Спецификация для заключительного (очного) этапа
Олимпиады «Я – профессионал» 2019-2020

Название направления	**«Безопасность информационных систем и технологий критически важных объектов»**
Указание уровня подготовки	**Категория «бакалавриат»**
Описание целевой аудитории	Данные задания подготовлены в рамках олимпиады «Я – профессионал» и предназначены для оценки знаний и навыков студентов бакалавриата, обучающихся в первую очередь по направлениям подготовки и специальностям: - «Информационная безопасность»; - «Информатика и вычислительная техника», а также студентов других направлений подготовки, интересующихся исследованиями и разработками в области безопасности информационных систем и технологий.
Максимальное количество баллов за задание	100 баллов
Время на выполнение	Два тура по 240 минут
Список ресурсов для самостоятельной подготовки	Теоретический тур Раздел 1. «Основы информационной безопасности» 1. Коблиц Н. Курс теории чисел и криптографии. – М.: Научное изд-во ТВП, 2001. 2. Фергюсон Н., Шнайер Б. Практическая криптография. – М.: Вильямс, 2005. 3. Аршинов М.Н., Садовский Л.Е. Коды и математика (рассказы о кодировании). Библиотечка «Квант». Выпуск 30. – Москва: Наука, 1983. Раздел 2. «Криптографические методы защиты информации» 1. Фомичёв В.М. Методы дискретной математики в криптологии. — М.: Диалог-МИФИ, 2010. 2. Paar C., and Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. — Springer-Verlag, 2010. 3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А. В. Основы криптографии. — М.: Гелиос АРВ, 2002. 4. Menezes A.J., Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press,2001. Раздел 3. «Безопасность информационных технологий и техническая защита информации» 1. Контроль защищенности речевой информации в помещениях. Аттестационные испытания ВП по

	требованиям безопасности информации: учебн. пособ. / В.С. Горбатов, А.П. Дураковский, И.В. Куницын; под общ. ред. Ю.Н. Лаврухина – М.: НИЯУ МИФИ, 2014. – 248 с. 2. Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации: учебн. пособ. / А.А. Голяков, В.С. Горбатов, А.П. Дураковский, А.Е. Панин; под общ. ред. Ю.Н. Лаврухина – М.: НИЯУ МИФИ, 2014. – 208с. 3. Хорев А.А. Техническая защита информации: учебное пособие для студентов вузов. В 3 т. Т.1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. – 436 с. 4. Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания ВТСС по требованиям безопасности информации: Учебн. пособ. – М.: НИЯУ МИФИ, 2015. – 152 с. 5. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности: пособие рекомендов. УМО вузов по образованию в области ИБ в качестве учебн. пособ. для студ. ВУЗ. М.: Гелиос АРВ, 2011. − 224 с. <u>Практический тур.</u> 1. Грег Хогланд, Гари Мак–Гроу. Взлом программного обеспечения. Анализ и использование кода. –М.: Издательский дом «Вильямс», 2005. 2. Джеймс К. Фостер, Винстент Лю. Разработка средств безопасности и эксплойтов. –СПб, : Питер, 2007. 3. КасперскиК. Компьютерные вирусы изнутри и снаружи. –СПб.: Питер, 2006. 4. Низамутдинов М.Ф. Тактика защиты и нападения на Web-приложения. –СПб.: БХВ–Петербург, 2005. 5. Скембрей Джоел, Мак-Клар Стюарт, Курц Джордж. Секреты Хакеров. Безопасность сетей –готовые решения. –М.: Издательский дом «Вильямс», 2004. 6. Кнут Э.Д. Искусство программирования, том 1. Основные алгоритмы. –М.: Издательский дом «Вильямс», 2000. 7. Грег Хогланд, Гари Мак–Гроу. Взлом программного обеспечения. Анализ и использование кода. –М.: Издательский дом «Вильямс», 2005. 8. Смит, Ричард, Э. Аутентификация: от паролей до открытых ключей. –М.: Издательский дом «Вильямс», 2002. 9. Book of DS19xx iButton Standardshttps://pdfserv.maximintegrated.com/en/an/AN937.pdf 10. https://nostarch.com/idapro2.htm 11. https://habr.com/ru/post/217885/ 12. https://avidreaders.ru/book/cifrovaya-steganografiya.html

