**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Астраханский государственный университет имени В.Н. Татищева»**

**(Астраханский государственный университет им. В.Н. Татищева)**

**РАЗРАБОТАНА УТВЕРЖДЕНО**

Кафедрой информационной Ученым советом Университета

безопасности

(заседание кафедры от от «\_\_\_» \_\_\_\_\_\_\_ 202\_\_ г., протокол № \_

«25» января 2024 г., протокол № 2)

**ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА**

**ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ**

в соответствии с темой диссертации на соискание ученой степени кандидата наук

*Направление подготовки*

**Информационные технологии и телекоммуникации**

*Профиль подготовки*

**2. 3. 6 Методы и системы защиты информации, информационная безопасность**

Астрахань – 2024 г.

Программа кандидатского экзамена и список основной и дополнительной литературы обновлен с учетом развития науки, культуры, экономики, техники, технологий и социальной сферы.

Форма контроля: кандидатский экзамен

Трудоемкость в ЗЕ – в соответствии с учебным планом.

Программу разработали:

Ажмухамедов И.М., профессор, д.т.н., профессор кафедры информационной безопасности, руководитель аспирантуры;

Демина Р.Ю., к.т.н., доцент кафедры информационной безопасности;

Ханова А.А., профессор, д.т.н., профессор кафедры информационных технологий.

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Кандидатский экзамен является составной частью аттестации научных и научно-педагогических кадров. Цель экзамена – установить глубину профессиональных знаний аспиранта (соискателя) ученой степени, уровень его подготовленности к самостоятельной научно-исследовательской работе.

Сдача кандидатского экзамена обязательна для присуждения ученой степени кандидата технических наук и проводится до представления диссертационной работы в совет по защите диссертации.

Кандидатский экзамен по специальности сдается по программе, состоящей из двух частей:

1. основной программы – минимум по специальности, утвержденной ВАК Минобрнауки РФ от 08.10.2007 г. № 274;
2. дополнительной (индивидуальной) программы аспиранта (соискателя).

Структура кандидатского экзамена по специальности предполагает проверку знаний по экзаменационному билету и собеседование по индивидуальной программе аспиранта

(соискателя).

Экзаменационный билет содержит 3 вопроса по представленным в программе разделам в соответствии с типовой программой. Время подготовки устного ответа аспиранта (соискателя) – 45-60 минут.

Собеседование по индивидуальной программе проводится по теме выполняемого диссертационного исследования аспиранта (соискателя). Цель собеседования – проверка у аспиранта (соискателя) теоретических знаний по теме диссертационного исследования, практических навыков применения методов и ряда специальных методик в ходе конкретного технического исследования.

**ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ**

|  |  |
| --- | --- |
| **Балл** | **Критерии оценивания** |
| 5  (отлично) | Ответ полный, без замечаний, хорошо структурированный, продемонстрировано хорошее знание теоретических под ходов к анализу и решению рассматриваемой проблемы, про иллюстрировано примерами, даны аргументированные, полные и логичные ответы на вопросы членов комиссии, проявлено творческое отношение к предмету. |
| 4  (хорошо) | Ответ полный с незначительными замечаниями, недостаточно структурирован, продемонстрировано знание основных теоретических подходов к анализу и решению рассматриваемо й проблемы, про иллюстрировано примерами, ответы на вопросы членов комиссии даны с незначительными замечаниями. |
| 3  (удовлетворительно) | В ответе есть упущения, ответ недостаточно структурирован, знание основных теоретических под ходов к анализу и решению рассматриваемой проблемы продемонстрировано с упущениями, есть затруднения при практическом применении теории, есть затруднения при ответе на вопросы комиссии. |
| 2  (неудовлетворительно) | В ответе есть значительные упущения и не точности, многие основные положения теоретических подходов к анализу и решению рассматриваемой проблемы не представлены или в их выводе допущены ошибки, ответ не структурирован, ответы на вопросы комиссии отсутствуют. |

**СОДЕРЖАНИЕ**

**Основная программа**

В основу настоящей программы положены следующие дисциплины: «Основы информационной безопасности», «Технические средства и методы защиты информации», «Криптографические методы защиты информации», «Программно-аппаратные средства обеспечения информационной безопасности».

*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.

*2 . Информационная безопасность*

Изучение традиционных симметричных криптосистем.

Основные понятия и определения; шифры перестановки; шифры замены; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.

Американский стандарта шифрования данных AES; отечественные стандарты шифрования данных; режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки; блочные и поточные шифры.

Применение ассиметричных 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 Эль-Гамаля.

