УТВЕРЖДАЮ
Проректор по научной работе
_____ И.В. Бычков
«28» 01 2022 г.

ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ

Группа научных специальностей – 2.3. Информационные технологии и телекоммуникации

Научная специальность – 2.3.6. Методы и системы защиты информации, информационная безопасность

Подготовка кадров высшей квалификации

Челябинск, 2022

Программа кандидатского экзамена по специальной дисциплине разработана кафедрой компьютерной безопасности и прикладной алгебры на основе паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Разработчик программы:

Зав. кафедрой компьютерной безопасности
и прикладной алгебры,
кандидат физико-математических наук, доцент А.Н. Ручай

Программа одобрена на заседании кафедры компьютерной безопасности и прикладной алгебры от «15» 01 2022 г., протокол № 6.

Зав. кафедрой компьютерной безопасности
и прикладной алгебры _____А.Н. Ручай

Программа принята на заседании Ученого совета математического факультета от «27» 01 2022 г., протокол № 5.

Согласовано:

Декан математического факультета _____Е.А. Сбродова

Зав. отделом аспирантуры
и докторантуры _____Н.В. Бочкарева

1. Общие положения

Кандидатские экзамены являются основной частью аттестации научных и научно-педагогических кадров. Цель экзамена – установить глубину профессиональных знаний прикрепленного лица, уровень подготовленности к самостоятельной научно-исследовательской работе.

От лица, сдающего экзамен, требуется четко, емко и кратко изложить теоретический материал, владеть соответствующей терминологией и проявить это в ответах.

Также необходимо представить реферат, в котором должны быть освещены проблемные аспекты темы иследования, даны ссылки на работы известных специалистов, свой взгляд на проблему и возможные пути ее решения. Изложение проблемы в реферате рекомендуется связать с темой диссертационного исследования.

При подготовке к кандидатскому экзамену и его сдаче в исключительных случаях (форс-мажор и т.п.) могут применяться электронное обучение, дистанционные образовательные технологии.

2. Процедура кандидатского экзамена

Экзамен по специальной дисциплине проводится по билетам, каждый из которых содержит 3 вопроса. Кроме того, на экзамене должны быть заданы дополнительные вопросы, как правило, два. Экзамен подразумевает также собеседование по содержанию полностью или частично подготовленного кандидатского исследования.

За экзамен выставляется единая оценка.

3. Содержание разделов кандидатского экзамена

3.1. Методы и системы защиты информации

Законодательные и правовые основы защиты компьютерной информации информационных технологий. Безопасность информационных ресурсов и документирование информации; государственные информационные ресурсы; персональные данные о гражданах; права на доступ к информации; разработка и производство информационных систем; вычислительные сети и защита информации; нормативно-правовая база функционирования систем защиты информации; компьютерные

преступления и особенности их расследования; российское законодательство по защите информационных технологий; промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

Проблемы защиты информации в информационных системах. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах; основные задачи обеспечения безопасности информации в информационных системах; защита локальных сетей и операционных систем; интеграция систем защиты; Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.

Содержание системы средств защиты компьютерной информации в информационных системах. Защищенная информационная система и система защиты информации; принципы построения систем защиты информации и их основы; законодательная, нормативно-методическая и научная база системы защиты информации.

Требования к содержанию нормативно-методических документов по защите информации; научно-методологический базис, стратегическая направленность и инструментальный базис защиты информации; структура и задачи (типовой перечень) органов, выполняющих защиту информации.

Организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры; политика безопасности: организация секретного делопроизводства и мероприятий по защите информации; программно-технические методы и средства защиты информации; программно-аппаратные методы и средства ограничения доступа к компонентам компьютера; типы несанкционированного доступа и условия работы средств защиты; вариант защиты от локального несанкционированного доступа и от удаленного ИСД.

Средства защиты, управляемые модемом, надежность средств защиты.

