ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утверждены решением
Ученого совета ДГУНХ,
протокол № 9
от 24 марта 2025 г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ

«БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ
10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОФИЛЬ «БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень высшего образования - бакалавриат

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00C5A9FA0FAD6D6153888A98846B419FD3
Владелец: Бучаев Ахмед Гамидович
Действителен: с 11.07.2024 до 04.10.2025

.

Махачкала – 2025

УДК 681.518(075.8)
ББК 32.81.73

Составитель – Гасанова Зарема Ахмедовна, кандидат педагогических наук, и.о. зав. кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Газимагомедов Ахмед Абдуллаевич, кандидат экономических наук, главный специалист научно – организационного отдела ДНЦ РАН.

Представитель работодателя – Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза».

Оценочные материалы по дисциплине «Безопасность вычислительных сетей» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Оценочные материалы по дисциплине «Безопасность вычислительных сетей» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Оценочные материалы по дисциплине «Безопасность вычислительных сетей» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2025 г. – 39 с.

Рекомендованы к утверждению Учебно-методическим советом ДГУНХ 10 марта 2025 г.

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрены на заседании кафедры «Информационные технологии и информационная безопасность» 24 февраля 2025 г., протокол № 7.

СОДЕРЖАНИЕ

Назначение оценочных материалов……..4

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины …..…….……5

1.1 Перечень формируемых компетенций……5

1.2 Перечень компетенций с указанием видов оценочных средств…….5

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине……16

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания……..31

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций…….34

Лист актуализации оценочных материалов по дисциплине……..39

Назначение оценочных материалов

Оценочные материалы разрабатываются для текущего контроля успеваемости (оценивания хода освоения дисциплины), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Безопасность вычислительных сетей» в целях определения соответствия их учебных достижений поэтапным требованиям образовательной программы высшего образования по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем».

Оценочные материалы по дисциплине «Безопасность вычислительных сетей» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; контрольные задания или иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине; методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций.

Оценочные материалы сформированы на основе ключевых принципов оценивания:

– валидности: объекты оценки должны соответствовать поставленным целям обучения;

– надежности: использование единообразных стандартов и критериев для оценивания достижений;

– объективности: разные обучающиеся должны иметь равные возможности для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

– предметная направленность (соответствие предмету изучения конкретной дисциплины);

– содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);

– объем (количественный состав оценочных материалов);

– качество оценочных материалов в целом, обеспечивающих получение объективных и достоверных результатов при проведении контроля с различными целями.

Раздел 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины

1.1. Перечень формируемых компетенций

Код компетенции	Формулировка компетенции
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1.	Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
ПК-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей	ИПК-1.3. Администрирует подсистему защиты информации компьютерных сетей	**Знать:** – методологические и технические основы обеспечения информационной безопасности сетевых автоматизированных систем, основные приемы настройки подсистем информационной безопасности компьютерных сетей, типовые модели атак, направленных на преодоление защиты	Пороговый уровень	Обучающийся слабо (частично) знает методологические и технические основы обеспечения информационной безопасности сетевых автоматизированных систем, основные приемы настройки подсистем информационной безопасности компьютерных сетей, типовые модели атак, направленных на преодоление	**Блок А** – задания репродуктивного уровня: – вопросы для обсуждения; – тестовые задания.

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
		сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения, перспективные направления развития технологий обеспечения безопасности в сетях, современных проблемах науки информационной безопасности и роли и месте защиты информации в сетях при решении задач, связанных с обеспечением комплексной информационной безопасности.		защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения, перспективные направления развития технологий обеспечения безопасности в сетях, современных проблемах науки информационной безопасности и роли и месте защиты информации в сетях при решении задач, связанных с обеспечением комплексной информационной безопасности..	
			Базовый уровень	Обучающийся с не-значительными ошибками и отдельными пробелами знает методологическ	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				ие и технические основы обеспечения информационной безопасности сетевых автоматизированных систем, основные приемы настройки подсистем информационной безопасности компьютерных сетей, типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения, перспективные направления развития технологий обеспечения безопасности в сетях, современных проблемах науки	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				информационной безопасности и роли и месте защиты информации в сетях при решении задач, связанных с обеспечением комплексной информационной безопасности.	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает методологические и технические основы обеспечения информационной безопасности сетевых автоматизированных систем, основные приемы настройки подсистем информационной безопасности компьютерных сетей, типовые модели атак, направленных на преодоление защиты	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения, перспективные направления развития технологий обеспечения безопасности в сетях, современных проблемах науки информационной безопасности и роли и месте защиты информации в сетях при решении задач, связанных с обеспечением комплексной информационной безопасности..	
		Умеет: – проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной	Пороговый уровень	Обучающийся слабо (частично) умеет проводить анализ сетевых автоматизированных систем с точки зрения	**Блок В** – задания реконструктивного уровня – комплект тематик для рефератов.

