ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уральский государственный университет путей сообщения»
(УрГУПС)

УТВЕРЖДАЮ:
Первый проректор, заместитель
председателя Приемной комиссии
_____Е.Б. Азаров
«18» 01 2024 г.

ПРОГРАММА
ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ
по направлению подготовки 10.04.01 «Информационная безопасность»
для поступающих на обучение по образовательным программам высшего образования – программам магистратуры

Екатеринбург
2024

СТРУКТУРА

ВВЕДЕНИЕ

Программа вступительного испытания по направлению подготовки 10.04.01 «Информационная безопасность» сформирована на основе Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. №1427.

Экзаменационная работа состоит из 3 частей и содержит 20 заданий.

Часть 1 содержит 8 заданий базового уровня сложности.

Часть 2 содержит 10 заданий повышенного уровня сложности.

Часть 3 содержит 2 задания высокого уровня сложности.

Задания из части 1 требуют базовых знаний в области информационной безопасности.

Задания из части 2 требуют углубленных знаний в области информационной безопасности.

Задания части 3 требуют навыков в решении практических задач в области информационной безопасности.

Правильное решение каждого из заданий части 1 оценивается в 4 балла.

Правильное решение каждого из заданий части 2 оценивается в 5 баллов.

Правильное решение каждого из заданий части 3 оценивается в 9 баллов.

Минимальное допустимое количество баллов за выполнение всей работы - 25.

Максимальное количество баллов за выполнение всей работы - 100.

На выполнение экзаменационной работы «Информационная безопасность» отводится 60 минут.

Справочные материалы для прохождения вступительного испытания не требуются, пользоваться вспомогательными материалами в ходе вступительного испытания не разрешается.

1. ЦЕЛЬ И ЗАДАЧИ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Цель вступительного испытания:

определить уровень качества подготовки поступающих, пригодность и соответствие знаний и умений необходимым для обучения в магистратуре.

Задачи вступительного испытания:

- оценить теоретические знания и практические умения и навыки, выявляющие владение основами информационной безопасности;
- оценить степень сформированности компетенций, значимых для успешного обучения в магистратуре по образовательной программе высшего образования – программе магистратуры 10.04.01 Информационная безопасность.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

Раздел 1. Основы информационной безопасности

Тема 1.1. Информация как объект защиты. Основные свойства информации. Классификация информации.

Тема 1.2. Угрозы информационной безопасности. Источники угроз. Возможные результаты реализации угроз по отношению к информационным ресурсам.
Тема 1.3. Способы защиты информации. Принципы и методы построения системы защиты информации.

Раздел 2. Организационное и правовое обеспечение информационной безопасности
Тема 2.1. Законодательство Российской Федерации в области информационной безопасности.
Тема 2.2. Правовой режим защиты информации, составляющей государственную тайну.
Тема 2.3. Правовые режимы защиты информации конфиденциального характера.
Тема 2.4. Организационное обеспечение информационной безопасности предприятия.

Раздел 3. Программно-аппаратная защита информации
Тема 3.1. Управление доступом в компьютерных системах.
Тема 3.2. Защита информации от воздействия вредоносных программ.
Тема 3.2. Защита современных информационных систем и сетей.

Раздел 4. Техническая защита информации
Тема 4.1. Источники и носители информации.
Тема 4.2. Демаскирующие признаки объектов защиты.
Тема 4.3. Технические каналы утечки информации.
Тема 4.4. Методы защиты информации техническими средствами.

Раздел 5. Криптографическая защита информации
Тема 5.1. Симметричные криптосистемы.
Тема 5.2. Асимметричные криптосистемы.
Тема 5.3. Криптографические протоколы и алгоритмы.

3. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Бабаш А. В. Криптографические методы защиты информации: Учебно-методическое пособие: Том 1. - Москва: Издательский Центр РИОР, 2018.
2. Бабаш А. В. Криптографические методы защиты информации: Учебно-методическое пособие: Том 2. - Москва: Издательский Центр РИОР, 2019.
3. Баранова Е. К., Бабаш А. В. Основы информационной безопасности: Учебник. - Москва: Издательский Центр РИОР, 2021.
4. Крамаров С. О., Тищенко Е. Н. Криптографическая защита информации: Учебное пособие. - Москва: Издательский Центр РИОР, 2021.
5. Нестеров С. А. Основы информационной безопасности: Учебник - Санкт-Петербург: Лань, 2021.
6. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2016.

7. Торокин А. А. Инженерно-техническая защита информации. - Москва: Гелиос АРВ, 2005.
8. Хорев П. Б. Программно-аппаратная защита информации: Учебное пособие. - Москва: Издательство «ФОРУМ», 2021.

Дополнительная литература

1. Гашков С. Б., Применко Э. А., Черепнев М. А. Криптографические средства защиты информации: учебное пособие для студентов вузов, обучающихся по направлению «Прикладная математика и информатика» и «Информационные технологии». - Москва: Академия, 2010.
2. Гришина Н. В. Основы информационной безопасности предприятия: Учебное пособие. - Москва: ООО «Научно-издательский центр ИНФРА-М», 2021.
3. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности. - Санкт-Петербург: НИУ ИТМО, 2014.
4. Исаева М. Ф. Техническая защита информации. - Санкт-Петербург: ПГУПС, 2017.
5. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для студентов вузов, обучающихся по направлению подготовки «Информационная безопасность». - Москва: Академия, 2013.

