НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ ПРОФСОЮЗОВ»

Кафедра Информатики и математики
(полное наименование кафедры)

УТВЕРЖДЕН
на заседании кафедры

Протокол №1 от 01.06.2020

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Информационная безопасность

(наименование дисциплины)

09.03.03 «Прикладная информатика»
(код наименования направления подготовки /специальности/)

Прикладная информатика в экономике
(направленность/профиль/)

Санкт-Петербург

1. Общие положения

Фонд оценочных средств (ФОС) по дисциплине используется в целях нормирования процедуры оценивания качества подготовки и осуществляет установление соответствия учебных достижений запланированным результатам обучения и требованиям образовательной программы дисциплины. Предметом оценивания являются знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций у обучающихся. Процедуры оценивания применяются в процессе обучения на каждом этапе формирования компетенций посредством определения для отдельных составных частей дисциплины методов контроля – оценочных средств. Основным механизмом оценки качества подготовки и формой контроля учебной работы студентов являются текущий контроль успеваемости и промежуточная аттестация.

1.1. Цель и задачи текущего контроля студентов по дисциплине

Цель текущего контроля – систематическая проверка степени освоения программы 09.03.03 «Прикладная информатика» дисциплины «Информационная безопасность» уровня достижения планируемых результатов обучения - знаний, умений, навыков, в ходе ее изучения при проведении занятий, предусмотренных учебным планом. Задачи текущего контроля:

1. обнаружение и устранение пробелов в освоении учебной дисциплины;
2. своевременное выполнение корректирующих действий по содержанию и организации процесса обучения;
3. определение индивидуального учебного рейтинга студентов;
4. подготовка к промежуточной аттестации.

В течение семестра при изучении дисциплины реализуется традиционная система поэтапного оценивания уровня освоения. За каждый вид учебных действий студенты получают оценку.

1.2. Цель и задачи промежуточной аттестации студентов по дисциплине.

Цель промежуточной аттестации – проверка степени усвоения студентами учебного материала, уровня достижения планируемых результатов обучения и сформированности компетенций на момент завершения изучения дисциплины. Промежуточная аттестация проходит в форме экзамена.

Задачи промежуточной аттестации:

1. определение уровня освоения учебной дисциплины;
2. определение уровня достижения планируемых результатов обучения и сформированности компетенций;
3. соотнесение планируемых результатов обучения с планируемыми результатами освоения образовательной программы в рамках изученной дисциплины.

2. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Таблица 1.

№ п\п	Контролируемые темы дисциплины	Код формируемой компетенции	Код и наименование индикатора достижения	Наименование оценочного средства
1	Социальные, политологические и правовые аспекты, виды безопасности	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности.	Опрос
2	Сетевые протоколы и модели взаимодействия открытых систем	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы Задания для самостоятельной работы
3	Тенденции развития безопасности операционных систем	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы Задания для самостоятельной работы
4	Средства и алгоритмы управления процессами, и памятью ОС	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложе-	Опрос

			ний. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Задания для самостоятельной работы
5	Безопасность клиентских приложений	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы
6	Клиентский и серверный скрипт с позиций информационной безопасности	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы
7	Каналы утечки информации. Способы несанкционированного доступа к конфиденциальной информации	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы
8	Классы задач защиты. Стратегии защиты информации	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы Задания для самостоятельной работы
9	Понятие уяз-	ОПК-3	ОПК-3.1. – Знать основные поня-	Опрос

	вимости информации, подходы к оценке уязвимости информации		тия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Задания для самостоятельной работы Задания для самостоятельной работы
10	Криптографическая защита информации в Интернете	ОПК-3	ОПК-3.1. – Знать основные понятия информационной безопасности. ОПК-3.2. – Уметь обеспечивать информационную безопасность клиентских и серверных приложений. ОПК-3.3. – Владеть алгоритмами шифрования и средствами защиты информации.	Опрос Задания для самостоятельной работы Задания для самостоятельной работы
Результат достижения планируемых результатов изучения дисциплины				экзамен

3. Описание показателей и критериев оценивания компетенций

3.1. Критерии оценивания (текущий контроль)

1. Оценка **«отлично»** выставляется студенту, если студент имеет глубокие знания учебного материала по теме практического задания, в логической последовательности излагает материал; смог ответить на все уточняющие и дополнительные вопросы;
2. Оценка **«хорошо»** выставляется, если студент показал знание учебного материала, смог ответить почти полностью на все заданные дополнительные и уточняющие вопросы;
3. Оценка **«удовлетворительно»** выставляется, если студент в целом освоил материал; однако, ответил не на все уточняющие и дополнительные вопросы;
4. Оценка **«неудовлетворительно»** выставляется студенту, если он имеет существенные пробелы в знаниях основного учебного материала по теме практического задания, который полностью не раскрыл содержание вопросов, не смог ответить на уточняющие и дополнительные вопросы.

