МЧС РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ
ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ

Программа вступительного экзамена по специальной дисциплине в адъюнктуру (аспирантуру) по направлению подготовки 10.07.01 (10.06.01) – Информационная безопасность направленность (профиль) «Методы и системы защиты информации, информационная безопасность» (очная и заочная формы обучения)

Санкт-Петербург– 2020

Содержание:

1. Цель и основные задачи экзамена

Экзамен, как форма вступительных испытаний, предназначен для выявления и отбора наиболее подготовленных кандидатов на обучение в адъюнктуре (аспирантуре) по очной и заочной форме обучения по направлению 10.07.01 (10.06.01) – «Информационная безопасность», направленность «Методы и системы защиты информации, информационная безопасность».

Цель вступительных испытаний – определить готовность и возможность лица, поступающего в адъюнктуру (аспирантуру) освоить выбранную программу адъюнктуры (аспирантуры), определить у поступающих базовый уровень подготовки в предметной области.

Основные задачи вступительных испытаний:

- проверить уровень знаний претендента;
- определить склонность к научно-исследовательской деятельности;
- выяснить мотивы поступления в адъюнктуру (аспирантуру);
- определить область научных интересов;
- определить уровень научной эрудиции претендента.

2. Основные требования к ответам экзаменующихся

В ходе вступительных испытаний поступающий должен показать:

- знание теоретических основ дисциплин направления;
- владение специальной профессиональной терминологией и лексикой;
- умение оперировать ссылками на соответствующие положения в учебной и научной литературе;
- владение культурой мышления, способностью в письменной и устной форме правильно формулировать результаты мыслительной деятельности;
- умение поставить цель и сформулировать задачи, связанные с реализацией профессиональных функций.

3. Критерии оценки знаний, умений, навыков

Экзамены как форма вступительных испытаний предназначена для выявления и отбора наиболее подготовленных кандидатов на обучение в адъюнктуре (аспирантуре) по очной и заочной форме обучения по направлению 10.07.01 (10.06.01) – «Информационная безопасность» , направленность «Методы и системы защиты информации, информационная безопасность».

Вопросы к экзамену распределены по билетам. Билет состоит из трех вопросов.

Знания обучающихся оцениваются по пятибалльной системе с выставлением обучающимся итоговой оценки *«отлично»*, либо *«хорошо»*, либо *«удовлетворительно»*, либо *«неудовлетворительно»*.

Оценка ***«отлично»*** при приеме экзамена выставляется в случае:

− полного, правильного и уверенного изложения учебного материала по каждому из вопросов билета;

− самостоятельной подготовки к ответу в установленные для этого сроки, исключающей использование нормативных источников, основной и дополнительной литературы и иного вспомогательного материала, кроме случаев специального указания или разрешения преподавателя;

− логически последовательного, взаимосвязанного и правильно структурированного изложения материала, умения устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;

− приведения надлежащей аргументации, наличия логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;

− лаконичного и правильного ответа на дополнительные вопросы преподавателя.

Оценка ***«хорошо»*** при приеме экзамена выставляется в случае:

− недостаточной полноты изложения материала по отдельным (одному или двум) вопросам билета при условии полного, правильного и уверенного изложения материала по как минимум одному вопросу билета;

− допущения незначительных ошибок и неточностей при изложении материала по отдельным (одному или двум) вопросам билета;

− самостоятельной подготовки к ответу в установленные для этого сроки, исключающей использование нормативных источников, основной и дополнительной литературы и иного вспомогательного материала, кроме случаев специального указания или разрешения преподавателя;

− нарушения логической последовательности, взаимосвязи и структуры изложения учебного материала по отдельным вопросам билета, недостаточного умения устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;

− приведения слабой аргументации, наличия у обучающегося недостаточно логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов материала по вопросам билета;

− допущения незначительных ошибок и неточностей при ответе на дополнительные вопросы преподавателя.

Любой из указанных недостатков может служить основанием для выставления обучающемуся оценки *«хорошо»*.

Оценка ***«удовлетворительно»*** при приеме экзамена выставляется в случае:

− невозможности изложения учебного материала по одному, любому из вопросов билета при условии полного, правильного и уверенного изложения материала по как минимум одному из вопросов билета;

− допущения существенных ошибок при изложении материала по отдельным (одному или двум) вопросам билета;

− самостоятельной подготовки к ответу в установленные для этого сроки, исключающей использование нормативных источников, основной и дополнительной литературы и иного вспомогательного материала, кроме случаев специального указания или разрешения преподавателя;

− существенного нарушения или отсутствия логической последовательности, взаимосвязи и структуры изложения учебного материала, неумения устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;

− отсутствия аргументации, логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов материала по вопросам билета;

− невозможности дать ответы на дополнительные вопросы преподавателя.

Любой из указанных недостатков может служить основанием для выставления обучающемуся оценки *«удовлетворительно»*.

Оценка ***«неудовлетворительно»*** при приеме экзамена выставляется в случае:

− отказа от ответа по билету с указанием, либо без указания причин;

− невозможности изложения учебного материала по двум или всем вопросам билета;

− допущения существенных ошибок при изложении учебного материала по двум или всем вопросам билета;

− скрытного или явного использования при подготовке к ответу нормативных источников, основной и дополнительной литературы, конспектов лекций и иного вспомогательного материала, кроме случаев специального указания или разрешения преподавателя;

− невозможности дать ответы на дополнительные вопросы преподавателя.

