ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДАЮ

Ректор _____ Ю. А. Трофимов

«31» 10 2023 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ В МАГИСТРАТУРУ

для поступающих на обучение по
направлению подготовки - 10.04.01 «Информационная безопасность»
Профиль «Безопасность информационных систем и технологий»

Иркутск, 2023

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

составлена в соответствии с требованиями Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Приказа Министерства образования и науки РФ от 05 апреля 2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры», а также приказа Министерства образования и науки РФ от от 21 августа 2020 года № 1076 «Об утверждении Порядка приема на обучение по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры». При составлении программы вступительных испытаний учтены требования к результатам освоения программы бакалавриата, приведенные в федеральном государственном образовательном стандарте высшего образования по направлению бакалавриата 10.03.01 «Информационная безопасность».

Программу составили:
доцент кафедры ИСиЗИ, к.э.н. Н. И. Глухов

Программа рассмотрена и одобрена на заседании кафедры «Информационные системы и защита информации»

Протокол № 2 от «18» сентября 2023 г.

Заведующий кафедрой _____ / Т. К. Кириллова

Программа разработана для организации и проведения вступительного испытания в виде комплексного междисциплинарного экзамена по направлению подготовки магистратуры – 10.04.01 «Информационная безопасность», осуществляемых для конкурсного отбора лиц, которые поступают в университет на обучение по программам магистратуры и имеют право сдавать вступительные испытания в форме, устанавливаемой университетом самостоятельно.

В программе перечислены основные элементы теоретического курса, проверяемые на вступительном испытании в магистратуру по направлению подготовки 10.04.01 «Информационная безопасность», указаны навыки и умения, которыми должен обладать кандидат для успешного прохождения вступительного испытания. Кроме того, программа определяет форму и порядок проведения вступительного испытания в магистратуру по направлению подготовки – 10.04.01 «Информационная безопасность», критерии и шкалы оценивания его результатов, а также список литературы для подготовки к вступительному испытанию.

Программа составлена на основе федерального государственного образовательного стандарта высшего образования по направлению магистратуры 10.04.01 «Информационная безопасность».

1. Цели и задачи вступительного испытания

Целями проведения вступительных испытаний являются:

– определение уровня теоретической и практической подготовленности лица, поступающего в магистратуру (кандидата), освоить выбранную магистерскую программу;

– объективная оценка способностей кандидатов к прохождению обучения по выбранным программам высшего образования, для привлечения к учебе наиболее подготовленных, целеустремленных, самостоятельно мыслящих, увлекающихся научными исследованиями;

– создание условий для проведения конкурса поступающих при приеме на обучение в университет.

Задачами проведения вступительного испытания в магистратуру по направлению подготовки 10.04.01 «Информационная безопасность» является:

– проверить уровень знаний поступающего;

– определить уровень научно-технической эрудиции поступающего;

– выявить у кандидата наличие знаний теоретических основ дисциплин бакалавриата по соответствующему направлению;

– выявить мотивы поступления в магистратуру данного направления;

– проверить умение оперировать ссылками на соответствующие положения в учебной и научной литературе;

– выявить способность в письменной форме правильно формулировать ответы на вопросы.

2. Форма проведения и продолжительность вступительного испытания

Вступительные испытания в виде комплексного междисциплинарного экзамена по направлению подготовки 10.04.01 «Информационная безопасность» осуществляются в форме устного экзамена (очно и/или с использованием дистанционных технологий) с использованием экзаменационных билетов, содержащих три контрольных задания различного уровня сложности. Каждый вопрос оценивается максимально на 33,3 балла. Максимальная сумма баллов – 100. Ориентировочная продолжительность устного экзамена – 180 мин.

