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

Колледж

УТВЕРЖДАЮ
директор Колледжа ДГУ
Д.Ш. Пирбудагова
«30» 04 2022г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

МДК.02.03. КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Махачкала - 2022

Составители:

Шахбанова М.И. - преподаватель кафедры естественно-научных и гуманитарных дисциплин Колледжа ФГБОУ ВО «Дагестанский государственный университет»

Шахбанова З.И. - к.э.н., доцент кафедры прикладной информатики в экономике факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Фонд оценочных средств дисциплины рассмотрен и рекомендован к утверждению кафедрой специальных дисциплин Колледжа ДГУ.

Протокол №__8__ от «30» 04 2022 г.

Зав.кафедрой специальных дисциплин к.ю.н.,доцент _____/Магомедова К.К./

Утвержден на заседании учебно-методического совета Колледжа ДГУ

Ст. методист _____/Шамсутдинова У.А./
подпись *Фамилия И.О.*

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
МДК.02.03. КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
1	**Раздел 1.** Основные понятия и характеристика шифров	ОК 1, ОК 2, ОК 3, ОК 4, ПК. 2.1, ПК. 2.2, ПК. 2.6.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	**2**	**3**	**4**
1.	Деловая и/или ролевая игра	Совместная деятельность группы обучающихся и педагогического работника под управлением педагогического работника с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема), концепция, роли и ожидаемый результат по каждой игре
2.	Кейс-задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.	Задания для решения кейс-задачи
3.	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования педагогического работника с обучающимися.	Вопросы по темам/разделам дисциплины
4.	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Комплект контрольных заданий по вариантам
5.	Круглый стол, дискуссия, полемика, диспут, дебаты	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.	Перечень дискуссионных тем.
6.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио

7.	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала.	Образец рабочей тетради
8.	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умение обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированное аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных проектов
9.	Разно-уровневые задачи и задания	*Различают задачи и задания:* а) репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; б) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; в) творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разно-уровневых задач и заданий
10.	Расчетно-графическая работа	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	Комплект заданий для выполнения расчетно-графической работы

11.	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов

КРИТЕРИИ ОЦЕНКИ
по дисциплине
МДК.02.03. КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Критерии оценки:

Оценка «отлично»: правильно выполнены все задания практической работы, правильно даны ответы на все контрольные вопросы, выполнены задания самостоятельной работы в полном объеме. Студент отвечает на вопросы, демонстрируя глубокие знания.

Оценка «хорошо»: выполнены все задания практической и контрольной работы с наличием несущественных ошибок, выполнены задания самостоятельной работы в неполном объеме, не противоречащих основным понятиям дисциплины. Студент уверенно отвечает на вопросы, демонстрируя достаточно высокий уровень знаний

Оценка «удовлетворительно»: выполнены все задания практической и контрольной работы с наличием грубых ошибок, выполнены задания самостоятельной работы в неполном объеме, противоречащих или искажающих основные понятия дисциплины. Студент демонстрирует достаточный уровень знаний, однако затрудняется отвечать на некоторые вопросы

Оценка «неудовлетворительно»: выполнены не все задания практической работы, даны не все ответы на контрольные вопросы, имеются грубые ошибки в выполнении практических заданий и/или ответах на контрольные вопросы, противоречащие или искажающие основные понятия дисциплины, самостоятельная работа не выполнена, либо выполнена на 50%. Студент затрудняется отвечать на вопросы.

