

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Кислова Наталья Николаевна

Должность: Проректор по учебно-методической работе

Дата подписания: 27.08.2019

Уникальный программный ключ:

52802513f5b14a975b3e9b13008093d5726b159bf6064f865ae65b96a966c035

## 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

Горбатов Сергей Васильевич

### ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения промежуточной аттестации по дисциплине  
«Информационная безопасность»

Направление подготовки 09.03.03 Прикладная информатика

Направленность (профиль):

«Прикладная информатика в государственном и муниципальном управлении»

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

Пояснительная записка

Фонд оценочных средств (далее – ФОС) для промежуточной аттестации по дисциплине «Информационная безопасность» разработан в соответствии с ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика (утвержден приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 922), основной профессиональной образовательной программой высшего образования по направлению подготовки 09.03.03 «Прикладная информатика» (профиль «Прикладная информатика в государственном и муниципальном управлении»), с учетом требований профессионального стандарта 06.015 «Специалист по информационным системам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. №896н (зарегистрирован Министерством юстиции Российской Федерации 24 декабря 2014 г., регистрационный №35361), с изменением, внесенным приказом Министерством труда и социальной защиты Российской Федерации от 12 декабря 2016 г. №727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный №45230).

Цель ФОС для промежуточной аттестации – установление уровня сформированности части общепрофессиональных компетенции ОПК-3, ОПК-4.

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

способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4).

Требования к процедуре оценки:

Помещение: компьютерный класс.

Оборудование: ноутбуки / персональные компьютеры, сетевое оборудование для доступа в Интернет.

Инструменты: особых требований нет.

Расходные материалы: не требуются.

Доступ к дополнительным справочным материалам: не предусмотрен.

Нормы времени: 120 мин.

**Комплект оценочных средств для проведения  
промежуточной аттестации  
Курс 4 Семестр 6**

**Проверяемая компетенция:**

**Общепрофессиональная компетенция ОПК-3.**

Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

**Проверяемый индикатор:**

**ОПК-3.1:** знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

**Проверяемые образовательные результаты:**

Знает: основные требования, предъявляемые к информационным системам в области защиты информации.

**Общепрофессиональная компетенция ОПК-4.**

Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.

**Проверяемый индикатор:**

**ОПК-4.1:** знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

**Проверяемые образовательные результаты:**

Знает: законодательную базу защиты информации в РФ, модели разграничения доступа, аутентификацию субъектов доступа.

**Задание 1.**

Тип (форма) задания: тест.

Содержание задания:

Задание №1 (ОПК-3.1)	
Максимальное расстояние между компьютерами в локальной сети Ethernet	
Выберите один из 5 вариантов ответа:	
1)	10 км.
2)	2500 м.
3)	90 м.
4)	1000 м.
5)	500 м.

Задание №2 (ОПК-3.1)	
Обмен информацией между компьютерными сетями, в которых действуют разные сетевые протоколы, осуществляется с использованием	
Выберите один из 5 вариантов ответа:	
1)	хост-компьютеров
2)	файл-серверов
3)	модемов
4)	шлюзов
5)	электронной почты

Задание №3 (ОПК-4.1)	
Сколько проводов использует стандарт 100Base-T4	
Выберите один из 4 вариантов ответа:	
1)	2
2)	1
3)	4

4)	8
----	---

## Задание №4 (ОПК-4.1)

В основе централизованной модели сертификации лежит уполномоченный орган, называемый

Выберите один из 4 вариантов ответа:

1)	удостоверяющим центром сертификации
2)	вышестоящим центром сертификации
3)	доверенным центром сертификации
4)	корневым центром сертификации

## Задание №5 (ОПК-3.1)

Какое оптоволокно более толстое?

Выберите один из 3 вариантов ответа:

1)	Одномодовое
2)	Коаксиальное
3)	Многомодовое

## Задание №6 (ОПК-3.1)

Какой способ реализации криптографических методов обладает максимальной скоростью обработки данных?

