

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ
КЫРГЫЗСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
ИМ. Ж.БАЛАСАГЫНА

ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ

«СОГЛАСОВАНО»

Начальник УУ

КНУ им. Ж. Баласагына

к.п.н.доц. Кыдыралиев А.Т.

УПРАВЛЕНИЕ

« 20 » 05 2024 г.



«УТВЕРЖДАЮ»

Проректор по уч. работе

КНУ им. Ж. Баласагына

к. ф.-м. н. доцент Бексултанов Ж.Т.

« 20 » 05 2024 г.



ПРОГРАММА

ИТОГОВОЙ ГОСУДАРСТВЕННОЙ АТТЕСТАЦИИ ВЫПУСКНИКОВ

Специальности подготовки: **100203 «Информационная безопасность»**
(указать шифр и название)

Квалификация: Техник по защите информации

Бишкек -2024

Организация – разработчик: **Профессиональный колледж**

Директор ПК



Каныбек уулу Ардакбек

Обсуждено и одобрено на заседании предметно-цикловой комиссии спец. дисциплин отделения информационных технологий

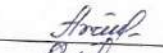
Протокол № 13 от « 13 » 03 2024 г.

Одобрено Учебно-методическим советом профессионального колледжа КНУ им. Ж. Баласагына

Протокол № 6 от « 29 » 03 2024 г.

Разработчик программы:

Зав. отделением информационных технологий  М.Ж. Мамбеталиев

Председатель ПЦК информационных технологий  А.А. Ажикулова

Преподаватель Профессионального колледжа  К.З. Медетканова

1. Общие положения.

В соответствии с Законом Кыргызской Республики «Об образовании в Кыргызской Республики» утвержденным постановлением Правительства Кыргызской Республики от 4 июля 2012 года N 470 итоговая аттестация выпускников, завершающих обучение по программам среднего профессионального образования в образовательных учреждениях среднего профессионального образования является обязательной. Итоговая государственная аттестация выпускников проводится в образовательных учреждениях среднего профессионального образования, имеющих государственную аккредитацию и завершается выдачей документа государственного образца об уровне образования и квалификации. Итоговая государственная аттестация выпускников проводится в соответствии с Положением о порядке проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования в Кыргызской Республики, утвержденным Приказом МОиН КР №197/1 от 16.02.2017. Государственная итоговая аттестация определяет, в какой степени выпускник готов к выполнению профессиональной деятельности в соответствии с его квалификационной характеристикой.

1.1. Цель итоговой государственной аттестации - установление соответствия уровня и качества подготовки выпускника Государственному образовательному стандарту среднего профессионального образования в части государственных требований к минимуму содержания и уровню подготовки выпускников, и дополнительным требованиям по конкретной специальности, а также квалификационной характеристики специалистов по специальности 100203 «Информационная безопасность».

Государственная итоговая аттестация по специальности 100203 «Информационная безопасность» проводится в виде итогового комплексного экзамена по специальности. Основанием для проведения является Приказ об утверждении порядка проведения государственной итоговой государственной аттестации по образовательным программам среднего профессионального образования.

К итоговой государственной аттестации допускаются лица, выполнившие требования, предусмотренные учебным планом СПО.

Итоговую государственную аттестацию осуществляет государственная аттестационная комиссия.

1.2. Программа итоговой государственной аттестации.

Программа итоговой государственной аттестации является частью основной профессиональной образовательной программы СПО по специальности «Техник по защите информации».

Программа итоговой государственной аттестации ежегодно разрабатывается цикловой методической комиссией технических дисциплин и утверждается.

Программа итоговой государственной аттестации доводится до сведения студентов не позднее, чем за 6 месяцев до начала итоговой государственной аттестации.

На основе составленных и объявленных студентам перечней вопросов, заданий, рекомендуемых для подготовки к итоговому комплексному экзамену по специальности, составляются экзаменационные билеты, содержание которых до студентов не доводится.

Количество экзаменационных билетов должно превышать количество студентов в учебной группе не менее, чем на 5.

Вид итоговой государственной аттестации определяется в соответствии с Государственными требованиями по специальности.

Объем времени на подготовку и проведение итоговой государственной аттестации установлен Государственными требованиями по специальности.

Сроки проведения итоговой государственной аттестации определяются СПО в соответствии с его учебным планом.

Экзаменационные материалы должны отражать объем проверяемых теоретических знаний и практических умений выпускников в соответствии с Государственными требованиями и дополнительными требованиями СПО по специальности 100203 «Информационная безопасность».

