

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Кислова Наталья Николаевна

Должность: Проректор по учебно-методической

Дата подписания: 01.09.2026 11:49:32

Уникальный программный ключ:

52802513f5b14a975b3e9b13008093d5726b159bf6064f865ae65b96a966c035

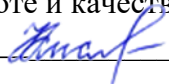
Федеральное государственное бюджетное образовательное учреждение высшего образования

«Самарский государственный социально-педагогический университет»

Кафедра информатики, прикладной математики и методики их преподавания

Утверждаю

Проректор по учебно-методической
работе и качеству образования

 Н.Н. Кислова

Добудько Александр Валерьянович

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации по дисциплине

«Информационная безопасность и защита информации»

Направление подготовки:

44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль)

«Информатика» и «Фиджитал-спорт»

Квалификация выпускника

Бакалавр

Рассмотрено

Протокол №11 от 23.06.2026

Заседания кафедры информатики, прикладной
математики и методики их преподавания

Одобрено

Начальник

образовательных программ

 Н.А. Доманина

Управления

Пояснительная записка

Фонд оценочных средств (далее – ФОС) для промежуточной аттестации по дисциплине «Информационная безопасность и защита информации» разработан в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), утвержденного приказом Министерства образования и науки Российской Федерации от 22 февраля 2018 г. № 125, основной профессиональной образовательной программой «Информатика» и «Фиджитал-спорт» с учетом требований профессионального стандарта 01.001 «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 октября 2013 г. № 544н (зарегистрирован Министерством юстиции Российской Федерации 6 декабря 2013 г., регистрационный № 30550), с изменениями, внесенными приказами Министерства труда и социальной защиты Российской Федерации от 25 декабря 2014 г. № 1115н (зарегистрирован Министерством юстиции Российской Федерации 19 февраля 2015 г., регистрационный № 36091) и от 5 августа 2016 г. № 422н (зарегистрирован Министерством юстиции Российской Федерации 23 августа 2016 г., регистрационный № 43326), 01.003 «Педагог дополнительного образования детей и взрослых» утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 22 сентября 2012 г. № 652н от 22.09.2021 г. (Зарегистрировано в Минюсте России 17.12.2021 N 66403).

Цель ФОС для промежуточной аттестации – установление уровня сформированности части компетенции ПК-1.

Задачи ФОС для промежуточной аттестации - контроль качества и уровня достижения результатов обучения по формируемым в соответствии с учебным планом компетенциям:

ПК-1. Способен осуществлять педагогическую деятельность по реализации образовательного процесса по предмету

ПК-1.1. Умеет реализовывать образовательную программу по предмету с учетом специфики содержания, методов и инструментов соответствующей области научного знания

Знает: основные понятия «информационной безопасности»; правовые основы информационной безопасности и защиты персональных данных; программные и технические средства защиты информации; основы криптографических методов защиты информации.

Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации.

ПК-1.2. Реализует образовательную программу по предмету с использованием технологий профессиональной деятельности

Умеет: использовать знания по информационной безопасности и защите информации при реализации образовательной программы по информатике.

Требования к процедуре оценки:

Помещение: компьютерный класс.

Оборудование: ноутбуки / персональные компьютеры.

Инструменты: особых требований нет.

Расходные материалы: бумага, ручка.

Доступ к дополнительным справочным материалам: не предусмотрен.

Нормы времени: 120 мин.

Комплект оценочных средств для проведения промежуточной аттестации

Проверяемая компетенция:

ПК-1. Способен осуществлять педагогическую деятельность по реализации образовательного процесса по предмету

Проверяемый индикатор достижения компетенции:

ПК-1.1. Умеет реализовывать образовательную программу по предмету с учетом специфики содержания, методов и инструментов соответствующей области научного знания

Проверяемые результаты обучения:

Знает: основные понятия «информационной безопасности»; правовые основы информационной безопасности и защиты персональных данных; программные и технические средства защиты информации; основы криптографических методов защиты информации.

Тип задания: Тестовые задания.

Оценочные материалы:

1. Основным средством антивирусной защиты является...