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
		безопасности. – реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения. – разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства. – применять защищенные протоколы и межсетевые экраны, необходимые для реализации системы защиты информации в сетях		обеспечения информационной безопасности, реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения, разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства, применять защищенные протоколы и межсетевые экраны, необходимые для реализации системы защиты информации в сетях	
			Базовый уровень	Обучающийся с незначительными	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				затруднениями умеет проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности, реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения, разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства, применять защищенные протоколы и межсетевые экраны, необходимые для реализации	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				системы защиты информации в сетях	
			Продвинутый уровень	Обучающийся умеет проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности, реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения, разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства, применять защищенные протоколы и	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				межсетевые экраны, необходимые для реализации системы защиты информации в сетях	
		Владеть: – навыками комплексного анализа и оценки сетевой безопасности. – навыками комплексного проектирования, построения, обслуживания и администрирования защищенных вычислительных сетей. – навыками проектирования защищенных сетей с целью обеспечения надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации. – построения и эксплуатации вычислительн	Пороговый уровень	Обучающийся слабо (частично) владеет навыками комплексного анализа и оценки сетевой безопасности, комплексного проектирования, построения, обслуживания и администрирования защищенных вычислительных сетей, навыками проектирования защищенных сетей с целью обеспечения надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации, построения и	**Блок С** – задания практико-ориентированного уровня – комплект кейс-задач.

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
		ых сетей; – навыками использовать аппаратные и программные средства обеспечения информационной безопасности.		эксплуатации вычислительных сетей, использовать аппаратные и программные средства обеспечения информационной безопасности.	
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками комплексного анализа и оценки сетевой безопасности, комплексного проектирования, построения, обслуживания и администрирования защищенных вычислительных сетей, навыками проектирования защищенных сетей с целью обеспечения надежности функционирования и отказоустойчивости аппаратных и программных средств	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				обработки информации, построения и эксплуатации вычислительных сетей, использовать аппаратные и программные средства обеспечения информационной безопасности.	
			Продвинутый уровень	Обучающийся свободно владеет навыками комплексного анализа и оценки сетевой безопасности, комплексного проектирования, построения, обслуживания и администрирования защищенных вычислительных сетей, навыками проектирования защищенных сетей с целью обеспечения надежности функционирования и отказоустойчивости аппаратных и	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				программных средств обработки информации, построения и эксплуатации вычислительных сетей, использовать аппаратные и программные средства обеспечения информационной безопасности.	

Раздел 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине

Для проверки сформированности компетенции ПК-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей
ИПК-1.3. Администрирует подсистему защиты информации компьютерных сетей

Блок А. Задания репродуктивного уровня («знать»)
<u>А.1 Фонд тестовых заданий по дисциплине</u>

1. Чем отличается протокол UDP от TCP?
    a. Количеством портов для работы;
    b. Размером пакета;
    c. Типом соединения;
    d. Номерами портов.
2. Что гарантирует tcp?
    a. Скорость;
    b. Соединение;
    c. Очередность пакетов;

d. Размер пакета.

3. TCP от UDP отличаются тем, что:
    a. В TCP есть соединение, а в UDP – нет;
    b. TCP может маршрутизироваться, а UDP – нет;
    c. TCP более новый протокол, а UDP – старый;
    d. TCP не используется для DNS, а UDP используется.
4. Какой протокол, UDP или TCP, обеспечивает более высокую скорость передачи данных и почему?
    a. UDP, так как не требует установки соединения и подтверждения доставки;
    b. TCP, так как не использует шифрование;
    c. TCP, так как не требует установки соединения и подтверждения доставки;
    d. Скоростью работы данные протоколы не отличаются.
5. Какая длина адреса у IPv6?
    a. 12;
    b. 256;
    c. 128;
    d. 16.
6. Если префикс маски /24, то чему равно максимально возможное количество хостов в данной подсети?
    a. 256;
    b. 24;
    c. 224;
    d. 128.
7. Являются ли перечисленные адреса внутренними или внешними: A. 192.168.144.100 B. 172.17.42.1
    a. Оба внутренние;
    b. Оба внешние;
    c. A – внешний, B – внутренний;
    d. A – внутренний, B – внешний.
8. Для входа в систему по ssh нужно знать/иметь (Выберите несколько вариантов ответа):
    a. пароль root от локальной системы;
    b. ip-адреса/имя системы и порт;
    c. ssl-сертификат;
    d. приватный ключ зарегистрированный в авторизованных ключах;
    e. имя пользователя.
9. Наиболее известные аппаратные уязвимости современных процессоров:
    a. WannaCry и EternalBlue;
    b. Meltdown и Spectre;
    c. CVE;
    d. WannaCry, EternalBlue, CVE.
10. На каком порту работает протокол SMB?

a. 12;
b. 1024;
c. 445;
d. 3389.