1.3. Организация работы государственной аттестационной комиссии.

Основные функции государственной аттестационной комиссии:

- комплексная оценка подготовки каждого выпускника СПО по специальности 100203 «Информационная безопасность»;
- принятие решения о присвоении профессиональной квалификации каждому выпускнику СПО по специальности 100203 «Информационная безопасность» и выдача соответствующего диплома государственного образца о среднем профессиональном образовании;
- анализ организации и содержания итоговой государственной аттестации в колледже;
- оценка уровня образования, осуществляемого СПО, его соответствие требованиям Государственного образовательного стандарта по специальности 100203 «Информационная безопасность»;
- разработка рекомендаций по совершенствованию подготовки специалистов по специальности 100203 «Информационная безопасность».

1.4. Расписание проведения итоговой Государственной аттестации выпускников

утверждается и доводится до сведения студентов не позднее, чем за 2 недели до начала работы государственной аттестационной комиссии.

Прием итогового комплексного экзамена осуществляется в специально подготовленном и оборудованном кабинете на открытых заседаниях государственной аттестационной комиссии с участием не менее двух третей ее состава.

В государственную аттестационную комиссию представляются следующие документы:

- приказ о составе государственной аттестационной комиссии;
- приказ о допуске студентов к итоговой государственной аттестации;
- государственные требования к минимуму содержания и уровню подготовки выпускников и дополнительные требования СПО;
- программа итоговой государственной аттестации;
- сводные ведомости успеваемости студентов;
- перечень наглядных пособий, материалов справочного характера, нормативных документов, разрешенных к использованию на экзамене;
- аттестационные материалы (экзаменационные билеты);

- протоколы итоговой государственной аттестации;
- экзаменационные ведомости;
- зачетные книжки студентов.

Каждое заседание государственной аттестационной комиссии протоколируется. Протоколы подписываются председателем, заместителем председателя, членами и секретарем комиссии.

Государственная аттестационная комиссия по результатам своей работы оформляет следующие документы:

- ведомости с оценками аттестуемых по итогам комплексного экзамена;
- протокол с оценками по итогам комплексного экзамена;
- протокол решения государственной аттестационной комиссии о присвоении квалификации по специальности 100203 «Информационная безопасность» и о выдаче диплома о среднем профессиональном образовании выпускникам;
- зачетные книжки студентов;
- отчет государственной аттестационной комиссии.

1.5. Отчет государственной аттестационной комиссии.

В отчете должна быть отражена следующая информация:

- качественный состав государственной аттестационной комиссии;
- вид итоговой государственной аттестации;
- характеристика общего уровня подготовки студентов по специальности 100203 «Информационная безопасность»;
- количество дипломов с отличием;
- анализ результатов итоговой государственной аттестации;
- недостатки в подготовке выпускников;
- выводы и предложения.

1.6. Экзамен по специальности проводится по группе дисциплин, определяемых с учетом профиля подготовки по данной специальности и направлен на выявление готовности выпускника к профессиональной деятельности.

В указанную группу входят:

- Организационно – правовое обеспечение информационной безопасности;
- Криптографические средства и методы защиты информации;
- Алгоритмизация и программирования;

Комплексный государственный экзамен по 100203 «Информационная безопасность» включает в себя содержание 3-х дисциплин:

1. Организационно – правовое обеспечение информационной безопасности;
2. Криптографические средства и методы защиты информации;
3. Алгоритмизация и программирования;

Каждый экзаменационный билет включает по 1 вопросу:

1. Организационно – правовое обеспечение информационной безопасности;
2. Криптографические средства и методы защиты информации;
3. Алгоритмизация и программирования;

Разрабатываемые экзаменационные материалы должны отражать весь объем проверяемых теоретических знаний и практических умений в соответствии с Государственными требованиями и дополнительными требованиями колледжа по специальности.

Экзаменационные материалы формируются на основе действующих учебных программ общепрофессиональных и специальных дисциплин, программ производственной (профессиональной) практики с учетом их объема и степени важности для данной специальности.