3.2. Критерии оценивания (экзамен)

Знания, умения, навыки и компетенции студентов оцениваются следующими оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» (Таблица 2.).

Таблица 1.

Оценка	Критерии оценивания
Отлично	Студент не только глубоко и прочно усвоил весь программный материал, но и проявил знания, выходящие за его пределы, почерпнутые из дополнительных источников (классическая литература, учебная литература, научно-популярная литература, научные статьи и монографии и т. п.); умеет самостоятельно обобщать программный материал, не допуская ошибок, проанализировать его с точки зрения раз- личных школ и взглядов; увязывает знания с практикой, приводит при- меры, демонстрирующие глубокое понимание материала или проблемы, свободно справляется с задачами и практическими заданиями; исчерпывающе, последовательно, грамотно и логически стройно выстраивает свой ответ.
Хорошо	Студент твердо знает программный материал, грамотно и последовательно его излагает, увязывает с практикой, не допускает существенных неточностей в ответе на вопросы, может правильно применять теоретические положения и владеет необходимыми умениями и навыками в выполнении практических заданий и решении задач, испытывает незначительные затруднения при самостоятельном обобщении программного материала.
Удовлетворительно	Студент усвоил только основной программный материал, но не знает его отдельных положений, в ответе допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала, не в полной мере владеет необходимыми умениями и навыками в выполнении практических заданий и решении задач, испытывает затруднения при самостоятельном обобщении программного материала.
Неудовлетворительно	Студент не знает значительной части основного программного материала, в ответе допускает существенные ошибки, неправильные формулировки, не владеет необходимыми умениями и навыками в выполнении практических заданий и решении задач, испытывает значительные затруднения при самостоятельном обобщении программного материала.

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Вопросы для подготовки к промежуточной аттестации по дисциплине (экзамену)

1. Основные понятия информационной безопасности – определения, руководящие документы. Угрозы информационной безопасности. Средства защиты информации.
2. Что располагается в области стандартной памяти MS-DOS.
3. Плоская модель памяти и её использование в программировании.
4. Назначение диспетчера виртуальной памяти Windows.
5. Механизм защиты процессора Intel: схемы управления памятью и защита по привилегиям
6. Права доступа к таблице страниц или к странице для программ с различными уровнями привилегий.
7. Службы управления доменом и их использование для обеспечения безопасности программ Windows.
8. Схема распределения возможного виртуального адресного пространства в системах Windows
9. Методы защиты доступа к пулам памяти.
10. Модели операционных систем –структурированная, неструктурированная и клиент – сервер.
11. Отображение виртуальной страницы памяти на физическую страницу.
12. Тест POST как средство диагностики компьютера.
13. Уровни привилегий для страниц памяти.
14. Механизм защиты процессора Intel: схемы управления памятью и защита по привилегиям.
15. Диспетчер виртуальной памяти (VMM).
16. Loadable Kernel Module атаки на операционную систему.
17. Преобразование адресов с использованием таблицы дескрипторов
18. Права доступа к таблице страниц или к странице для программ с различными уровнями привилегий.
19. Сегментация памяти в защищённом режиме
20. Логическое, линейное и физическое адресных пространства при реализации защищенного режима работы 32-разрядных процессоров
21. Механизм подключения файле config. sys драйвера himem.sys и драйвера emm386.exe
22. Механизмы защиты memory pools. Атаки на Windows NT путем воздействия на ядро операционной системы и объекты ядра.
23. Уровни привилегий супервизора (U/S = 0), пользователя (U/S = 1), как средство обеспечения безопасности страниц памяти.
24. Определение тестом POST объема установленной памяти.
25. Механизм работы Virtual Memory Manager
26. Краткая характеристика компьютерных вирусов — источники и категории атак. Стратегии взломщиков.
27. Сетевые мониторы как средство обеспечения информационной безопасности.