11. Используя какую из нижеперечисленных команд, можно проверить, открыт ли TCP порт 8080 на удаленной машине?
    a. telnet ip_address 8080;
    b. ping -c 8080 ip_address;
    c. echo ip_address:8080;
    d. curl ip_address 8080.
12. Какой командой можно активировать/деактивировать сетевой интерфейс {name} в Linux?
    a. no interface {name} down/interface {name} down;
    b. create/destoy {name};
    c. netsh netif {name} up/down;
    d. ip link set {name} up/down.
13. Какая из нижеперечисленных команд позволит получить информацию о сетевых интерфейсах на Linux машине?
    a. iconfig;
    b. ps aux;
    c. cat /etc/hosts;
    d. ip addr show.
14. Какой командой можно менять настройки IP сетевого интерфейса в Linux?
    a. ip;
    b. netsh ifdev config;
    c. interface;
    d. conf t.
15. Текущее имя системы можно посмотреть с помощью команды:
    a. uname -n;
    b. nslookup;
    c. dig;
    d. host 127.0.0.1.
16. Имя системы хранится в файле:
    a. /etc/fqdn;
    b. /etc/hosts;
    c. /etc/uname;
    d. /etc/hostname.
17. В файле /etc/hosts находится:
    a. список root-hint'ов;
    b. локальная база сопоставления ip-адресов и имен серверов;
    c. список хостов с которых разрешено ходить без пароля;
    d. локальный кэш DNS.
18. Настройки порядка разрешения имен в системе хранятся в файле:
    a. /etc/network/resolver;

b. /etc/nsswitch.conf;
c. /etc/resolve.order;
d. /etc/resolv.priority.

19. Где поменять настройки подключения к DNS серверу на Linux машине?
    a. /etc/sysctl.conf;
    b. /etc/bashrc;
    c. /etc/resolv.conf;
    d. /etc/defaults.
20. Настройки DNS-клиента хранятся в:
    a. /etc/nameservers;
    b. ядре;
    c. /etc/libdnsresolv.conf;
    d. /etc/resolv.conf.
21. Характерным действием вредоносной программы типа бэкдор (backdoor) является:
    a. изменение политик и настроек систем безопасности ПК;
    b. несанкционированное шифрование файлов;
    c. скрытое подключение к сети зараженных ПК, управляемых удаленно злоумышленником;
    d. осуществление сетевых атак других компьютеров.
22. Характерным действием вредоносной программы типа «ботнет» является:
    a. изменение политик и настроек систем безопасности ПК;
    b. несанкционированное шифрование файлов;
    c. скрытое подключение к сети зараженных ПК, управляемых удаленно злоумышленником;
    d. запоминание нажатий клавиш на клавиатуре.
23. Выберите только один вариант со всеми типовыми правильно перечисленными атаками для контейнеров на базе Docker:
    a. DDoS, fake image, man-in-the-middle, spoofing;
    b. escape from host, DDoS, fake image;
    c. fake image, man-in-the-middle, spoofing;
    d. rootkits, CVE, DDoS, spoofing.
24. Выберите только один вариант со всеми правильно перечисленными методами фильтрации спама в фильтре SpamAssassin:
    a. DNSBL, Sender Policy Framework, DomainKeys, DKIM, Razor;
    b. DNSBL, DomainKeys, DKIM, ClamAV, SSH;
    c. DNSBL, DKIM, Razor, Kaspersky check;
    d. DNSBL, Razor, DomainKeys, DKIM, Machine learning.
25. Что такое уязвимость нулевого дня:
    a. Термин означает, что у разработчиков было 0 дней на исправление дефекта: уязвимость или атака становится публично известна до момента выпуска производителем ПО исправлений ошибки;
    b. Разработчик не хочет исправлять данную уязвимость;

c. Термин означает, что разработчик изначально заложил в программу уязвимость, чтобы в дальнейшем использовать ее в своих целях;
d. Уязвимость, когда дата ОС переводится в нулевое значение.

26. Основной задачей теста на проникновение является:
a. оценка возможности обнаружения атаки службой ИБ;
b. проверка времени реакции службы ИБ;
c. оценка возможности осуществления атаки из Интернет на информационную систему;
d. оценка возможных потерь при реализации атаки.

27. К сервисам безопасности относят:
a. идентификация/аутентификация;
b. протоколирование/аудит;
c. шифрование;
d. аудит.

28. Потенциальные угрозы, определяющие задачи защиты информации в компьютерных сетях:
a. прослушивание каналов;
b. умышленное уничтожение или искажение информации;
c. выход из строя операционной системы;
d. внедрение сетевых вирусов.

