МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Севастопольский государственный университет»

УТВЕРЖДАЮ

Председатель приемной комиссии

Ректор

_____ В.Д. Нечаев
(подпись) *(Ф.И.О)*

«20» января 2026 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Профессиональное вступительное испытание
(название вступительного испытания)

направление подготовки **10.04.01 Информационная безопасность**
(шифр и название направления подготовки)

уровень высшего образования **магистратура**
(название уровня ВО)

квалификация **магистр**
(название)

Севастополь
2026

Программа профессионального вступительного испытания при приеме на обучение по направлению подготовки 10.04.01 Информационная безопасность:

1. **Разработана** на кафедре «Информационная безопасность» ФГАОУ ВО «Севастопольский государственный университет» в соответствии со следующими нормативными документами:

– Порядок приема на обучение по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденный Приказом Минобрнауки России от 27.11.2024 № 821;

– Правила приема в федеральное государственного автономное учреждение высшего образования «Севастопольский государственный университет» на обучение по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в 2026 году;

– Положение о приемной комиссии федерального государственного автономного учреждения «Севастопольский государственный университет»;

– Положение об экзаменационных комиссиях федерального государственного автономного учреждения высшего образования «Севастопольский государственный университет»;

– Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата), утвержденный приказом Министерства образования и науки Российской Федерации от 17.11.2020 № 1427;

– Основная образовательная программа высшего образования по направлению подготовки 10.03.01 Информационная безопасность (профиль – Организация и технологии защиты информации), утвержденная ректором ФГАОУ ВО «Севастопольский государственный университет» от «28» мая 2021 г.

2. **Разработчики программы**: Руководитель рабочей группы – Ожиганова М.И., заведующий кафедрой «Информационная безопасность», Гончаренко Ю.Ю., доктор технических наук, профессор кафедры «Информационная безопасность», Костюков Александр Дмитриевич, кандидат юридических наук, доцент кафедры «Информационная безопасность»

3. **Утверждена** на заседании кафедры «Информационная безопасность» от «08» 12 2025 г., протокол № 6.

Председатель профессиональной
экзаменационной комиссии,
заведующий кафедрой
«Информационная безопасность» _____ _____ М.И. Ожиганова
(подпись) (дата)

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ И ПОРЯДОК ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительное испытание по профпредмету проводится аттестационной комиссией, персональный состав которой утверждается приказом ректора СевГУ.

Программа конкурсного вступительного испытания предназначена для абитуриентов, поступающих на обучение по программе магистратуры по направлению 10.04.01 Информационная безопасность.

Назначением программы конкурсного вступительного испытания по специальности является оказание помощи абитуриентам в самостоятельной подготовке к сдаче экзамена, систематизации и закреплении знаний, полученных в процессе обучения по дисциплинам цикла профессиональной подготовки по специальности. Программа ориентирует студентов на обобщение знаний о методах и средствах организации защиты информации, циркулирующей на объектах информационной деятельности. Основной целью конкурсного вступительного испытания является формирование конкурсного балла, который помимо оценки по испытанию содержит средний балл диплома бакалавра.

Форма и содержание конкурсного вступительного испытания обеспечивает контроль выполнения требований, предъявляемых к уровню подготовки абитуриентов, которые имеют диплом бакалавра по направлению 10.03.01 Информационная безопасность.

Абитуриент должен уметь оценивать состояние защищенности объекта информационной деятельности на предмет утечек информации по техническим каналам, знать основные языки программирования, хорошо ориентироваться в современных методах и средствах защиты информации в том числе и в информационных системах, знать базовые принципы организации компьютерных сетей и их уязвимости, хорошо ориентироваться в современных государственных стандартах, в области криптографической защиты информации.

Списки абитуриентов, допущенных к конкурсному вступительному испытанию по специальности, утверждаются протоколом приемной комиссии.

