МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ»
(МТУСИ)

УТВЕРЖДАЮ

Начальник отдела «Приемная комиссия»

_____ / С.Р. Сабитова

М.П.

«17» января 2025 г.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

«Методы и системы защиты информации, информационная безопасность»

ПВИ-А-05

Москва 2025

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Цели и задачи вступительного испытания.

Целью вступительных испытаний в аспирантуру по научной специальности *2.3.6. Методы и системы защиты информации, информационная безопасность* является проверка уровня знаний поступающего в профессиональной сфере деятельности, достаточного для продолжения высшего образования в аспирантуре по программам подготовки научных и научно-педагогических кадров.

В аспирантуру принимаются лица, имеющие высшее профессиональное образование, подтвержденное дипломом специалиста или магистра, или имеющие высшее профессиональное образование, полученное в образовательных учреждениях иностранных государств. За счет бюджетных средств имеют право обучаться лица, получающие образование данного уровня впервые (специалисты и магистры). Прием в аспирантуру регламентируется «Правилами приема на обучение по образовательным программам высшего образования - программам подготовки научных и научно-педагогических кадров в аспирантуре МТУСИ в 2025-2026 учебном году» (далее – Правила приема).

2. Требования к уровню подготовки поступающих.

Программа вступительных испытаний включает основные темы дисциплин ОП ВО базовой части профессионального цикла подготовки специалистов и магистров по направлению «Информатика и вычислительная техника», дополненные дисциплинами вариативной части профессионального цикла, отражающими отраслевые особенности в сфере инфокоммуникаций. Программа сформирована на основе федеральных государственных образовательных стандартов высшего образования по программам специалитета или магистратуры.

3. Порядок и форма проведения вступительного испытания.

Оценка знаний по специальной дисциплине проводится в устной форме с обязательным оформлением ответов на вопросы билета в письменном виде.

На вступительном испытании не допускается использование аудио- или видеоустройства с использованием электронных или других типов носителей,

позволяющих принимать, передавать, хранить и обрабатывать информацию (инженерные калькуляторы, рации, переговорные устройства, мобильные телефоны, планшеты, компьютеры, электронные и умные часы, Bluetooth и Wi-fi аксессуары, включая наушники, смарт-очки, иные средства связи)

4. Описание вида контрольно-измерительных материалов.

Поступающий получает два вопроса, соответствующих программе экзамена, третье задание предполагает проверку уровня владения иностранным языком (чтение и краткий пересказ текста по специальности со словарем).

5. Продолжительность вступительного испытания.

Поступающему предоставляется 40 минут на подготовку ответов по вопросам билета, после чего его заслушивает комиссия. Поступающему могут быть заданы дополнительные вопросы или задачи в рамках программы экзамена.

6. Шкала оценивания.

1. Максимальный балл за вступительное испытание 100 баллов = 40 баллов (вопрос 1)+ 40 баллов (вопрос 2)+ 20 баллов (задание 3 «чтение и перевод текста на иностранном языке»).
2. Критерии оценки **1-го и 2-го вопроса**:

40-31 баллов – вопросы раскрыты полно и правильно, поступающий демонстрирует глубокие теоретические знания, умение сравнивать и оценивать различные научные подходы, пользоваться современной научной терминологией.

30-21 баллов - даны в целом правильные ответы на вопросы, но неполные, при этом поступающий недостаточно аргументирует ответы, пропускает ряд важных деталей или затрагивает посторонние вопросы; базовой терминологией владеет.

20-11 баллов – в знаниях имеются существенные пробелы; выводы и обобщения аргументирует слабо, допускает ошибки и неточности в использовании терминологии; определения понятий даёт недостаточно четкие.

10-0 баллов – поступающий демонстрирует непонимание основного содержания теоретического материала, поверхностность и слабую аргументацию суждений или допущены значительные ошибки.

3. Критерии оценки задания 3 «**чтение и перевод текста на иностранном языке»**:

20-14 баллов - поступающий демонстрирует полное понимание технического текста на иностранном языке, отвечая на вопросы, поставленные экзаменационной комиссией.

13-8 баллов - поступающий демонстрирует неполное понимание технического текста на иностранном языке, отвечая на вопросы, поставленные экзаменационной комиссией.

7-0 баллов – поступающий демонстрирует непонимание технического текста на иностранном языке, не может ответить на вопросы, поставленные экзаменационной комиссией.

4. Индивидуальные достижения поступающего оформляются в виде списка согласно приложению 1 Правил приема (отдельно для каждой научной специальности, указанной в заявлении) и сдаются в бумажном или электронном виде при подаче документов.

Баллы, полученные за индивидуальные достижения суммируются с баллами, полученными на вступительном испытании.

7. Язык проведения вступительного испытания.