29. Конфиденциальность - это:
a. предотвращение пассивных атак для передаваемых или хранимых данных;
b. защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных;
c. подтверждении подлинности взаимодействующих объектов;
d. защита от несанкционированного использования ресурсов сети.

30. К механизмам безопасности относят:
a. хэш-функции;
b. целостность сообщения;
c. алгоритмы симметричного шифрования;
d. невозможность отказа от полученного сообщения.

31. Активные угрозы становятся видимыми на уровне (модели OSI):
a. физическом;
b. канальном;
c. сетевом;
d. транспортном.

32. Алгоритм, использующий для шифровки два разных ключа (открытый и закрытый):
a. алгоритм симметричного шифрования;
b. алгоритм асимметричного шифрования;
c. алгоритм использования контрольных сумм;
d. алгоритм проверки подлинности.

33. Двоичные программы, внедряемые в web-страницу:

a. JavaScript;
b. Java-апплеты;
c. activeX;
d. VBScript.

34. Цифровая подпись – это:
    a. способ введения электронной метки для файла данных;
    b. файл, подтверждающий ваши права;
    c. сведения о пользователе помещаемые в файл;
    d. идентификатор документа.
35. Обозначение, семейства протоколов, охватывающих проблемы безопасности на IP-уровне:
    a. FTP;
    b. UDP;
    c. TCP/IP;
    d. Ipsec.
36. Основные протоколы транспортного уровня, применяемые в Интернете:
    a. FTP;
    b. STP;
    c. TCP;
    d. UDP.

А2. Вопросы для обсуждения

1. Классификация сетей по способам распределения данных.
2. Основные сетевые стандарты и протоколы.
3. Семейство протоколов TCP/IP.
4. Семейство протоколов UDP.
5. Сетевое активное и пассивное оборудование.
6. Примеры типовых атак и рекомендации по построению систем защиты.
7. Регламентирующие документы в области безопасности вычислительных сетей.
8. Понятие политики безопасности.
9. Правовые основы защиты информации в сетях.
10. Сканирование портов.
11. Разновидности DDOS-атак.
12. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
13. Защита компонентов сети от несанкционированного доступа.
14. Защита от сбоев электропитания аппаратного и программного обеспечения.
15. Контроль и распределение нагрузки на вычислительную сеть.
16. Инвентаризация службы SNMP.
17. Протоколы и правила управления криптографическими ключами.
18. Базовые протоколы семейства TCP/IP.

19. Протоколы управления сетью.
20. Протоколы FTP, SFTP, FTPS. Возможные атаки.
21. Инвентаризация службы сеансов NetBIOS.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов

1. Сравнительная характеристика различных типов сетей.
2. Сетевые операционные системы.
3. Обеспечение безопасности в компьютерах и корпоративных сетях.
4. DNS-сервера и использование сервиса WhoIs.
5. Методы сканирования сетей.
6. Основы классификации сетевых угроз и атак.
7. Стандарты безопасности вычислительных сетей и их компонентов.
8. Основные шаги по реализации политики безопасности.
9. Основные критерии анализа сетевой безопасности.
10. Защита от сканирования портов.
11. Административные методы защиты от DDOS-атак.
12. Базовые источники правового обеспечения информационной безопасности.
13. Методика подготовки экспертного заключения о реализации методов защиты.
14. Виды используемых в Интернет каналов связи.
15. Способы подбора паролей. Возможные контрмеры.
16. Сбор идентификационных маркеров автоматически и вручную с помощью утилит telnet и netcat. Возможные контрмеры.
17. Настройка маршрутизаторов и межсетевых экранов для обеспечения информационной безопасности.
18. Виртуальные частные сети.
19. Криптографические сетевые протоколы.
20. Электронная цифровая подпись.
21. Основные механизмы обеспечения безопасности и управления распределенными ресурсами.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Лабораторные работы.

Лабораторная работа «Сбор информации о сетевых узлах».

Целью лабораторной работы является обучение методам и средствам сбора предварительной информации в Интернет об анализируемой КС.

Постановка задачи: Выполнить предварительный сбор информации о домене tsu.ru. Работа выполняется на АРМ, имеющем доступ в сеть Интернет.

Последовательность действий:

Шаг 1. Перейти по адресу http://www.ripn.net/nic/whois. Указать в строке поиска в базе данных РосНИИРОС домен dgunh.ru. Проанализировать полученные данные. Найти DNS-имена и IP-адреса серверов имен. В строке поиска базы данных RIPE задать IP-адреса серверов имен. Определить диапазоны IP-адресов, выделенные организации. Проанализировать данные по администраторами и контактным лицам организации. Найти используемые почтовые адреса.