Выберите один из 4 вариантов ответа:

1)	программный
2)	аппаратный
3)	электромеханический
4)	ручной

## Задание №7 (ОПК-3.1)

Расшифруйте сообщение @-\*(-)^#\*, зашифрованное с помощью шифра №2. Ответ запишите прописными буквами. Если ответ состоит из нескольких слов, запишите его пробелами, например: НОВОЕ ЗАДАНИЕ

Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2
А	В	^	М	Т	№	Ч	М	Σ
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	†
Г	А	+	П	Ж	=	Ъ	Э	№
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∇	Т	Х	%	Э	Ы	ω
З	Б	◆	У	С	⊗	Ю	Ш	\$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	пробел	♥	Х	Ч	№	пробел	Ф	∞
Л	Р	♠	Ц	З	⊗	.	Я	♣

## Задание №8 (ОПК-4.1)

Шифрование – это:

Выберите один из 3 вариантов ответа:

1)	процесс создания алгоритмов шифрования
2)	процесс сжатия информации
3)	процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется

## Задание №9 (ОПК-4.1)

Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:

Выберите один из 3 вариантов ответа:

1)	на основе только шифротекста
2)	на основе произвольно выбранного шифротекста

3)	на основе произвольно выбранного открытого текста
----	---

## Задание №10 (ОПК-4.1)

Что в криптографии называют открытым текстом?

Выберите один из 4 вариантов ответа:

1)	открытый ключ шифрования
2)	сообщение, полученное после преобразования с использованием любого шифра
3)	исходное сообщение (сообщение до шифрования)
4)	электронную цифровую подпись

## Задание №11 (ОПК-3.1)

Расшифруйте сообщение ИБЛКНАКУ, зашифрованное методом перестановки с фиксированным переводом  $d=6$  с ключом 73825146.

## Задание №12 (ОПК-3.1)

Шифр, который заключается в перестановках структурных элементов шифруемого блока данных-битов, символов, цифр – это:

Выберите один из 3 вариантов ответа:

1)	шифр замен
2)	шифр перестановок
3)	шифр функциональных преобразований

## Задание №13 (ОПК-3.1)

Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им массива открытых данных размера  $n$  используется в анализе:

Выберите один из 3 вариантов ответа:

1)	на основе произвольно выбранного открытого текста
2)	на основе произвольно выбранного шифротекста
3)	правильного ответа нет

## Задание №14 (ОПК-3.1)

Как называется "исторический" шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?

Выберите один из 4 вариантов ответа:

1)	шифр Цезаря
2)	шифр Бэббиджа
3)	шифр Маркова
4)	шифр Энигма

## Задание №15 (ОПК-3.1)

Определите ключи шифра Цезаря, если известны следующая пара открытый текст-шифротекст: ГРУША-КЛОУНЫ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

## Задание №16

Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:

Выберите один из 3 вариантов ответа:

1)	со стороны законного получателя сообщения
2)	со стороны злоумышленника
3)	со стороны законного отправителя сообщения

## Задание №17 (ОПК-4.1)

Определите ключ в системе шифрования, использующий перестановку с фиксированным периодом  $d=5$  по паре открытых и зашифрованных сообщений: ОДНА\_БУКВА-\_НОАДАКБВУ. Ответ запишите в виде последовательности цифр без пробелов.

## Задание №18 (ОПК-4.1)

Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется:

Выберите один из 3 вариантов ответа:

- 1) расшифровка
- 2) дешифровка
- 3) шифрование

## Задание №19 (ОПК-4.1)

Расшифруйте сообщение  $!(^*=%-+(\wedge\text{№}\text{№}\wedge)$ , зашифрованное с помощью шифра №2. Ответ запишите прописными буквами. Если ответ состоит из нескольких слов, запишите его пробелами, например: НОВОЕ ЗАДАНИЕ

Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2	Откр. текст	Шифр 1	Шифр 2
А	В	^	М	Т	№	Ч	М	Σ
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	†
Г	А	+	П	Ж	=	Ъ	Э	∞
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∇	Т	Х	%	Э	Ы	ω
З	Б	◆	У	С	⊗	Ю	Ш	\$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	пробел	♥	Х	Ч	№	пробел	Ф	∞
Л	Р	♠	Ц	З	⊗	.	Я	♣

## Задание №20 (ОПК-4.1)

Как называется шифр, в котором каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе символом другого алфавита?