3. Элементы программы бакалавриата по направлению подготовки 10.04.01 «Информационная безопасность», проверяемые на вступительном испытании

Модуль 1 – Организационное и правовое обеспечение информационной безопасности

1. Правовые основы информационной безопасности.
2. Общие положения федерального законодательства в области защиты информации ограниченного доступа.
3. Основные положения федерального закона «Об информации, информационных технологиях и о защите информации», 149-ФЗ от 27 июля 2006 года.
4. Основные положения федерального закона «О коммерческой тайне», 98-ФЗ от 29 июля 2004 года.
5. Уголовная и административная ответственность за нарушение требований по защите информации (КоАП РФ, УК РФ, ТК РФ).
6. Организационная защита информации как один из основных инструментов обеспечения информационной безопасности организации.
7. Соотношение организационных методов защиты информации с правовыми и техническими.
8. Источники конфиденциальной информации: люди, документы, изделия, технические носители и средства коммуникации.
9. Понятие "пропускной режим". Цели и задачи пропускного режима. Организация пропускного режима.
10. Контрольно-пропускные пункты, их оборудование и организация работы.
11. Понятие конфиденциальный документооборот.
12. Понятие и основные направления информационно-аналитической деятельности по выявлению угроз защищаемой информации.
13. Нормативно-правовое обеспечение ПДн, обрабатываемых в ИСПДн.

Модуль 2 – Программно – аппаратные средства обеспечения информационной безопасности. Криптографические методы защиты информации

1. Методы и средства хранения ключевой информации: магнитные и интеллектуальные карты;
2. Устройство хранения ключей типа iButton (Touch Memory);

3. Электронные идентификаторы ruToken, «Шипка». Электронный замок «Соболь»: назначение, варианты применения, основные принципы функционирования.
4. Средство защиты информации от НСД «Dallas Lock 8.0-C»: назначение и состав системы защиты.
5. Средство защиты информации от НСД SecretNet 7 – сетевой вариант: назначение и варианты применения системы, общая архитектура и компоненты.
6. Безопасность операционных систем.
7. Защита в ОС Windows: объекты доступа; субъекты доступа; права доступа к объектам; привилегии субъектов.
8. Защита в ОС Windows: маркер доступа пользователя; дескриптор защиты объекта, DACL, SACL.
9. Защита в ОС Windows: подсистема идентификации и аутентификации. Алгоритм DES.
10. Двойной и тройной DES.
11. Режимы выполнения алгоритмов симметричного шифрования.
12. Алгоритм ГОСТ 28147-89 Алгоритм RSA. Хэш - алгоритм MD5.Стандарт ГОСТ Р 34.10-2012.

Модуль 3 – Технические средства и методы защиты информации. Безопасность систем баз данных. Безопасность вычислительных сетей. Средства сетевых СУБД

1. Понятие утечки конфиденциальной информации.
2. Демаскирующие признаки объектов наблюдения.
3. Классификация и основные характеристики технических каналов утечки информации.
4. Виды контроля эффективности технической защиты информации.
5. Государственная система противодействия технической разведке.
6. Специсследования защищаемых помещений.
7. Скрытие речевой информации в каналах связи.
8. Уязвимость систем баз данных (СБД); угрозы для СБД; основные средства (меры) обеспечения безопасности СБД; методы резервного копирования, восстановления, репликация в СБД.
9. Средства защиты СУБД Microsoft Access: защита на уровне пользователя; активизация системы защиты; защита объектов базы данных, парольная защита.
10. Система безопасности SQL Server: содержание многоуровневой модели; безопасность сетевого протокола; доменная безопасность; безопасность локального компьютера; безопасность SQL Server; аутентификация и авторизация; транзакции, группы и роли, правила.
11. Средства языка SQL, обеспечивающие права доступа и безопасность, передача и изъятие прав.
12. Классификация компьютерных сетей.
13. Типовые угрозы сетевой безопасности.