Вопросы к экзамену:

1. Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п.
2. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке.
3. Установка и настройка агентского мониторинга.
4. Проведение синхронизации с LDAPсервером, разделе персоны.
5. Запуск системы корпоративной защиты от внутренних угроз.
6. Угрозы информационной безопасности.
7. Изучение структуры организации на основании полученных материалов («модели организации»), проведение обследования корпоративных информационных систем. Определение объекта защиты.
8. Перечень субъектов/персон сформулированных верно, роли пользователей, права доступа.
9. Политика безопасности.
10. Разработка новой и/или модифицирование существующей политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания.
11. Использование различных технологий защиты: печатей, бланков, графических объектов, баз данных и т.п.
12. Модифицирование политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата.
13. Применение политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности.
14. Работа с интерфейсом управления системы корпоративной защиты информации.
15. Технология анализа и защиты сетевого трафика.
16. Развёртывание, настройка и проверка работоспособности VPN -сети на существующей и вычислительной инфраструктуре.
17. Развёртывание, настройка и проверка работоспособности IDS -системы на существующей и вычислительной.
18. Работа с узлами и пользователями. VPN. Компрометация узлов, ключей, пользователей. Восстановление связи.
19. Обновление ключевой информации. VPN. Межсетевое взаимодействие и туннелированные. VPN.
20. Централизованная политика безопасности.
21. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий.
22. Технологии агентского мониторинга.
23. Демонстрация знания механизмов работы агентского мониторинга.

24. Разработать и применить политику агентского мониторинга для работы с носителями и устройствами.
25. Разработка и применение политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата.
26. Анализ выявленных инцидентов. Подготовка отчётов о нарушениях.
27. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов.
28. Проведение классификацию уровня угроз инцидентов.
29. Оценка ущерба. Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса.
30. Выявление инцидентов и противодействие нарушителям с опорой на нормативную базу.

Кейс-задание

Задание

В следующем исходном коде показана стандартная структура теста Golang с использованием Terratest:

```
package test

import (
   "testing"

   "github.com/gruntwork-io/terratest/modules/terraform"
   test_structure "github.com/gruntwork-io/terratest/modules/test-structure"
)

func TestEndToEndDeploymentScenario(t *testing.T) {
   t.Parallel()

   fixtureFolder := "../"

   // User Terratest to deploy the infrastructure
   test_structure.RunTestStage(t, "setup", func() {
      terraformOptions := &terraform.Options{
         // Indicate the directory that contains the Terraform configuration to deploy
         TerraformDir: fixtureFolder,
      }

      // Save options for later test stages
      test_structure.SaveTerraformOptions(t, fixtureFolder, terraformOptions)

      // Triggers the terraform init and terraform apply command
      terraform.InitAndApply(t, terraformOptions)
   })
```

```
    test_structure.RunTestStage(t, "validate", func() {
        // run validation checks here
        terraformOptions := test_structure.LoadTerraformOptions(t, fixtureFolder)
            publicIpAddress := terraform.Output(t, terraformOptions,
"public_ip_address")
    })

    // When the test is completed, teardown the infrastructure by calling terraform
destroy
    test_structure.RunTestStage(t, "teardown", func() {
        terraformOptions := test_structure.LoadTerraformOptions(t, fixtureFolder)
        terraform.Destroy(t, terraformOptions)
    })
}
```

Как видно из предыдущего фрагмента кода, этот тест включает следующие этапы:

а) настройка (Terraform запускается для развертывания конфигурации);
б) проверка (Выполняются проверки и утверждения);
в) демонтаж (Инфраструктура очищается после выполнения теста);
г) все этапы.

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично;

допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений):

1. Информация и информационные потоки.
2. Внутренние и внешние угрозы ИБ.
3. Модели угроз ИБ.
4. Классификация нарушителей корпоративной ИБ.
5. Особенности оценки ущерба.
6. Системы DLP и требования по информационной безопасности.
7. Категорирование информации в РФ.
8. Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; специальные технические средства.
9. Меры по обеспечению юридической значимости DLP (Pre-DLP).
10. Обзор практики право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).
11. Формирование процессов и процедур аудита ИБ.
12. Обследование корпоративных информационных систем.
13. Состояние корпоративной информации.
14. Инструменты и технологии обеспечения корпоративной защиты от внутренних угроз.
15. Критерии эффективности проекта по обеспечению корпоративной защиты от внутренних угроз.
16. Препятствия реализации проектов по обеспечению корпоративной защиты от внутренних угроз.
17. Назначение системы IW Traffic monitor (IW TM).
18. Контролируемые каналы передачи данных.
19. Архитектура продукта IW TM.
20. Технологии анализа детектируемых объектов.
21. Задачи и принципы работы дополнительных модулей системы IW Device monitor (IW DM) и IW Crawler.

