного незащищенного элемента системы - это
a) непреднамеренное воздействие
b) риск
c) атака
d) угроза

17) Какая процедура связана с ситуациями:



a) резервное копирование
b) аутентификация
c) аудит
d) шифрование

18) Перехват или прослушивание сетевого трафика, например, в публичных Wi-Fi сетях с целью злонамеренного использования - это вид атаки:
a) фладдинг
b) сниффинг
c) спуффинг
d) бомбинг

19) К основным составляющим информационной безопасности можно отнести:
a) апеллируемость
b) ресурсообеспеченность
c) доступность
d) конфиденциальность
e) идентификацию
f) аутентификацию
g) целостность

20)

ID	Название	Класс
001	Пожар	Непреднамеренные
..		
200	Взлом	Преднамеренные
..	…	

Простой перечень возможных угроз безопасности информационной системе, включая стихийные бедствия - это
a) стратегия минимизации рисков
b) список угроз
c) модель угроз
d) статистика инцидентов

21) Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям через поддельные сайты или приложения, это
a) спамминг
b) кибербуллинг
c) хакинг
d) фишинг

22) Совокупность методов и способов обратимого преобразования информации с целью ее защиты от несанкционированного доступа в большей степени соответствует понятию
a) кэширования
b) хэширования
c) шифрования
d) кодирования

23) Вредоносная программа, отдельный фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки с целью захвата контроля над системой (повышение привилегий или нарушения её функционирования - это
a) сетевой червь
b) вирус-шифровальщик
c) эксплойт
d) макровирус

3.2.4. Критерии оценивания по оценочному средству, представленному в п. 3.2.3:

Оценка	Требования
Зачтено	Оценка «Зачтено» выставляется обучающемуся, если он верно ответил на 14 и более вопросов.
Не зачтено	Оценка «не зачтено» выставляется обучающемуся, если он неверно ответил на 9 и более вопросов.

4. Фонд оценочных средств для текущего контроля успеваемости

4.1. Фонды оценочных средств текущего контроля успеваемости включают: набор контрольных работ и набор кейсовых заданий.

4.2.1. Оценочное средство «Набор контрольных работ» и критерии оценивания отдельных работ

Контрольная работа № 1

1. Выпишите названия и краткое описание основных нормативных документов в области информационного права, результаты представьте в виде таблицы.

№	Документ (название, выходные данные)	Регулирует, предписывает	Ключевые понятия

2. Перечислите государственные органы РФ, контролирующие деятельность в области защиты информации

№	Название	Основные функции	Подчиненные структуры

3. Используя не менее, чем 5 различных источников дать определения следующим понятиям: 1) информационная безопасность; 2) уровни и составляющие информационной безопасности 3) защита информации; 4) компьютерная безопасность.

4. Изучите актуальную редакцию Стратегии развития информационного общества в Российской Федерации, определите и выпишите какие позиции данного документа связаны с вопросами информационной безопасности РФ.

5. Приведите и расшифруйте основные категории стандартной модели информационной безопасности.

6. Приведите основные составляющие информационной безопасности с точки зрения системного подхода, приведите их описания.

7. **Индивидуально** напишите развернутый ответ (7-8 предложений) на следующий вопрос: «Какова роль педагога в вопросах становления информационного общества с точки зрения информационной безопасности?».

Критерии оценивания

Критерий	2,5 балла	0 баллов
– Приведены корректные ссылки на нормативно-распорядительные документы, достоверно приведен их анализ (не менее 70% из представленного)	Имеется	Не имеется
– Корректно определены ключевые понятия задания (не менее 70%)	Имеется	Не имеется
– Наличие в ответах на задания 4-6 признаков корректного понимания основных составляющих и категорий информационной безопасности	Имеется	Не имеется
– Представленный ответ на задание 7 соответствует поставленному вопросу	Имеется	Не имеется
Итого	10	0

Оценка «зачтено» ставится при условии суммы баллов по критериям не менее 6.
В иных случаях ставится оценка «не зачтено».

Контрольная работа № 2

1. Создайте в тетради или текстовом процессоре таблицу Вижинера размерностью 7×3 и алфавитом А={Н, А, Д, О, В, Р}. Зашифруйте слово ДВОР с помощью ключа ДНО.