14. Защита топологии сети.
15. Методы и средства защиты от НСД в сети.
16. Криптографические сетевые протоколы.
17. Основы технологии виртуальных защищенных сетей VPN.
18. Технологии межсетевых экранов (МЭ).
19. Реляционные БД.
20. Промышленные СУБД.
21. Проектирование БД (основные этапы и средства).
22. Реляционная алгебра.
23. Нормализация и основные НФ (нормальные формы).
24. Языки DML и DDL.
25. Язык SQL.
26. Запросы на выборку данных из одной и нескольких таблиц. Условия отбора, группировка, фильтрация и сортировка выборок. Объединения таблиц.
27. Основные типы данных. Первичные и внешние ключи. Индексы. Представления.
28. Функции пользователя, хранимые процедуры, триггеры. Транзакции. Фиксация и откат. Основные требования.
29. Структура сетевых СУБД.
30. Клиентская и серверная части.
31. Распределенные БД.
32. Администрирование БД.
33. Основные моменты программирования БД на языках высокого уровня.
34. Доступ к сетевым ресурсам и формирование результатов выборок.
35. Основные типы данных (ассемблер и Pascal и их соответствие).
36. Основные конструкции языков программирования: циклы различной структуры, CASE, условные операторы и т. д.
37. Функции, процедуры, макросредства. Основные конструкции.
38. Связь подпрограмм, написанных на языках высокого уровня и ассемблере (Pascal и ассемблер)
39. Динамические компонуемые библиотеки.
40. Понятие функций API Windows.
41. Типы аргументов и вызов.
42. Включаемые файлы и библиотеки.
43. Скелетные файлы Windows – приложений или содержащих только диалог. Главная процедура и оконная процедура, охарактеризовать основные моменты.
44. Программирование основных элементов Win – приложений (меню, кнопки, страницы, панели инструментов, полей редактирования).

4. Требования (умения), проверяемые на вступительном испытании

Лица, имеющие диплом бакалавра или специалиста и желающие освоить магистерскую программу по направлению подготовки 10.04.01 «Инфор-

мационная безопасность», зачисляются по результатам вступительных испытаний. Кандидат должен:

знать:

– нормативно-правовые источники и методические документы регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

– основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки программных средств для решения задач в профессиональной деятельности, Администрирование систем баз данных;

– средства криптографической и технической защиты информации для решения задач профессиональной деятельности

– основные требования к формированию политики информационной безопасности, программные средства скрытого информационного воздействия, утечки информации по техническим каналам;

– основные методы проведения экспериментальной части по созданию систем защиты информации;

– основы экономического обоснования для проектов по защите информации;

уметь:

– применять нормативно-правовые акты и специализированные документы регламентирующие вопросы информационной безопасности в сфере профессиональной деятельности;

– применять языки программирования и работы с базами данных, современные программные среды разработки программных средств для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ;

– применять доверенное хранение, защиту каналов связи и электронного документооборота

– применять методы определения причин, видов, источников и каналов утечки, искажения информации, организовывает и поддерживает выполнение комплекса мер по обеспечению информационной безопасности;

– проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и экономического обоснования.

владеть

– навыками работы с нормативно-правовыми источниками и методическими документами для решения задач по защите информации в профессиональной деятельности;

– навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач навыки программирования, отладки и тестирования прототипов программно-технических комплексов задач;

– навыки работы технического специалиста по организации и обеспечению информационной безопасности компьютерных систем при обработке информации на объекте защиты;

– навыки сбора данных для обеспечения защиты информации и экономического обоснования соответствующих проектных решений.

5. Структура экзаменационного билета

Экзаменационный билет состоит из трех контрольных заданий различного уровня сложности.

Задания модуля 1 направлены на проверку освоения базовых умений и практических навыков по вопросам технического вооружения железнодорожной транспортной системы, рационального использования имеющихся технических ресурсов. Посредством заданий модуля 2 осуществляется проверка знаний технологии работы железнодорожной транспортной системы и ее отдельных структурных подразделений, ответственных за организацию перевозочного процесса, грузовой и коммерческой работы. Модуль 3 позволяет осуществить проверку знаний кандидата по вопросам технологии формирования транспортно-логистических цепей, клиентоориентированной стратегии развития железнодорожной транспортной системы, транспортно-логистического взаимодействия в рамках единой транспортной системы, организации рационального взаимодействия участников процесса доставки грузов.