Формат состязаний. Требования к содержанию и оформлению заданий.	Очный этап проводится в два подряд идущих дня, один из которых посвящен заданиям фундаментального характера, а второй – практическим заданиям, разработанным совместно с работодателями. Участникам заключительного (очного) этапа предоставляется для проживания общежитие НИЯУ МИФИ. Все задания разработаны с учетом трудовых функций соответствующих профессиональных стандартов, связанных с безопасностью информационных систем и технологий. Продолжительность заключительного (очного) этапа − 2 дня. Теоретический тур первого конкурсного дня включает в себя задачи из трех разделов. Раздел 1. «Основы информационной безопасности». Темы, знание которых потребуется при решении задач раздела 1: • Простейшие шифры. • Генераторы псевдослучайных чисел на регистрах сдвига с линейными обратными связями. • Программно-аппаратные средства защиты информации. • Защита информации в компьютерных системах и сетях. • Основы теории конечных полей. Раздел 2. «Криптографические методы защиты информации». Темы, знание которых потребуется при решении задач раздела 2: • Математические основы криптологии. • Криптосистемы с открытым ключом; ранцевая криптосистема, криптосистема RSA и другие. • Криптосистемы с секретным ключом; шифры Магма, Кузнечик, AES и другие. • Режимы использования блочных шифров. • Криптографические хеш-функции. • Поточные шифры; шифры RC4, Spritz и другие. • Коды аутентификации сообщений. • Криптоанализ простейших шифров замены и перестановки. • Скрытые и клептографические каналы передачи информации. • Криптографические протоколы защищенного взаимодействия удаленных абонентов. Раздел 3. «Безопасность информационных технологий и техническая защита информации». Темы, знание которых потребуется при решении задач раздела 3: • Поиск уязвимостей в программном обеспечении. • Защищенность речевой информации от утечки по каналам: акустическим, виброакустическим,

	акустоэлектрическим преобразованиям, акустоэлектромагнитным преобразованиям. • Защищенность информации от утечки за счет ПЭМИН. • Элементы физики и техники инфравизуализации. На выполнение конкурсных заданий теоретического тура отводится 4 часа. Максимальная оценка – 50 баллов. Практический тур второго конкурсного дня «Безопасность веб-приложений и обнаружение вредоносного ПО» включает в себя задания по нахождению уязвимостей в криптографических и стеганографических алгоритмах, созданию программных средств для оценки их надежности, задания на нейтрализацию вредоносного ПО, поиск и исследование уязвимостей веб-приложений и программно-аппаратных комплексов. На выполнение конкурсных заданий практического тура отводится 4 часа. Максимальная оценка – 50 баллов Перед проведением практического тура участники проходят обучение возможностям и применению предлагаемого к использованию программного обеспечения. Итоговый результат каждого участника определяется в результате сложения результатов первого и второго дня проведения состязания.
Дополнительная информация/инструкции для участников, которые не вошли в Регламент по направлению	нет
Краткое описание структуры задания и его основные характеристики. Система оценивания заданий.	Задания 1-го дня очного тура состоит из десяти заданий, разделённых на 3 раздела различной тематической направленности: **Первый раздел «Основы информационной безопасности»** состоит из 4-х заданий средней сложности по тематикам: · Основы информационной безопасности; · Простейшие шифры; · Операции в конечных полях. Схемотехника; · Операции в конечных полях. Программирование. Задание 1, требующее развернутого ответа, оценивается в 2 балла. Задание 2, предполагающее решение поставленной в условии задачи с введением ответа, оценивается в 3 балла. Задание 3, где необходимо изобразить логическую схему устройства, оценивается в 5 баллов. Задание 4, где необходимо изобразить