1.7. Содержание итогового государственного комплексного экзамена

По дисциплине: «Организационно-правовое обеспечения информационной безопасности» \ «Маалыматтык коопсуздукту уюштуруучулук жана укуктук камсыздоо»

1. Правовая база обеспечения информационной безопасности личности (общества, государства) / Инсандын (коомдун, мамлекеттин) маалыматтык коопсуздугун камсыз кылуунун укуктук негиздери.
2. Внешние (внутренние) источники угроз информационной безопасности государства / Мамлекеттин маалыматтык коопсуздугуна коркунучтун тышкы (ички) булактары.
3. Информационное оружие, его классификация и возможности / Маалыматтык куралдар, алардын классификациясы жана мүмкүнчүлүктөрү.
4. Модели, стратегии и системы обеспечения информационной безопасности / Маалыматтык коопсуздукту камсыз кылуунун моделдери, стратегиялары жана системалары.
5. Компьютерная система как объект информационной безопасности / Компьютердик система маалыматтык коопсуздуктун объектиси катары.
6. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности / Маалыматтык коопсуздукту камсыз кылуунун уюштуруу укуктук, техникалык жана криптографиялык ыкмалары.
7. Программно-аппаратные средства обеспечения информационной безопасности / Маалыматтык коопсуздукту камсыз кылуу үчүн программалык жана техникалык каражаттар.

8. . Определить место информационной безопасности в обеспечении системы общественной безопасности / Мамлекеттик коопсуздук системасын камсыз кылууда маалыматтык коопсуздуктун ордун аныктоо.
9. Классифицировать виды каналов несанкционированного доступа к информации / Маалыматка уруксатсыз жетүү үчүн каналдардын түрлөрүн классификациялаңыз.
10. Основные направления правовой защиты информации / Маалыматты укуктук коргоонун негизги багыттары.
11. Порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Кыргызской Республики о СМИ / Кыргыз Республикасынын жалпыга маалымдоо каражаттары жөнүндө мыйзамдары менен жарандардын жеке сырына жана жеке турмушуна болгон укуктарын коргоонун тартиби.
12. Объекты интеллектуальной собственности, защищаемые патентным законодательством / Патенттик мыйзамдар менен корголуучу интеллектуалдык менчик объектилер.
13. Дать определение государственной тайны и назвать грифы секретности / Мамлекеттик сырларга аныктама бериңиз жана купуялуулуктун классификациясын атаңыз.
14. Порядок отнесения сведений к государственной тайне и их засекречивая / Маалыматтарды мамлекеттик сырга киргизүүнүн жана аны жашыруун сырга киргизүүнүн тартиби.
15. Прогресс информационных технологий и информационной безопасности / Маалыматтык технологиялардын жана маалыматтык коопсуздуктун прогресси.
16. Нормативно-правовые аспекты информационной объектов / Маалымат объектеринин ченемдик-укуктук аспектилер.
17. Классификация угроз безопасности информационных объектов / Маалыматтык объектердин коопсуздук коркунучтарынын классификациясы.
18. Умышленные и неумышленные угрозы информационной безопасности / Маалыматтык коопсуздукка атайын жана кокустан боло турган коркунучтар.
19. Внешние угрозы информационной безопасности / Маалыматтык коопсуздуктун тышкы коркунучтары.
20. Статьи уголовного кодекса о компьютерных преступлениях / Кылмыш-жаза кодексинин компьютердик кылмыштар боюнча беренелери.
21. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение / Компьютердик маалымат чөйрөсүндөгү кылмыштардын криминологиялык мүнөздөмөлөрү жана алардын алдын алуу.
22. Программно-технические методы обеспечения информационной безопасности / Маалыматтык коопсуздукту камсыз кылуунун программалык-аппараттык ыкмалары.
23. Концепция информационной безопасности Кыргызской Республики / Кыргыз Республикасынын маалыматтык коопсуздугунун концепциясы.
24. Государственное регулирование информационной безопасности в Кыргызской Республики / Кыргыз Республикасында маалыматтык коопсуздукту мамлекеттик жөнгө салуу.
25. Человеческие факторы, обуславливающие информационные угрозы / Маалыматтык коркунучтарды пайда кылуучу адам факторлору.
26. Уголовно-правовая характеристика компьютерных преступлений / Компьютердик кылмыштардын кылмыш-укуктук мүнөздөмөсү.

27. Субъективная и объективная сторона компьютерных преступлений / Компьютердик кылмыштардын субъективдүү жана объективдүү жагы.
28. Способы совершения компьютерных преступлений / Компьютердик кылмыштарды жасоонун ыкмалары.
29. Причины и условия, способствующие совершению компьютерных преступлений / Компьютердик кылмыштарды жасоого көмөктөшүүчү себептер жана шарттар.
30. Меры предупреждения преступлений в сфере компьютерной информации / Компьютердик маалымат чөйрөсүндө кылмыштуулуктун алдын алуу боюнча чаралар.