Конкурсное вступительное испытание по специальности включает задания по следующим дисциплинам цикла профессиональной подготовки по направлению 10.03.01 Информационная безопасность:

— Программно-аппаратные средства защиты информации;
— Криптографические методы защиты информации;
— Системы защиты баз данных;
— Теория вероятностей и математическая статистика;
— Техническая защита информации;
— Комплексные системы зашиты информации;
— Организационное и правовое обеспечение информационной безопасности;
— Основы управления информационной безопасностью;
— Теория информации;

— Основы защиты программного обеспечения.

Конкурсное вступительное испытание проводится в письменной форме. Задание на вступительное испытание определяется билетом, в котором приведены теоретические и практические задания по дисциплинам, включенным в конкурсное испытание.

Результаты конкурсного вступительного испытания определяются по стобальной (100) системе.

Решение аттестационной комиссии об оценке знаний, выявленных при сдаче конкурсного вступительного испытания, и о рекомендациях приема на квалификационный уровень магистр, принимаются аттестационной комиссией на закрытом заседании. Оценки и рекомендации о приеме на квалификационный уровень магистр объявляются абитуриентам после оформления ведомости проведения конкурсного испытания на следующий день после экзамена.

В случае если абитуриент не согласен с оценкой, выставленной аттестационной комиссией, он имеет право подать апелляцию в порядке, определенном Положением о приемной комиссии СевГУ.

2. ОСНОВНОЕ СОДЕРЖАНИЕ ПРОГРАММЫ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

2.1. Программно-аппаратные средства защиты информации

Безопасность компьютерной сети. Сканеры. Защита от анализаторов протоколов. Межсетевые экраны. Классификация межсетевых экранов.

Идентификация пользователей КС Идентификация субъекта, понятие протокола идентификации, идентифицирующая информация. Локальная и удаленная идентификация.

Средства и методы ограничения доступа к файлам. Основные подходы к защите данных от несанкционированного доступа. Модели управления доступом. Реализация механизмов безопасности на аппаратном уровне. Защита на уровне расширений BIOS. Защита на уровне загрузчиков операционной среды.

Программно-аппаратные средства шифрования. Аппаратные и программно-аппаратные средства криптозащиты данных. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, принцип чувствительной области, принцип главного ключа.

Защита программ от несанкционированного копирования. Хранение ключевой информации. Защита программ от изучения. Создание защищенной операционной системы.

Концепция информационной безопасности. Актуальность информационной безопасности. Лицензирование и сертификация в области защиты информации. Основные нормативные руководящие документы. Угрозы информации. Информационная безопасность сетей. Способы совершения компьютерных преступлений. Уязвимость сети Интернет.

Виды возможных нарушений информационной системы. Компьютерные преступления. Вредоносные программы. Вирусы.

Информационная безопасность информационных систем. Теория информационной безопасности информационных систем. Криптографические способы защиты информации. Организация информационной безопасности компании.

Методы и средства защиты компьютерной информации. Обеспечения информационной безопасности. Контроль доступа к информации.

Методы и средства защиты информации. Антивирусное ПО.

2.2. Криптографические методы защиты информации

Метод полного перебора. Атака по ключам. Метод «встречи посередине». Криптоанализ симметричных шифров. Криптоанализ асимметричных шифров. Криптоанализ хеш-функций. Криптоанализ по побочным каналам.

Основные классы симметричных криптосистем. Элементарные шифры. Потоковые шифры. Качество и периодичность гаммы. Блочные шифры.

Основные характеристики и структура алгоритмов DES и ГОСТ 28147-89.

Основы асимметричных систем. Процедура открытого распределения ключей Диффи-Хеллмана. Криптосистема RSA. Шифр Эль-Гамаля. Особенности использования асимметричных криптосистем на практике. Способы увеличения стойкости шифров.

Задача аутентификации и цифровая подпись. Протоколы аутентификации. Проектирование и анализ потоковых шифров.

2.3. Системы защиты баз данных

Теория реляционных баз данных. Обзор моделей представления данных.

Язык описания данных. Язык манипулирования данными. Организация сложных запросов. Основы проектирования реляционных БД на основе принципов нормализации. Физические модели баз данных. Администрирование баз данных. Применение навыков проектирования баз данных на практике. Современные технологии проектирования баз данных.