Вступительное испытание проводится на русском языке. По решению комиссии вступительное испытание может быть проведено на английском языке.

ПЕРЕЧЕНЬ ТЕМ И РАЗДЕЛОВ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Основные разделы науки и темы, по которым проверяются знания:

Основы обеспечения информационной безопасности

Основные термины и определения в области информационной безопасности. Информационная безопасность и защита информации. Понятие угрозы безопасности информации. Классификация угроз. Основные аспекты информационной безопасности: конфиденциальность, целостность, доступность. Понятие национальной безопасности; виды безопасности; информационная безопасность в системе национальной безопасности Российской Федерации. Классификация информации (К, С, СС, ОВ). Перечень информации, которой не может быть присвоен статус ограниченного распространения. Различные категории информации, подлежащие защите

(государственная тайна, коммерческая тайна, персональные данные…). Доктрина информационной безопасности Российской Федерации. Органы государственной власти, регулирующие деятельность в области обеспечения информационной безопасности. Структура нормативной правовой базы Российской Федерации в области обеспечения информационной безопасности. Деятельность государственных органов РФ, контролирующих деятельность в области информационной безопасности, их роль в формировании и актуализации государственной системы защиты информации в РФ. Управление информационной безопасностью. Процессный подход. Понятие системы управления информационной безопасностью (СУИБ). Стандарты серии ISO 27000. Понятие риска информационной безопасности. Анализ рисков. Основные процессы СУИБ. Документирование СУИБ. Технические каналы утечки информации. Защита информации от утечки по техническим каналам. Специальные исследования технических средств на наличие технических каналов утечки информации

Криптографические методы защиты информации

Криптология. Понятия криптографии, криптоанализа, стеганографии.

Основные термины и определения: шифрование, расшифрование, дешифрование. Симметричные криптосистемы. Принципы работы и основные понятия. Пример реализации.

Асимметричные криптосистемы. Принципы работы и основные понятия. Пример реализации.

Потоковые и блочные шифры.

Цифровая подпись. Протокол цифровой подписи на симметричном шифре. Цифровая подпись. Протокол цифровой подписи на асимметричных крипто алгоритмах.

Алгоритмы блочного шифрования AES, DES, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015. Слабые ключи итеративных симметричных блочных шифров.

Протоколы аутентификации. Базовые конструкции протоколов аутентификации. Аутентификация по паролю (списки паролей, протокол Лампорта). Аутентификация «запрос – ответ» (ISO/IEC 9798). Принцип аутентификации, основанный на нулевом разглашении (протоколы Фиата – Шамира, Файге – Фиата – Шамира).

Случайные процессы и статистический анализ

Имитационное моделирование. Методы генерации случайных величин.

Случайные процессы. Марковские случайные процессы. Цепи Маркова с дискретным и непрерывным временем, метод динамики средних.

Регрессионный анализ. Спектральный и Корреляционный анализ. Задачи классификации; дискриминантный и кластерный анализ.

Методы и средства обработки информации в современных информационных системах

Этапы проектирования базы данных. Процесс нормализации отношений в реляционной базе данных. Хранилища данных. Оперативная аналитическая обработка (OLAP). Понятия "данные", "информация", "знания" в приложении к Data Mining. Классификация методов Data mining. Основные компоненты объектно-ориентированного подхода. Объекты и классы с точки зрения проектирования и программирования. Обработка ошибок в современном программном обеспечении. Обработка исключительных ситуаций, структурная обработка аппаратных исключений. Структурные и функциональные методы тестирования программ. Методы оценки надёжности программных комплексов. Принципы построения современных операционных систем. Архитектура памяти, процессы, многозадачность. Основные ситуации, требующие синхронизации. сновные принципы построения систем реального времени. Области применения, требования, особенности разработки. Технологии систем хранения данных: основные задачи, подходы к организации.

Программно-аппаратные средства обеспечения информационной безопасности

Классификация АС по требованиям безопасности информации (РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»). Установление подлинности пользователя. Парольные, физические и биометрические методы подтверждения подлинности. Понятие факторность методов подтверждения подлинности. Сравнение методов по степени обеспечения уровня информационной

безопасности. Этапы развития криптографической подсистемы. Цифровой сертификат. ЭЦП. Технология «цифрового конверта». Основные принципы создания системы защиты информации от несанкционированного доступа (принцип персональной ответственности, принцип чистоты повторно используемых ресурсов, монитор обращений). Основные принципы создания системы защиты информации от несанкционированного доступа (принцип достаточной глубины контроля доступа, принцип разграничения потоков информации, монитор обращений). Классификация и краткая характеристика средств обеспечения информационной безопасности в компьютерных сетях. Системы анализа защищенности. Организация и использование средств доказательной регистрации событий (аудита).. Межсетевые экраны. Фильтрация трафика. Системы обнаружения и предотвращения вторжений (IDS/IPS). SIEM-системы

