МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ

УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

УТВЕРЖДАЮ

Проректор по научной работе и инновациям

_____Лощилов А.Г.

«14» марта 2022 г.

ПРОГРАММА

вступительного испытания по специальной дисциплине
соответствующей научной специальности программы подготовки научных и научно-педагогических кадров в аспирантуре

2.3.6 Методы и системы защиты информации, информационная безопасность

шифр и наименование научной специальности

Томск – 2022

Программа вступительных испытаний при приеме на обучение по программе подготовки научно-педагогических кадров в аспирантуре формируется на основе федеральных государственных образовательных стандартов высшего образования по программам специалитета или магистратуры.

Составители программы: Шелупанов А.А., зав. кафедрой КИБЭВС, Конев А.А., доцент кафедры КИБЭВС, Костюченко Е.Ю., доцент кафедры КИБЭВС

ПРОГРАММА РАССМОТРЕНА И УТВЕРЖДЕНА на заседании кафедры КИБЭВС от 11 марта 2022 г. протокол № 3

СОГЛАСОВАНО:

Зав. кафедрой КИБЭВС Шелупанов А.А.

Разработчики Шелупанов А.А.

Конев А.А.

Костюченко Е.Ю.

Руководитель образовательной программы Шелупанов А.А.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Программа вступительного испытания по специальной дисциплине соответствующей научной специальности программы подготовки научных и научно-педагогических кадров в аспирантуре 2.3.6 Методы и системы защиты информации, информационная безопасность (далее – Программа), сформирована на основе требований федеральных государственных образовательных стандартов высшего образования к программам магистратуры (специалитета) по соответствующим направлениям (специальностям) подготовки. Программа разработана для поступления на обучение в аспирантуру ТУСУРа.

Программой устанавливается:

- форма, структура, процедура сдачи вступительного испытания;
- шкала оценивания;
- максимальное и минимальное количество баллов для успешного прохождения вступительного испытания;
- критерии оценки ответов.

1.2 Организация и проведение вступительного испытания осуществляется в соответствии с Правилами приема, утвержденными приказом ректора ТУСУРа, действующими на текущий год поступления.

1.3 По результатам вступительного испытания, поступающий имеет право подать на апелляцию о нарушении, по мнению поступающего, установленного порядка проведения вступительного испытания и (или) о несогласии с полученной оценкой результатов вступительного испытания в порядке, установленном Правилами приема, действующими на текущий год поступления.

2. ФОРМА, СТРУКТУРА, ПРОЦЕДУРА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ И ШКАЛА ОЦЕНИВАНИЯ ОТВЕТОВ

2.1 Вступительное испытание проводится на русском языке.

2.2 Вступительное испытание по специальной дисциплине проводится в форме экзамена (с сочетанием письменной и устной форм) в соответствии с перечнем тем и (или) вопросов, установленных данной Программой.

2.3 Структура экзамена:

Вступительные испытания проводятся в смешанной форме – тестирование, 20 вопросов – не более 10 минут, письменный ответ на билет, 3 вопроса – не более 30 минут, собеседование по итогам предыдущих этапов с учетом тематики предполагаемого исследования – не более 10 минут.

2.4 Вступительное испытание проводится экзаменационной комиссией, действующей на основании приказа ректора.

Итоговая оценка за экзамен определяется как средний балл, выставленный всеми членами экзаменационной комиссии.

Результаты проведения вступительного испытания оформляются протоколом, в котором фиксируются вопросы экзаменаторов к поступающему. На каждого поступающего ведется отдельный протокол. Протокол приема вступительного испытания подписывается членами комиссии, которые присутствовали на экзамене, с указанием их ученой степени, ученого звания, занимаемой должности и утверждается председателем комиссии. Протоколы приема вступительных испытаний после утверждения хранятся в личном деле поступающего

2.5 Шкала оценивания ответов на экзамене.

неудовлетворительно	удовлетворительно	хорошо	отлично
до 44 баллов	45 – 75 баллов	76 – 84 баллов	85 – 100 баллов

Баллы складываются из итогов тестирования – до 20 баллов, письменного ответа на вопросы – 3*20=60 баллов, устного собеседования – 20 баллов.

Максимальное количество баллов за экзамен – 100. Минимальное количество баллов для успешного прохождения экзамена – 45. Поступающий, набравший менее 45 баллов за экзамен, не может быть зачислен в аспирантуру.

Критерии оценивания отдельных письменных вопросов и устного собеседования

Балл	Уровень владения темой
до 8	Поступающий при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи делает принципиальные ошибки
19-13	Поступающий при ответе на вопросы не дает определение некоторых основных понятий, не способен показать причинно-следственные связи некоторых явлений, при решении задачи делает принципиальные ошибки
14-17	Поступающий при ответе на вопросы дает определение некоторых основных понятий, может показать причинно-следственные связи явлений, при решении задачи не допускает принципиальные ошибки
18-20	Поступающий при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи.