Выберите один из 4 вариантов ответа:

- 1) Шифром Цезаря
- 2) Шифром одноалфавитной подстановки
- 3) Шифром замены
- 4) Шифром многоалфавитной подстановки

## Правильные ответы к заданию 1

Номер вопроса	Правильный ответ	Максимальное количество баллов
#1	3	1
#2	4	1
#3	3	1
#4	4	1
#5	1	1
#6	1	1
#7	Ответ = БОИФРОВАНИ	1
#8	3	1
#9	2	1
#10	3	1
#11	Ответ = КЛУБНИКА	1
#12	2	1
#13	1	1
#14	1	1
#15	Ответ = 28	1

#16	2	1
#17	Ответ = 5314210897	1
#18	2	1
#19	Ответ = КРИПТОГРАММА	1
#20	2	1

**Проверяемый индикатор:**

**ОПК-3.2:** умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

**Проверяемые образовательные результаты:**

Умеет: использовать нормативные документы в области защиты информации и информационной безопасности; формировать теоретическую модель угроз информационной безопасности.

**Задание 2.**

Содержание задания:

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам (оформить в виде отчета):

1. Виды возможных угроз.
2. Характер происхождения угроз.
3. Классы каналов несанкционированного получения информации.
4. Источники появления угроз.
5. Причины нарушения целостности информации.
6. Потенциально возможные злоумышленные действия.
7. Определить класс защищенности автоматизированной системы.

Приоритет	Виды угроз	Субъекты угроз			
		Стихия	Нарушитель	Злоумышленник	
				На территории	Вне территории
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудования, техники	+	+	+	+
3	Повреждение систем жизнеобеспечения	+	+	+	+
4	Несанкционированное изменение технологического процесса		+	+	
5	Использование нерегламентированных технических и программных средств		+	+	
6	Дезорганизация функционирования предприятия	+		+	
7	Хищение материальных ценностей			+	
8	Уничтожение или перехват данных путем хищения носителей информации			+	
9	Устное разглашение конфиденциальной информации		+		
10	Несанкционированный съем информации			+	+
11	Нарушение правил эксплуатации средств защиты		+	+	

**Оценочный лист к заданию 2.**

Показатель результативности	Индикатор ОПК-3	Максимальное количество баллов
отчетный документ расположен электронной информационно-образовательной среде	ОПК-3.2	2
преподавателю предоставлен доступ к отчетному документу для оценивания	ОПК-3.2	2
студент демонстрирует развитые навыки поиска информации в поисковых системах сети Интернет, электронных	ОПК-3.2	2

библиотечных системах, электронной информационно-образовательной среде СГСПУ		
отчет содержит список использованных источников, оформленный по ГОСТР 7.0.5–2008	ОПК-3.2	2
отчет содержит инструкцию по загрузке дистрибутива из центра академического программного обеспечения с описанием процесса поиска	ОПК-3.2	2

**Проверяемый индикатор:**

**ОПК-3.3:** владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

**Проверяемые образовательные результаты:**

Способен объективно оценить необходимый уровень информационной безопасности при подготовке публикаций обзорного характера о деятельности органов государственного и муниципального управления.

**Задание 3.**

Содержание задания (оформить в виде отчета):

1. Определить полный перечень персональных данных, обрабатываемых в организации.
2. Определить категории обрабатываемых персональных данных.
3. Определить перечень сотрудников, работающих с персональными данными и для каждого установить перечень ПДн.
4. Определить класс информационной системы обработки ПДн
5. Описать соответствующие меры по защите ПДн.

**Описание:**

Задание выполняется в соответствии с лекционным материалом и дополнительной литературой к данной лабораторной работе.