Обнаружение вторжений в компьютерные сети

Этапы сетевой атаки. База знаний Mitre Att&ck. Принципы работы систем обнаружения атак (СОА) . Основные типы СОА. Параметры сетевого трафика, анализируемые СОА. Примеры. Законодательство РФ в области защиты критической информационной инфраструктуры. Ответственность за неправомерное воздействие на КИИ РФ. Особенности компьютерного следообразования в операционных система семейства Windows и Linux. Аудит событий и его безопасность. Основные свойства файловой системы NTFS. Структура метаданных и их размещение на дисковом пространстве. Права доступа. Работа с объектами файловой системы. Преступления в сфере компьютерной информации; экспертиза преступлений в области компьютерной информации; криминалистические аспекты проведения расследований.

Анализ методов обнаружения аномалий и атак на уровне сети и хоста. Экспертные системы, статистический анализ, нейросети. Обнаружение следов атак в "ручном" режиме. Контроль изменений файлов и каталогов. Анализ журналов регистрации и сетевого трафика. Признаки атак

Системы обнаружения атак (СОА), основные способы построения. СОА на основе сигнатурного анализа. Обнаружение аномалий на основе нейронных сетей

Алгоритмы классификации и кластеризации методами машинного обучения

Интеллектуальные технологии информационной безопасности

Основные понятия и свойства интеллектуальных систем защиты информации (ИСЗИ) . Архитектура ИСЗИ. Методы искусственного интеллекта в задачах обеспечения безопасности компьютерных сетей.

Методы интеллектуального анализа данных. Деревья решений. Нейронные сети. Методы математической статистики. Методы визуализации. Генетические алгоритмы. Эволюционное программирование

Ассоциативный анализ. Технологии KDD и Data Mining. Выборка данных. Очистка данных. Трансформация данных. Классификация. Регрессия. Кластеризация– Ассоциация. Машинное обучение (machine learning). Программное обеспечение Data Mining

Классификация. Основы обучения с учителем. Классификация на основе ассоциативных правил. Классификация IP-трафика на основе портов; на основе полезной нагрузки; на основе статистических методов . Особенности применения методов машинного обучения в системах ИБ. Иерархические и неиерархически методы кластеризации. Методы поиска аномалий, основанные на кластеризации. Методы и системы на основе кластеризации и выбросов. Методы и системы на основе баз знаний и экспертные системы Применение технологий машинного обучения для решения задачи обнаружения вредоносных интернет-страниц.

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Содержание заданий по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность соответствует основным темам, включенным в программу вступительного испытания.

Пример билета

Билет №1

1. Основные термины и определения в области информационной безопасности.
2. Криптология. Понятия криптографии, криптоанализа, стеганографии. Основные термины и определения: шифрование, расшифрование, дешифрование. Симметричные

криптосистемы. Принципы работы и основные понятия. Пример реализации.

3. Чтение и перевод текста на иностранном языке.

Security and privacy concerns in cloud-based scientific and business workflows: A systematic review

Workflows are commonly used application models that consist of a series of computational tasks logically connected by data- and control-flow dependencies. There are two main types of workflows: The first type – scientific workflows, typically involve a large amount of data processing, analysis, and computing, requiring high computing and storage capacities. The second type of workflows is business workflows, applied predominantly in (business) information systems and enables process automation and improvement. Unlike scientific workflows, individual activities/tasks in business workflows usually require lower computing power and fewer storage resources, although the number of concurrently running workflow instances is typically large and the communication time between tasks needs to be kept as short as possible.

Cloud computing plays a key role in workflow management since it can deliver a large amount of computing resources ondemand for running data-intensive and compute-intensive applications. It also promises to reduce running costs and maximize revenues while maintaining or even improving the Quality of Service (QoS). Making use of cloud computing by Workflow Management Systems (WfMSs) can further increase the productivity of the system. Seen from the point of view of cloud computing users, cloud workflows provide an abstract definition of complex distributed applications, flexible configuration, and automated scalable operation, and also improve the QoS of the workflow execution environments (i.e. the WfMS) and hence the processes themselves.

Despite all the above-mentioned advantages of cloud-based workflows, cloud security is a major area of concern that is restricting their use for certain applications, especially for the workflows dealing with sensitive data and tasks. In fact, when a workflow or part of it is outsourced to the cloud, the WfMS loses control over tasks that can lead to increased security risks and make them vulnerable to malicious attacks. The security challenges associated with cloud computing arise primarily from two factors. Firstly, the nature of cloud infrastructure means that computing and storage resources are shared with other users, and sensitive data

is transferred among cloud components, such as Data Centers (DCs), over potentially untrusted network channels. Secondly, the distributed nature of workflows means that they can dynamically bind to cloud services during execution for various reasons, while these services may experience security issues that were not known at the time of binding. In addition, the cloud is honest-but-curious in the sense that the cloud service provider may faithfully follow the established protocols but at the same time, it may be curious to deduce valuable information about the users' data and the workflow logic. Since the deduced information may be leaked or even sold to third parties by malicious cloud providers, some users are reluctant to use the cloud (deployment model).