2. С помощью этой же таблицы зашифруйте произвольное слово (не более 6 букв) с ключом РОВ. Напишите получившуюся шифрограмму. Расшифруйте шифрограмму ОРНВТ.

3. С помощью этой же таблицы зашифруйте произвольное слово (не более 6 букв) с произвольным ключом (не более 4 букв). Какой метод для подбора ключа бы будете использовать?

4. Создайте в тетради или текстовом процессоре квадрат Бьюфорта размерностью 5×5 и алфавитом А={А, Е, О, П, Р}. Расшифруйте шифрограмму ЕААР с помощью ключа ПА.

5. С помощью этого же квадрата расшифруйте шифрограмму ЕАЕАПН, если известно, что размерность ключа от 3 до 6 символов.

6. Зашифруйте с помощью этого же квадрата произвольное слово не более чем из 5 символов и ключом ПЕРО с количеством раундов = 2.

7. Используя интерфейс, аналогичный программе «Квадрат Полибия» напишите алгоритм шифрования текстовых файлов (UTF-8) методом Вижинера или Бьюфорта.

Критерии оценивания

Критерий	2,5 балла	0 баллов
– Ответы на задания 1-2 соответствуют верным ответам (1 – РНАВ, 2 – ДОБРО)	Имеется	Не имеется
– Ответы на задания 3-4 соответствуют верным ответам (3 – индекс таблицы, 4 – АББА)	Имеется	Не имеется
– Ответы на задания 5-6 соответствуют верным ответам (5 – ВОРОНА, 6 – произвольный верный ответ)	Имеется	Не имеется
– Представленный алгоритм позволяет шифровать текстовые файлы в кодировке UTF-8	Имеется	Не имеется
Итого	10	0

Оценка «зачтено» ставится при условии суммы баллов по критериям не менее 6.
В иных случаях ставится оценка «не зачтено».

Контрольная работа № 3

1. Зашифруйте при помощи шифра A1Z26 файл с текстом: «Шифрование может быть симметричным и асимметричным» (кодировка ANSI) в файл Primer1_C.txt, напишите, что получилось в результате.

2. Расшифруйте файл Photo1_C.jpg методом XOR в файл Result.jpg, если известно, что ключ – это символ ASCII и лежит в пределах от «%» до «<« .

3. Создайте произвольное изображение (включите в него текст с любым посланием) с помощью MS Paint, сохраните его как Ваша_фамилия.jpg. Зашифруйте данный файл методом XOR с произвольным потоковым ключом длины 64. Отправьте ключ.