Шаг 2. Перейти по адресу http://network-tools.com/nslook. Задать параметры: домен – tsu.ru, тип запроса – ANY. Определить почтовый сервер организации.

Шаг 3. Выполнить предыдущие проверки, используя средства nslookup, host и dig.

Шаг 4. Определить DNS-имена и роли узлов из выделенных диапазонов IP-адресов. Использовать веб-средства http://dnsstuff.com и http://dnsreport.com.

Шаг 5. Проверить наличие узлов найденных сетей в базах данных спам-отправителей и бот-сетях, используя для этого веб-средства http://www.spamcop.net, http://www.spamcop.net и http://rbls.org.

Шаг 6. Проверить возможность выполнения переноса зоны на первичном и вторичном DNS-серверах:

C:\nslookup
>server ns.dgunh.ru
>set type=any
>ls –d dgunh.ru

Шаг 7. Перейти по адресу http://google.ru. Задать следующие поисковые запросы и проанализировать результаты:

– «site:dgunh.ru filetype: docx для служебного пользования»;
– «site:dgunh.ru filetype: doc для служебного пользования»;
– «site:dgunh.ru filetype: doc секретно»;
– «site:dgunh.ru filetype:doc ФИО».

Шаг 8. Выполнить метод анализа mail bouncing. Сформировать и отправить некорректные почтовые сообщения: сообщения на несуществующие адреса, сообщения, размер которых превышает допустимый и т.д. Проанализировать полученные ответы.

Шаг 9. Используя веб-инструмент traceroute, расположенный на веб-ресурсе http://network-tools.com, определить маршруты прохождения IP-дейтаграмм до исследуемой сети.

Лабораторная работа «Защита инфраструктуры маршрутизации».

Целью лабораторной работы является обучение методам и средствам проектирования и защиты инфраструктуры маршрутизации отказоустойчивых иерархических компьютерных сетей на основе протокола маршрутизации OSPF.

Постановка задачи: На маршрутизаторах СПД выполнить настройки протокола OSPF, обеспечивающие корректную работу сети и защиту инфраструктуры маршрутизации.

Последовательность действий:

Шаг 1. Настроить модель коммутаторов Frame Relay, используя элемент Cloud-PT набора WAN Emulation.

Шаг 2. Построить модель компьютерной сети в соответствии со схемой, представленной на рис. 1. Определить уровень каждого маршрутизатора СПД в ее иерархической модели.

Шаг 3. На маршрутизаторе R7 выполнить настройки интерфейсов, а также настройки протокола маршрутизации OSPF для области 120 (полностью тупиковой), обеспечивающие регистрацию событий маршрутизации, аутентификацию соседей и активацию пассивных интерфейсов:

router ospf 10
log-adjacency-changes
area 120 stub
passive-interface default
no passive-interface Se0/0/0
network 0.0.0.0 255.255.255.255 area 120 interface Se0/0/0
description Link to R4
ip address 192.168.100.26 255.255.255.252
ip ospf message-digest-key 10 md5 H4&hdn3&
ip ospf authentication message-digest interface Loopback0
description Loopback interface
ip address 192.168.0.7 255.255.255.255

Выполнить аналогичные настройки на маршрутизаторе R6.

Шаг 4. Убедиться в корректности настроек маршрутизаторов, проверить возможность использования резервных маршрутов при разрыве основных каналов связи.

Шаг 5. Внедрить в СПД ложный маршрутизатор. Убедиться в невозможности установки сессий между маршрутизаторами СПД и ложным маршрутизатором, а также внедрения ложной маршрутной информации без знания пароля для алгоритма MD5.

Шаг 6. К маршрутизатору R4 подключить коммутатор ЛВС. Проанализировать сетевые информационные потоки ЛВС и убедиться в отсутствии в ней рассылки пакетов OSPF при активации пассивных интерфейсов.

Лабораторная работа «Защита инфраструктуры коммутации».

Целью лабораторной работы является обучение методам и средствам защиты инфраструктуры коммутации при использовании технологии виртуальных ЛВС (VLAN), их настройке и маршрутизации.

Постановка задачи: ЛВС филиала банка построена на базе двух коммутаторов уровня доступа филиала Cisco Catalyst 2960 (SW4-2, SW4-3), коммутатора уровня ядра-распределения филиала Cisco Catalyst 3560 (SW4-1) и маршрутизатора доступа Cisco 2811 (R4). Требуется создать VLAN с номерами для рабочих станций, принтеров и серверов банка в соответствии со схемой, (по вариантам), настроить маршрутизацию между этими VLAN при их подключении к маршрутизатору R4 по магистральному каналу, а также выполнить настройки в соответствии с приведенными выше рекомендациями.