	блок-схему алгоритма, оценивается в 5 баллов. Каждое из заданий оценивается дихотомически (верный ответ – максимальный балл, неверный ответ – 0 баллов). **Второй раздел «Криптографические методы защиты информации»** состоит из 3-х заданий высокой сложности по тематикам: · Поточные шифры; · Симметричные блочные шифры; · Асимметричные криптосистемы. Все задания предполагают развернутый аргументированный ответ. Каждое из заданий оценивается по шкале от 0 до 5 баллов. **Третий раздел «Безопасность информационных технологий и техническая защита информации»** состоит из 3-х заданий высокой сложности по тематикам: · Поиск уязвимостей в программном обеспечении, · Специальные исследования акустических и виброакустических каналов, · Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок. Все задания требуют развернутого аргументированного ответа и оцениваются по шкале: 8-е задание от 0 до 6 баллов, 9-е задание от 0 до 7 баллов, 10-е задание от 0 до 7 баллов. Максимальное количество баллов за первый день состязаний – 50 баллов. **<u>Второй день состязания.</u>** Проводится конкурс на решение практических заданий. Разработка осуществляется на компьютере с помощью программного обеспечения, предоставляемого организатором. Практический тур включает десять заданий среднего и высокого уровня сложности. Каждое из заданий оценивается дихотомически (верный ответ – максимальный балл, неверный ответ – 0 баллов). • Задание 1 на тему «Stegano - стеганография - способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения)» оценивается в 4 балла. • Задание 2 на тему «Reverse + PPC. Reverse − обратный (реверс) инжиниринг − умение восстанавливать исходный код исполняемых файлов и его анализировать. PPC − программирование - умение написать программу на любом языке для решения поставленной задачи» оценивается в 4 балла. • Задание 3 на тему «Reverse − обратный (реверс) инжиниринг (умение восстанавливать исходный код исполняемых файлов и его анализировать)» оценивается в 4 балла. • Задание 4 на тему «Binary Exploitation − эксплуатация бинарных уязвимостей − умение находить и

	эксплуатировать уязвимости в нативных приложениях» требует знание Reverse и оценивается в 6 баллов. • Задания 5,6 на тему «Crypto − криптография − умение определять используемую криптографическую схему по зашифрованным данным, анализировать безопасность криптографических схем» оцениваются по 6 баллов. • Задания 7,8 на тему «Web - веб -умение находить и эксплуатировать уязвимости в веб-ресурсах» оцениваются по 4 балла. • Задания 9,10 на тему «Forensics − форенсика − умение анализировать низкоуровневые снимки данных - образы носителей информации, дампы сетевого трафика, исследовать физический уровень передачи данных» оцениваются по 6 баллов. Максимальных количество баллов за 2-й день – 50 баллов. Итоговый балл участника определяется сложением результатов за первый и второй день состязаний.
Информация об элементах практикоориентированности в заданиях (участие работодателей в составлении заданий)	Задачи теоретического тура (1-й день состязания) и практического тура (2-й день состязаний) составлены с участием или согласованы с представителями следующих предприятий и организаций работодателей, представляющих генерального партнера ГК «Росатом»: АО «ФЦНИВТ «СНПО «Элерон», Концерн «Росэнергоатом», а также с такими известными организациями в области обеспечения информационной безопасности, как АО «НПО «Эшелон», компания «BI.ZONE», АО «Лаборатория Касперского». Задания практического тура, составленные с участием работодателей, оценивают следующие знания и умения участников: умение восстанавливать исходный код исполняемых файлов и проводить их анализ, умение находить и эксплуатировать уязвимости в нативных приложениях, умение определять используемую криптографическую схему по зашифрованным данным, анализировать безопасность криптографических схем, умение находить и эксплуатировать уязвимости в веб-ресурсах, умение анализировать низкоуровневые снимки данных – образы носителей информации, дампы сетевого трафика, исследовать физический уровень передачи данных, умение передавать или хранить информацию с учётом сохранения в тайне самого факта такой передачи (хранения).