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; однонаправленные хэш-функции на основе симметричных блочных алгоритмов; отечественный стандарт хэш-функции; алгоритм цифровой подписи RSA; алгоритм цифровой подписи Эль Гамаля (EGSA); 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.

Методы защита 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; 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.

**Дополнительная программа**

В дополнительной (индивидуальной) программе должны быть отражены последние достижения в области науки, в рамках которой проведено диссертационное исследование, использована новейшая научная отечественная и зарубежная литература, интернет-издания, а также справочно-информационные издания по соответствующей тематике.

Индивидуальная программа разрабатывается научным руководителем аспиранта (соискателя) на основании диссертационного исследования аспиранта (соискателя) и должна быть предоставлена на кафедру информационных технологий не позднее, чем за 2 недели до даты сдачи кандидатского экзамена по специальности в печатном и электронном виде.

Индивидуальная программа должна содержать:

1. Титульный лист с указанием автора(ов) программы, номера и даты протоколы утверждения индивидуальной программы аспиранта (соискателя) на заседании кафедры информационных технологий (приложение 1).
2. Перечень вопросов, раскрывающих содержание диссертации, используемые методы научного исследования и последние достижения в научной отрасли, в рамках которой проведено диссертационное исследование. В программе рекомендуется выделить не менее 2 разделов, в каждом их которых не менее 10 вопросов по научной специальности.
3. Список используемой литературы (не менее 10 наименований за последние 6 лет, в том числе на иностранном языке), который включает в себя: журналы, рекомендованные ВАК; научные и учебные издания; перечень электронных ресурсов. Оформляется в соответствии с действующими требованиями и правилами составления библиографических записей, описаний электронных ресурсов.

Вопросы индивидуальной программы не должны дублировать основную программу.

**ЛИТЕРАТУРА**

**Основная**

1. Горев, А. И. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. — Омск : Омская академия МВД России, 2016. — 88 c. — ISBN 978-5-88651-642-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/72856.html>
2. Кирпичников, А. П. Криптографические методы защиты компьютерной информации : учебное пособие / А. П. Кирпичников, З. М. Хайбуллина. — Казань : Казанский национальный исследовательский технологический университет, 2016. — 100 c. — ISBN 978-5-7882-2052-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/79313.html
3. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 c. — ISBN 978-5-4488-0091-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87998.html
4. Бизнес-безопасность / И.Н. Кузнецов. - 4-е изд. - М. : Дашков и К, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785394026546.html ЭБС «Консультант студента»).
5. Системный подход к обеспечению информационной безопасности предприятия (фирмы) [Электронный ресурс] : Монография / Трайнев В.А. - 3-е изд. - М. : Дашков и К, 2020. Режим доступа: http://www.studentlibrary.ru/book/ISBN9785394037504.html
6. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 21 c. — ISBN 978-5-906953-22-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/98199.html>
7. Проверка и оценка деятельности по управлению информационной безопасностью [Электронный ресурс] : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202756.html (ЭБС «Консультант студента»).
8. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202749.html (ЭБС «Консультант студента»).
9. Маглинец, Ю. А. Анализ требований к автоматизированным информационным системам : учебное пособие / Ю. А. Маглинец. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 191 c. — ISBN 978-5-4497-0301-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89417.html
10. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2017. Режим доступа: https://www.studentlibrary.ru/book/ISBN9785970604397.html
11. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 267 c. — ISBN 978-5-9515-0426-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101929.html
12. Пушкарев, В. П. Защита информационных процессов в компьютерных системах : учебное пособие / В. П. Пушкарев, В. В. Пушкарев. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. — 131 c. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/13929.html
13. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург : Интермедия, 2018. — 168 c. — ISBN 978-5-4383-0161-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/73641.html
14. Оценка состояния организационных систем: принципы, модели, технология [Электронный ресурс] / Я.П. Демидов, Н.Г. Багаутдинова, Л.Б. Шабанова - Казань : Изд-во Казан. ун-та, 2016. - http://www.studentlibrary.ru/book/ISBN9785000196151.html
15. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : Учебное пособие / Коваленко Ю.И. - М. : Горячая линия - Телеком, 2012. - http://www.studentlibrary.ru/book/ISBN9785991202619.html
16. Аудит информационной безопасности органов исполнительной власти [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский - М. : ФЛИНТА, 2016. - http://www.studentlibrary.ru/book/ISBN9785976512771.html
17. Защита информации ограниченного доступа от утечки по техническим каналам

/ Г.А. Бузов - М. : Горячая линия - Телеком, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html (ЭБС «Консультант студента»).