Структура итогового теста:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования

MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Корпоративная защита от внутренних угроз информационной безопасности»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	Оценка знаний
90-100	5 «отлично»
80-89	4 «хорошо»
70-79	3 «удовлетворительно»
Менее 70	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ)

1. Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:
    а) отнесенные к государственной тайне;
    б) отнесенные к служебной тайне (информации для служебного пользования),персональные данные (и другие виды тайн);
    в) отнесенные к информации о прогнозах погоды;
    г) все верны ответы.
2. К информации ограниченного доступа относятся:
    а) государственная тайна;
    б) конфиденциальная информация;
    в) персональные данные;
    г) все ответы верны.
3. К методам защиты корпоративной информационной среды относятся:
    а) система управления идентификацией и доступом пользователей (Identity and Access Management (IAM)); система управления событиями информационной безопасности (Security Information Event Management (SIEM)); средства предотвращения потери данных (Data Loss/Leak Prevention (DLP));
    б) система управления идентификацией и доступом пользователей (Identity and Access Management (IAM)); система управления событиями информационной безопасности (Security Information Event Management (SIEM)).
4. Средства предотвращения потери данных (Data Loss/Leak Prevention (DLP)) это:
    а) контроль рабочих станций сотрудников, контроль трафика корпоративной сети, контроль сетевых хранилищ информации;
    б) контроль рабочих станций сотрудников, контроль трафика корпоративной сети, контроль сетевых хранилищ информации, контроль посещения работы.
5. Установка, конфигурирование и устранение неисправностей в системах корпоративной защиты от внутренних угроз входит следующее:
    а) DLP – применение (IW Traffic Monitor);
    б) Linux, Windows администрирование DLP – установка, VPN установка/настройка, настройка политик домена;
    в) технологии агентского мониторинга.
6. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз включает:
    а) установка, конфигурирование и устранение неисправностей в системах корпоративной защиты от внутренних угроз;

б) исследование (аудит) организации с целью защиты от внутренних угроз;
в) DLP – применение (IW Traffic Monitor)

7. Основными источниками угроз информационной безопасности являются все указанное в списке?
   а) хищение жестких дисков, подключение к сети, инсайдерство;
   б) перехват данных, хищение данных, изменение архитектуры системы;
   в) хищение данных, подкуп системных администраторов, нарушение регламента работы.
8. Наиболее важным при реализации защитных мер политики безопасности является:
   а) аудит, анализ затрат на проведение защитных мер
   б) аудит, анализ безопасности
   в) аудит, анализ уязвимостей, риск-ситуаций
9. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
   а) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования;
   б) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации;
   в) улучшить контроль за безопасностью этой информации;
   г) снизить уровень классификации этой информации.
10. Что самое главное должно продумать руководство при классификации данных?
   а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным;
   б) Необходимый уровень доступности, целостности и конфиденциальности
   в) Оценить уровень риска и отменить контрмеры
   г) Управление доступом, которое должно защищать данные
11. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
   а) поддержка высшего руководства
   б) эффективные защитные меры и методы их внедрения
   в) актуальные и адекватные политики и процедуры безопасности
   г) ароведение тренингов по безопасности для всех сотруднико
12. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности
   а) список стандартов, процедур и политик для разработки программы безопасности;
   б) текущая версия iso 17799;
   в) структура, которая была разработана для снижения внутреннего мошенничества в компаниях;

г) открытый стандарт, определяющий цели контроля.