Образец экзаменационного билета

ИРГУПС **2023-2024 уч. год**	**Экзаменационный билет № 1** комплексный междисциплинарный экзамен по направлению подготовки 10.04.01 «Информационная безопасность» Профиль «Безопасность информационных систем и технологий»	**Утверждаю** Ректор ИрГУПС _____ Ю. А. Трофимов
1. Правовые основы информационной безопасности. 2. Методы и средства хранения ключевой информации. 3. Понятие утечки конфиденциальной информации.		

6. Оценивание результатов вступительного испытания

Критерии и шкала оценивания выполнения заданий экзаменационного билета

Номер задания	Критерий оценивания	Баллы по заданиям
1-3	При ответе кандидат показывает свободное владение программным учебным материалом различной степени сложности, отличное знание зависимостей между статистическими категориями, а также творческое использование этих знаний в обосновании утверждений. Использование условных или реальных статистических данных для аргументации ответа. Допускается один несущественный недочет. Ответил на все дополнительные вопросы.	ОТЛИЧНЫЙ (27-33,3 балла)
	При полном ответе на теоретический вопрос в рамках данной программы имеются один-два недочета, которые не искажают существа излагаемого вопроса. Теоретические положения подтверждены статистическими данными и примерами, возможно только условными. Ответил на большинство дополнительных вопросов.	БАЗОВЫЙ (20-26 баллов)
	Изложение теоретического материала приводится с существенными ошибками, неточно или схематично или на конкретных примерах. Кандидат может применять свои знания только в типичной знакомой ситуации, а при незначительном её изменении испытывает затруднения. Допустил много неточностей при ответе на дополнительные вопросы.	МИНИМАЛЬНЫЙ (от 13-19 баллов)
	При ответе усвоены лишь отдельные понятия и факты программного материала. Наличие грубых ошибок в ответе. Кандидат не может применять свои знания в типичной знакомой ситуации. При ответах на дополнительные вопросы допущено множество неправильных ответов.	НИЗКИЙ (менее 13 баллов)

Шкала оценивания уровня подготовленности к обучению по результатам вступительного испытания

Вторичный балл за вступительное испытание	Уровень подготовленности к обучению	Характеристика уровня подготовленности
80 - 100	Отличный	Кандидат отлично подготовлен для дальнейшего обучения в магистратуре по направлению подготовки – 23.04.01 «Технология транспортных процессов»
60 - 79	Базовый	Кандидат показал хороший уровень подготовки для поступления в магистратуру по направлению подготовки – 23.04.01 «Технология транспортных процессов»
40 - 59	Минимальный	Кандидат обладает минимальным уровнем компетентностей, необходимых для освоения программы магистратуры по направлению подготовки – 23.04.01 «Технология транспортных процессов»
0 - 39	Низкий	Кандидат не готов к обучению в магистратуры по направлению подготовки – 23.04.01 «Техно-

		логия транспортных процессов»

7. Порядок проведения вступительных испытаний

Вступительные испытания в виде комплексного междисциплинарного экзамена по направлению подготовки магистратуры 10.04.01 «Информационная безопасность» проводятся в соответствии с графиком их проведения в период работы приемной комиссии.

Подготовка и проведение вступительных испытаний осуществляется предметной комиссией по магистерской программе по направлению подготовки 10.04.01 «Информационная безопасность», назначаемой приказом ректора университета.

Варианты экзаменационных билетов для проведения вступительных испытаний в виде комплексного междисциплинарного экзамена разрабатываются председателем предметной комиссии по магистерской программе по направлению подготовки 10.04.01 «Информационная безопасность» и подписываются ректором университета не позже чем за месяц до начала вступительных испытаний. Варианты экзаменационных билетов для конкретной группы (потока) кандидатов должны выдаваться председателю предметной комиссии в день проведения испытания.