4. ДЕМО-ВАРИАНТ

Часть 1 – Базовый уровень сложности

Задание 1

Определение информации согласно нормативным правовым документам Российской Федерации

+ Сведения (сообщения, данные) независимо от формы их представления

- Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

- Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

- Данные, переданные или полученные пользователем информационно-телекоммуникационной сети

Задание 2

Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя - это свойство

+ конфиденциальности информации

- целостности информации

- доступности информации

- подлинности информации

Задание 3

Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно - это свойство

- конфиденциальности информации
- целостности информации
+ доступности информации
- подлинности информации

Задание 4

Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право - это свойство

- конфиденциальности информации
+ целостности информации
- доступности информации
- подлинности информации

Задание 5

Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность – это

+ персональные данные
- коммерческая тайна
- служебная тайна
- профессиональная тайна

Задание 6

Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации – это

+ угроза
- фактор, воздействующий на защищаемую информацию
- источник угрозы безопасности информации
- уязвимость

Задание 7

Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением - это

- физическая защита информации
- организационная защита информации
+ правовая защита информации
- техническая защита информации

Задание 8

Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии

с действующим законодательством, с применением технических, программных и программно-технических средств - это
- физическая защита информации
- организационная защита информации
- правовая защита информации
+ техническая защита информации

Часть 2 – Повышенный уровень сложности

Задание 9

Установите соответствие

1 – Законность	а - Установление экспертным путем целесообразности засекречивания конкретных сведений
2 – Обоснованность	б - Установление ограничения на распространение сведений с момента их получения или заблаговременно
3 – Своевременность	в – Соответствие засекречиваемых сведений положениям действующего законодательства о государственной тайне
	г - Установление ущерба от распространения секретных сведений

Верный ответ: 1 – в, 2 – а, 3 – б

Задание 10

К органам защиты государственной тайны относятся:
+ Межведомственная комиссия по защите государственной тайны
+ Предприятия и учреждения
+ Федеральная служба по техническому и экспортному контролю
+ Министерство обороны
- Должностные лица
+ Подразделения по защите государственной тайны

Задание 11

Сеть передачи данных, использующая открытую телекоммуникационную инфраструктуру и сохраняющая при этом конфиденциальность передаваемых данных посредством применения потоков туннелирования и средств защиты информации, называется
- антивирусной системой
- системой восстановления данных
+ виртуальной сетью
- системой аудита

Задание 12

Установите хронологию передачи информации в локальных системах обнаружения вторжений

1. унификация данных, фильтрация, сохранение

2. сохранение данных о подозрительной активности
3. сбор информации сенсорами
4. контроль за работой системы безопасности
5. выявление злоумышленной активности

Верный ответ: 3 – 1 – 5 – 2 - 4

Задание 13

Шумоподавление информационного сигнала относится к методам защиты информации
+ активным
- полуактивным
- пассивным
- условно пассивным

Задание 14

По результатам комплексной специальной проверки помещений были проведены работы по дополнительной звукоизоляции для ликвидации акустического канала утечки информации. После этого необходимы
+ акустические измерения и расчеты
- изменения в нормативно-правовых документах организации
- измерения электромагнитных полей, а также побочных электромагнитных излучений и наводок
- измерения цепей электропитания и заземления и установка фильтров

Задание 15

Элементы технического канала утечки информации
+ источник сигнала
+ среда распространения сигнала
+ приемник сигнала
- способ распространения сигнала

Задание 16

Технический канал утечки информации - это
- совокупность объекта, технических средств передачи и приема информации, а также физической среды ее распространения
- субъект (материальный объект, информационный процесс или физическое явление), являющийся непосредственной причиной возникновения пути небезопасной передачи информации
- совокупность информации, ее носителя и информационного процесса, который передает информационный сигнал
+ совокупность объекта разведки, технического средства разведки и физической среды, в которой распространяется информационный сигнал

Задание 17

Зашифруйте шифром Цезаря со сдвигом в 4 буквы вправо (+4) слово «учеба» по приведенному алфавиту. Введите ответ.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Верный ответ: ЧЫЙЕД

Задание 18

Зашифруйте шифром Виженера слово «работа» с паролем «духи». Введите ответ.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Верный ответ: ХФЧЧЧФ

Часть 3 – Высокий уровень сложности

Задание 19

Решите задачу дискретного логарифмирования методом перебора. Введите ответ одной цифрой.

$3^x=9 \bmod 13$. Чему равен x?

Верный ответ: 5

Задание 20

Определите уровень защищенности персональных данных. Введите ответ одной цифрой.

В базе данных системы контроля и управления доступом хранятся шаблоны отпечатков пальцев 1 500 сотрудников предприятия. Для системы не актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в программном обеспечении.

Верный ответ: 3

Разработчик:
к.т.н., доцент кафедры
«Информационные технологии
и защита информации»

Зырянова Т.Ю.