По дисциплине: «Криптографические средства и методы защиты информации» / «Маалыматты коргоонун криптографиялык каражаттары жана ыкмалары»

1. Что такое ключ в криптографии и зачем он нужен? / Криптографияда ачкыч деген эмне жана ал эмне үчүн керек?
2. Каким образом криптография может помочь в защите данных при передаче через сеть? / Тармак аркылуу берүүдө Криптография маалыматтарды коргоого кандайча жардам берет?
3. Какие вызовы и угрозы существуют для современных криптографических систем, и каковы способы их преодоления? /Заманбап крипто системалары үчүн кандай чакырыктар жана коркунучтар бар жана аларды жеңүүнүн кандай жолдору бар?
4. Обеспечения безопасности в системах умного дома. / Акылдуу үй системаларында коопсуздукту камсыз кылуу.
5. Какую роль играет квантовая криптография в современной защите информации? / Заманбап маалыматты коргоодо кванттык криптография кандай роль ойнойт?
6. Как работает процесс шифрования и дешифрования данных? / Маалыматтарды шифрлөө жана чечмелөө процесси кандайча иштейт?
7. Какие основные типы шифрования существуют? Расскажите о различиях между симметричным и асимметричным шифрованием. / Шифрлөөнүн негизги түрлөрү кандай? Симметриялык жана асимметриялык шифрлөөнүн айырмачылыктарын айтып бергиле.
8. Что такое атаки на криптографические хэш-функции? Какие методы защиты от них существуют? / Криптографиялык хэш функцияларына кол салуу деген эмне? Алардан коргонуунун кандай ыкмалары бар?
9. Какие роли выполняют асимметричное и симметричное шифрование в современных системах безопасности? / Заманбап коопсуздук тутумдарында асимметриялык жана Симметриялык шифрлөө кандай ролдорду аткарат?
10. Каким образом криптография влияет на различные области, такие как финансы. / Криптография каржы сыяктуу ар кандай тармактарга кандайча таасир этет.
11. Какие алгоритмы криптографии чаще всего используются в протоколах безопасной связи в Интернете. / Интернеттеги коопсуз байланыш протоколдорунда кайсы криптографиялык алгоритмдер көп колдонулат.
12. Что такое хэш-функция? Для чего они используются в криптографии? / Хэш функциясы деген эмне? Алар криптографияда эмне үчүн колдонулат?

13. Что такое шифрование и зачем оно используется? / Шифрлөө деген эмне жана ал эмне үчүн колдонулат?
14. Что такое электронная подпись и для чего она используется в контексте криптографии? / Электрондук кол тамга деген эмне жана ал криптографиянын контекстинде эмне үчүн колдонулат?
15. Тип алгоритмов шифрования вы знаете и в чем их основные различия? / Шифрлөө алгоритмдеринин түрүн билесизби жана алардын негизги айырмачылыктары эмнеде?
16. Что такое аутентификация и как она связана с криптографией в системах безопасности? / Аутентификация деген эмне жана анын коопсуздук тутумдарындагы Криптография менен кандай байланышы бар?
17. Шифр Цезаря. / Цезардын Шифри.
18. Конфиденциальность и целостность данных при передаче через интернет? / Интернет аркылуу өткөрүүдө маалыматтардын купуялуулугу жана бүтүндүгү?
19. Безопасность данных в облаке при передаче и хранении информации? / Маалыматты берүү жана сактоо учурунда Булуттагы маалыматтын коопсуздугу?
20. Как работает и зачем нужен цифровой ключ в криптографии? / Криптографияда санариптик ачкыч кантип иштейт жана эмне үчүн керек?
21. Каким образом криптография влияет на обеспечение конфиденциальности при использовании систем умного видеонаблюдения и безопасности дома? / Акылдуу видеобайкоо жана үйдөгү коопсуздук тутумдарын колдонууда Криптография купуялуулукка кандай таасир этет?
22. Квантовая криптография. / Кванттык криптография.
23. Как криптография применяется для обеспечения конфиденциальности и безопасности в области государственных информационных систем и правительственных служб. / Мамлекеттик маалымат тутумдарынын жана мамлекеттик кызматтардын купуялуулугун жана коопсуздугун камсыз кылуу үчүн криптография кандайча колдонулат?
24. Криптография и защита информации. / Криптография жана маалыматты коргоо.
25. Аутентификация и контроль доступа. / Аутентификация жана кирүүнү көзөмөлдөө.
26. Аутентификация и контроль доступа. / Аутентификация жана кирүүнү көзөмөлдөө.
27. Многофакторная аутентификация. / Көп факторлуу аутентификация.
28. Какая основная цель использования криптографии в повседневной жизни? / Күнүмдүк жашоодо криптографияны колдонуунун негизги максаты эмнеде?
29. Какие методы аутентификации применяются в криптографии для подтверждения личности в системах биометрической идентификации? / Биометрикалык идентификация тутумдарында инсандыкты тастыктоо үчүн криптографияда кандай аутентификация ыкмалары колдонулат?
30. Какие виды алгоритмов шифрования вы знаете? / Шифрлөө алгоритмдеринин кандай түрлөрүн билесиз?