Итоговый балл получается сложением отдельных компонентов.

Таблица критериев оценки устных и письменных ответов (при наличии)

Вид деятельности		
Оценка	Балл	Уровень владения темой
неудовлетворительно	до 44	Поступающий при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи делает принципиальные ошибки
удовлетворительно	45-75	Поступающий при ответе на вопросы не дает определение некоторых основных понятий, не способен показать причинно-следственные связи некоторых явлений, при решении задачи делает принципиальные ошибки
хорошо	76-84	Поступающий при ответе на вопросы дает определение некоторых основных понятий, может

		показать причинно-следственные связи явлений, при решении задачи не допускает принципиальные ошибки
отлично	85-100	Поступающий при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи.

2.6 Во время проведения вступительных испытаний их участникам и лицам, привлекаемым к их проведению, запрещается иметь при себе и использовать средства связи. Участники вступительных испытаний не могут иметь при себе и использовать справочные материалы и электронно-вычислительную технику, за исключением письменных принадлежностей.

При нарушении поступающим во время проведения вступительных испытаний правил приема, утвержденных организацией, уполномоченные должностные лица организации вправе удалить его с места проведения вступительного испытания с составлением акта об удалении.

3. СОДЕРЖАНИЕ ПРОГРАММЫ

Примерный перечень тем и вопросов для подготовки к сдаче экзамена *(и формирования билетов или тестов):*

1. Законодательные акты Российской Федерации в области информационной безопасности.
2. Система защиты информации, составляющей государственную тайну в Российской Федерации.
3. Нормативно-правовое обеспечение лицензирования и сертификации в области защиты информации в Российской Федерации.
4. Политика безопасности. «Адекватная политика безопасности».
5. Этапы защиты операционных систем.
6. Политика безопасности. Категории и требования безопасности.
7. Проблемы информационной безопасности при распределенной обработке данных и тиражировании.
8. Организация аудита событий в базе данных и средства контроля целостности информации в них.
9. Технические каналы утечки информации, технические средства приема, обработки, хранения и передачи информации, вспомогательные технические средства и системы. Характеристики каналов утечки информации и указанные средства.
10. Средства перехвата акустических сигналов по воздушным и виброакустическим каналам.
11. Способы перехвата акустических сигналов по электроакустическим и оптико-электронным каналам утечки информации.

12. Физическая природа паразитных связей между проводными линиями передачи информации. Виды паразитных связей в реальной электронной аппаратуре.
13. Демаскирующие признаки объектов технической разведки в видимом и инфракрасном диапазонах электромагнитного спектра.
14. Инженерно-технические средства обеспечения безопасности объектов.
15. Методы и средства защиты электронных устройств и объектов от побочных электромагнитных излучений.
16. Способы защиты информации от утечки при передаче ее по слаботочным линиям.
17. Демаскирующие признаки радиоэлектронных средств обработки и передачи информации.
18. Способы контроля и прослушивания телефонных каналов связи.
19. Демаскирующие признаки радиоэлектронные средства и акустические закладки.
20. Понятие «монитор безопасности объектов» и «монитор безопасности субъектов».
21. Понятие «изолированная программная среда».
22. Стадии и этапы проектирования Комплексной системы обеспечения информационной безопасности.
23. Основы игровых моделей принятия решений системы информационной безопасности, анализ информированности в них.
24. Организационное управление защитой информации. Организационно-функциональные задачи службы безопасности.
25. Жизненный цикл автоматизированной системы. Среда безопасности продукта информационных технологий. Область действия функции безопасности объекта оценки.
26. Функции заказчиков и разработчиков. Содержание профиля защиты изделия информационных технологий. Базовая стойкость функций безопасности.
27. Архитектура защищенных систем. Источники требований безопасности изделия информационных технологий. Стойкость функции безопасности.
28. Функциональная и обеспечивающая часть сложной системы. Функциональные компоненты безопасности изделия информационных технологий. Средняя стойкость функции безопасности.
29. Архитектура защищенных систем. Структура функциональных компонент безопасности изделия информационных технологий. Атрибут безопасности.
30. Ядро безопасности. Структура класса функционального компонента безопасности автоматизированной системы. Понятие секрет.
31. Методы реализации моделей безопасности. Структура семейства функционального компонента безопасности автоматизированной системы. Понятие «функция безопасности».
32. Реализация систем контроля доступа. Ранжирование компонентов. Ресурс объекта оценки.
33. Технологический цикл реализации защищенной системы обработки и хранения информации. Классы и семейства класса функциональных компонент безопасности.