3.2. Информационная безопасность

Изучение традиционных симметричных криптосистем. Основные понятия и определения; шифры перестановки; шифр перестановки «скитала»; шифрующие таблицы; применение магических квадратов; шифры простой замены; полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом

Вернама; роторные машины; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

Применение симметричных криптосистем для защиты компьютерной информации в информационных системах. Изучение американского стандарта шифрования данных DES; основные режимы работы алгоритма DES; отечественный стандарт шифрования данных; режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки; блочные и поточные шифры.

Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах. Концепция криптосистемы с открытым ключом; однонаправленные функции; криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе); безопасность и быстродействие криптосистемы RSA; схема шифрования Полига—Хеллмана; схема шифрования эль-Гамаля, комбинированный метод шифрования.

Методы идентификации и проверки подлинности пользователей компьютерных систем. Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных и электронная цифровая подпись; однонаправленные хэш-функции; алгоритм безопасного дешифрования SHA; однонаправленные хэш-функции на основе симметричных блочных алгоритмов; отечественный стандарт хэш-функции; алгоритм цифровой подписи RSA; алгоритм цифровой подписи эль-Гамаля (EGSA); алгоритм цифровой подписи DSA; отечественный стандарт цифровой подписи.

Защита компьютерных систем от удаленных атак через сеть Internet

Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН. Основные элементы средств защиты сети от несанкционированного доступа; устройства криптографической защиты

данных; контроллер смарт-карт SCAT-200; программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО; защита от НСД со стороны сети; абонентское шифрование и ЭЦП; шифрование пакетов; аутентификация; защита компонентов ЛВС от НСД; защита абонентского пункта, маршрутизаторов и устройств контроля; технология работы с ключами.

Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; компьютерные вирусы как особый класс разрушающих программных воздействий; защита от РПВ; понятие изолированной программной среды.

Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. Возможности СИИТ для обеспечения комплексной защиты программ в момент их выполнения и данных при их обработке в компьютере; метод верификации программного обеспечения для контроля корректности, реализуемости и защиты от закладок.

Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.

Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах; основные направления создания защищенных компьютерных систем нового поколения на основе СИИТ.

3.3. Примерный перечень вопросов кандидатского экзамена

1. Понятие нарушителя. Исходные предположения о возможностях нарушителя. Цели информационной безопасности.
2. Законы Российской Федерации, составляющие основу информации в стране.
3. Особенности российского законодательства в части защиты государственной тайны, коммерческой тайны и авторских прав.

4. Порядок лицензирования и сертификации деятельности в области защиты информации.
5. Математические модели формальной теории защиты информации.
6. Угрозы информации и политика безопасности.
7. Классификация систем защиты.
8. Международные и отечественные стандарты в области защиты информации.
9. Криптографические стандарты Российской Федерации, стандартизации.
10. Понятия теоретической, практической и временной стойкость. Методы получения оценок стойкости.
11. Понятие надежности. Методология обоснования надежности криптографической защиты.
12. Автоматное определение шифра. Криптографические параметры узлов и блоков шифрующих автоматов.
13. Методы получения псевдослучайных последовательностей.
14. Генераторы псевдослучайных последовательностей и их свойства.
15. Блочные и поточные шифры.
16. Режимы использования блочных шифров.
17. Алгоритмы выработки имитовставки. Методы оценки имитозащищенности.
18. Режимы аутентифицированного шифрования. Современные стандартизированные решения.
19. Ключевые системы, методы распределения ключей.
20. Методы выработки производных ключей, принципы оценки качества производной ключевой информации.
21. Асимметричные криптографические схемы.
22. Гибридные схемы шифрования. Практические примеры реализации гибридных схем.
23. Электронная подпись, инфраструктура открытых ключей. Удостоверяющие центры. Методы обеспечения подлинности физических лиц.
24. Атаки на криптографические алгоритмы: алгоритмические, статистические.
25. Свойства безопасности криптографических протоколов.
26. Методы и средства обеспечения заданных свойств безопасности криптографических протоколов.
27. Протоколы выработки общего ключа.