To understand the currently available approaches towards addressing workflow security concerns, in particular in Cloud-based environments, and identify the gaps in the body of available knowledge, two main goals should be achieved:

(1) To establish the current state of the art in addressing and maintaining security properties of cloud-based workflows throughout their complete life cycle, including a special focus on an additional life cycle phase accounting for runtime adaptation.

(2) To identify the gaps in the state of the art and subsequently the needs for future research.

Nafiseh Soveizi, Fatih Turkmen, Dimka Karastoyanova

Future Generation Computer Systems

Vol. 148, 2023, pp. 184-200

СПИСОК ЛИТЕРАТУРЫ

Основная литература.

1. Бессмертный И.А. Искусственный интеллект: Учебное пособие. - СПб: СПбГУ ИТМО, 2010. - 132 с.

2. Большаков А.А., Каримов Р.Н. Методы обработки многомерных данных и временных рядов. Серия: Специальность. Для высших учебных заведений. Издательство: Горячая Линия - Телеком, 2007 г

3. Буч Г., Максимчук Р., Энгл М., Янг Б., Коналлен Дж., Хьюстон К. Объектно ориентированный анализ и проектирование с примерами приложений. Вильямс, 2010 г.

4. Гагарина Л.Г., Киселев Д.В., Федотова Е.Л. Разработка и эксплуатация автоматизированных информационных систем. – М.: ИД «ФОРУМ»-ИНФРА-М, 2009. – 383с.

5. Гордеев А.В. Операционные системы : учебник для вузов / А. В. Гордеев. - 2-е изд. - СПб. : Питер, 2009. - 416 с. 12. Чио К., Фримэн 6.Д. Машинное обучение и безопасность / пер. с анг. А. В. Снастина. – М.: ДМК ..Пресс, 2020. – 388 с.: ил.

6. Дейтел П.Дж., Дейтел Х.М., Чофнес Д.Р. Операционные системы. Распределенные системы, сети, безопасность 2011 г., 704 с

7. Древс Ю.Г. Системы реального времени: технические и программные средства: Учебное пособие. М.: МИФИ, 2010. 320 с.

8. Илюшечкин В.М. Основы использования и проектирования баз данных. -М.: Юрайт, 2010. -214 с.

9. Шелухин О. И., Ерохин С.Д., Полковников МВ. Технологии машинного обучения в сетевой безопасности. / Под ред. О. И. Шелухина. – М.: Горячая линия – Телеком, 2021. – 360 с.

10. Шелухин О. И., Осин А.В. Безопасность сетевых приложений./ Под ред. О. И. Шелухина. – М.: Горячая линия – Телеком, 2021. – 224с

11. Шелухин О. И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. – М.: Горячая линия –Телеком, 2019. – 448 с.

Дополнительная литература.

1. Ясницкий Л.Н. Интеллектуальные системы. – М.: Лаборатория знаний, 2016. –243с.

2. Тишина, Н. А. Прикладные задачи безопасности информационно-телекоммуникационных систем [Электронный ресурс]: учебное пособие / Н. А. Тишина, Е. Н. Чернопрудова. — Электрон. текстовые данные. — Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2017. — 122 с. — 978-5-7410-1892-7. — Режим доступа: http://www.iprbookshop.ru/78818.html - ЭБС «IPRbooks»,

3. Олифер В.Г., Олифер Н.А. «Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов» 4-е изд. - СПб.: Питер, 2010. – 944 с.

4. Олифер В.Г., Олифер Н.А. «Сетевые операционные системы» – СПб.: Питер, 2009. – 672 с.

5. Редько В. Эволюция, нейронные сети, интеллект. Модели и концепция эволюционной кибернетики. М.: УРСС 2013.

6. Ясницкий Л.Н. Введение в искусственный интеллект: Учебное пособие для вузов Изд. 2-е, испр. – М.: Академия, 2008 г. – 176 с. 32. Малюк А.А. [и др.] Введение в информационную безопасность. – М.: «Горячая линия – Телеком», 2011. – 290 с.

7. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с. 10.

8. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с

9. Алферов А.П. Основы криптографии. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Учебное пособие. – Москва : Гелиос АРВ, 2005. – 480 с. 21. Мао В. Современная криптография: теория и практика.– Москва: Издательский дом Вильямс, 2005. – 768 стр.

10. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.

11. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ Петербург, 2009.-564 с