28. Клиентский и серверный скрипт с позиций информационной безопасности.
29. Использование JavaScript для написания клиентских скриптов. Примеры задач.
30. Создание дочерних окон средствами JavaScript в клиентских и серверных скриптах.
31. Объектно-ориентированное программирование и объекты скриптовых языков. Языки на базе классов и языки на базе прототипов.
32. Инициализация объектов в скриптовых языках.
33. Наследование свойств объектов в JavaScript.
34. Функции-конструкторы в JavaScript.
35. 16. Определение методов в JavaScript.
36. Объект Array. Создание массива, наполнение массива, Методы объекта Array.
37. Объект Document.
38. Объект Response.
39. Использование методов объекта Document и объекта Response — сравнение с позиций информационной безопасности.
40. Объект Request.
41. Передача данных методом GET.
42. Передача данных методом POST.
43. Обработка событий в ASP.
44. Поля login и password как средство обеспечения информационной безопасности.
45. Создание сайтов, в которых права доступа обеспечиваются константами, размещенными непосредственно на самих страницах.
46. Создание сайтов, в которых права доступа обеспечиваются базой данных, содержащей сведения о правах доступа.
47. Криптографическая защита информации в Интернете — симметричное и асимметричное шифрование.
48. Интернет-протоколы для защищенных соединений. Настройка SSL на стороне сервера IIS и на клиентской стороне.
49. Информационная безопасность беспроводных сетей. Технология WAP (Wireless Application Protocol). Технический стандарт RADIUS (Remote Authentication Dial-In User Service).
50. Целостность информации. Алгоритмы хэширования. Пример вычисления хэш-функции.
51. Сертификаты. Служба сертификатов Микрософт. Просмотр сертификатов на компьютере — расположение сертификатов.
52. Просмотр сертификатов на компьютере — основные поля сертификата.
53. Технология создания электронной цифровой подписи.
54. Генерация ЭЦП и проверка ЭЦП.

.

4. Типовые контрольные задания (тесты, рефераты, курсовые работы, кейсы и др.) и методические материалы, процедуры оценивания знаний, умений и навыков

ТЕКУЩИЙ КОНТРОЛЬ

Методические рекомендации по написанию контрольных работ

Важнейшей формой учебной отчётности студента является **контрольная работа**.

Выполнение контрольной работы является промежуточной формой отчётности по изучаемой дисциплине и преследует цель лишь оценить способность студента к самостоятельному поиску источников, формированию содержания и его письменного изложения по указанной проблеме. Это важная составляющая изучения дисциплины, а также эффективная форма контроля знаний. При заочном обучении она выступает как обязательная, основная форма самостоятельной работы. В контрольной работе (в соответствии с учебным планом) студент обязан самостоятельно глубоко разобраться в изучаемых проблемах, усвоить суть темы, уяснить её содержание и только затем письменно представить свою отчётную работу.

Выполнение контрольной работы является одним из условий допуска студента к сдаче экзамена. Работа должна соответствовать установленным требованиям, то есть в ней должны быть раскрыты все проблемы, определённые темой. Для этого студент обязан самостоятельно проанализировать первоисточники и дать исчерпывающие ответы на вопросы темы. Контрольная работа – серьёзное учебное задание, и чтобы написать её как следует, необходимо использовать те первоисточники и учебные пособия, которые позволяют полнее разобраться в проблеме. Студент должен регулярно работать в университетской и городской библиотеке, вдумчиво конспектировать лекции преподавателей.

При написании контрольной работы следует обращать особое внимание на грамотное использование терминологии. При употреблении впервые тех или иных терминов и понятий следует давать их определения либо в самом тексте, либо в сносках.

Приступая к контрольной работе, требуется сначала ознакомиться с имеющейся литературой по теме, изучить первоисточники и составить план. Здесь, в отличие от курсовой работы, план предполагает рассмотрение одной, причём довольно широкой, проблемы, и он может состоять из двух-трёх вопросов. Минимальное количество первоисточников, привлекаемых для написания курсовой работы — пять наименований.

Как правило, контрольные работы по дисциплине сугубо индивидуальны, то есть их тематика персонифицирована. Однако в отдельных случаях темы контрольных работ могут быть адресованы и сразу нескольким, и группе в целом. Таким приёмом преподаватель выявляет степень усвоения какой-то важной учебной проблемы и определяет необходимость проведения дополнительных занятий по какой-либо теме. В настоящее время широко используется методика компьютерного тестирования знаний студентов по дисциплинам, в результате чего появляется возможность быстро проверять знания по наиболее важным темам и объективно оценивать их. Эта форма также может выступать как вид контрольной работы.

В качестве контрольной работы широко применяется самостоятельное изучение монографического исследования по конкретной, крайне важной проблеме, требующей глубокого рассмотрения. Этот вид работы предполагает не простое знакомство с определённым монографическим исследованием, а детальное его изучение. Для этого студенту важно знать некоторые правила работы с первоисточником, которым для него будет являться монография. Следует выяснить фамилию автора, его имя и отчество, учёную степень и звание, а также что побудило его взяться за изучение данной проблемы; обратить внимание на основные вопросы монографии и их разрешение автором, уметь раскрывать их в ходе собеседования с преподавателем.