Последовательность действий:

Шаг 1. На коммутаторе уровня доступа филиала SW4-3 отключить протокол VTP, создать необходимые VLAN, настроить магистральный порт и порты доступа коммутатора:

```
vtp mode transparent
vlan 30
name AS_Client_Bank
vlan 40
name Service
vlan 700
name unused ports
vlan 701
name native
```

Шаг 2. Настроить используемые магистральные порты и порты доступа коммутатора SW4-3:

```
interface fastEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 701
interface fastEthernet 0/2
switchport mode access
switchport nonegotiate
switchport access vlan 30
```

Шаг 3. Настроить неиспользуемые порты коммутатора SW4-3, используя возможность указания диапазона портов:

```
interface range fastEthernet 0/4-24
switchport mode access
switchport nonegotiate
switchport access vlan 700
shutdown
```

Шаг 4. Выполнить аналогичные настройки с учетом требуемых VLAN, на коммутаторе SW4-2.

Шаг 5. На коммутаторе уровня ядра-распределения филиала SW4-1 настроить магистральные порты для соединения с маршрутизатором и коммутаторами доступа по схеме магистрального подключения. Выполнить настройки безопасности согласно приведенным выше рекомендациям:

```
ip routing
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 701
switchport trunk allowed vlan 10,20,30,40
```

Шаг 6. На маршрутизаторе филиала R4 создать необходимые VLAN, настроить sub-интерфейсы на порту Fa0/1 и включить инкапсуляцию по протоколу IEEE 802.1Q:

```
interface fa0/1
no shutdown
no ip address
interface fa0/1.2
encapsulation dot1q 10
ip address 10.194.4.1 255.255.255.192
interface fa0/1.3
encapsulation dot1q 20
ip address 10.194.4.65 255.255.255.192 interface fa0/1.4
encapsulation dot1q 30
ip address 10.194.4.129 255.255.255.192 interface fa0/1.5
encapsulation dot1q 40
ip address 10.194.4.193 255.255.255.192
```

Шаг 7. Проверить доступность серверов АС с рабочих станций, исследовать формат кадров, передающихся по магистральному каналу между коммутатором ядра-распределения и маршрутизатором. Убедиться в невозможности взаимодействия с серверами АС из VLAN 700.

Шаг 8. Убедиться, что кадры native VLAN не инкапсулируются протоколом IEEE 802.1q при их передаче по магистральному каналу.

Лабораторная работа «Защита ЛВС от петель на канальном уровне».

Целью лабораторной работы является изучение методов и средств построения, защиты и оптимизации отказоустойчивых ЛВС на основе протокола STP.

Постановка задачи:

На коммутаторах ЛВС филиала банка выполнить настройки протокола STP и механизмов его защиты. Построенная ЛВС должна обеспечивать состояние доступности при отказе:

– одного из коммутаторов SW7-1 или SW7-2;

– активного коммутируемого порта маршрутизатора R7;

– одной из линий связи канала EtherChannel;

– активного порта линии связи между коммутатором уровня доступа и коммутатором уровня ядра-распределения.

Последовательность действий:

Шаг 1. Построить схему логического соединения коммутаторов ЛВС и найти возможные циклы на канальном уровне (по выданной схеме). Определить оптимальное положение корневого коммутатора в соответствии с маршрутами информационных потоков.

Шаг 2. К маршрутизатору R7 в слот № 3 подключить модуль HWIC-4ESW, обеспечивающий наличие дополнительных четырех коммутируемых Ethernet-портов. Создать на коммутирующем модуле маршрутизатора виртуальные ЛВС и

для каждой из них настроить интерфейс SVI, обеспечивающий маршрутизацию виртуальных ЛВС:

```
vlan database
vlan 10 name Servers
vlan 20 name AS_Filial
vlan 30 name AS_Client_Bank
vlan 40 name Service
interface vlan10
ip address 10.194.7.1 255.255.255.192
interface vlan20
ip address 10.194.7.65 255.255.255.192
interface vlan30
ip address 10.194.7.129 255.255.255.192
interface vlan40
ip address 10.194.7.193 255.255.255.192
interface fastEthernet 3/0/0
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
switchport trunk native vlan 701 interface fastEthernet 3/0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
switchport trunk native vlan 701
```

Шаг 3. На коммутирующем модуле маршрутизатора R7 настроить протокол Rapid-PVST для требуемых VLAN: spanning-tree mode rapid-pvst

Шаг 4. Между коммутаторами SW7-1 и SW7-2 настроить агрегирование двух каналов передачи данных по технологии Etherchannel:

```
interface GigabitEthernet0/1
channel-protocol lacp
channel-group 1 mode on
interface GigabitEthernet0/2
channel-protocol lacp
channel-group 1 mode on
interface port-channel 1
no shutdown
switchport mode trunk
switchport trunk native vlan 701
switchport trunk allowed vlan 10,20,30,40
```