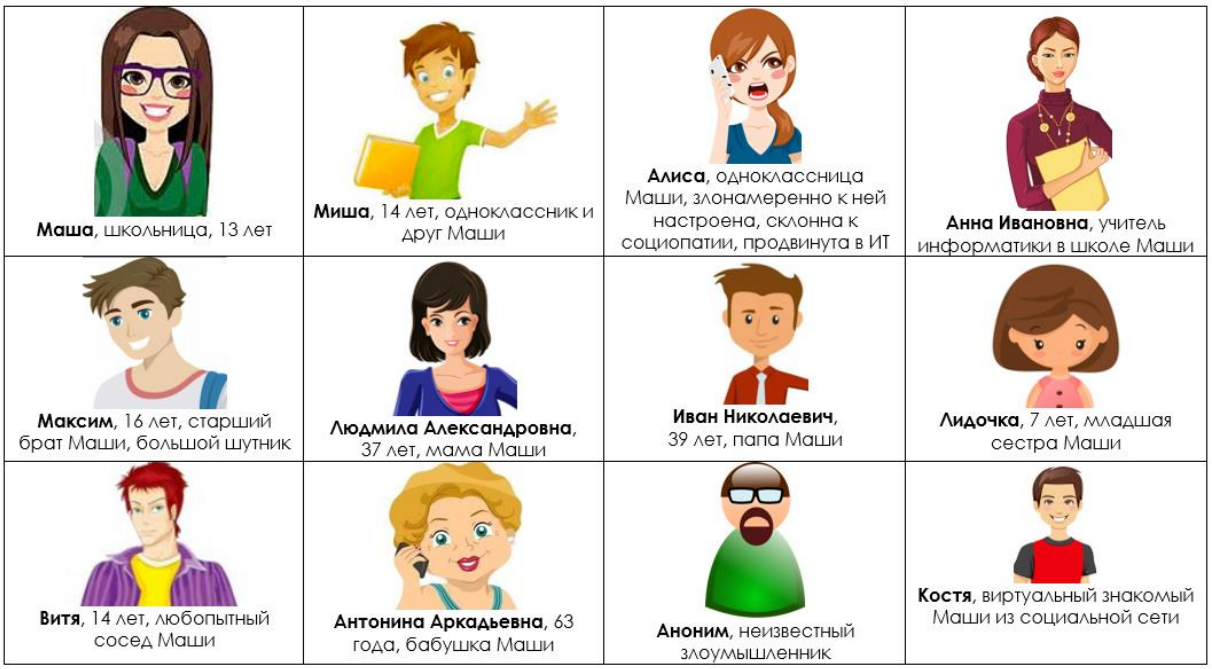
Критерии оценивания

Критерий	2,5 балла	0 баллов
– Ответ на задание 1 соответствует: 26-10-22-18-16-3-1-15-10-6 14-16-8-6-20 2-29-20-30 19-10-14-14-6-20-18-10-25-15-29-14 10 1-19-10-14-14-6-20-18-10-25-15-29-14	Имеется	Не имеется
– В ответе на задание 2 содержится верно расшифрованный файл	Имеется	Не имеется
– С помощью отправленного ключа удалось расшифровать исходный файл в ответе на задание 3	Имеется	Не имеется
– Удалось извлечь зашифрованное послание из ответа на задание 3	Имеется	Не имеется
Итого	10	0

Оценка «зачтено» ставится при условии суммы баллов по критериям не менее 6.
В иных случаях ставится оценка «не зачтено».

4.2.2. Оценочное средство «Набор кейсовых заданий» и критерии оценивания отдельных работ

Действующие лица кейсовых заданий



Кейс № 1. Домашние компьютеры

Вы: Анна Ивановна, учитель информатики в школе Маши

Маша обратилась к вам за советом, сообщив, что в их семье имеется 3 компьютера, 1 планшет, к которым все дети имеют доступ. При этом 1 персональный стационарный ПК находится в комнате Максима, 2 ноутбука 15” и 17”. У Маши и Максима есть смартфоны на базе ОС Android. Доступно подключение по витой паре к роутеру и Wi-Fi.

Девочка спросила о том, каким образом им лучше всего настроить устройства, на которых установлены: на стационарном ПК ОС Windows 10, на ноутбуках Ubuntu 17 и MacOS X Leopard. При уточнении выяснилось, что Маше необходимо:

- Чтобы Максим и Лидочка не могли прочитать или испортить ее файлы, хранимые на стационарном ПК;
- Максим перестал бы отправлять от ее имени поддельные сообщения в социальной сети и по электронной почте и вообще не смог бы получить доступ к ее аккаунту, она меняла пароль несколько раз, но он все равно входил;
- Лидочка не могла бы пользовать ноутбуками самостоятельно;
- На стационарном ПК, который в основном используется для подготовки уроков была бы возможность быстрого его восстановления, так как несколько раз он уже ломался (не загружалась ОС);
- Родители попросили ее узнать, как лучше всего настроить браузер для безопасного серфинга, особенно для Лидочки, чтобы не было рекламы и взрослого контента.

Какие рекомендации вы дадите Маше? Опишите в виде инструкции, снабдив ее скриншотами и дополнительными ссылками, чтобы Маша почитала более подробно при возникновении затруднений.

Критерии оценивания кейса № 1

Критерий	5 баллов	2,5 балла	0 баллов
Наличие ответов на поставленные в ситуации вопросы	Имеется	Частично имеется	Не имеется
Полнота анализа ситуации	Имеется	Частично имеется	Не имеется
Достаточность инструкции для действия	Имеется	Частично имеется	Не имеется
Наличие альтернативных вариантов решений	Имеется	Частично имеется	Не имеется
Адекватная идентификация проблем и решений	Имеется	Частично имеется	Не имеется
Презентация (защита) решений, владение темой	Имеется	Частично имеется	Не имеется
Итого	30		

Оценка «зачтено» ставится при условии суммы баллов по критериям не менее 16.
В иных случаях ставится оценка «не зачтено».