2019/2020 учебный год

Всероссийская олимпиада студентов «Я – профессионал»

Демонстрационный вариант

задания заключительного (очного) этапа по направлению

«Безопасность информационных систем и технологий критически важных объектов»

Категория участия: «Бакалавриат»

(для поступающих в магистратуру)

Задачи теоретического тура (1-й день заключительного этапа)

Максимальный балл за теоретический тур - 50

Раздел 1. «Основы информационной безопасности»

Задача 1 (2 балла)

Какой из PIN-кодов надежнее 2301 или 3021? Ответ обосновать.

Ответ: Второй, так как первый может быть парой "день-месяц".

Задача 2 (3 балла)

Перехвачен шифртекст, полученный с использованием афинного отображения $C \equiv aM + b \pmod{26}$, где (a, b) – ключ зашифрования, M – численное представление буквы исходного текста, C – численное представление буквы шифртекста. Численное представление букв алфавита имеет вид A = 0, B = 1, C = 2, …, Y = 24, Z = 25. Известно, что в шифртексте чаще всего встречаются буквы D и W (в указанном порядке). Определить ключ зашифрования; определить уравнение расшифрования $M \equiv a^*C + b^* \pmod{26}$, вычислив ключ расшифрования (a^*, b^*), и определить фрагмент исходного текста, соответствующий заданному фрагменту шифртекста KRTTFHQAJYHHBL.

Ответ: PASSWORDGLOOMY

Задача 3 (5 баллов)

РСЛОС – регистр сдвига с линейной обратной связью.

Задан РСЛОС, характеристический многочлен которого имеет вид

$$\varphi(x) = x^7 + x^4 + 1 \text{ (рис. 1)},$$

который может использоваться в качестве счетчика по модулю $2^7 - 1$. Синтезировать на его основе логическую схему счетчика по модулю 2^7.

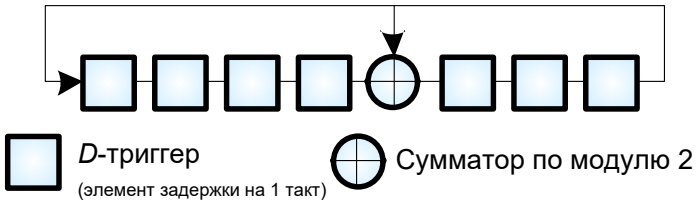
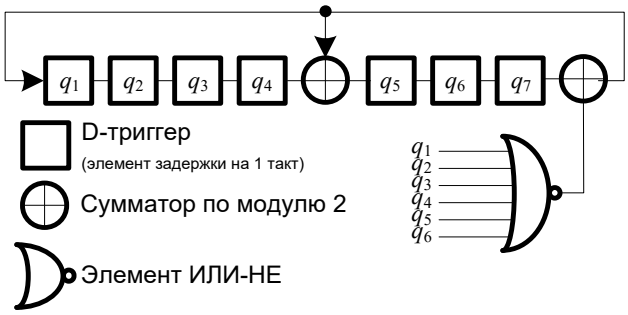


Рис. 1 – Схема счетчика модулю $2^7 - 1$.

Ответ: Необходимо выбрать одно из состояний счетчика с единственной единицей (например, 0000001) и в момент нахождения счетчика в этом состоянии инвертировать сигнал на входах тех элементов памяти, куда эта единица поступает. См. рис. ниже.



Задача 4 (5 баллов)

Разработать блок-схему алгоритма определения обратного элемента α^{-1} для заданного ненулевого элемента $\alpha \in GF(2^8)$, где $GF(2^8)$ – поле Галуа из 2^8 элементов.

Ответ:

1. Зафиксировать состояние генератора ненулевых элементов поля.
2. Подсчитать число *N* тактов работы генератора от состояния α (альфа) до состояния 1.
3. Выполнить *N* тактов генератора.
4. Считать α^{-1}.