28. Протоколы распределения ключей.
29. Протоколы с разделением секрета.
30. Протоколы с подписью в слепую и протоколы электронного голосования.
31. Протоколы семейства TLS, область их применения, методы оценки безопасности.
32. Протокол SSH, область его применения, реализуемые методы аутентифицированного удаленного доступа.
33. Протокол SESPAKE выработки общего ключа на основе пароля, область его применения, принципы обоснования сложности перебора паролей.
34. Протокол защищенного взаимодействия SP-FIOT. Обоснование свойств безопасности, отличия от других протоколов.
35. Криптографические механизмы протокола IPSec. Обеспечиваемые безопасности.
36. Принципы организации виртуальных частных сетей (VPN). Обеспечиваемые свойства безопасности. Программные средства реализации VPN.
37. Анонимизирующие сети. Принципы их построения, обеспечиваемые безопасности. Криптографические механизмы, используемые в анонимизитрующих сетях.
38. Методы разграничения доступа.
39. Программные и аппаратные средства разграничения доступа.
40. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
41. Методы и средства хранения ключевой информации.
42. Средства обеспечения безопасности в ОС семейств Windows и UNIX, критерии защищенности ОС.
43. Средства обеспечения безопасности в сетях.
44. Принципы и протоколы аутентификации при удаленном доступе. Отличия от криптографических протоколов.
45. Средства защиты серверов и рабочих станций.
46. Средства защиты локальных сетей при подключении к Internet.
47. Межсетевые экраны, электронные замки, криптофильтры, крипторoутеры.
48. Области применения, достоинства, недостатки, реализуемые политики безопасности.
49. Методы оценки качества применяемых средств защиты.

50. Методы и средства защиты информации в СУБД.
51. Средства идентификации и аутентификации, управление доступом, средства контроля, аудит безопасности.
52. Критерии защищенности БД и АИС.
53. Методы и системы обнаружения компьютерных атак.
54. Основные физические каналы утечки информации информационной системы.
55. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки.
56. Примеры современных атак на средства защиты информации, основанные на изучении побочных сигналов.
57. Технические параметры современных средств перехвата побочных сигналов.
58. Математические модели побочных каналов утечки.
59. Выделение полезных сигналов на фоне помех.
60. Методы и средства защиты от инженерно-технической разведки.
61. Алгоритмические средства защиты ключевой и криптографически опасной информации от утечек по побочным каналам информации.
62. Методика оценки качества инженерно-технической защиты.
63. Определение компьютерного вируса. Классификация компьютерных вирусов.
64. Методы выявления и защиты от вирусов.
65. Определение понятия изолированной программной среды. Примеры.
66. Методы защиты от изменения, контроль целостности.
67. Криптографический контроль целостности программных средств при их распространении и эксплуатации.
68. Методы защиты от изучения программных средств.
69. Методы восстановления алгоритмов защиты в программных продуктах.
70. Метод черного ящика при исследовании программных реализаций средств защиты информации.
71. Метод оценки уровня криптографической защиты типовых программных продуктов.
72. Анализ особенностей выработки и распределения ключей.
73. Анализ возможности и способы внедрения криптографических закладок.
74. Методы удаленного исследования компьютеров и средств защиты информации.

75. Проведение экспресс-анализа защищенности сетевого компьютера.
76. Сетевые атаки. Классификация атак.
77. Методы и технические средства защиты от сетевых атак.
78. Принципы реализации средств криптографической защиты информации.
79. Требования к ключевой системе средств защиты информации.
80. Требования к криптографическим и инженерно-криптографическим методам защиты, реализуемым в средствах защиты информации.
81. Механизмы документирования исходных текстов программ.
82. Методы анализа исходных текстов с целью поиска уязвимостей.
83. Инструментальные средства для проведения статистического и динамического анализа исходных текстов.
84. Методы и инструментальные средства тестирования программного обеспечения.