Кейс № 2. Семейный архив

Вы: Иван Николаевич, 39 лет, папа Маши.

За многое время жизни и отдыха вашей семьи (более 18 лет!) накопилось множество фотографий и видео. Однажды, ваша жена, Людмила Александровна захотела пересмотреть детские видео Максима, которые были записаны на CD обнаружила, что диск никак не читается. При этом несколько лет назад у вас вышел из строя семейный компьютер, который ремонту не подлежал и был отправлен в утиль. Видео оказались безвозвратно утеряны. Также полгода назад Людмила Александровна хотела напечатать фотографии с прошедших праздников, которые копировала на стационарный ПК и оказалось, что Маша их случайно удалила, а флэш-карту от фотоаппарата она форматировала перед летним отпуском.
Озадачившись сохранением семейных реликвий, вы задались вопросами:

- В течение какого времени безопасно хранить файлы на цифровых носителях? Какие устройства для хранения архивов дома необходимо иметь?
- Как защитить данные на общих устройствах от случайного искажения или потери?
- Что делать, если файлы удалили недавно? Можно ли их восстановить и как?
- Можно ли хранить файлы на бесплатных облачных сервисах, но так, чтобы они случайно или намеренно не попали в чужие руки? Как их защитить?
- Как защитить цифровые носители, чтобы информацию нельзя было распространить, если их вдруг украдут?

Напишите в виде инструкции, чтобы вы сделали на месте Ивана Николаевича, чтобы, с одной стороны сохранить семейные архивы в цифровом виде, с другой – уберечь из от посторонних. Для иллюстрации добавьте скриншоты и ссылки на дополнительные статьи.

Критерии оценивания кейса № 2

Критерий	5 баллов	2,5 балла	0 баллов
Наличие ответов на поставленные в ситуации вопросы	Имеется	Частично имеется	Не имеется
Полнота анализа ситуации	Имеется	Частично имеется	Не имеется
Достаточность инструкции для действия	Имеется	Частично имеется	Не имеется

Наличие альтернативных вариантов решений	Имеется	Частично имеется	Не имеется
Адекватная идентификация проблем и решений	Имеется	Частично имеется	Не имеется
Презентация (защита) решений, владение темой	Имеется	Частично имеется	Не имеется
Итого	30		

Оценка «зачтено» ставится при условии суммы баллов по критериям не менее 16.
В иных случаях ставится оценка «не зачтено».

Кейс № 3. Маша в слезах

Вы: Максим, 16 лет, старший брат Маши, большой шутник

Однажды Маша пришла из школы очень расстроенная, в слезах и сильно переживая, она пожаловалась вам, что кто-то разместил фотографии (причем много! и даже старые) с ее телефона и пишет обидные сообщения друзьям в социальных сетях, а сегодня на стене опубликовались всякие глупости от ее имени. Кроме того, ее смартфон постоянно стал «глючить», и часть приложений не работает. Выясняя ситуацию, вы обнаружили, что несколько дней назад ее одноклассница, Алиса, просила у нее телефон в школе – поиграть. При этом несколько раз телефон был вне поля зрения Маши.
Решив защитить сестру, вы озадачились:

- Как кто-то мог заполучить фотографии с телефона Маши?
- Почему могут продолжаться публикации? И даже после смены пароля?
- Что делать, чтобы защитить данные на устройстве?
- За что и как можно привлечь обидчика к ответственности?
- В чем причина «глюков» и как восстановить устройство?

Напишите в виде инструкции, чтобы вы сделали на месте Максима, чтобы, с одной стороны восстановить спокойствие сестры, с другой – уберечь от подобных ситуаций себя и близких. Для иллюстрации добавьте скриншоты и ссылки на дополнительные статьи.