34. Криптографические методы защиты информации. Шифрование, хэширование, электронная подпись.
35. Криптографические протоколы.
36. Межсетевые экраны.
37. Виртуальные частные сети.
38. Служба безопасности организации. Организационное обеспечение информационной безопасности предприятия.
39. Усиленная аутентификация.
40. Защита от несанкционированного доступа.

4. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА ДЛЯ СДАЧИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

ЭКЗАМЕН

по направлению 10.06.01 «Информационная безопасность»

Билет 1.

1. Укажите основные свойства безопасности информации.

а). Конфиденциальность, целостность, достоверность.
б). Конфиденциальность, целостность, доступность.
в). Целостность, непротиворечивость, достоверность.
г). Целостность, аутентичность, доступность.

2. Какой из принципов обеспечения информационной безопасности в автоматизированных системах предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов?

а). Принцип системности.
б). Принцип непрерывности защиты.
в). Принцип разумной достаточности.
г). Принцип гибкости управления и применения.

3. Что из перечисленного входит в канал утечки информации?

а). Нарушитель.
б). Угроза утечки информации.
в). Способ реализации угрозы утечки информации.
г). Источник информации.

4. Какой из перечисленных методов защиты информации не предназначен для обеспечения защиты от реализации угрозы нарушения конфиденциальности информации?

а). Разграничение прав доступа.
б). Электронная подпись.
в). Шифрование.

г). Парольная защита.

5. Какова основная цель мандатной политики разграничения прав доступа?

а). Предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа.
б). Предотвращение утечки информации от объектов с низким уровнем доступа к объектам с высоким уровнем доступа.
в). Противодействие утечке прав доступа.
г). Противодействие хищению прав доступа.

6. Для чего предназначены токены?

а). Хранение ключевой информации.
б). Обеспечение антивирусной защиты.
в). Выявление каналов утечки информации.
г). Выявление инцидентов безопасности.

7. Укажите правильную последовательность уровней модели OSI от верхнего к нижнему.

а). Прикладной, сеансовый, представительский, транспортный, сетевой, канальный, физический
б). Прикладной, представительский, канальный, сеансовый, транспортный, сетевой, физический.
в). Прикладной, представительский, сеансовый, транспортный, сетевой, канальный, физический.
г). Прикладной, представительский, сеансовый, сетевой, транспортный, канальный, физический.

8. В чем заключается различие между симметричными и асимметричными криптосистемами?

а). В решаемых задачах защиты информации.
б). В показателях криптографической стойкости.
в). В количестве и назначении используемых ключей.
г). Принципиальных различий нет.

9. Чем шифр «Магма» отличается от шифра, определенного в стандарте ГОСТ 28147-89?

а). Длиной ключа.
б). Невозможностью использования произвольной таблицы замен.
в). Это два принципиально разных симметричных блочных шифра.
г). Количеством раундов.

10. Что является основой проблемой криптографии с открытым ключом?

а). Обеспечение аутентичности закрытых ключей.
б). Обеспечение конфиденциальности закрытых ключей.
в). Обеспечение аутентичности открытых ключей.
г). Обеспечение конфиденциальности открытых ключей.

11. Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа называется:

a) Характеристика нарушителя;
b) Модель нарушителя;
c) Сценарий нарушителя;
d) Модель источников угроз.

12. Какое из нижеперечисленных направлений не относится к аттестации объектов информатизации по требованиям безопасности информации:

a) Аттестация автоматизированных систем, средств связи, обработки и передачи информации;
b) Аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
c) Аттестация рабочих мест с целью оценки условий труда;
d) Аттестация технических средств, установленных в выделенных помещениях и защищаемых помещениях.

13. Стратегия (метод) тестирования функционального поведения объекта (программы, системы) с точки зрения внешнего мира, при котором не используется знание о внутреннем устройстве тестируемого объекта

a) Тестировение черного ящика;
b) Тестирование белого ящика;
c) Тестирование красного ящика;
d) Тестирование неизвестного ящика.

14. Методика тестирования на проникновение называется:

a) Аудит;
b) Пентест;
c) Honeypot;
d) Metasploit.

15. Что из нижеперечисленного не относится к этапу анализа рисков информационной безопасности:

a) Построение модели нарушителя;
b) Идентификация ресурсов;
c) Идентификация бизнес-требований и требований законодательства, применимых к идентифицированным ресурсам;
d) Оценивание идентифицированных ресурсов с учетом выявленных бизнес требований и требований законодательства, а также последствий нарушения их конфиденциальности, целостности и доступности.

16. Какая угроза безопасности информации является преднамеренной ?

a) Ошибки персонала;
b) Сбой программного обеспечения;
c) Фальсификация, подделка документов;
d) Открытие электронного письма, содержащего вирус.

17. Территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных называется …

a) Неконтролируемой зоной
b) Зоной помещений автоматизированной системы
c) Зоной баз данных защищаемой системы
d) Зоной контролируемой территории.

18. Угроза диверсии относится к …

a) Субъективной преднамеренной причине нарушения целостности информации;
b) Субъективной непреднамеренной причине нарушения целостности информации;
c) Объективной непреднамеренной причине нарушения целостности информации;
d) Объективной преднамеренной причине нарушения целостности информации.

19. Перехват данных является угрозой:

a) Доступности;
b) Конфиденциальности;
c) Целостности;
d) Достоверности.

20. Продолжите тезис верно: Класс задач «Легендирование» по защите информации…

a) Не существует;
b) Потерял актуальность в связи с переходом на новые стандарты симметричных криптосистем;
c) Предполагает включение в состав элементов системы обработки информации дополнительных компонентов;
d) Объединяет задачи по обеспечению получения злоумышленником искаженного представления о характере и предназначении объекта.

ФИО поступающего _____

Дата_____ Подпись_____

5. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

5.1. Основная литература

1. Шелупанов А.А. Идентификация и аутентификация в цифровом мире: монография / А.Г. Сабанов, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2022 – 356 с.: ил. – ISBN 978-5-9912-0976-2. – (Серия «Технологии доверенного взаимодействия»).

2. Шелупанов А.А. Форензика. Теория и практика расследования киберпреступлений: монография / А.А. Шелупанов, А.Р. Смолина. – М.: Горячая линия – Телеком, 2018. – 104 с. – ISBN 978-5-9912-0769-0.

3. Шелупанов А.А. Современные методы и способы идентификации. Теория и практика: монография / А.Ю. Исхаков, Р.В. Мещеряков, А.А. Шелупанов, С.Ю. Исхаков. – Томск: Изд-во Томского государственного университета систем управления и радиоэлектроники, 2016. – 114 с. – ISBN 978-5-86889-761-0.

4. Основы информационной безопасности. Учебное пособие для вузов / Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. – М.: Горячая линия – Телеком, 2006. – 544 с. (81 экз.).

5. Зайцев А.П. Технические средства и методы защиты информации. Учебное пособие для вузов / А. П. Зайцев, А. А. Шелупанов. – Томск: В-Спектр, 2006. – 383 с. (61 экз.).

6. Зайцев А.П. Программно-аппаратные средства обеспечения информационной безопасности.Учебное пособие. Раздел 1. – 2-е изд., перераб. и доп. – Томск: В-Спектр, 2007. – 143 с. (66 экз.).

7. Зайцев А.П. Программно-аппаратные средства обеспечения информационной безопасности. Учебное пособие. Раздел 2. – 2-е изд., перераб. и доп. – Томск: В-Спектр, 2007. – 118 с. (66 экз.).

5.2. Дополнительная литература

1. Основы криптографии. Учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – 3-е изд., испр. и доп. – М.: Гелиос АРВ, 2005. – 479 с. (28 экз.).

2. Баричев С.Г. Основы современной криптографии. Учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – 2-е изд., перераб. и доп. – М.: Горячая линия-Телеком, 2002. – 176 с. (51 экз.).

3. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: ПИТЕР, 2013. – 944 с. (20 экз.).

4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие для вузов. – М.: ИНФРА-М, 2012. – 592 с. (30 экз.).

5.3. Периодические издания

1. Журнал «Вопросы защиты информации».
2. Журнал «Безопасность информационных технологий».
3. Журнал «Вопросы кибербезопасности».
4. Журнал «Защита информации. Инсайд».
5. Журнал «Компьютерная оптика».
6. Журнал «Доклады ТУСУР».
7. Журнал «Информационные технологии».

5.4. Перечень интернет-ресурсов

1. Нормативные акты ФСТЭК [Электронный ресурс]. – Режим доступа: https://fstec.ru/
2. Нормативные акты ФСБ [Электронный ресурс]. – Режим доступа: http://www.fsb.ru/
3. Нормативные акты федерального законодательства в сфере ИБ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/
4. Научная электронная библиотека eLIBRARY.RU. [Электронный ресурс]. – Режим доступа: https://elibrary.ru/defaultx.asp
5. База данных Scopus. [Электронный ресурс]. – Режим доступа: https://www.scopus.com
6. База данных SpringerLink. [Электронный ресурс]. – Режим доступа: https://link.springer.com/
7. База данных ScienceDirect [Электронный ресурс]. – Режим доступа: http://www.sciencedirect.com/
8. Цифровая библиотека IEEE Xplore [Электронный ресурс]. – Режим доступа: http://ieeexplore.ieee.org/Xplore/home.jsp
9. Научно-образовательный портал ТУСУР[Электронный ресурс]. – Режим доступа: https://edu.tusur.ru/