4. Требования к результатам освоения специальной дисциплины

В результате освоения соискатель должен:

знать: основные методы и системы защиты информации, информационной безопасности; методические основы обучения математики и информатики; основы нормативно-правового обеспечения образовательного процесса и защиты авторского права на учебные ресурсы; средства поддержки преподавателя при использовании современных педагогических технологий и виртуальных обучающих сред; основы концепции непрерывного образования;

уметь: обосновывать выбор методов защиты информации при ее передаче и хранении; выявлять попытки несанкционированного доступа в информационные системы, обнаружения вредоносных программ, разрабатывать технические задания, проектировать подсистемы с учетом действующих нормативных и методических документов; разрабатывать учебно-методические материалы на основе модульного принципа; искать и применять в учебном процессе дидактически обоснованные образовательные ресурсы; применять разнообразные формы контроля учебного процесса;

владеть: навыками применения существующих защищенных протоколов обмена информацией; современными методами и средствами защиты информации при ее передаче и хранении; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками

использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; умениями организации и проведения образовательного процесса при обучении обучающихся с использованием современных информационных технологий.

5. Критерии оценки результатов кандидатского экзамена

5.1.Критерии оценивания результатов устного ответа

Оценка **«Отлично»** ставится при соблюдении следующих условий:

- грамотное и правильное использование в ответах научной терминологии;
- безошибочное владение категориальным аппаратом;
- умение правильно сформулировать и доказать основные теоремы, соответствующие содержащимся в билетах вопросам;
- владение методами решения задач, соответствующих теоретической части вопросов;
- логичность, связность ответа, умение анализировать, сравнивать и делать умозаключения по предложенному материалу;
- уверенное владение предметным содержанием и профессиональной терминологией, демонстрирование уверенных знаний трудов ведущих ученых по специальности.

Оценка **«Хорошо»** ставится при соблюдении следующих условий:

- грамотное и правильное использование в ответах научной терминологии;
- владение категориальным аппаратом в целом, но допустимость незначительных ошибок;
- умение анализировать и делать умозаключения по предложенному материалу;
- отдельные ошибки при формулировке и доказательстве основных теорем, соответствующих содержащимся в билетах вопросам;
- владение основными методами решения задач, соответствующих теоретической части вопросов;
- логичность, связность ответа.

Оценка «**Удовлетворительно»** ставится, если аспирант:

- недостаточно владеет категориальным аппаратом; лишь отчасти знаком с трудами ведущих ученых по специальности

- допускает ошибки при формулировке и доказательстве основных теорем, соответствующих содержащимся в билетах вопросам;
- поверхностное владеет методами решения задач, соответствующих теоретической части вопросов;
- демонстрирует неполное владение предметным содержанием и профессиональной терминологией;
- опираясь на наводящие вопросы, может сравнивать, анализировать, делать умозаключения.

Оценка **«Неудовлетворительно»** ставится, если аспирант:

- неуверенно владеет предметным содержанием и профессиональной терминологией по дисциплине, не знаком с трудами ведущих ученых по специальности;
- не приводит в ответах необходимую научную терминологию;
- допускает грубые ошибки при формулировке и доказательстве основных теорем, соответствующих содержащимся в билетах вопросам;
- не умеет анализировать, сравнивать и делать умозаключения по предложенному материалу;
- нарушает логичность, связность ответа.

5.2.Критерии оценивания представленного реферата

Оценка **«Отлично»** за реферат ставится, если:

- содержание реферата точно соответствует теме, отсутствуют ошибки в изложении и оформлении реферата;
- материал освещен в проблемном аспекте при достаточном фактологическом изложении;
- ссылки на работы известных ученых и новейшую литературу отличаются полнотой;
- изложено свое видение проблемы и аргументация своей позиции с помощью фактов;
- содержание связано с темой диссертационного исследования.