Критерии оценивания кейса № 3

Критерий	5 баллов	2,5 балла	0 баллов
Наличие ответов на поставленные в ситуации вопросы	Имеется	Частично имеется	Не имеется
Полнота анализа ситуации	Имеется	Частично имеется	Не имеется
Достаточность инструкции для действия	Имеется	Частично имеется	Не имеется
Наличие альтернативных вариантов решений	Имеется	Частично имеется	Не имеется
Адекватная идентификация проблем и решений	Имеется	Частично имеется	Не имеется
Презентация (защита) решений, владение темой	Имеется	Частично имеется	Не имеется
Итого	30		

Оценка «зачтено» ставится при условии суммы баллов по критериям не менее 16.
В иных случаях ставится оценка «не зачтено».

Кейс № 4. Любопытный сосед

Вы: Маша, школьница, 13 лет

На прошлой неделе в вашем доме начали происходить странные вещи. Во-первых, несколько раз принтер, подключенный к домашнему ПК произвольно печатал картинки из Интернета. Во-вторых, при просмотре телевизора (у вас устройство серии Sony Bravia смарт-ТВ) несколько раз включались какие-то видео. Затем домашний проводной Интернет и Wi-Fi отказывались работать – подключались, но скорость была минимальная. В итоге Wi-Fi совсем исчез – сеть с вашим SSID перестала определяться, но появилась какая-то новая. Наконец, домашняя сеть вовсе исчезла. В доме стало неспокойно. Зная, что ваш сосед по площадке, Витя очень любит всякие эксперименты, связанные с информационными технологиями, вы подумали на него. Но он все отрицал, да и дома у вас он был в последний раз очень давно (и вы не помните, что делал).

Решив самостоятельно справиться с ситуацией, вы озадачились:

- Как кто-то мог получить доступ к принтеру? Почему это произошло?
- Что могло произойти с телевизором?
- Как можно было нарушить работу домашнего Интернета? Что нужно делать в первую очередь при появлении таких признаков?
- Если были признаки у принтера, сети и телевизора, что еще могли сделать с нашей техникой? Смотрели ли за вами по веб-камере, подслушивали разговоры?
- В чем причины и как избежать в будущем подобных ситуаций?

Напишите в виде инструкции, чтобы вы сделали на месте Маши, чтобы, с одной стороны восстановить спокойствие дома, с другой – уберечь от подобных ситуаций себя и близких. Для иллюстрации добавьте скриншоты и ссылки на дополнительные статьи.

Критерии оценивания кейса № 4

Критерий	5 баллов	2,5 балла	0 баллов
Наличие ответов на поставленные в ситуации вопросы	Имеется	Частично имеется	Не имеется
Полнота анализа ситуации	Имеется	Частично имеется	Не имеется
Достаточность инструкции для действия	Имеется	Частично имеется	Не имеется
Наличие альтернативных вариантов решений	Имеется	Частично имеется	Не имеется
Адекватная идентификация проблем и решений	Имеется	Частично имеется	Не имеется
Презентация (защита) решений, владение темой	Имеется	Частично имеется	Не имеется
Итого	30		

Оценка «зачтено» ставится при условии суммы баллов по критериям не менее 16.
В иных случаях ставится оценка «не зачтено».

Лист внесения изменений

Дополнения и изменения в рабочей программе дисциплины на 2019/2020 учебный год.

Рабочая программа разработана впервые для данной ОПОП (ФГОС 3++).

Рабочая программа рассмотрена и одобрена на заседании кафедры информатики и информационных технологий в образовании.

Внесенные изменения утверждаю:

Протокол № 9 от «08» мая 2019 г.

Заведующий кафедрой _____ Н.И. Пак

Одобрено научно-методическим советом ИМФИ

Протокол № 8 от «16» мая 2019 г.

Председатель _____ С.В. Бортновский

Лист внесения изменений

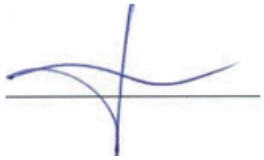
Дополнения и изменения в рабочую программу дисциплины
на 2020/2021 учебный год

В программу вносятся следующие изменения:

1. Обновлены титульные листы рабочей программы, фонда оценочных средств.
2. Обновлена и согласована с Научной библиотекой КГПУ им. В.П. Астафьева «Карта литературного обеспечения (включая электронные ресурсы)», содержащая основную и дополнительную литературу, современные профессиональные базы данных и информационные справочные системы.
3. Обновлена «Карта материально-технической базы дисциплины», включающая аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля успеваемости и промежуточной аттестации, помещения для самостоятельной работы обучающихся в КГПУ им. В.П. Астафьева) и комплекс лицензионного и свободно распространяемого программного обеспечения.

