МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

УТВЕРЖДАЮ
Проректор по научной работе и инновациям
_____ Мещеряков Р.В.
«___»_____ 2017 г.

ПРОГРАММА
Вступительного испытания по специальной дисциплине

по направлению подготовки
10.06.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

профиль программы
05.13.19 — МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Томск 2017

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.

В основу программы положены следующие вузовские дисциплины: «Основы информационной безопасности», «Криптографические методы защиты информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Технические средства и методы защиты информации» (специальности высшего образования 10.05.02, 10.05.03, 10.05.04).

Составители программы: Шелупанов А.А., заведующий кафедрой комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС); Мещеряков Р.В., д-р техн. наук, профессор, заведующий кафедрой безопасности информационных систем (БИС); Евсютин О.О., канд. техн. наук, доцент кафедры БИС.

ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА на заседании кафедры КИБЭВС, протокол № ____ от _____ 2017 г.

СОГЛАСОВАНО

Декан	факультета безопасности		Е.М. Давыдова
Зав. кафедрой	КИБЭВС		А.А. Шелупанов

Разработчики:

Зав. кафедрой БИС, д-р техн. наук		Р.В. Мещеряков
Доцент каф. БИС, канд. техн. наук		О.О. Евсютин

Зав. аспирантурой и докторантурой Т.Ю. Коротина

1. ОБЩИЕ ПОЛОЖЕНИЯ

Программа вступительного испытания по специальности **05.13.19 – Методы и системы защиты информации, информационная безопасность** предназначена для поступающих в аспирантуру в качестве руководящего учебно-методического документа для целенаправленной подготовки к сдаче вступительного испытания.

Программа включает содержание профилирующих учебных дисциплин, входящих в Основную образовательную программу высшего образования, по которой осуществляется подготовка студентов, в соответствии с требованиями федерального государственного образовательного стандарта.

Целью программы вступительных испытаний является определение уровня знаний, готовности и возможности поступающего к освоению программы подготовки в аспирантуре, к самостоятельному выполнению научной работы, подготовке и защите диссертации на соискание ученой степени кандидата наук по научной специальности **05.13.19 – Методы и системы защиты информации, информационная безопасность**.

Поступающий в аспирантуру должен продемонстрировать высокий уровень практического и теоретического владения материалом вузовского курса.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

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.

3. ПОРЯДОК ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительные испытания проводятся в тестовой форме. Продолжительность проведения письменного экзамена – не более 60 минут.

Уровень знаний поступающего оценивается по 100 балльной шкале. Минимальный балл, подтверждающий успешной прохождения вступительного испытания, равен 45.

Протокол приема вступительного экзамена подписывается членами комиссии с указанием их ученой степени, ученого звания, занимаемой должности.

Протокол заседания экзаменационной комиссии после утверждения ректором (проректором по научной работе) ТУСУРа хранятся в отделе аспирантуры и докторантуры.

Во время проведения вступительных испытаний их участникам и лицам, привлекаемым к их проведению, запрещается иметь при себе и использовать средства

связи. Участники вступительных испытаний могут иметь при себе и использовать справочные материалы и электронно-вычислительную технику.

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.

4. ОБРАЗЦЫ ЭКЗАМЕНАЦИОННЫХ БИЛЕТОВ ДЛЯ СДАЧИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

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.

Билет 2.

1. Укажите составляющие элементы комплекса мер по обеспечению информационной безопасности.

а). Организационный, правовой, инженерно-технический, программно-аппаратный, криптографический, специальный.
б). Организационный, инженерно-технический, программно-аппаратный, криптографический.
в). Организационный, правовой, инженерно-технический, программный, криптографический.
г). Организационный, правовой, инженерно-технический, программно-аппаратный, криптографический.

2. Какой из принципов обеспечения информационной безопасности в автоматизированных системах предполагает принятие мер по защите информации на всех этапах жизненного цикла автоматизированной системы?

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

3. Какой из перечисленных каналов утечки информации не относится к техническим каналам утечки речевой информации?

а). Акустический.
б). Индукционный.
в). Виброакустический.
г). Оптико-электронный.