Раздел 2. «Криптографические методы защиты информации»

Задача 5 (5 баллов)

Пусть чисто периодическая двоичная последовательность имеет длину периода 15 и начинается с отрезка 010110000101010. Каков ее минимальный характеристический многочлен? Какова ее линейная сложность?

Ответ: 6, $\lambda^6 \oplus \lambda^4 \oplus \lambda^5 \oplus \lambda^3 \oplus 1$

Задача 6 (5 баллов)

Пусть E_1, E_2 – симметричные блочные шифры с ключами длины 128, 256. Чему равна эффективная длина ключа алгоритма $E_1E_2E_2$?

Ответ: 384

Задача 7 (5 баллов)

Рассмотрим криптосистему RSA с модулем $n = pq$ и открытой экспонентой e. Чему равно количество решений уравнения $m^u = 1 \pmod p$, если u делит $p - 1$?

Ответ: 1

Раздел 3. «Безопасность информационных технологий и техническая защита информации».

Задача 8 (6 баллов)

Найти уязвимость в программе:

```
import random
lucky_num = random.randint(1,10000)
print "Choose a number between 1 and 10000"
while True:
  res = input("Guess a number: ")
  if res == lucky_num:
    print "You win!"
    break
  else:
    continue
```

Ответ: В Python 2.6 небезопасно использовать функцию input(), например, str не подлежат обработке в input(), к примеру, если нужно вбивать туда текст, то используйте raw_input. (Можно привести другие примеры).

Задача 9 (7 баллов)

При проведении измерений в акустическом канале утечки информации были получены следующие результаты:

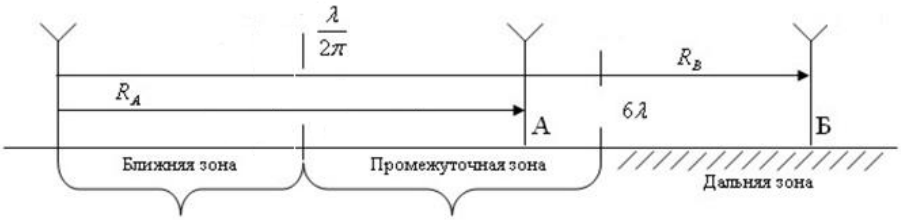
- уровень звукового давления тестового сигнала в 3-ой октаве: $L_{ТС3}$ =85дБ;
- уровень звукового давления и шума за пределами контролируемой зоны (КЗ) в 3-ой октаве: $L_{с+ш3}$ =54дБ;
- уровень звукового давления шума за пределами КЗ в третьей октаве $L_{ш3}$ =57дБ;

Рассчитать отношение сигнал/шум в третьей октаве E_3 за пределами КЗ, если известно, что нормированный уровень звукового давления в третьей октаве $L_{н3}$ =51дБ.

Ответ: Решения нет!!! $L_{с+ш3}$ не может быть меньше $L_{ш3}$.

Задача 10 (7 баллов)

Необходимо получить расчетную формулу для определения коэффициента затухания от точки А до точки Б, находящейся на границе контролируемой зоны, по стандартному закону затухания поля.



R_A - расстояние от источника излучения до точки А, измерения напряженности поля; R_B - расстояние от источника излучения до границы контролируемой зоны, точки Б; λ - длина волны излучения.

Ответ: Коэффициент затухания электромагнитного поля на частоте F рассчитывается в соответствии со стандартным законом затухания:
- если расстояние *R* (R_A) от измерительной антенны до ТС удовлетворяет условию *R* ≤ λ/2*π*, где λ - длина волны, то на расстоянии *D* (R_B) коэффициент затухания *K* рассчитывается по формулам для каждой из трех зон. В соответствии со стандартным законом затухания коэффициент затухания ЭП зависит от коэффициентов на каждом участке. В результате несложных преобразований получаем: затухание от точки А до точки Б будет равно

$$Z = \left(\frac{6\lambda}{\frac{\lambda}{2\pi}}\right)^2 \cdot \left(\frac{R_B}{6\lambda}\right).$$

Задачи практического тура
(2-й день заключительного этапа)

Максимальный балл за практический тур - 50.