Шаг 5. На коммутаторе SW7-1 настроить протокол Rapid-PVST для требуемых виртуальных ЛВС и задать наивысший приоритет коммутатора, обеспечив ему роль корневого моста в указанных VLAN:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,701 root primary
```

Шаг 6. На коммутаторе SW7-2 настроить протокол Rapid-PVST для требуемых VLAN и задать наивысший приоритет коммутатора, обеспечив ему

роль корневого моста в указанных VLAN в случае выхода из строя коммутатора SW7-1:

spanning-tree mode rapid-pvst

spanning-tree vlan 10,20,30,40,701 root secondary

Шаг 7. На коммутаторах SW7-1 и SW7-2 настроить механизм Root Guard:

interface range fa0/2-3

spanning-tree guard root

Шаг 8. На коммутаторах SW7-3 и SW7-4 настроить протокол Rapid-PVST для требуемых VLAN:

spanning-tree mode rapid-pvst

spanning-tree vlan 20,30,40,701

Шаг 9. На портах доступа коммутаторов SW7-3 и SW7-4 настроить протокол STP в режиме portfast, включить механизмы защиты BPDU Guard:

interface range fa0/3-4

switchport mode access

spanning-tree bpduguard enable

spanning-tree portfast

Шаг 10. Убедиться в корректности настройки протокола STP на коммутаторах ЛВС. Проверить возможность функционирования сети при отключении порта Fa0/0/1 маршрутизатора R7, при отключении порта Gi0/1 коммутатора SW7-1, при отключении коммутатора SW7-1 или при отключении порта Fa0/1 коммутатора SW7-3.

Лабораторная работа «Защита ЛВС от атак канального уровня».

Целью лабораторной работы является изучение методов проектирования, развертывания и настройки механизмов защиты в коммутируемых ЛВС от атак канального уровня типа MAC-flooding и MAC-spoofing.

Постановка задачи: В сегменте ЛВС филиала, построенном на базе двух коммутаторов уровня доступа Cisco Catalyst 2960 и коммутатора уровня ядра-распределения Cisco Catalyst 3560, обеспечить защиту от атак типа MAC-flooding и MAC-spoofing.

Последовательность действий:

Шаг 1. На коммутаторе уровня доступа SW4-3 настроить механизм port security в динамическом режиме для рабочих станций:

interface range fa0/2-3

switchport mode access

switchport port-security

switchport port-security maximum 1

switchport port-security violation protect

Шаг 2. Выполнить аналогичные настройки механизма port security на коммутаторе SW4-2.

Шаг 3. На коммутаторе уровня ядра-распределения SW4-1 настроить механизм port security в статическом режиме с привязкой к заданному MAC-адресу для порта FastEthernet0/4:

interface fa0/4
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address xxxx.yyyy.zzzz
switchport port-security violation shutdown

Шаг 4. На коммутаторе уровня ядра-распределения SW4-1 настроить механизм port security в статическом режиме с опцией sticky для порта FastEthernet0/5:

interface fa0/5
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown

Шаг 5. Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-spoofing. Задать MAC-адрес рабочей станции, подключенной к порту коммутатора со статическим методом формирования списка MAC-адресов, несоответствующий требованиям политики безопасности. Убедиться в переводе порта коммутатора в режим shutdown или protect.

Шаг 6. Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-flooding. На порт коммутатора с динамическим методом формирования списка разрешенных MAC-адресов подключить коммутатор с несколькими рабочими станциями. Убедиться в переводе порта коммутатора в режим shutdown или protect.

Лабораторная работа «Построение маршрутизируемой ЛВС».

Целью лабораторной работы является обучение методам построения и настройки маршрутизируемой ЛВС с высокой доступностью на основе протокола маршрутизации OSPF.

Постановка задачи: Выполнить настройки коммутаторов ЛВС банка, обеспечивающие реализацию архитектуры полностью маршрутизируемой ЛВС с высокой доступностью.

Последовательность действий:

Шаг 1. Построить сеть, в соответствии со схемой маршрутизации, согласно варианту. При необходимости ввести необходимые элементы и включить дополнительные механизмы. Выполнить настройки интерфейса SVI на коммутаторе уровня доступа SW8:

vlan 192
interface vlan192
ip address 10.194.192.1 255.255.255.0
interface fastEthernet 0/10
switchport access vlan 192

Шаг 2. Выполнить настройки протокола маршрутизации OSPF на коммутаторе уровня доступа SW8, обеспечив аутентификацию соседей и инициализацию пассивных интерфейсов:

