МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
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
«Методы и технологии защиты информации»
Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль): «Информатика» и «Дополнительное образование (в области информатики и ИКТ)»
Квалификация выпускника
Бакалавр

Рассмотрено
Протокол № 1 от 27.08.2019
Заседания кафедры информатики, прикладной математики и методики их преподавания

Одобрено
Начальник Управления образовательных программ
Н.А. Доманина

Самара 2019

Пояснительная записка

Фонд оценочных средств (далее – ФОС) для промежуточной аттестации по дисциплине «Методы и технологии защиты информации» разработан в соответствии с требованиями Федерального государственного образовательного стандарта 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 (зарегистрирован Министерством юстиции Российской Федерации 15 марта 2018 г., регистрационный № 50358), с изменениями, внесенными приказами Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1456 (зарегистрирован Министерством юстиции Российской Федерации 27 мая 2021 г., регистрационный № 63650) и от 8 февраля 2021 г. № 83 (зарегистрирован Министерством юстиции Российской Федерации 12 марта 2021 г., регистрационный № 62739), основной профессиональной образовательной программой «Информатика» и «Дополнительное образование (в области информатики и ИКТ)» с учетом требований профессионального стандарта «01.001 Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», утвержденного 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 ОПК-1.

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

Общепрофессиональная компетенция – ОПК-1

Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики

Знает: положения основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений

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

Владеет: приемами защиты информации обучающихся в образовательном процессе при работе со средствами информационно-коммуникационных технологий.

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:

Общепрофессиональная компетенция – ОПК-1

Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики

Проверяемый индикатор достижения компетенции:

ОПК-1.1. Знает: положения основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений.

Проверяемые результаты обучения:

Знает: положения основных нормативных документов, регламентирующих деятельность в области защиты информации образовательных учреждений

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 защищёнными 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 изменён во время передачи;
в) удостовериться в корректности отправителя документа и удостовериться в том, что документ не изменён во время передачи;
г) только удостовериться в том, что документ не изменён 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	1
Вопрос 2	1
Вопрос 3	1
Вопрос 4	1
Вопрос 5	1
Вопрос 6	1
Вопрос 7	1
Вопрос 8	1
Вопрос 9	1
Вопрос 10	1
Вопрос 11	1
Вопрос 12	1
Вопрос 13	1
Вопрос 14	1
Вопрос 15	1
Вопрос 16	1
Вопрос 17	1
Вопрос 18	1
Вопрос 19	1
Вопрос 20	1

Проверяемый индикатор достижения компетенции:

ОПК-1.2. Умеет: применять основные нормативно-правовые акты в сфере образования и нормы профессиональной этики.

ОПК-1.3. Владеет действиями по соблюдению правовых, нравственных и этических норм, требований профессиональной этики в условиях реальных педагогических ситуаций; действиями по осуществлению профессиональной деятельности в соответствии с требованиями федеральных государственных образовательных стандартов в части анализа содержания современных подходов к организации и функционированию системы образования.

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.

Владеет: приемами защиты информации обучающихся в образовательном процессе при работе со средствами информационно-коммуникационных технологий.

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 индексовые 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	ОПК-1.2	5
Выявлено достаточное количество рисков, либо объяснено, почему искомые риски отсутствуют	ОПК-1.2	10
Дан верный ответ на вопрос 3, даны ссылки на соответствующие нормативно-правовые акты (указание статей и пунктов конкретных НПА не требуется)	ОПК-1.2	5
Даны рекомендации по использовании заданного сервиса в образовательном процессе, рекомендации адекватны, соответствуют закону и общепринятым этическим нормам	ОПК-1.3	20

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%)
ОПК-1.1	Тестовые задания	20	20	12-14	15-17	18-20
ОПК-1.2	Практическое задание	20	20	12-14	15-17	18-20
ОПК-1.3	Практическое задание	20	20	12-14	15-17	18-20

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