4. Что понимается под учетной записью пользователя в информационной системе?
а). Совокупность идентификатора пользователя и пароля.
б). Совокупность идентификатора пользователя и его открытого ключа.
в). Совокупность идентификатора пользователя и его закрытого ключа.
г). Совокупность открытого и закрытого ключа пользователя.

5. Что понимается под доменом безопасности в субъектно-объектном представлении автоматизированной системы?
а). Совокупность субъектов, которым разрешен доступ к конкретному объекту.
б). Безопасное состояние автоматизированной системы.
в). Совокупность объектов, к которым разрешен доступ конкретному субъекту.
г). Множество безопасных состояний автоматизированной системы.

6. Для чего предназначен криптопровайдер?
а). Для шифрования информации на машинных носителях.
б). Для предоставления криптографических функций.
в). Для управления ключами пользователей.
г). Для аутентификации пользователей.

7. Сколько уровней включает модель OSI?
а). 6.
б). 7.
в). 8.
г). 9.

8. Почему асимметричные криптосистемы не используются для непосредственного шифрования видеотрафика?
а). В связи с недостаточной криптографической стойкостью асимметричных криптосистем.
б). В связи с недостаточным быстродействием асимметричных криптосистем.
в). В связи с отсутствием соответствующих стандартов.
г). Асимметричные криптосистемы используются для непосредственного шифрования видеотрафика.

9. Сопоставьте действующие отечественные криптографические стандарты с перечисленными криптографическими методами защиты информации в порядке их перечисления: алгоритм шифрования, функция хеширования, схема электронной подписи.
а). ГОСТ Р 34.12–2015, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2012.
б). ГОСТ Р 34.12–2015, ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012.
в). ГОСТ 28147-89, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2012.
г). ГОСТ Р 34.12–2015, ГОСТ Р 34.11–94, ГОСТ Р 34.10–2012.

10. Для чего нужна перекрестная сертификация.
а). Для проверки подлинности сертификата открытого ключа, выданного неизвестным центром сертификации.
б). Для обеспечения возможности одновременного функционирования более чем одного центра сертификации.
в). Для обеспечения возможности одновременного подписания одного электронного документа разными пользователями.

г). Для повышения уровня доверия к сертификатам открытого ключа.

Билет 3.

1. Какая из приведенных угроз информационной безопасности является опосредованной?

а). Угроза нарушения конфиденциальности.
б). Угроза нарушения целостности.
в). Угроза нарушения доступности.
г). Угроза раскрытия параметров автоматизированной системы.

2. Какой из принципов обеспечения информационной безопасности в автоматизированных системах предполагает выбор уровня зашиты, обеспечивающего приемлемый уровень затрат, риска и размер возможного ущерба?

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

3. Какой из перечисленных каналов утечки информации не относится к техническим каналы утечки информации при передаче ее по каналам связи?

а). Электромагнитный.
б). Акустоэлектрический.
в). Электрический.
г). Индукционный.

4. Какую цель преследует принудительная смена пароля при первой регистрации пользователя в информационной системе?

а). Защиту от выбора слабого пароля.
б). Защиту от неправомерных действий других пользователей.
в). Защиту от подглядывания пароля.
г). Защиту от неправомерных действий администратора.

5. Какая из перечисленных моделей формализует дискреционное разграничение прав доступа?

а). Модель Харрисона–Рузо–Ульмана.
б). Модель Биба.
в). Модель Белла–ЛаПадула.
г). Модель Take-Grant.

6. Что из перечисленного относится к двухфакторной аутентификации пользователей?

а). Знание двух различных паролей.
б). Знание закрытого ключа и открытого ключа.
в). Владение аппаратным устройством аутентификации и знание PIN-кода.
г). Владение аппаратным устройство аутентификации.

7. Какой из приведенных уровней отсутствует в модели OSI?

а). Физический
б). Сетевой.
в). Представительский.
г). Аппаратный.

8. Для чего в схемах электронной подписи используются функции хеширования?

а). Для повышения криптографической стойкости схемы электронной подписи.
б). Для представления подписываемого сообщения в виде строки данных фиксированной длины.
в). Для обеспечения контроля целостности подписываемого сообщения.
г). Для представления подписанного сообщения в виде строки данных фиксированной длины.

9. На каком математическом аппарате основана схема электронной подписи, определенная в стандарте ГОСТ Р 34.10–2012.
а). Кольца классов вычетов.
б). Группы подстановок.
в). Поля Галуа.
г). Эллиптические кривые.