**Контрольные вопросы:**

1. Что такое персональные данные?
2. На основании, каких документов составляется перечень ПДн?
3. Перечислите все категории ПДн.
4. Какими критериями служат для определения категории ПДн?
5. На основании, каких документов определяется перечень сотрудников обрабатывающих ПДн.
6. Что такое класс информационной системы обработки ПДн?
7. Опишите методику определения класса информационной системы обработки ПДн.
8. Назовите основные организационные меры, которые используются для защиты ПДн.
9. Назовите основные виды программных и программно-аппаратных средств, использующихся при защите ПДн.

**Оценочный лист к заданию 3.**

Показатель результативности	Индикатор ОПК-3	Максимальное количество баллов
отчетный документ расположен электронной информационно-образовательной среде	ОПК-3.3	2
преподавателю предоставлен доступ к отчетному документу для оценивания	ОПК-3.3	2
студент демонстрирует развитые навыки поиска информации в поисковых системах сети Интернет, электронных библиотечных системах, электронной информационно-образовательной среде СГСПУ	ОПК-3.3	2
отчет содержит список использованных источников, оформленный по ГОСТР 7.0.5–2008	ОПК-3.3	2
отчет содержит инструкцию по загрузке дистрибутива из центра академического программного обеспечения с описанием процесса поиска	ОПК-3.3	2

**Проверяемый индикатор:**

**ОПК-4.2:** умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

**Проверяемые образовательные результаты:**

Умеет: использовать нормативные документы в области защиты информации и информационной безопасности.

**Задание 4.**

Содержание задания:

1. Запустите виртуальную машину Ubuntu. Определить настройки протокола TCP/IP Вашего компьютера с помощью команды ifconfig. Сделайте экранный снимок сетевых настроек.



2. Для использования утилиты iptables требуются привилегии суперпользователя (root). В консоли введите команду su root и далее пароль суперпользователя.
3. Установите политику по умолчанию ACCEPT для цепочек INPUT, FORWARD и OUTPUT. В отчет вставьте введенные правила.
4. Закройте порт 80 цепочки INPUT для всех IP адресов. Остальные порты цепочки INPUT должны быть открыты. В отчет вставьте введенные правила. Перейдите в браузере по адресу http://localhost/. Проанализируйте в Wireshark какие изменения произошли в сетевом трафике после закрытия 80 порта цепочки INPUT.
5. Закройте порт 80 цепочки INPUT только для одного выбранного IP адреса. Для всех остальных IP адресов порт 80 должен быть открыт. В отчет вставьте введенные правила.
6. Закройте порт 80 цепочки OUTPUT для всех IP адресов. Остальные порты цепочки OUTPUT должны быть открыты. В отчет вставьте введенные правила. Перейдите в браузере по адресу <http://localhost/>. Проанализируйте в Wireshark какие изменения произошли в сетевом трафике после закрытия 80 порта цепочки OUTPUT.
7. Закройте порт 80 цепочки OUTPUT только для одного выбранного IP адреса. Для всех остальных IP адресов порт 80 должен быть открыт. В отчет вставьте введенные правила.
8. Откройте возможность работы с локальным Web-сервером только Вашему компьютеру. Все остальные IP адреса не должны иметь доступ к Web-серверу компьютера. В отчет вставьте введенные правила.
9. Заблокируйте с помощью межсетевого экрана выбранные Вами Webсайты. В отчет вставьте введенные правила.
10. Ограничьте количество возможных подключений к 22 порту openssh сервера (не более 3-х подключений в минуту). Проверку осуществляйте путем 4-х подключений подряд, вбивая в консоль команду ssh localhost. В отчет вставьте введенные правила.
11. Ограничьте количество запросов на 80 порт в секунду/минуту от одного пользователя. Проверку правильности правила осуществляйте с помощью команды "ab -n 10000 -c 100 http://localhost/". В отчет вставьте введенные правила.
12. Выполните шаги 4-11, установив политику по умолчанию DROP для цепочек INPUT, FORWARD и OUTPUT (подсказка: правила придется переписать и использовать состояние соединения NEW и ESTABLISHED). Заблокируйте доступ к локальному Web-серверу пользователю с заданным MAC-адресом. В отчет вставьте введенное правило.
13. Удалите любое выбранное правило из цепочки INPUT. В отчет вставьте введенное правило. Продемонстрируйте возможности межсетевого экрана Netfilter по логированию сетевых пакетов. В отчет вставьте полученный лог и введенные правила.