Любой из указанных недостатков может служить основанием для выставления обучающемуся оценки *«неудовлетворительно».*

Кандидат на поступление имеет право отказаться от ответа по выбранному билету с указанием, либо без указания причин и взять другой билет. При этом с учетом приведенных выше критериев оценка должна быть выставлена на один балл ниже заслуживаемой им.

Дополнительные вопросы могут быть заданы в случае:

− необходимости конкретизации и изложенной информации по вопросам билета с целью проверки глубины знаний отвечающего по связанным между собой темам и проблемам;

− необходимости проверки знаний по основным темам и проблемам при недостаточной полноте его ответа по вопросам билета.

Во время проведения вступительных испытаний участникам указанных мероприятий и лицам, привлекаемым к их проведению, запрещается иметь при себе и использовать средства связи и электронно-вычислительной техники (в том числе калькуляторы), за исключением случаев, установленных нормативными правовыми актами Российской Федерации.

4. Перечень вопросов к экзамену

1) Общие положения по безопасности информационных систем.
2) Законодательная и нормативная база информационной безопасности.
3) Организационные мероприятия по защите информации.
4) Руководящие документы в области защиты информации.
5) Административные меры по защите информации в организациях.
6) Категорирование и аттестация объектов информационных систем.
7) Уязвимости информационных систем.
8) Классификация и модели компьютерных атак.
9) Этапы компьютерных атак.
10) Неформальная модель нарушителя компьютерной безопасности.
11) Основные понятия и определения в области безопасности информации.
12) Уголовная ответственность за компьютерные преступления
13) Защита элементов информационных систем патентами.
14) Компьютерные программы и базы данных как объекты защиты авторского права.
15) Сущность и история развития криптографии. Классификация методов шифрования. Стойкость шифров. Понятие о хэш-функции.
16) Общие схемы блочного и поточного шифрования.
17) Стандарты симметричного шифрования.
18) Основы криптоанализа.
19) Работа с программами криптографического закрытия информации.
20) Сущность и задачи асимметричного шифрования.
21) Алгоритмы асимметричного шифрования.
22) Основы электронной цифровой подписи.
23) Освоение программных средств электронной цифровой подписи.
24) Реализация криптографических методов защиты информации.
25) Управление ключами.
26) Шифрование потоков данных и сообщений большого объема.

27) Использование «блуждающих ключей».
28) Шифрование, помехоустойчивое кодирование и сжатие информации.
29) Защита информации средствами операционных систем.
30) Аппаратные средства защиты информации в персональном компьютере.
31) Программная защита информации в персональном компьютере.
32) Основы компьютерной стеганографии.
33) Понятие о квантовой криптографии.
34) Защита информации от копирования и несанкционированного использования.
35) Методы и средства построения отказоустойчивых компьютерных систем. RAID-технологии.
36) Организация резервного копирования информации.
37) Источники утечки информации по каналам ПЭМИН.
38) Средства и методы защиты информации от утечки по каналам ПЭМИН.
39) Обнаружение атак на локальные сети.
40) Экранирование локальных сетей.
41) Контроль доступа к информации в локальных сетях.
42) Организация виртуальных сетей (технология VPN).
43) Способы создания демилитаризованной зоны.
44) Технология туннелирования.
45) Методы и средства построения виртуальных сетей.
46) Обеспечение безопасности почтовой переписки.
47) Защита публикуемой в сети Internet информации.
48) Защита от вредоносных программ.
49) Специфика защиты информации в базах данных.
50) Задачи протоколов сетевой безопасности.
51) Анализ основных протоколов сетевой безопасности.
52) Сущность и задачи технологии виртуальных локальных сетей

(VLAN).

53) Средства построения VLAN.

54) Экранирование локальных сетей.

55) Способы создания демилитаризованной зоны.

56) Методы и средства построения виртуальных сетей.

57) Математическая модель базы данных с адаптивной структурой.

58) Характеристика типовой СУБД для построения локальных баз данных.

59) Основы исчисления предикатов.

60) Общая схема проектирования базы данных.

61) Языки запросов.

62) Многомерно-реляционная модель.

5. Рекомендуемая литература:

Основная:

1. Информационная безопасность и защита информации: учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 3-е изд., стер. - М. : ACADEMIA, 2008. - 336 с. : рис., схемы. - (Высшее профессиональное образование).
2. Безопасность информационных систем и защита информации в МЧС России: учебное пособие: [гриф МЧС] / Ю.И. Синещук [и др.]; ред. В.С. Артамонов; С.-Петерб. гос. ун-т гос. противопож. службы МЧС России. – СПб.: СПбУ ГПС МЧС России, 2012. – 300 с.
3. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов / П. Б. Хорев. - 3-е изд., стер. - М.: "Академия", 2007. - 256 с. : рис., табл. - (Высшее профессиональное образование).
4. Введение в защиту информации в автоматизированных системах: учебное пособие для вузов / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - 2-е изд. - М.: Горячая линия - Телеком, 2004. - 147 с., ил.

Дополнительная:

1. Чмора А.Л. Современная прикладная криптография.- М.: Гелиос АРВ, 2001.
2. Федеральный Закон от 21 июля 1993 г. № 5485-1 «О Государственной тайне».
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5. Федеральный Закон от 07 июля 2003 г. № 126-ФЗ «О связи».
6. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
7. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Основные технические требования».

Рассмотрена на заседании кафедры прикладной математики и информационных технологий протокол № _____ от «____»_____20___ г.

Заведующий кафедры прикладной математики и
информационных технологий А.В. Матвеев