10. Для чего предназначена инфраструктура открытого ключа.
а). Для обеспечения возможности подтверждения аутентичности открытых ключей пользователей.
б). Для обеспечения конфиденциальности закрытых ключей пользователей.
в). Для организации безопасной передачи конфиденциальной информации по открытым каналам связи.
г). Для безопасного хранения открытых ключей пользователей.

Билет 4.

1. Как называется перечень возможных угроз автоматизированной системе?
а). Моделью нарушителя.
б). Моделью злоумышленника.
в). Моделью угроз.
г). Моделью рисков.

2. Какой из принципов обеспечения информационной безопасности в автоматизированных системах предполагает возможность варьирования уровня защищенности автоматизированной системы?
а). Принцип системности.
б). Принцип непрерывности защиты.
в). Принцип разумной достаточности.
г). Принцип гибкости управления и применения.

3. Что является средой распространения в виброакустическом канале утечки информации?
а). Воздух.
б). Строительные конструкции.
в). Цепи электропитания.
г). Цепи заземления.

4. Какой из перечисленных методов защиты информации не предназначен для обеспечения защиты от реализации угрозы нарушения целостности информации?
а). Шифрование.
б). Создание резервных копий информации.
в). Хеширование.
г). Электронная подпись.

5. Для чего предназначена модель Take-Grant?
а). Для анализа защищенности автоматизированных систем.

б). Для анализа путей распространения прав доступа в системах с дискреционным разграничением прав доступа.
в). Для анализа путей распространения прав доступа в системах с мандатным разграничением прав доступа.
г). Для анализа путей распространения прав доступа в системах с ролевым разграничением прав доступа.

6. Каким образом можно защититься от невыявленных программно-аппаратных закладок?
а). С помощью антивирусного программного обеспечения.
б). С помощью организации доверенной вычислительной среды.
в). С помощью использования шифрованной файловой системы.
г). С помощью многофакторной аутентификации.

7. Какой из уровней модели OSI обеспечивает управление диалогом между обслуживаемыми процессами на уровне представления?
а). Представительский.
б). Сеансовый.
в). Транспортный.
г). Канальный.

8. Чем имитовставка отличается от хеш-кода?
а). Хеш-код рассчитывается на основании сообщения, а имитовставка — на основании сообщения и секретного ключа.
б). Имитовставка рассчитывается на основании сообщения, а хеш-код — на основании сообщения и секретного ключа.
в). Это синонимы.
г). Имитовставка не может использоваться для обеспечения контроля целостности информации.

9. В каком из режимов работы симметричных блочных шифров результат зашифрования очередного блока открытого текста при фиксированном ключе зависит только от порядкового номера данного блока.
а). Режим простой замены.
б). Режим гаммирования.
в). Режим гаммирования с обратной связью по выходу.
г). Режим гаммирования с обратной связью по шифртексту.

10. Для чего служат цифровые сертификаты?
а). Для подтверждения подлинности открытых ключей пользователей.
б). Для обеспечения секретности закрытых ключей пользователей.
в). Для подтверждения подлинности центра сертификации, выдавшего сертификат.
г). Для обеспечения невозможности компрометации закрытых ключей пользователей.

5. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

5.1. Основная литература

1. 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.).

2. 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.).

3. 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.).

4. 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. Смарт Н. Криптография. Учебник для вузов. – М.: Техносфера, 2005. – 525 с. (11 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. Научная электронная библиотека eLIBRARY.RU. [Электронный ресурс]. – Режим доступа: https://elibrary.ru/defaultx.asp
2. База данных Scopus. [Электронный ресурс]. – Режим доступа: https://www.scopus.com
3. База данных SpringerLink. [Электронный ресурс]. – Режим доступа: https://link.springer.com/
4. База данных ScienceDirect [Электронный ресурс]. – Режим доступа: http://www.sciencedirect.com/
5. Цифровая библиотека IEEE Xplore [Электронный ресурс]. – Режим доступа: http://ieeexplore.ieee.org/Xplore/home.jsp
6. Научно-образовательный портал ТУСУР[Электронный ресурс]. – Режим доступа: https://edu.tusur.ru/