По дисциплине «Алгоритмизация и программирования» / «Алгоритмдөө жана программалоо»

1. Какие базовые типы данных предоставляет язык программирования C#? / C# программалоо тили кандай негизги маалымат түрлөрүн камсыз кылат?
2. Какова разница между значимыми (value types) и ссылочными (reference types) типами данных в C#? / C# программалоо тилиндеги маанилердин түрлөрү (value types) менен маалымдама түрлөрүнүн (reference types) ортосунда кандай айырма бар?
3. Что такое переменная и какой тип данных ей можно присвоить в C#? / Өзгөрмө (перменный) деген эмне жана ага C# тилинде кандай маалымат түрүн ыйгарса болот?
4. Как объявить массив в C# и какие типы данных могут быть использованы в массиве? / C# тилинде массивди кантип жарыялоо керек жана массивде кандай маалымат түрлөрүн колдонсо болот?
5. Какие специальные типы данных в C# предназначены для работы с логическими значениями и чем они отличаются от числовых типов данных? / C# тилиндеги кандай атайын маалымат түрлөрү логикалык маанилер менен иштөө үчүн иштелип чыккан жана алар сандык маалымат түрлөрүнөн (числовые типы данных) эмнеси менен айырмаланат?
6. Каким образом можно передавать параметры в функции и возвращать значения из них в C#? Расскажите о различных типах параметров и возвращаемых значений. / Кантип C# ичинде функцияларга параметрлерди өткөрүп, алардын маанилерин кайтара аласыз? Параметрлердин ар кандай түрлөрүн жана кайтарым маанилерин түшүндүрүңүз.
7. Как работают локальные переменные в функциях C# и почему они считаются важными для обеспечения безопасности и эффективности кода? / Жергиликтүү (локальные) өзгөрмөлөр C# функцияларында кантип иштешет жана эмне үчүн алар коопсуздук жана эффективдүү код үчүн маанилүү деп эсептелет?
8. Что такое тип данных в C# / C# тагы маалымат түрү деген эмне?
9. Какие ключевые слова используются для объявления переменных различных типов данных в C#? / Кандай ачкыч сөздөр C# та ар кандай маалымат типтеринин өзгөрмөлөрүн жарыялоо үчүн колдонулат?
10. Какой тип данных используется для хранения чисел с плавающей точкой в C#? C# тилинде калкыма чекиттерди сактоо үчүн кандай маалымат түрү колдонулат?
11. Чем отличаются типы данных int и long в C#? / C# тагы int жана long маалымат түрлөрүнүн ортосунда кандай айырма бар?
12. Что произойдет, если условие в операторе if не выполнится? / Эгерде оператордогу шарт (If) аткарылбаса эмне болот?
13. Какой будет результат выполнения кода, если условие в операторе if выполняется? / Кыймыл операторундагы шарт (if) аткарылса, коддун аткарылышынын натыйжасы кандай болот?
14. Как создать многомерный массив c#? / C# тилинде көп өлчөмдүү массивди кантип түзүүгө болот?
15. Какой синтаксис использовать, если нужно написать оператор if с несколькими условиями? / Операторду жазуу керек болсо, кайсы Синтаксисти колдонуу керек бир нече шарттар менен?