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стереотип. - М. : Горячая линия - Телеком, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785991202572.html (ЭБС «Консультант студента»).
2. Интеллектуальные системы защиты информации : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785942756673.html (ЭБС «Консультант студента»).
3. Интеллектуальные интерактивные системы и технологии управления удаленным доступом (Методы и модели управления процессами защиты и сопровождения интеллектуальной собственности в сети Internet/Intranet): Учебное пособие / Ботуз С.П. - 3-е изд., доп. - М. : СОЛОН-ПРЕСС, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785913591326.html (ЭБС «Консультант студента»).
4. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин ; под редакцией Т. С. Кулаковой. — Санкт-Петербург : Интермедия, 2019. — 216 c. — ISBN 978-5-4383-0182-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95271.html
5. Концептуальные основы создания и применения системы защиты объектов [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 1. - М. : Горячая линия - Телеком, 2012. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202404.html (ЭБС «Консультант студента»).
6. Комплексные (интегрированные) системы обеспечения безопасности [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 7. - М. : Горячая линия - Телеком, 2013. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202381.html (ЭБС «Консультант студента»).
7. Организационно-правовое обеспечение информационной безопасности : учебник / А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев [и др.] ; под редакцией А. А. Александрова, М. П. Сычева. — Москва : Московский государственный технический университет имени Н.Э. Баумана, 2018. — 292 c. — ISBN 978-5-7038-4723-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/110777.html/>
8. Ильин, М. Е. Теоретико-числовые методы в криптографии. Ч.1 : учебное пособие / М. Е. Ильин, К. А. Ципоркова. — Рязань : Рязанский государственный радиотехнический университет, 2020. — 112 c. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/121800.html>
9. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М. : Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html