а) периодическая проверка списка загруженных программ;

б) использование сетевых экранов при работе в сети Интернет;

в) периодическая проверка компьютера с помощью антивирусного программного обеспечения;

г) периодическая проверка списка автоматически загружаемых программ.

2. Выберите составляющие сетевого аудита:
 - а) аудит безопасности каждой новой системы (как программной, так и аппаратной) при ее инсталляции в сеть;
 - б) регулярный автоматизированный аудит сети
 - в) антивирусная проверка сети
 - г) выборочный аудит безопасности
3. Принципиальным отличием межсетевых экранов от систем обнаружения атак является следующее:
 - а) первые были разработаны для активного или пассивного обнаружения, а вторые – для активной или пассивной защиты;
 - б) первые были разработаны для активной или пассивной защиты, а вторые – для активного или пассивного обнаружения;
 - в) первые работают только на сетевом уровне, а вторые – еще и на физическом;
 - г) отличий нет.
4. Сетевые черви представляют собой:
 - а) вредоносные программы, действие которых заключается в создании сбоев при питании компьютера от электрической сети;
 - б) программы, которые изменяют файлы на дисках, и распространяются в пределах компьютера;
 - в) программы, которые не изменяют файлы на дисках, а распространяются в компьютерной сети, проникают в операционную систему компьютера, находят адреса других компьютеров или пользователей и рассылают по этим адресам свои копии;
 - г) программы, распространяющиеся только при помощи электронной почты.
5. Наиболее защищенными от несанкционированного доступа линиями связи сегодня являются...
 - а) радио;
 - б) электрические;
 - в) инфракрасные;
 - г) оптоволоконные.
6. Электронно-цифровая подпись (ЭЦП) документа позволяет получателю ...
 - а) только удостовериться в истинности отправителя документа, но не проверить подлинность документа;
 - б) либо удостовериться в корректности отправителя документа, либо удостовериться в том, что документ не изменен во время передачи;
 - в) удостовериться в корректности отправителя документа и удостовериться в том, что документ не изменен во время передачи;
 - г) только удостовериться в том, что документ не изменен во время передачи.
7. Метод защиты информации «разграничение доступа» заключается в:
 - а) создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям;
 - б) разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
 - в) том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
 - г) преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду.
8. Метод защиты информации «разделение доступа (привилегий)» заключается в:
 - а) создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям;
 - б) разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
 - в) том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
 - г) преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду.
9. Метод защиты информации «ограничение доступа» заключается в:
 - а) создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям;
 - б) разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;

в) том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;

г) преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду.

10. Что означает термин «правовые меры защиты информации»?

а) это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией;

б) это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения;

в) регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой;

г) это механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.

11. Что означает термин «морально-этические меры защиты информации»?

а) это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией;

б) это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения;

в) регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой;

г) это механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.

12. Что означает термин «организационные меры защиты информации»?

а) это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией;

б) это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения;

в) регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой;

г) это механические или электронно-механические устройства и сооружения, специально предназначенные для создания различных препятствий на возможных путях проникновения доступа потенциальных нарушителей к компонентам защищаемой информации.

13. Назовите программные продукты, осуществляющие контент-фильтрацию информации из сети Интернет:

а) WinZip, WinRAR;

б) Secret Disk, USB Block;

в) Panda Security, Norton Security;

г) Content Keeper, KidGid.

14. Наука о способах шифрования информации называется ...

15. Наука о методах и способах вскрытия шифров называется ...

16. Расшифруйте сообщение НСХ, зашифрованное с помощью шифра Цезаря со сдвигом 3.

Русский алфавит:

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

17. Зашифруйте сообщение СОК, зашифрованное с помощью шифра Цезаря со сдвигом 2.

Русский алфавит:

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

18. Функция, которая сообщение любой длины превращает в короткий код, называется ...

19. Совпадение хэш-кодов двух различных строк называется ...

20. Набор символов, который получен в результате шифрования хэш-кода передаваемого сообщения с помощью личного секретного кода отправителя с целью защиты от подделки, называется ...