16. Какова разница между операторами if-else и switch-case в C#? / if-else жана switch-case операторлордун айырмасы эмнеде?
17. Можно ли вложить один оператор if в другой в C#? Если да, то как это сделать? / Бир операторду if экинчисинин ичине киргизуу мумкунбу C#? Андай болсо, муну кантип кыласыз?
18. Какая разница между оператором == и методом Equals () при сравнении строк в C# с использованием if-else? / If-else аркылуу C# тилиндеги саптарды салыштырганда == оператору менен Equals() методунун ортосунда кандай айырма бар?
19. Что такое массив, понятие, структуры и виды массива c#? / Массив деген эмне? Массив түшүнүгү, структуралары жана түрлөрү?
20. Какие типы данных могут содержать элементы массива c#? / Массив элементтери C# тилиндеги маалыматтардын кандай түрлөрүн камтышы мүмкүн?
21. Как определить количество элементов в массиве c#? / C# тилинде массивдеги элементтердин санын кантип аныктоого болот?
22. Какие методы предоставляются для работы с массивами в классе Array c#? / C# тилинде «Array» классында массивдер менен иштөө үчүн кандай ыкмалар каралган?
23. Какие существуют способы инициализации массива c#? / C# тилинде массивди инициализациялоонун кандай жолдору бар?
24. Какие 3 вида конструкций используются в структурном программировании? / Структуралык программалоодо конструкциялардын 3 түрү кандай?
25. С помощью каких служебных слов записывается оператор цикла с постусловием? / Кийинки шарттагы цикл билдирүүсү кандай кызматтык сөздөр менен жазылат?
26. Если условие продолжения цикла не определено на момент начала цикла, какой тип циклов предпочтительно использовать? / Эгерде циклды улантуу шарты цикл башталганда аныкталбаса, циклдын кайсы түрүн колдонуу артык?
27. Для чего применяются вложенные циклы в c#: / Уяланган циклдер эмне үчүн колдонулат c#:
28. Совместно с каким оператором обычно используются операторы break и continue в теле цикла? / break жана continue операторлору көбүнчө циклдин корпусунда кайсы оператор менен бирге колдонулат?
29. Какие 3 оператора используются для преждевременного выхода из цикла? / Циклден эрте чыгуу үчүн кандай 3 оператор колдонулат?
30. Сколько операторов break и/или continue может быть записано в теле цикла? / Канча операторлорду break/continue циклдин корпусуна жазууга болот?

1.8. Критерии оценки знаний студентов

ОИТ ПК СПО на итоговой государственной аттестации по специальности «Прикладная информатика»

Оценка «5» (отлично) ставится в том случае, если студент:

- обнаруживает знания программного материала, а также основного содержания лекционного курса по сравнению с учебной литературой;
- дает точное определение и понимание основных понятий и терминов;
- сопровождает ответ примерами, умеет применять знания в конкретной ситуации;
- может работать со справочной литературой.

Оценка «4» (хорошо) ставится, если студент:

- неполно излагает материал и допускает не существенные ошибки в определении и толковании основных понятий и терминов;
- допускает незначительные ошибки;
- приводит примеры, но недостаточно четко комментирует их.

Оценка «3» (удовлетворительно) ставится, если студент:

- обнаружил отдельные пробелы в знании дисциплины;
- умеет применять полученные знания, но затрудняется прокомментировать.

Оценка «2» (неудовлетворительно) ставится, если студент:

- не овладел основными знаниями и умениями в соответствии с требованиями программы по специальности.

Литература

«Организационно-правовое обеспечения информационной безопасности»

Основная литература:

1. Ярочкин В.И. Информационная безопасность, учебник М.:2005
2. Лапоница О.Р. Основы безопасности компьютерных сетей, учебник М.:2003
3. Стрельцов А.А. Обеспечение информационной безопасности России . – М., 2002
4. Ярочкин В.И. Информационная безопасность: учебное пособие [Текст]. – М, 2000
5. Чеботарева А.А. Научные подходы к определению понятия «информационная безопасность» // Информационное право. 2011.
6. Чеботарева А.А. Теоретико-правовое исследование понятия «информационная безопасность личности» // Юридический мир. 2010.
7. Чеботарева А.А. Обеспечение информационной безопасности в Интернете: история и проблемы развития законодательства // История государства и права. 2010. №11
8. Аксенов С.Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти // Безопасность бизнеса. 2008.