На вступительные испытания кандидат должен прибыть с паспортом (либо документом, заменяющим паспорт). Перед началом вступительного испытания поступающему выдается экзаменационный лист, который необходимо сдать вместе с письменной работой после прохождения вступительного испытания.

Перед началом вступительного испытания каждому кандидату вручается титульный лист письменной работы, вариант экзаменационного билета, бланк ответов для записи ответов на задания с развернутым ответом, а также чистые листы бумаги для ведения черновых записей. Кандидат обязан висать в титульный лист необходимые идентификационные сведения о себе (ФИО в именительном падеже либо номер СНИЛС), на листе бумаги в верхнем правом углу записать номер группы (потока), с которой он прибыл на вступительные испытания, номер варианта экзаменационного билета.

Во время проведения вступительного испытания кандидат может покинуть аудиторию только один раз не более чем на пять минут по разрешению экзаменатора.

Во время проведения вступительного испытания кандидатам запрещается:

– общаться с другими кандидатами;

– самовольно пересаживаться на другие места в экзаменационной аудитории;

– делать какие-либо пометки, условные знаки на листах письменных работ, по которым может быть установлено их авторство;

– использовать какие-либо вспомогательные и справочные материалы, не разрешенные предметными экзаменационными комиссиями (учебники, методические пособия, справочники и др.);

– иметь при себе мобильные телефоны и иные средства связи, электронно- вычислительную технику (планшеты, ноутбуки и т. п.);

– выносить за пределы аудитории экзаменационную работу и любые другие записи.

Результаты вступительного испытания заносятся в экзаменационную ведомость и доводятся до кандидатов не позднее третьего рабочего дня после проведения вступительного испытания.

В случае если кандидат не набирает минимального порогового количества баллов, считается, что экзамен он не сдал и не может принимать дальнейшее участие в конкурсе. Поступающие, не прошедшие вступительные испытания по уважительной причине (болезнь или иные обстоятельства, подтвержденные документально), допускаются к проведению вступительного испытания в другой группе или в резервный день в соответствии с расписанием проведения вступительных испытаний.

Спорные вопросы, возникшие при проведении вступительного испытания, разрешаются апелляционной комиссией. Заявление (апелляция) о нарушении порядка проведения вступительного испытания и/или несогласие с результатами вступительного испытания, подается кандидатом лично на следующий день после объявления итоговой оценки вступительного испытания.

Порядок проведения дистанционного компьютерного тестирования

Платформами для проведения дистанционных вступительных испытаний являются корпоративной платформы Microsoft Teams и системы электронного обучения Moodle.

Перед выполнением компьютерного теста проводится процедура аутентификации личности поступающего, то есть осуществляется проверка подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных пользователей.

Затем осуществляется визуальная (экспертная) идентификация личности поступающего посредством установления визуального соответствия личности обучающегося документам, удостоверяющим его личность.

Выполнение компьютерного теста осуществляется при экспертном видео-прокторинге, то есть при помощи визуального контроля за ходом дистанционного испытания посредством видеосвязи.

При отсутствии у обучающегося в комплектации компьютера вебкамеры и микрофона, экспертные идентификация личности и видеопрокторинг могут проводиться с помощью мобильного телефона с использованием мобильных версий указанных выше платформ.

8. Список литературы для подготовки к вступительному испытанию

1. Глухих В. И. Information security and data protection: учебное пособие для магистров по направлению "Информатика и вычислительная