Правильные ответы на вопросы теста

1. в

2. а,б,г

3. б
4. в
5. г
6. а
7. б
8. в
9. а
10. б
11. а
12. в
13. г
14. криптография
15. криптоанализ
16. КОТ
17. УРМ
18. Хэш
19. Коллизия
20. Цифровая подпись

Оценочный лист

Критерий	Максимальное количество баллов
Вопрос 1	0,5
Вопрос 2	0,5
Вопрос 3	0,5
Вопрос 4	0,5
Вопрос 5	0,5
Вопрос 6	0,5
Вопрос 7	0,5
Вопрос 8	0,5
Вопрос 9	0,5
Вопрос 10	0,5
Вопрос 11	0,5
Вопрос 12	0,5
Вопрос 13	0,5
Вопрос 14	0,5
Вопрос 15	0,5
Вопрос 16	0,5
Вопрос 17	0,5
Вопрос 18	0,5
Вопрос 19	0,5
Вопрос 20	0,5

Проверяемый индикатор достижения компетенции:

ПК-1.1. Умеет реализовывать образовательную программу по предмету с учетом специфики содержания, методов и инструментов соответствующей области научного знания

ПК-1.2. Реализует образовательную программу по предмету с использованием технологий профессиональной деятельности

Проверяемые результаты обучения:

Умеет: оценивать возможные последствия существующих угроз информационного общества, выбирать способы защиты от угроз, анализировать и обобщать информацию о состоянии информационной среды образовательной организации.

Умеет: использовать знания по информационной безопасности и защите информации при реализации образовательной программы по информатике.

Тип (форма) задания: Практическое задание.

Пример типового практического задания.

В настоящее время в учебном процессе используется большое количество образовательных онлайн-сервисов. Например, популярным способом заучивания информации являются индексные карточки, работу с которыми существенно упрощает сервис Quizlet. Для использования данного сервиса требуется регистрация, подразумевающая принятие пользовательского соглашения и политики обработки персональных данных.

Вам предлагается проанализировать пользовательское соглашение (условия предоставления услуг) и политику обработки персональных данных (политику конфиденциальности) данного сервиса согласно представленному ниже плану.

Пользовательское соглашение (условия предоставления услуг): <https://quizlet.com/ru/tos>.

Политика обработки персональных данных (конфиденциальности): <https://quizlet.com/privacy>.

1. Соответствуют ли положения настоящего соглашения и политики конфиденциальности основным положениям законодательства РФ в области защиты персональных данных, защиты информации образовательных учреждений, защиты несовершеннолетних от нежелательной информации?
2. Какие риски использования данного сервиса в учебном процессе с точки зрения информационной безопасности?
3. Допустимо ли создание карточек преподавателями на основе уже готовых бумажных наборов карточек, приобретённых ими в магазинах, согласно условиям сервиса?
4. Какие вы можете дать рекомендации по минимизации известных цифровых угроз при использовании данного сервиса в образовательной организации?

Оценочный лист к практическому заданию.

Показатель результативности	Индикатор	Максимальное количество баллов
Дан верный и полный ответ на вопрос 1, продемонстрировано знание основных положений информационного законодательства	ПК-1.1	4
Выявлено достаточное количество рисков, либо объяснено, почему искомые риски отсутствуют	ПК-1.1	4
Дан верный ответ на вопрос 3, даны ссылки на соответствующие нормативно-правовые акты (указание статей и пунктов конкретных НПА не требуется)	ПК-1.1	4
Даны рекомендации по использованию заданного сервиса в образовательном процессе, рекомендации адекватны, соответствуют закону и общепринятым этическим нормам	ПК-1.2	6

Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации

Код контролируемой компетенции (индикаторы)	Наименование оценочного средства	Максимальное количество баллов	Всего баллов	Уровень освоения компетенции (в баллах)		
				Пороговый (56-70%)	Продвинутый (71-85%)	Высокий (86-100%)
ПК-1.1	Тестовые задания	10	10	6-7	7	9-10
ПК-1.1	Практическое задание	12	12	8-9	10-11	11-12
ПК-1.2	Практическое задание	6	6	4	5	6

Полученное число баллов выставляется в графу «Промежуточная аттестация» балльно-рейтинговой карты дисциплины.