Дополнительная литература:

1. Куприянов А.И., Сахаров А.В., Щевцов В.А., Основы защиты информации, уч. пособие М.:2008
2. Девякин П.Н., Модели безопасности компьютерных систем, уч. пособие М.:2005

Электронные ресурсы:

1. <http://www.ict.edu.ru/catalog/index.php>
2. [www. Intuit.ru](http://www.Intuit.ru)

«Криптографические средства и методы защиты информации»

Основная литература:

1. В.М. Фомичев, Д.А. Мельников Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: Учебник Юрайт, 2018
2. М. В. Адаменко Основы классической криптологии: секреты шифров и кодов: ДМК Пресс, 2016

3. Л.К. Бабенко, Е.А. Ищукова Криптографическая защита информации: симметричное шифрование: Учебное пособие Юрайт, 2018
4. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линияТелеком, 2016. — 232 с.
5. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — 2-е изд., перераб. и доп. — М.: Горячая линия-Телеком, 2002. — 176 с.
6. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с.

Дополнительная литература:

1. Фомичев В.М., Мельников Д.А. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В 2 Ч. ЧАСТЬ 2. СИСТЕМНЫЕ И ПРИКЛАДНЫЕ АСПЕКТЫ. Учебник для академического бакалавриата: Гриф УМО ВО М.:Издательство Юрайт, 2018
2. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 [1] с.
3. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ:

Электронные ресурсы:

1. portal.edu.asu.ru

«Алгоритмизация и программирования»

Основная литература:

1. Канцедал С. А. Алгоритмизация и программирование : Учебное пособие / С.А. Канцедал. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 352 с.: ил. - ISBN 978-5-8199-0355-1. - Режим доступа : <http://znanium.com/bookread.php?book=391351>.
2. Колдаев В. Д. Основы алгоритмизации и программирования [Электронный ресурс] : учебное пособие / В. Д. Колдаев; под ред. Л.Г. Гагариной. - Москва: ФОРУМ, 2012. - 416 с. - (Профессиональное образование). - ISBN 978-5-8199-0279-0. - Режим доступа: <http://znanium.com/go.php?id=336649>.
3. Конова Е.А. Алгоритмы и программы. Язык С++ [Электронный ресурс] : учеб. пособие / Е.А. Конова, Г.А. Поллак. - Санкт-Петербург : Лань, 2017. - 384 с. - ISBN 9978-5-8114-2020-9. - Режим доступа: <https://e.lanbook.com/book/90158>. 7.2.

Дополнительная литература:

1. Колдаев В. Д. Структуры и алгоритмы обработки данных [Электронный ресурс] : учебное пособие / В. Д. Колдаев. - Москва: ИЦ РИОР, 2014. - 296 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01264-2. - Режим доступа: <http://znanium.com/go.php?id=418290>.
2. Серебряков В. А. Теория и реализация языков программирования [Текст] / В. А. Серебряков. - Москва : Физматлит, 2012. - 235 с. : табл., рис. - Библиогр.: с. 234-235. - ISBN 978-5-9221-1417-2 - Точка доступа : http://e.lanbook.com/books/element.php?pl1_id=5294.
3. Немцова Т. И. Программирование на языке высокого уровня. Программир. на языке

- C++: Уч. пос. / Т.И.Немцова и др.; Под ред. Л.Г.Гагариной - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 512 с.: ил. - ISBN 978-5-8199-0492-3. - Точка доступа : <http://znanium.com/bookread.php?book=244875>.
4. Окулов С.М. Основы программирования [Электронный ресурс] : учеб. пособие / С. М. Окулов. - Москва : Издательство 'Лаборатория знаний', 2015. - 339 с. - ISBN 978-5-9963-2917-5. - Режим доступа: <https://e.lanbook.com/book/66119>. Программа дисциплины "Основы алгоритмизации и программирование"; 27.03.04 Управление в технических системах; старший преподаватель, б/с Мышкина И.Ю. Регистрационный номер 900641518 Страница 14 из 16.
5. Златопольский Д.М. Программирование: типовые задачи, алгоритмы, методы [Электронный ресурс] / Д. М. Златопольский. - Москва : Издательство 'Лаборатория знаний', 2015. - 226 с. - ISBN 978-5-9963-2932-8. - Режим доступа: <https://e.lanbook.com/book/70753>.

Электронные ресурсы:

1. MSDN - сеть разработчиков Microsoft - <https://msdn.microsoft.com/ru-ru/dn308572.aspx>
2. RSDN : сайт, посвященный разработке программного обеспечения - <http://rstdn.ru>
3. Клуб программистов - <http://www.programmersclub.ru>