13. К внутренним нарушителям информационной безопасности относится:
    а) клиенты;
    б) пользователи системы;
    в) посетители;
    г) любые лица, находящиеся внутри контролируемой территории;
    д) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
    е) персонал обслуживающий технические средства;
    ж) сотрудники отделов разработки и сопровождения ПО;
    з) технический персонал, обслуживающий здание.
14. Активный перехват информации это перехват, который: Варианты ответа:
    а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
    б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
    в) неправомерно использует технологические отходы информационного процесса; г) осуществляется путем использования оптической техники;
    г) осуществляется с помощью подключения телекоммуникационному оборудованию компьютера.
15. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
    а) анализ связующего дерева;
    б) AS/NZS;
    в) NIST;
    г) анализ сбоев и дефектов.
16. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
    а) NIST и OCTAVE являются корпоративными;
    б) NIST и OCTAVE ориентирован на ИТ;
    в) AS/NZS ориентирован на ИТ;
    г) NIST и AS/NZS являются корпоративными;
17. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
    а) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам;
    б) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень;
    в) COSO учитывает корпоративную культуру и разработку политик;
    г) COSO – это система отказоустойчивости.
18. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

а) чтобы убедиться, что проводится справедливая оценка;
б) для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ;
в) поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа;
г) поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.

20. WorldSkills - это:
а) международное некоммерческое Движение, целью которого является повышение престижа рабочих профессий и развитие профессионального образования путем гармонизации лучших практик и профессиональных стандартов во всем мире посредством организации и проведения конкурсов по профессиональному мастерству, как в каждой из 80+ стран-членов Движения WSI, так в мире в целом;
б) форма оценки соответствия уровня знаний, умений, навыков студентов и выпускников, осваивающих программы подготовки квалифицированных рабочих, служащих, специалистов среднего звена, позволяющих вести профессиональную деятельность в определенной сфере и (или) выполнять работу по конкретным профессии или специальности в соответствии со стандартами Ворлдсиллзт Россия.

Основная литература:

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2020. - 161 с. - (Профессиональное образование). - ISBN 978-5-534-13948-8. - Текст: электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/467356 .
2. Моргунов А.В. Информационная безопасность: учебно-методическое пособие Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 83 с.: ил., табл. - 978-5- 7782-3918-0 https://biblioclub.ru/index.php?page=book&id=576726
3. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2022. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497642

Дополнительная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2022. - 161 с. - (Высшее образование). - ISBN 978-5-534-07248-8. - URL : https://urait.ru/bcode/490277
2. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. - 2-е изд., испр. и доп. - Москва : Издательство Юрайт, 2021. - 246 с. - (Высшее образование). - ISBN 978-5-534-01679-6. - URL : https://urait.ru/bcode/468273
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва : Издательство Юрайт, 2022. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - URL : https://urait.ru/bcode/490019
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. www.standartgost.ru 3. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru
5. 5. ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru 5. ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» www.standartgost.ru

Интернет-ресурсы:

1. Библиотека Альдебаран – компьютерная литература [Электронный ресурс]. – Режим доступа: http://www.aldebarans.ru/komp, свободный. – Загл. с экрана.
2. Википедия – Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org, свободный. – Загл. с экрана.
3. Официальный сайт Министерства образования и науки Российской Федерации. – Режим доступа: http://www.mon.gov.ru, свободный. – Загл. с экрана.
4. Педагогика.ру – Справочный сайт [Электронный ресурс]. – Режим доступа: http://www.pedagogy.ru, свободный. – Загл. с экрана.
5. Портал нормативно-технической документации [Электронный ресурс]. – Режим доступа: http://www.pntdoc.ru, свободный. – Загл. с экрана.
6. Российское образование. Федеральный портал [Электронный ресурс].. – Режим доступа: http://www.edu.ru, свободный. – Загл. с экрана.
7. Техническая литература [Электронный ресурс]. – Режим доступа: http://www.tehlit.ru, свободный. – Загл. с экрана