**Дополнительная**

1. Милославская Н.Г., Управление рисками информационной безопасности : Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 2. - М. : Горячая линия - Телеком, 2013. - 130 с. (Серия "Вопросы управления информационной безопасностью") - ISBN 978-5-9912-0272-5 - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991202725.html
2. Математические основы теории риска [Электронный ресурс] : Учебн. пособ. / Королев В.Ю., Бенинг В.Е., Шоргин С.Я. - 2-е изд., перераб. и доп. - М. : ФИЗМАТЛИТ, 2011. - URL: http://www.studentlibrary.ru/book/ISBN9785922112673.html ЭБС «Консультант студента»).
3. Анализ и оценка риска производственной деятельности : Учеб. пособие / П.П. Кукин, В.Н. Шлыков, Н.Л. Пономарев, Н.И. Сердюк. - М. : Абрис, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785437200483.html (ЭБС «Консультант студента»).
4. Искусство управления информационными рисками / Астахов А.М. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745747.html (ЭБС «Консультант студента»).
5. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А. - М. : ДМК Пресс, 2004. - (Информ. технологии для инженеров). - http://www.studentlibrary.ru/book/ISBN5940742467.html ЭБС «Консультант студента»).
6. Автоматизированные системы. Защитаотнесанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992.
7. ГОСТ 34.10-94. Информационная технология, Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
8. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методический документ ФСТЭК России, 2008 г.
10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методический документ ФСТЭК России, 2008г.
11. Приказ от 25 декабря 2017 г. N 239 об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. Приказа ФСТЭК России от 26 марта 2019 г. N 60)
12. Приказ от от 29 апреля 2021 г. N 77 об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну
13. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. М. ГТК РФ, 1992.
14. Средства вычислительной техники. Защитаотнесанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М.-.ГТК РФ, 1992.
15. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия; уч. пособие. -2 изд. – М.: Издат.-торговая корпорация «Дашков и К», 2005, – 336 ч. (45 экз.)
16. Основы организационного обеспечения информационной безопасности объектов информатизации : Доп. УМО по образованию в области ИБ качестве учеб. пособ. по специальностям в области ИБ / С.Н. Семкин [и др.].. : Гелиос АРВ, 2005. - 192 с. (55 экз.)
17. Технические средства и методы защиты информации [Электронный ресурс] : Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. - М. : Горячая линия - Телеком, 2012. http://www.studentlibrary.ru/book/ISBN9785991202336.html
18. Дудихин В.В., Конкурентная разведка в Internet. Советы аналитика [Электронный ресурс] / Дудихин В.В., Дудихина О.В. - М. : ДМК Пресс, 2009. - 192 с. - ISBN 5-94074-178-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN5940741789.html
19. Защита предпринимательства (экономическая и информационная безопасность): учебное пособие / Одинцов А.А. - М. : Международные отношения, 2003. - URL: http://www.studentlibrary.ru/book/ISBN5713311694.html (ЭБС «Консультант студента»).
20. Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. - 2-е изд., перераб. и доп. - М. :ЦИПСиР, 2011. - URL: http://www.studentlibrary.ru/book/ISBN9785961413649.html (ЭБС «Консультант студента»).
21. Карминский А.М., Информационно-аналитическая составляющая бизнеса: методология и практика [Электронный ресурс] / А.М. Карминский. - М. : Финансы и статистика, 2007. - 272 с. - ISBN 978-5-279-03299-0 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785279032990.html
22. Барский, А. Б. Искусственный интеллект и логические нейронные сети : учебное пособие / А. Б. Барский. — Санкт-Петербург : Интермедия, 2019. — 360 c. — ISBN 978-5-4383-0155-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95270.html (дата обращения: 21.12.2022). — Режим доступа: для авторизир. Пользователей
23. Долженко, А. И. Управление информационными системами : учебное пособие / А. И. Долженко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 180 c. — ISBN 978-5-4497-0911-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102074.html
24. Защита информации в компьютерных системах и сетях [Электронный ресурс] / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2012. Режим доступа: <https://www.studentlibrary.ru/book/ISBN9785940748335.html>
25. Политики безопасности компании при работе в Интернет [Электронный ресурс] / С.А. Петренко, В.А. Курбатов - М. : ДМК Пресс, 2018. - http://www.studentlibrary.ru/book/ISBN9785937000576.html.
26. Криптографические методы защиты информации. Шифры: учебное пособие / Котов Ю.А. - Новосибирск : Изд-во НГТУ, 2016. - URL: http://www.studentlibrary.ru/book/ISBN9785778229594.html (ЭБС «Консультант студента»).
27. Основы современной криптографии и стеганографии / Рябко Б.Я., Фионов А.Н. - 2-е изд. - М. : Горячая линия - Телеком, 2013. - URL: http://www.studentlibrary.ru/book/ISBN9785991203500.html (ЭБС «Консультант студента»).
28. Системы блочного шифрования: учеб. пособие по курсу "Криптографические методы защиты информации" / А. Е. Жуков. - М. : Издательство МГТУ им. Н. Э. Баумана, 2013." - URL: http://www.studentlibrary.ru/book/ISBN9785703837535.html (ЭБС «Консультант студента»).
29. Защита брендов: стратегии, системы, методы [Электронный ресурс] / Ворожевич А.С. - М. : Проспект, 2017. - URL: http://www.studentlibrary.ru/book/ISBN9785392235483.html (ЭБС «Консультант студента»).