Студенту следует письменно (предельно кратко) очертить те вопросы (полностью или частично), которые поставлены автором в монографическом исследовании; при изложении их следует указывать страницы источника.

Задания для написания контрольных работ (для заочной формы обучения)

1. Обзор факторов, механизмов и инструментария информационной безопасности.
2. Информационная безопасность в постиндустриальном и информационном обществе.
3. Информационная безопасность в государственном управлении. Доктрина информационной безопасности Российской Федерации.
4. Информационная безопасность в бизнесе и быту.
5. Служба информационной безопасности в структуре предприятия.
6. Проблемы информационной безопасности малых предприятий.
7. Политика информационной безопасности организации, ее разработка, реализация, модификация.
8. Нормативное обеспечение работы службы информационной безопасности.
9. Исторический обзор развития криптографии, стеганографии, криптоанализа и их основные методы.
10. Обзор методов цифровой потоковой и блочной криптографии.
11. Обзор цифровых блочных шифров DES, ГОСТ 28147-89.
12. Обзор цифровых блочных шифров TEA, IDEA.
13. Конкурс AES и цифровой блочный шифр RIJNDAEL.
14. Конкурс AES и цифровой блочный шифр SERPENT.
15. Конкурс AES и цифровой блочный шифр TWOFISH.
16. Конкурс AES и цифровой блочный шифр RC6.
17. Конкурс AES и цифровой блочный шифр MARS.
18. Обзор технологий асимметричной криптографии и электронной цифровой подписи.
19. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технология RSA.
20. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технология Рабина.
21. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технология Эль Гамаль.
22. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технологии на основе эллиптических кривых.
23. Обзор технологий асимметричной криптографии и электронной цифровой подписи, технология Мак-Элиса.
24. Обзор технологий асимметричной криптографии и электронной цифровой подписи, ГОСТ Р 34.10-2001.
25. Криптографические хеш-функции.
26. Обзор возможных атак на информационные системы: локальные атаки; удаленные атаки; атаки на поток данных.
27. Обзор информационной безопасности Windows и Unix-систем, компьютерные вирусы и защита от них.
28. Контроль физического доступа: системы охраны периметра, управления доступом, видеонаблюдения, пожарной сигнализации и др.
29. Сетевая безопасность организации: протоколы сетевой безопасности; антивирусные программы; межсетевые экраны; системы обнаружения атак; технологии VPN и VLAN.
30. Теория открытых систем как теоретическая основа стандартизации, обзор оценочных стандартов и спецификаций информационной безопасности.
31. Стандарты информационной безопасности «Оранжевая книга», «Гостехкомиссия России. Руководящий документ», «Общие критерии» (ГОСТ Р ИСО/МЭК 15408) и их использование в государственном управлении и бизнесе.
32. Спецификации интернет-сообщества по информационной безопасности и их использование в государственном управлении и бизнесе.

Принципы выбора темы работы

Студенты при написании контрольной работы могут выбрать любую из предложенных тем на своё усмотрение.

Требования к оформлению контрольной работы подробно представлены в Положении о бюро контрольных работ, размещённом на сайте Университета в личном кабинете на странице в Системе поддержки самостоятельной работы студентов **ПОЛОЖЕНИЕ О БЮРО КОНТРОЛЬНЫХ РАБОТ _ для работ студентов заочной формы обучения.**

Тестовые материалы

ПАСПОРТ ТЕСТОВЫХ ЗАДАНИЙ

1. Общее количество тестовых заданий в базе – 100.
2. Ограничение времени выполнения теста (в минутах) – одна попытка, 35 минут.
3. Автоматическое перемешивание вопросов в тесте: - **да** (нет).
4. Случайный порядок ответов в тестовом задании: - **да** (нет).
5. Критерии оценки результатов тестирования:
   - Неудовлетворительно – 0 –55% правильных ответов.
   - Удовлетворительно -55 – 75% правильных ответов.
   - Хорошо – 75 -90% правильных ответов
   - Отлично – 90% и более правильных ответов

Пример тестовых заданий для текущего контроля представлен ниже:

1. Как называется свойство информации, подразумевающее возможность получения требуемой услуги за приемлемое время?
   a. Доступность.
   b. Целостность.
   c. Конфиденциальность.
2. Какой уровень модели открытых систем отвечает за управление общим доступом к сети?
   a. Прикладной уровень.
   b. Представительский уровень.
   c. Сетевой уровень.
   d. Транспортный уровень.
3. К какому уровню в модели открытых систем относится протокол TCP?
   a. Прикладной уровень.
   b. Представительский уровень.
   c. Сетевой уровень.
   d. Транспортный уровень.