Оценка **«Хорошо»** за реферат ставится, если:

- содержание реферата соответствует теме, допущены негрубые ошибки в изложении и оформлении реферата;
- обозначены основные проблемы изучения заявленного в теме вопроса при достаточном фактологическом изложении;
- даны ссылки на работы известных ученых и новейшую литературу;

- изложено свое видение проблемы и приведен ряд аргументов своей позиции с помощью фактов;
- содержание связано с темой диссертационного исследования.

Оценка **«Удовлетворительно»** за реферат ставится, если:

- содержание реферата соответствует теме, допущены ошибки в изложении и оформлении реферата;
- поверхностное фактологическое изложение;
- даны ссылки на ряд работ известных ученых и новейшую литературу;
- содержание связано с темой диссертационного исследования.

Оценка **«Неудовлетворительно»** за реферат ставится, если:

- содержание реферата не соответствует теме, допущены грубые ошибки в изложении и оформлении реферата;
- не изложено свое видение проблемы и не приведены аргументы своей позиции;
- содержание не связано с темой диссертационного исследования.

6. Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене.

При проведении процедуры оценивания результатов кандидатского экзамена инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства.

Процедура оценивания результатов кандидатского экзамена инвалидов и лиц с ограниченными возможностями здоровья по спецдисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

– в форме аудиофайла,
– в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,
– в форме аудиофайла.

При проведении процедуры оценивания результатов кандидатского экзамена инвалидов и лиц с ограниченными возможностями здоровья по спецдисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме на языке Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно на языке Брайля, с использованием услуг ассистента, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов кандидатского экзамена по спецдисциплине может проводиться в несколько этапов.

В исключительных случаях (форс-мажорные обстоятельства и др.) электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

7. Список рекомендуемой литературы

7.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Ресурс
1.	Щеглов А. Ю., Щеглов К. А.	Математические модели и методы формального проектирования систем защиты информационных систем (https://e.lanbook.com/books/element.php?pl1_id=70897)	Санкт-Петербург : НИУ ИТМО, 2015	ЭБС
2.	Каторин Ю. Ф., Разумовский А. В., Спивак А. И.	Техническая защита информации: Лабораторный практикум (http://e.lanbook.com/books/element.php?pl1_id=71124)	Санкт-Петербург : НИУ ИТМО, 2013	ЭБС
3.	Скрипник Д. А.	Общие вопросы технической защиты информации (https://biblioclub.ru/index.php?page=book&id=429070)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
4.		Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: практикум (https://biblioclub.ru/index.php?page=book&id=458012)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016	ЭБС
5.		Нестандартные методы защиты информации: лабораторный практикум: практикум (https://biblioclub.ru/index.php?page=book&id=458132)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016	ЭБС
6.	Рогозин В. Ю., Галушкин И. Б., Новиков В., Вепрев С. Б.	Основы информационной безопасности: учебник (https://biblioclub.ru/index.php?page=book&id=562348)	Москва : Юнити-Дана|Закон и право, 2018	ЭБС
7.	Гришина Н. В.	Основы информационной безопасности предприятия: учебное пособие (http://znanium.com/catalog/document?id=379717)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2021	ЭБС
8.	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: учебное пособие (http://znanium.com/catalog/document?id=364622)	Москва : Издательский Дом "ФОРУМ", 2021	ЭБС