**ПЕРЕЧЕНЬ ВОПРОСОВ К КАНДИДАТСКОМУ ЭКЗАМЕНУ**

1. Государственные информационные системы, ПДн.
2. Вычислительные сети и защита информации.
3. Нормативно-правовая база функционирования систем защиты информации.
4. Промышленный шпионаж и законодательство.
5. Меры по обеспечению сохранности информации и угрозы ее безопасности в ИС.
6. Основные задачи обеспечения безопасности информации в ИС.
7. Защита локальных сетей и операционных систем.
8. Интеграция систем защиты.
9. Рекомендации по защите информации в сети Интернет.
10. Принципы построения систем защиты и их основы.
11. Законодательная, нормативно-методическая и научная база систем защиты информации.
12. Структура и задачи органов выполняющих защиту информации.
13. Организационно-правовой статус службы информационной безопасности.
14. Организационно-технические и режимные меры.
15. Политика безопасности: организация секретного делопроизводства и мероприятий по ЗИ.
16. Программно-аппаратные методы и средства ограничения доступа.
17. Типы НСД и защита от них.
18. Надежность средств защиты.
19. Основные понятия и определения традиционных симметричных криптосистем.
20. Шифры перестановки.
21. Шифры замены.
22. Шифрование методом гаммирования.
23. Методы генерации случайных последовательностей.
24. Американский стандарта шифрования AES.
25. Российский стандарт шифрования данных ГОСТ 28147-89.
26. Российский стандарт шифрования данных ГОСТ 34.13-2018.
27. Концепция системы с открытым ключом.
28. Схема шифрования RSA.
29. Схема шифрования Эль-Гамаля.
30. Идентификация и механизмы подтверждения подлинности пользователя.
31. Протоколы идентификации с нулевой передачей знаний.
32. Однонаправленные хэш-функции.
33. Ключевые системы, методы распределения ключей.
34. Электронная подпись, инфраструктура открытых ключей. Удостоверяющие центры. Методы обеспечения подлинности физических лиц.
35. Атаки на криптографические алгоритмы: алгоритмические, алгебраические, статистические.
36. Свойства безопасности криптографических протоколов.
37. Протоколы выработки общего ключа.
38. Протоколы распределения ключей.
39. Протоколы с разделением секрета.
40. Протоколы с подписью в слепую и протоколы электронного голосования.
41. Межсетевые экраны.
42. Маршрутизаторы.
43. Основные схемы сетевой защиты на базе МЭ.
44. Методы защиты от изучения программных средств. Защита от отладок и дизассемблирования.
45. Способы встраивания защитных механизмов в ПО.
46. Методы перехвата и навязывания информации.
47. Методы внедрения программных закладок.
48. Понятие нарушителя. Исходные предположения о возможностях нарушителя.
49. Законы Российской Федерации, составляющие основу правовой базы защиты информации в стране.
50. Особенности российского законодательства в части защиты государственной тайны, коммерческой тайны и авторских прав.
51. Порядок лицензирования и сертификации деятельности в области защиты информации.
52. Математические модели формальной теории защиты информации.
53. Угрозы информации и политика безопасности.
54. Классификация систем защиты.
55. Принципы организации виртуальных частных сетей (VPN). Обеспечиваемые свойства безопасности. Программные средства реализации VPN.
56. Методы разграничения доступа.
57. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
58. Методы и средства хранения ключевой информации.
59. Средства обеспечения безопасности в ОС семейств Windows и UNIX, критерии защищенности ОС.
60. Средства обеспечения безопасности в сетях.
61. Средства защиты серверов и рабочих станций.
62. Средства защиты локальных сетей при подключении к Internet.
63. Методы оценки качества применяемых средств защиты.
64. Методы и средства защиты информации в СУБД.
65. Методы и системы обнаружения компьютерных атак.
66. Примеры атак на средства защиты информации, основанные на изучении побочных сигналов.
67. Выделение полезных сигналов на фоне помех.
68. Методы и средства защиты от инженерно-технической разведки.
69. Определение компьютерного вируса. Классификация компьютерных вирусов. Методы выявления и защиты от вирусов.
70. Определение понятия изолированной программной среды. Примеры.
71. Методы защиты от изменения, контроль целостности.
72. Метод черного ящика при исследовании программных реализаций средств защиты информации.
73. Сетевые атаки. Классификация атак.
74. Методы и технические средства защиты от сетевых атак.
75. Методы анализа исходных текстов с целью поиска уязвимостей, специальные инструментальные средства анализа.
76. Методы и инструментальные средства тестирования программного обеспечения.

ПРИЛОЖЕНИЕ 1

**Федеральное государственное бюджетное**

**образовательное учреждение высшего образования**

**«Астраханский государственный университет имени В.Н. Татищева»**

УТВЕРЖДАЮ

И.о. заведующего кафедрой информационной

безопасности

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Т.Г. Гурская

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

ИНДИВИДУАЛЬНАЯ ПРОГРАММА

для сдачи кандидатского экзамена по направлению

(шифр, наименование специальности)

аспиранта (соискателя) кафедры\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (наименование кафедры)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО аспиранта (соискателя) в родительном падеже)

Тема диссертации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Составитель программы:**

Научный руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(подпись) (ученая степень, ученое звание, ФИО)

**Согласовано:**

Руководитель аспирантуры \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(подпись) (ученая степень, ученое звание, ФИО)

Индивидуальная программа утверждена на заседании кафедры информационной безопасности, протокол №\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

Астрахань 20\_\_

Продолжение приложения 1

**ВОПРОСЫ К ЭКЗАМЕНУ**

НАЗВАНИЕ ПЕРВОГО РАЗДЕЛА

Вопрос 1

Вопрос 2

Вопрос 3

Вопрос 4

Вопрос 5

Вопрос 6

Вопрос 7

Вопрос 8

Вопрос 9

Вопрос 10

…..

НАЗВАНИЕ ВТОРОГО РАЗДЕЛА

Вопрос 1

Вопрос 2

Вопрос 3

Вопрос 4

Вопрос 5

Вопрос 6

Вопрос 7

Вопрос 8

Вопрос 9 Вопрос 10

…..

**СПИСОК ЛИТЕРАТУРЫ**

1. …..
2. …..
3. ……