#### Оценочный лист к заданию 4.

Показатель результативности	Индикатор ОПК-4	Максимальное количество баллов
отчетный документ расположен электронной информационно-образовательной среде	ОПК-4.2	2
преподавателю предоставлен доступ к отчетному документу для оценивания	ОПК-4.2	2
студент демонстрирует развитые навыки поиска информации в поисковых системах сети Интернет, электронных библиотечных системах, электронной информационно-образовательной среде СГСПУ	ОПК-4.2	2
отчет содержит список использованных источников, оформленный по ГОСТР 7.0.5–2008	ОПК-4.2	2
отчет содержит инструкцию по загрузке дистрибутива из центра академического программного обеспечения с описанием процесса поиска	ОПК-4.2	2

#### Проверяемый индикатор:

**ОПК-4.3:** владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.

#### Проверяемые образовательные результаты:

Имеет опыт подготовки технической документации для этапов проектирования, внедрения и эксплуатации информационной системы.

#### Задание 5.

Содержание задания:

1. Настройте брандмауэр Windows. Определите список программ, которым разрешено обрабатывать данные, поступающие в компьютер из внешнего окружения. Не нужно ли сократить этот список?
2. Запустите оснастку Службы. Просмотрите список установленных и работающих служб. Все ли они необходимы для вашей повседневной работы. Остановите ненужные службы.
3. В целях конфиденциальности вашей информации проведите очистку четырех частей данных браузера: списка вводимых адресов, журнала с историей посещения веб-сайтов, списка временных файлов Интернета и списка cookie-файлов.

4. Измените интерфейс Windows компьютера в целях повышения конфиденциальности вашей работы на компьютере: очистите список часто запускавшихся приложений; очистите список последних открывавшихся документов; удалите временные файлы с жесткого диска; удалите сохраненные пароли; назначьте необходимые разрешения к файлам и папкам; зашифруйте важную для вас информацию.
5. Подготовьте список документов, связанных с информационной безопасностью и защитой персональных данных по следующим категориям (Документы Университета в области информационной безопасности, образцы организационно-распорядительных документов, Федеральное законодательство, указы Президента РФ, Постановления Правительства РФ, Документы уполномоченных федеральных органов, ФСБ России, ФСТЭК России, Роскомнадзор России, Национальные стандарты в области, информационной безопасности, Нормативно-методические и руководящие документы).

**Оценочный лист к заданию 5.**

Показатель результативности	Индикатор ОПК-4	Максимальное количество баллов
отчетный документ расположен электронной информационно-образовательной среде	ОПК-4.3	2
преподавателю предоставлен доступ к отчетному документу для оценивания	ОПК-4.3	2
студент демонстрирует развитые навыки поиска информации в поисковых системах сети Интернет, электронных библиотечных системах, электронной информационно-образовательной среде СГСПУ	ОПК-4.3	2
отчет содержит список использованных источников, оформленный по ГОСТР 7.0.5–2008	ОПК-4.3	2
отчет содержит инструкцию по загрузке дистрибутива из центра академического программного обеспечения с описанием процесса поиска	ОПК-4.3	2

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

од 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-3.1	Задание 1	10	10	5-6	7-8	9-10
ОПК-3.2	Задание 2	10	10	5-6	7-8	9-10
ОПК-3.3	Задание 3	10	10	5-6	7-8	9-10
ОПК-4.1	Задание 1	10	10	5-6	7-8	9-10
ОПК-4.2	Задание 4	10	10	5-6	7-8	9-10
ОПК-4.3	Задание 5	10	10	5-6	7-8	9-10