7.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Ресурс
1.	Сомко А. С., Федорова Е. А.	Профессиональный иностранный язык для специалистов в области компьютерной безопасности (https://e.lanbook.com/book/91405)	Санкт- Петербург : НИУ ИТМО, 2016	ЭБС
2.	Кармановский Н. С., Михайличенко О. В., Прохожев Н. Н.	Организационно-правовое и методическое обеспечение информационной безопасности (https://e.lanbook.com/book/91449)	Санкт- Петербург : НИУ ИТМО, 2016	ЭБС
3.	Степанов-Егиянц В. Г.	Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография (https://biblioclub.ru/index.php?page=book&id=452481)	Москва : Статут, 2016	ЭБС
4.	Садыкова У. В.	Разработка информационной системы выявления потенциальных нарушителей информационной безопасности на основе психодиагностических методик: выпускная квалификационная работа (бакалаврская работа): студенческая научная работа (https://biblioclub.ru/index.php?page=book&id=463142)	Астрахань : [б. и.], 2017	ЭБС
5.	Пелешенко В. С., Говорова С. В., Лапина М. А.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие (https://biblioclub.ru/index.php?page=book&id=467139)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017	ЭБС
6.	Веселов Г.Е., Абрамов Е.С.	Менеджмент риска информационной безопасности: учебное пособие (http://znanium.com/catalog/document?id=330790)	Ростов-на-Дону : Издательство Южного федерального университета (ЮФУ), 2016	ЭБС
7.	Галатенко В. А., Бетелин В. Б.	Стандарты информационной безопасности: курс лекций (https://biblioclub.ru/index.php?page=book&id=233065)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006	ЭБС

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Лань [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Лань. – URL: http://e.lanbook.com/
2. Официальный интернет-портал правовой информации. Государственная система правовой информации http://pravo.gov.ru Раздел «Официальное опубликование правовых актов» в электронном виде» http://publication.pravo.gov.ru/
3. Министерство науки и высшего образования Российской Федерации (Минобрнауки России) - официальный сайт https://www.minobrnauki.gov.ru
4. Федеральный портал «Российское образование» http:// www.edu.ru
5. Единое окно доступа к образовательным ресурсам - федеральная информационная система открытого доступа к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для всех уровней образования: дошкольное, общее, среднее профессиональное, высшее, дополнительное.http://window.edu.ru
6. Высшая аттестационная комиссия (ВАК) - официальный сайт [см. Перечень рецензируемых научных изданий: http://vak.ed.gov.ru/87] http://vak.ed.gov.ru
7. Российский научный фонд (РНФ) - официальный сайт http://rscf .ru /ru
8. Научная электронная библиотека. Монографии, изданные в издательстве Российской Академии Естествознания полнотекстовый ресурс научных и учебных изданий РАЕ https://www.monographies.ru/
9. Научная педагогическая электронная библиотека (НПЭБ) - многофункциональная информационно-поисковая система Российской академии образования http://elib.gnpbu.ru
10. Университетская информационная система РОССИЯ (УИС РОССИЯ) - тематическая электронная библиотека и база данных для исследований и учебных курсов http://www.uisrussia.msu.ru
11. Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет - официальный сайт http://xn--h1ajgms.xn--p1ai
12. Электронные библиографические указатели - каталог Российской книжной палаты - филиала ИТАР ТАСС http://gbu.bookchamber.ru/index.html
13. ГОСТы (официальные тексты) в помощь оформлению курсовых, выпускных квалификационных работ, диссертационных исследований - коллекция ссылок на на ресурсы сайта Федерального агентства по техническому регулированию и метрологии (Росстандарт), размещённая на сайте филиала http://www.sgpi.ru/?n=2417
14. Научная электронная библиотека eLIBRARY.RU» - раздел "Журналы открытого доступа" (https://elibrary.ru/projects/subscription/rus_titles_free.asp) на 01.10.2018 г. содержит более 6000 научных журналов http://www.elibrary.ru
15. КиберЛенинка - научная электронная библиотека (журналы) http://cyberleninka.ru
16. Библиографические базы данных ИНИОН РАН [Электронный ресурс] : сайт. – URL: http://inion.ru/resources/bazy-dannykh-inion-ran/.