2.4. Теория вероятностей и математическая статистика

Статистические оценки параметров распределения. Понятие вариационного ряда. Статистические оценки параметров распределения. Точечные, интервальные оценки. Нахождение сводных характеристик выборки.

Марковские, Пуассоновские случайные процессы. Марковские случайные процессы. Пуассоновский случайный процесс.

Точечные и интервальные оценки параметров распределений. Точечные и интервальные оценки параметров распределений. Проверка гипотез. Метод наименьших квадратов.

Числовые характеристики непрерывных случайных величин. Нормальное распределение функции от случайных величин. Случайные величины и их распределение. Основные выборочные характеристики.

Дискретные случайные величины. Дискретные случайные величины и их числовые характеристики. Биномиальное распределение. Геометрическое распределение. Пуассоновское распределение

Классическая вероятность. Элементы комбинаторики. Простейшие теоремы о вероятностях сложных событий. Формула полной вероятности и формула Байеса. Схема Бернулли. Элементы комбинаторики. Простейшие теоремы о вероятностях сложных событий. Формула полной вероятности и формула Байеса. Схема Бернулли. Дискретные случайные величины и их числовые характеристики. Биномиальное распределение. Геометрическое распределение. Пуассоновское распределение. Нормальное распределение

функции от случайных величин. Случайные величины и их распределение. Основные выборочные характеристики. Точечные и интервальные оценки параметров распределений. Проверка гипотез. Метод наименьших квадратов. Марковские случайные процессы. Пуассоновский случайный процесс. Понятие вариационного ряда. Статистические оценки параметров распределения. Точечные, интервальные оценки. Нахождение сводных характеристик выборки.

2.5. Техническая защита информации

Демаскирующие признаки объектов и источники информации для технических средств разведки. Классификация, структура, характеристики средств радиомониторинга. Обнаружение, наблюдение, перехват и обработка данных, полученных при помощи средств радиомониторинга, как средства оперативного получения информации. Системы радиомониторинга и определения местоположения источников радиоизлучения. Демаскирующие признаки объектов и источники информации для технических средств разведки. Лазерные системы и их демаскирующие признаки.

Демаскирующие признаки радиоэлектронных средств и систем. Радиолокационные характеристики объектов разведки и их отличительные признаки. Побочные электромагнитные излучения и наводки. Каналы утечки информации при эксплуатации технических средств передачи, обработки и хранения информации. Радиоактивные излучения как источник информации о предприятиях атомной промышленности и их продукции.

Способы и средства защиты объектов и информации от технических разведок. Защита объектов от технической разведки. Защита объектов от оптической разведки. Защита от оптико-электронных средств разведки. Защита радиоэлектронных средств и информации от радио- и радиотехнической разведки. Защита объектов от радиолокационных средств разведки. Возможные мероприятия по защите лазерных систем от технических разведок. Защита от гидроакустических средств разведки. Защита от средств акустической разведки. Защита технических средств передачи, обработки и хранения информации. Защита информации в средствах электронно-вычислительной техники. Технический контроль эффективности принятых мер защиты.

2.6. Организационное и правовое обеспечение информационной безопасности

Основы правового регулирования отношений в информационной сфере. Конституционные гарантии прав граждан на получение информации и механизм их реализации. Понятия и виды защищаемой информации по законодательству РФ. Основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности.

Понятие и виды компьютерных преступлений. Организационное обеспечение защиты информации.

2.7. Комплексные системы зашиты информации

Сущность и задачи комплексной системы защиты информации. Принципы организации и этапы разработки комплексной системы защиты информации. Факторы, влияющие на организацию комплексной системы защиты информации. Определение и нормативное закрепление состава защищаемой информации. Определение объектов защиты. Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию. Определение потенциальных каналов и методов несанкционированного доступа к информации. Определение возможностей несанкционированного доступа к защищаемой информации. Определение компонентов комплексной системы защиты информации. Определение условий функционирования комплексной системы защиты информации. Разработка модели комплексной системы защиты информации. Технологическое и организационное построение комплексной системы защиты информации. Кадровое обеспечение функционирования комплексной системы защиты информации. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации. Назначение, структура и содержание управления комплексной системой защиты информации.