Практический тур выполняется на компьютерах, предоставляемых организаторами направления.

Задача 1 (4 балла)

На компьютере сотрудника «Modular&Prime» был найден странный текстовой файл, содержащий фразу, являющуюся паролем к архивам, содержащим сведения о нелегальной коммерческой деятельности. Помогите аналитикам получить пароль и отправьте его md5-сумму на проверку через форму ниже.

Ответ: f68762a532c15a8954be87b3d3fc3c31

Задача 2 (4 балла)

В послании было обнаружено упоминание о некотором самораспаковывающемся архиве. Необходимо подобрать пароль к архиву и извлечь его содержимое. Найденный пароль отправьте на проверку через форму ниже.

Ответ: 730482fbb31353a27ec17b721aca2a60

Задача 3 (4 балла)

Внутри архива оказалось некоторое приложение, требующее пароль для запуска. Узнайте аутентификационные данные для приложения. Найденный пароль отправьте на проверку через форму ниже.

Подсказки

1. Программа принимает множество паролей, а где же ключ?
2. Добавлена x32-версия приложения

Ответ: b3ffff83dc91eec493b36905fafb0bac

Задача 4 (6 баллов)

После запуска приложение осуществляет подключение к некоторому серверу на tcp-порт 2019. Прочитайте содержимое файла /home/task4/flag.txt данного сервера и отправьте его содержимое на проверку через форму ниже.

Ответ: 1afae761d41b0c1dc7eb59fdd3748131

Задача 5 (6 баллов)

Вредоносная программа с сервера зашифровала файлы на компьютере судьи Сергея Валерьевича. Ключ #1, представляющий собой численное значение, и ключ #2, представляющий собой строковое значение, «Modular&Prime» зашифровал в странном формате.

Определите ключ 2, зашифрованный выше, при том, что произведение одного ключа на другой имеет вид:

0x04b7 0x0671 0x07c5 0x07a3 0x07a3

MD5-сумму от ключа 2 отправьте на проверку через форму ниже.

Ответ: edc41fb7bf8bdac012523d1bcd949a4f

Задача 6 (6 баллов)

Расшифруйте текст, используя один из найденных в Задаче 5 ключей, и отправьте его md5-сумму на проверку через форму ниже.

Ответ: 3edaa62926e352586fe3fea77dffa992

Задача 7 (4 балла)

В расшифрованном сообщении оказался адрес некоторого веб-сайта. Найдите пароль пользователя в базе данных сайта и отправьте его на проверку через форму ниже.

Ответ: 858794982a4cd75ab19072a422948e93

Задача 8 (4 балла)

Узнайте имя пользователя из файла /etc/passwd данного сайта. Найденный логин отправьте на проверку через форму ниже.

Ответ: 0fdb2ca7f964aa524e0f62ac5bb5483c

Задача 9 (6 баллов)

В социальных сетях удалось обнаружить пользователя с найденным ником, в профиле которого был указан адрес некоторой многоэтажки. Перед домом нашлась связка домофонных ключей. Судя по огромному количеству ключей, в их идентификаторах явно что-то зашифровано. Расшифрованное сообщение отправьте на проверку через форму ниже.

Ответ: 28ceb3f8ea9008f87788d3faf3cf7024

Задача 10 (6 баллов)

Домофон удалось открыть, но за ним оказалась вторая дверь с сенсорной панелью. С помощью логического анализатора **Kingst** удалось записать данные, передаваемые по кабелю, проходящему мимо сенсорной панели. Преобразуйте перехваченные данные в текстовый вид и отправьте их md5-сумму на проверку через форму ниже.

Подсказки

1. На первом ключе записана фраза "Key is"

Ответ: aa3d985077b1ddd4183dcaed478b01f1