9. Лицензионное программное обеспечение

Вуз имеет необходимый комплект лицензионного программного обеспечения:

№ п/п	Наименование программного обеспечения	Тип лицензии и продукта
1.	Notepad++	Открытое лицензионное соглашение (General Public License)
2.	WinDjView	Открытое лицензионное соглашение (General Public License)
3.	Eclipse	Открытое лицензионное соглашение (Eclipse Public License)
4.	CodeBlocks	Открытое лицензионное соглашение (General Public License)
5.	Microsoft MPI	Открытое лицензионное соглашение (General Public License)
6.	Dev-C++	Открытое лицензионное соглашение (General Public License)
7.	Lazarus	Открытое лицензионное соглашение (General Public License)
8.	CUDA	Открытое лицензионное соглашение (General Public License)
9.	Far Manager	Открытое лицензионное соглашение (General Public License)
10.	PascalABC	Открытое лицензионное соглашение (General Public License)
11.	Bochs	Открытое лицензионное соглашение (Lesser General Public License)
12.	Java Development Kit	Открытое лицензионное соглашение (General Public License)
13.	Java Runtime Environment	Открытое лицензионное соглашение (General Public License)
14.	MiKTeX	Открытое лицензионное соглашение (General Public License)
15.	Ghostscript	Открытое лицензионное соглашение (General Public License)
16.	LibreOffice 6.2	Открытое лицензионное соглашение (Lesser General Public License)

17.	Microsoft Visual Studio 2008, 2013, 2015, 2017, 2019	MSDN Academic Alliance, Электронная лицензия для образовательного учреждения (Full License Education, TLP)
18.	Mozilla Firefox	Открытое лицензионное соглашение (Mozilla Public License)
19.	Google Chrome	Лицензионное соглашение с конечным пользователем
20.	Foxit Reader	Лицензионное соглашение с конечным пользователем
21.	doPDF 10	Лицензионное соглашение с конечным пользователем
22.	PyCharm	Открытое лицензионное соглашение (General Public License)
23.	Python 2.7, 3.7	Открытое лицензионное соглашение (General Public License)
24.	WinSCP	Открытое лицензионное соглашение (General Public License)
25.	Wireshark	Открытое лицензионное соглашение (General Public License)
26.	nmap	Открытое лицензионное соглашение (General Public License)
27.	VirtualBox	Открытое лицензионное соглашение (General Public License)
28.	Операционная система Windows 7	MSDN Academic Alliance, Электронная лицензия для образовательного учреждения (Full License Education, TLP)
29.	Kali Linux	Лицензионное соглашение с конечным пользователем
30.	Cisco Packet Tracer	Cisco Networking Academy, Электронная лицензия для образовательного учреждения
31.	PuTTY	Открытое лицензионное соглашение (MIT)
32.	Win10Pcap	Открытое лицензионное соглашение (General Public License)
33.	WinRAR	Лицензионное соглашение с конечным пользователем
34.	7-Zip	Открытое лицензионное соглашение

		(Lesser General Public License)
35.	MinGW	Открытое лицензионное соглашение (General Public License)
36.	AIMP	Открытое лицензионное соглашение (Lesser General Public License)
37.	CCleaner	Лицензионное соглашение с конечным пользователем
38.	CPUID	Лицензионное соглашение с конечным пользователем
39.	ActivePerl	Лицензионное соглашение с конечным пользователем
40.	FASM	Открытое лицензионное соглашение
41.	JWasm	Лицензионное соглашение с конечным пользователем
42.	VMware Workstation Player	Лицензионное соглашение с конечным пользователем
43.	QEMU	Открытое лицензионное соглашение (General Public License)
44.	OllyDbg	Лицензионное соглашение с конечным пользователем
45.	Immunity Debugger	Лицензионное соглашение с конечным пользователем
46.	IDA free	Лицензионное соглашение с конечным пользователем
47.	Metasploit Framework	Лицензионное соглашение с конечным пользователем

Форма билета кандидатского экзамена

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)

Наименование факультета
Наименование кафедры

Группа научных специальностей – шифр и наименование
Научная специальность – шифр и наименование

Кандидатский экзамен по специальной дисциплине

Экзаменационный билет №____

1.
2.
3.

Зав. кафедрой Ф.И.О.