2.8. Основы управления информационной безопасностью

Понятие информационной безопасности. Основные составляющие информационной безопасности. Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности.

Оценочные стандарты в информационной безопасности. Роль стандартов ИБ. «Оранжевая книга» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

Стандарты управления информационной безопасностью. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.

Создание СУИБ на предприятии. Этапы разработки и внедрения системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ.

Методика оценки рисков информационной безопасности предприятия. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей.

Методика оценки рисков информационной организации. Метод оценки рисков на основе модели информационных потоков. Описание архитектуры ИС. Расчет рисков по угрозе конфиденциальность.

Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками.

Разработка корпоративной методики анализа рисков. Постановка задачи. Методы оценивания информационных рисков. Табличные методы оценки рисков. Оценка рисков по двум факторам. Разделение рисков на приемлемые и неприемлемые. Оценка рисков по трем факторам.

Современные методы и средства анализа и управление рисками информационных систем компаний. Обоснование необходимости инвестиций в информационную безопасность компании.

2.9. Теория информации

Основы теории информации. Безусловная энтропия. Введение в курс. Основные понятия теории информации и задачи курса. Виды оценки информации. Мера Хартли. Энтропия Шеннона. Характеристика информационного канала. Численная оценка канала связи с шумами. Условная энтропия. Условная энтропия. Энтропия объединения Кодирование информации. Определение избыточности сообщений. Обнаружение и исправление ошибок в сообщениях. Корректирующие коды. Алгоритмы сжатия информации

2.10. Языки программирования.

Организация программ. Введение в языки программирования. Позиционные системы счисления. Понятие алгоритма и типовые алгоритмические структуры программирования. Элементы алгоритмических языков. Структурное программирование: последовательность, ветвление и циклы. Процедурно-ориентированное программирование. Структуры данных и алгоритмы. Организация данных и алгоритмы их обработки. Файловые структуры данных. Динамические структуры данных и алгоритмы их обработки.

3. ШКАЛА ОЦЕНИВАНИЯ И МИНИМАЛЬНОЕ КОЛИЧЕСТВО БАЛЛОВ, ПОДТВЕРЖДАЮЩЕЕ УСПЕШНОСТЬ ПРОХОЖДЕНИЯ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Конкурсное вступительное испытание проводится в письменной форме. Задание на вступительное испытание определяется лист-заданием, содержащим тестовые задания.

Результаты конкурсного вступительного испытания определяются по 100-бальной системе. Всего лист-задание содержит 15 тестовых вопросов. Правильный ответ на каждый вопрос оценивается в 1 балл. Суммарный результат конкурсного вступительного испытания пересчитывается в оценку по 100-бальной шкале согласно пропорции.

Сопоставление национальной и стобальной оценочных шкал представлено в следующей таблице.

Уровень компетентности	Оценка по национальной шкале	Сумма баллов по 100-бальной шкале
Высокий (творческий)	Отлично	81-100
Достаточный (конструктивно-вариативный)	Хорошо	51-80
Средний (репродуктивный)	Удовлетворительно	25-50
Низкий (рецептивно-производительный)	Неудовлетворительно	0-24

Минимальное количество баллов, подтверждающее успешность прохождения вступительного испытания – 25.

Минимальный проходной балл для обучения за счет бюджетных ассигнований федерального бюджета определяется на конкурсной основе Правилами приёма Севастопольского государственного университета.

4. СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-437163
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учеб. пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Серия : Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/book/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-441287
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/452368
4. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — М. : ИНФРА-М, 2019. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/13571. - Режим доступа: http://znanium.com/catalog/product/991792
5. Программно-аппаратная защита информации: Учебное пособие / Хорев П.Б., - 2-е изд., испр. и доп. - М.:Форум, НИЦ ИНФРА-М, 2015. - 352 с.: 60x90 1/16. - (Высшее образование) ISBN 978-5-00091-004-7 - Режим доступа: http://znanium.com/catalog/product/489084
6. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва : Юрайт, 2019. — 349 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/book/kriptograficheskie-metody-zaschity-informacii-433610
7. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Юрайт, 2019. — 473 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-10673-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/book/kriptograficheskie-metody-zaschity-informacii-431164