техника" / В. И. Глухих; Нац. исслед. Иркут. гос. техн. ун-т. - Томск: СПБ Графикс, 2012г. - 276с.
2. Грибунин В.Г. Комплексная система защиты информации на предприятии. М.: Академия, 2009г., 411с.
3. Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для вузов по специальности 230201 "Информ. системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 5-е изд., стер. - М.: Академия, 2011г. - 330с.
4. Глухов Н.И., Туренко Б.Г. Оценка информационных рисков: теория и практика - Иркутск: Изд-во БГУЭП, 2010г.
5. Технические средства и методы защиты информации: учебное пособие для вузов / А. П. Зайцев [и др.]. - Москва: Горячая линия - Телеком, 2012г. - 615с.
6. Глухих В. И. Информационная безопасность и защита данных: учебное пособие / В. И. Глухих; М-во образования и науки РФ, Иркут. гос. техн. ун-т. - Иркутск: Изд-во ИрГТУ, 2012г. - 244с.
7. Н.И. Глухов. Оценка информационных рисков предприятия, учебное пособие. Иркутск: изд-во ИрГУПС, 2013, 157с.
8. Гатченко, Н.А. Криптографическая защита информации. Учебное пособие [Электронный ресурс] : учебное пособие / Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев. — Электрон. дан. — Спб. : НИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2012. — 142 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=40849
9. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. Москва: Горячая линия–Телеком, 2013 г. , 232 с. (ibooks)
10. Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. и др. Под редакцией А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие. – Москва: Горячая линия–Телеком, 2012 г. , 550 с. (ibooks.ru)
11. Белов, С. В. Изучение основ функционирования систем физической безопасности : учебное пособие / С. В. Белов, Ш. Ш. Иксанов, Н. В. Давидюк ; составители С. В. Белов [и др.]. — Санкт-Петербург : Интермедия, 2020. — 82 с. — ISBN 978-5-4383-0203-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161335 (дата обращения: 02.07.2021). — Режим доступа: для авториз. пользователей.

12. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 (дата обращения: 02.07.2021). — Режим доступа: для авториз. пользователей.
13. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 02.07.2021). — Режим доступа: для авториз. пользователей.
14. Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 (дата обращения: 02.07.2021). — Режим доступа: для авториз. пользователей.
15. Свинарев, Н.А. Инструментальный контроль и защита информации [Электронный ресурс] : учебное пособие / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин [и др.]. — Электрон. дан. — Воронеж : ВГУИТ (Воронежский государственный университет инженерных технологий), 2013. — 192 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=72884
16. Федеральный закон РФ «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ.
17. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 02.07.2021). — Режим доступа: для авториз. пользователей.
18. Ермаков А.А. Основы надежности информационных систем учеб. пособие. Иркутск: ИрГУПС, 2006. - 152 с.
19. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с. — Режим доступа:
20. Дейт К .Дж. Введение в системы баз данных (7_изд). – М.: Изд. Дом Вильямс, 2005.
21. А. Горев, С. Макашарипов, Р. Ахаян. Эффективная работа с СУБД.
22. Ребекка Райордан. Основы Реляционных Баз Данных. М.: Издат.-торговый дом «Русская редакция»,2001.

23. Коннолли_Томас, Бегг_Каролин. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – М.: 2003.
24. П.Роб,К.Коронел. Системы баз данных. – СпБ.: 2004.
25. Н.Г.Голубь. Искусство программирования на Ассемблере. Лекции и упражнения. – М.: 2002.
26. В. И. Юров - Assembler. Учебник для ВУЗов. – М.: 2003.
27. Шварц Б., Зайцев П., Ткаченко В. и др. - MySQL. Оптимизация производительности (2-е издание) – М.: 2010.
28. Ларри Ульман. MySQL. М.:2004.
29. Красиков И.В., Красикова И.Е. - Алгоритмы. Просто как 2x2. – М.: 2007.
30. Род Стиввенс. Delphi. Готовые алгоритмы(2-е издание). М.: 2004.
31. Марко Кэнту. Delphi7 для профессионалов. – СпБ.: 2004
32. http://e.lanbook.com/books/element.php?pl1_id=50578
33. Режим доступа: http://www.securitycode.ru/products/secret_net/documentation/
34. Режим доступа: http://www.securitycode.ru/products/pak_sobol/documentation/
35. Режим доступа: http://www.dallaslock.ru/sub-doc.html