Программа пересмотрена и одобрена на заседании кафедры
20 мая 2020 г., протокол № 11

Внесенные изменения утверждаю:

Заведующий кафедрой  Н.И. Пак

Одобрено НМСС(Н)

20 мая 2020 г., протокол №8

Председатель  С.В. Бортновский

Лист внесения изменений

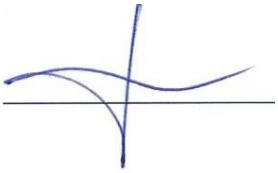
Дополнения и изменения в рабочей программе дисциплины на 2021/2022 учебный год.

В рабочую программу дисциплины вносятся следующие изменения:

1. Обновлены титульные листы рабочей программы и фонда оценочных средств.
2. Актуализирована карта материально-технической базы дисциплины в соответствии с состоянием аудиторного фонда.

Программа рассмотрена и одобрена на заседании кафедры информатики и информационных технологий в образовании

Протокол № 9 от «12» мая 2021 г.

Заведующий кафедрой  Н.И. Пак

Одобрено научно-методическим советом ИМФИ

Протокол № 7 от «21» мая 2021 г.

Председатель  Бортновский С.В.

4.РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Карта литературного обеспечения дисциплины

Наименование	Место хранения/ электронный адрес	Кол-во экземпляров/ точек доступа
ОСНОВНАЯ ЛИТЕРАТУРА		
Артемов, А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.: табл., схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605	ЭБС «Университетская библиотека онлайн»	Индивидуальный неограниченный доступ
Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил.; [Электронный ресурс] URL: http://biblioclub.ru/index.php?page=book&id=428820	ЭБС «Университетская библиотека онлайн»	Индивидуальный неограниченный доступ
Информационная безопасность [Текст] : учебное пособие / С. В. Петров [и др.] ; М-во образования и науки Российской Федерации, ФГБОУ ВПО «Новосибирский гос. пед. ун-т», ФГБОУ ВПО «Московский пед. гос. ун-т». - Новосибирск : АРТА, 2012. [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=425587	ЭБС «Университетская библиотека онлайн»	Индивидуальный неограниченный доступ
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА		
Современные компьютерные технологии : учебное пособие / Р.Г. Хисматов, Р.Г. Сафин, Д.В. Тунцев, Н.Ф. Тимербаев. - Казань: Издательство КНИТУ, 2014. - 83 с. : схем. - Библиогр. в кн. - ISBN 978-5-7882-1559-4; [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428016	ЭБС «Университетская библиотека онлайн»	Индивидуальный неограниченный доступ

Партыка, Т.Л. Информационная безопасность: учебное пособие/Т.Л. Партыка. –М.: ФОРУМ: ИНФРА-М, 2013. – 368 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=111911	ЭБС «Университетская библиотека онлайн	Индивидуальный неограниченный доступ
Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895	ЭБС «Университетская библиотека онлайн	Индивидуальный неограниченный доступ
Соснин, В.В. Облачные вычисления в образовании / В.В. Соснин. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 110 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429074	ЭБС «Университетская библиотека онлайн	Индивидуальный неограниченный доступ
Защита информации: учебное пособие / А. П. Жук [и др.]. - 2-е изд. - Москва : ИЦ РИОР ; Москва : НИЦ ИНФРА-М, 2015. - 392 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=426587	ЭБС «Университетская библиотека онлайн	Индивидуальный неограниченный доступ
УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ		
Мельников, В. П. Методы и средства хранения и защиты компьютерной информации [Текст]: учебник для студентов вузов / В. П. Мельников. - Старый Оскол : ТНТ, 2014. - [Электронный ресурс]. URL: https://icdlib.nspu.ru/view/icdlib/6415/read.php	Межвузовская электронная библиотека (МЭБ)	Индивидуальный неограниченный доступ
Электронный учебный курс «Защита информации» авт. Ломаско П.С., КГПУ им. В. П. Астафьева URL: http://e.kspu.ru/course/view.php?id=282	Электронный университет сайт КГПУ им. В.П. Астафьева	Индивидуальный доступ
РЕСУРСЫ СЕТИ ИНТЕРНЕТ		
Толковый словарь терминов понятийного аппарата информатизации образования / составители И.В. Роберт, Т.А. Лавина. – М.: БИНОМ. Лаборатория знаний, 2012. – 69 с.: ил. - (Информатизация образования).	http://www.iiorao.ru/iio/pages/fonds/dict/Dictionary.pdf	Свободный доступ

ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ И ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ		
Научная библиотека КГПУ им. В.П. Астафьева	http://library.kspu.ru/jirbis2/	Локальная сеть вуза
Межвузовская электронная библиотека (МЭБ)	https://icdlib.nspu.ru/	Индивидуальный неограниченный доступ
Elibrary.ru [Электронный ресурс): электронная библиотечная система : база данных содержит сведения об отечественных книгах и периодических изданиях но информатике / Рос. информ. портал. - Москва. 2000- . - Режим доступа: http:// elibrary.ru.	http://elibrary.ru	Свободный доступ

Согласовано:

Главный библиотекарь _____/ Фортова А.А.
(должность структурного подразделения) (подпись) (Фамилия И.О.)

4.2 Карта материально-технической базы дисциплины

Аудитория	**Оборудование** **(наглядные пособия, макеты, модели, лабораторное оборудование, компьютеры, интерактивные доски, проекторы, программное обеспечение)**
для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля успеваемости и промежуточной аттестации	
для проведения занятий лекционного типа	
Перенсона,7 **(Корпус №4)** № 2-04	**Оборудование** Маркерная доска – 1 шт., ноутбук – 10шт., мультимедийный демонстрационный комплекс (проектор, интерактивная доска, колонки, USB-камера) – 1шт., система видеоконференцсвязи Policom – 1шт. **Программное обеспечение** Альт Образование 8 (лицензия № AAO.0006.00, договор № ДС 14-2017 от 27.12.2017
Перенсона, 7 **(Корпус №4)** № 2-06	**Оборудование** Компьютер– 9шт., проектор – 1шт., наглядные пособия (стенды), маркерная доска – 1шт. с устройством для интерактивной доски, доска маркерная – 1шт. **Программное обеспечение** Альт Образование 8 (лицензия № AAO.0006.00, договор № ДС 14-2017 от 27.12.2017
Перенсона, 7 **(Корпус №4)** № 2-11	**Оборудование** Учебная доска-1шт., проектор-1шт., компьютер-1шт., маркерная доска-1шт., демонстрационный стол-1шт **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-01	**Оборудование** Интерактивная доска – 1шт., магнитно-маркерная доска – шт., документ-камера – 1шт., демонстрационная панель (телевизор) – 1шт., ноутбуки -13шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)**	**Оборудование** Компьютер- 1шт., интерактивная доска - 1 шт., система видеоконференцсвязи Policom – 1 шт. (без сети), учебная

№ 3-02	доска-1шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-11	**Оборудование** Учебная доска-1шт., экран-1шт., проектор-1шт., компьютер-1шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-12	**Оборудование** Компьютер -10шт., учебная доска-1 шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-13,3-14	**Оборудование** Компьютер-15шт., принтер-1шт., маркерная доска-1шт., проектор-1шт., интерактивная доска-1шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-15	**Оборудование** Проектор-1шт., компьютер-12шт., маркерная доска-1шт., интерактивная доска-1шт. **Программное обеспечение** Microsoft® Windows® 8.1 Professional (OEM лицензия, контракт № 20А/2015 от 05.10.2015); Kaspersky Endpoint Security – Лиц сертификат №1B08-190415-050007-883-951; 7-Zip - (Свободная лицензия GPL); Adobe Acrobat Reader – (Свободная лицензия); Google Chrome – (Свободная лицензия); Mozilla Firefox – (Свободная лицензия); LibreOffice – (Свободная лицензия GPL); XnView – (Свободная лицензия); Java – (Свободная лицензия); VLC – (Свободная лицензия); Живая математика 5.0 (Контракт НКС-ДБ-294/15 от 21.09.2015, лицензия № 201515111); GeoGebra (Свободно распространяемая в некоммерческих (учебных) целях лицензия)
Перенсона, 7 **(Корпус №4)** № 4-02	**Оборудование** Компьютер -1шт., проектор-1шт., интерактивная доска-1шт., маркерная доска-1шт., учебная доска-1шт. **Программное обеспечение**

	Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 4-11	**Оборудование** Учебная доска-1шт. **Программное обеспечение** Нет
Перенсона, 7 **(Корпус №4)** № 4-12	**Оборудование** Компьютер – 10 шт., проектор – 1 шт., интерактивная доска – 1шт., маркерная доска – 1 шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
для проведения семинаров и лабораторных работ	
Перенсона,7 **(Корпус №4)** № 2-04	**Оборудование** Маркерная доска – 1 шт., ноутбук – 10шт., мультимедийный демонстрационный комплекс (проектор, интерактивная доска, колонки, USB-камера) – 1шт., система видеоконференцсвязи Policom – 1шт. **Программное обеспечение** Альт Образование 8 (лицензия № ААО.0006.00, договор № ДС 14-2017 от 27.12.2017
Перенсона,7 **(Корпус №4)** №1-09	**Оборудование** Компьютер-3шт., 3D-принтер-1шт., сервер-1шт., проектор-1шт., принтер-1 шт., интерактивная доска-1шт., маркерная доска -1шт., система видеокнференцсвязи Поликом **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 2-06	**Оборудование** Компьютер– 9шт., проектор – 1шт., наглядные пособия (стенды), маркерная доска – 1шт. с устройством для интерактивной доски, доска маркерная – 1шт. **Программное обеспечение** Альт Образование 8 (лицензия № ААО.0006.00, договор № ДС 14-2017 от 27.12.2017
Перенсона, 7 **(Корпус №4)**	**Оборудование** Интерактивная доска – 1шт., магнитно-маркерная доска – шт., документ-камера – 1шт.,

№ 3-01	демонстрационная панель (телевизор) – 1шт., ноутбуки -13шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-07	**Оборудование** Компьютер - 12 шт., интерактивная доска – 1шт., доска флипчарт – 1 шт., проектор – 1 шт., колонки – 1 шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-08	**Оборудование** Компьютер - 8 шт., интерактивная доска – 1шт., телевизор – 1 шт., маркерная доска – 1 шт., проектор-1шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-12	**Оборудование** Компьютер -10шт., учебная доска-1 шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-13,3-14	**Оборудование** Компьютер-15шт., принтер-1шт., маркерная доска-1шт., проектор-1шт., интерактивная доска-1шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
Перенсона, 7 **(Корпус №4)** № 3-15	**Оборудование** Проектор-1шт., компьютер-12шт., маркерная доска-1шт., интерактивная доска-1шт. **Программное обеспечение** Microsoft® Windows® 8.1 Professional (OEM лицензия, контракт № 20А/2015 от 05.10.2015); Kaspersky Endpoint Security – Лиц сертификат №1B08-190415-050007-883-951; 7-Zip - (Свободная лицензия GPL); Adobe Acrobat Reader – (Свободная лицензия); Google Chrome – (Свободная лицензия); Mozilla Firefox – (Свободная лицензия); LibreOffice – (Свободная лицензия GPL); XnView – (Свободная лицензия); Java – (Свободная лицензия); VLC – (Свободная лицензия);

	Живая математика 5.0 (Контракт НКС-ДБ-294/15 от 21.09.2015, лицензия № 201515111); GeoGebra (Свободно распространяемая в некоммерческих (учебных) целях лицензия)
Перенсона, 7 **(Корпус №4)** № 4-12	**Оборудование** Компьютер – 10 шт., проектор – 1 шт., интерактивная доска – 1шт., маркерная доска – 1 шт. **Программное обеспечение** Linux Mint – (Свободная лицензия GPL)
для самостоятельной работы	
Перенсона,7 **(Корпус №4)** №1-02	**Оборудование** Компьютер-10шт., принтер-1шт. **Программное обеспечение** Альт Образование 8 (лицензия № ААО.0006.00, договор № ДС 14-2017 от 27.12.2017