8. Виноградов, И. М. Основы теории чисел [Электронный ресурс] : учебное пособие / И. М. Виноградов. — Электрон. дан. — Санкт-Петербург : Лань, 2019. — 176 с. — Режим доступа : https://e.lanbook.com/book/115195
9. Осокин, А. Н. Теория информации : учеб. пособие для прикладного бакалавриата / А. Н. Осокин, А. Н. Мальчуков. — Москва : Юрайт, 2019. — 205 с. — (Университеты России). — ISBN 978-5-9916-7064-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434040
10. Иванов, И. В. Теория информационных процессов и систем + доп. Материалы в ЭБС : учеб. пособие для академического бакалавриата / И. В. Иванов. — 3-е изд., перераб. и доп. — Москва : Юрайт, 2019. — 228 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-05705-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/438821
11. Гмурман, В. Е. Руководство к решению задач по теории вероятностей и математической статистике : учеб. пособие для бакалавриата и специалитета / В. Е. Гмурман. — 11-е изд., перераб. и доп. — Москва : Юрайт, 2019. — 406 с. — (Бакалавр и специалист). — ISBN 978-5-534-08389-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/book/rukovodstvo-k-resheniyu-zadach-po-teorii-veroyatnostey-i-matematicheskoy-statistike-431094
12. Усенко, О. А. Приложения теории информации и криптографии в радиотехнических системах : учебное пособие / О. А. Усенко ; Южный Федеральный университет. — Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. — 170 с. —— Режим доступа : http://znanium.com/catalog/product/1021618 ISBN 978-5-9275-2569-0
13. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2019. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433420
14. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/451486
15. Буре, В.М. Теория вероятностей и вероятностные модели : учебник / В.М. Буре, Е.М. Парилина, А.А. Седаков. — Санкт-Петербург : Лань, 2020. — 296 с. — ISBN 978-5-8114-3168-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/108328

16. Гладков, Л.Л. Теория вероятностей и математическая статистика : учебное пособие / Л.Л. Гладков, Г.А. Гладкова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 196 с. — ISBN 978-5-8114-3982-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130156
17. Иванов, Б.Н. Теория вероятностей и математическая статистика : учебное пособие / Б.Н. Иванов. — 2-е изд., испр. и доп. — Санкт-Петербург : Лань, 2019. — 224 с. — ISBN 978-5-8114-3636-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/113901
18. Базы данных [Электронный ресурс] : учеб. пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. — 4-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 400 с. — (Высшее образование: бакалавриат). - Режим доступа: http://znanium.com/catalog/product/1019244
19. Мартишин, С. А. Базы данных. Практическое применение СУБД SQL и NoSQL-типа для проектирования информационных систем : учеб. пособие / С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. — М. : ИД «ФОРУМ» : ИНФРА-М, 2019. — 368 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/1001370
20. Новиков, Б. А. Основы технологий баз данных / Б. А. Новиков ; под редакцией Е. В. Рогова. — Москва : ДМК Пресс, 2019. — 240 с. — ISBN 978-5-94074-820-5. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/123699
21. Стружкин, Н. П.Базы данных: проектирование : учебник для академического бакалавриата / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2019. — 477 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-00229-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL:https://biblio-online.ru/bcode/432177
22. Тумбинская, М.В. Защита информации на предприятии : учебное пособие / М.В. Тумбинская, М.В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184
23. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/449285
24. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/422772

25. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/449350
26. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/450371
27. Огнева, М. В. Программирование на языке C++: практический курс : учебное пособие для вузов / М. В. Огнева, Е. В. Кудрина. — Москва : Издательство Юрайт, 2020. — 335 с. — (Высшее образование). — ISBN 978-5-534-05123-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/454165
28. Трофимов, В. В. Алгоритмизация и программирование : учебник для вузов / В. В. Трофимов, Т. А. Павловская ; под редакцией В. В. Трофимова. — Москва : Издательство Юрайт, 2020. — 137 с. — (Высшее образование). — ISBN 978-5-534-07834-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/452333