```
router ospf 10
log-adjacency-changes
area 50 stub
passive-interface default
no passive-interface fastEthernet 0/1
no passive-interface fastEthernet 0/2
network 10.194.0.0 0.0.255.255 area 50
interface fastEthernet 0/1
no switchport
ip address 10.194.240.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 10 md5 H4&hdn3& interface fastEthernet 0/2
no switchport
ip address 10.194.240.10 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 10 md5 H4&hdn3&
```

Шаг 3. Выполнить аналогичные настройки на коммутаторе уровня доступа SW7.

Шаг 4. Выполнить настройки протокола маршрутизации OSPF на коммутаторе уровня ядра-распределения SW5, обеспечив аутентификацию соседей, инициализацию пассивных интерфейсов аутентификации соседей и полностью тупиковых областей. Для последней выполняется настройка:

```
router ospf 10
area 50 stub no-summary
```

Шаг 5. Выполнить аналогичные настройки на коммутаторе уровня ядра-распределения SW6.

Шаг 6. Выполнить аналогичные настройки протокола маршрутизации OSPF на маршрутизаторах R1, IBR и FWR. На пограничном маршрутизаторе автономной системы IBR дополнительно настроить объявление внешнего маршрута в OSPF-систему:

```
router ospf 10
network 212.192.98.152 0.0.0.7 area 100
default-information originate
```

Шаг 7. Проверить доступность всех узлов и отказоустойчивость ЛВС.

Шаг 8. Убедиться в прохождении пакетов по разным альтернативным маршрутам (технология ECMP). Выполнить настройки по изменению стоимости интерфейсов коммутаторов так, чтобы все IP-пакеты проходили только через коммутатор SW5, а при его отказе – через коммутатор SW6. Убедиться в прохождении пакетов по одному маршруту:

```
interface fastEthernet 0/2
ip ospf cost 2.
```

Блок D. Задания для использования в рамках промежуточной аттестации

D1. Перечень вопросов к экзамену

1. Основные понятия: сеть, каналы связи, логический канал, протокол, трафик, метод доступа, топология, архитектура.
2. Методы доступа к сети.
3. Организация беспроводных сетей.
4. Протоколы. Стандартные стеки коммуникационных протоколов и соответствие уровням модели OSI.
5. Спецификация IEEE 802.
6. Типы сетевой топологии.
7. Система доменных имен DNS.
8. Адресация в сетях IP. Форматы адресов и их преобразование.
9. Маска подсети. Классы сетей.
10. Подсети. Определение диапазона адресов подсети.
11. Организация Доменов и доменных имен. Определение имен уровня DNS.
12. Требования, предъявляемые к сетям: надежность и безопасность.
13. Требования, предъявляемые к сетям: производительность сети и способы ее повышения.
14. Службы сети Интернет: терминальный режим, электронная почта.
15. Службы сети Интернет: списки рассылки, служба телеконференций.
16. Службы сети Интернет: служба World Wide Web (WWW).
17. Службы сети Интернет: служба FTP.
18. Автоматизация процесса назначения IP-адресов узлам сети – протокол DHCP.
19. Принципы работы и правила настройки маршрутизаторов.
20. Принципы работы и правила настройки коммутаторов.
21. Принципы работы и правила настройки шлюзов.
22. Принципы работы и правила настройки файерволов.
23. Принципы работы и правила настройки 4G-модемов.
24. Принципы работы и правила настройки сетевых адаптеров.

Раздел 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов,

полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции(й) по дисциплине складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции(й) в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции(й) обучающихся на экзамене (максимум – 30 баллов).

Для студентов очно-заочной формы обучения применятся 4-балльная шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

Уровни освоения компетенций	Продвинутый уровень	Базовый уровень	Пороговый уровень	Допороговый уровень
100 – балльная шкала	85 и ≥	70 – 84	51 – 69	0 – 50
4 – балльная шкала	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Выполнение лабораторных работ	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Устный опрос	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение и публичная защиты реферата	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-50	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины
51-69	«удовлетворительно»	Пороговый уровень	Не менее 50% заданий, подлежащих текущему контролю успеваемости, выполнены без существенных ошибок
70-84	«хорошо»	Базовый уровень	Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок
85-100	«отлично»	Продвинутый уровень	100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами

Шкала оценок по промежуточной аттестации

Наименование формы промежуточной аттестации	***Баллы***	***Оценка***
Экзамен	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-9	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы
10-16	«удовлетворительно»	Пороговый уровень	Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме.
17-23	«хорошо»	Базовый уровень	Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по дисциплине компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примерами; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала и полностью выполнил практические задания
25-30	«отлично»	Продвинутый уровень	Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал

			и выполняет практические задания с подробными пояснениями и аргументированными выводами

Раздел 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдаю очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до отдельного аспекта обсуждаемой темы.

Методика оценивания ответов на устные вопросы

Баллы	***Оценка***	***Показатели***	***Критерии***
9-10	«отлично»	1. Полнота данных ответов; 2. Правильность ответов на вопросы.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, привести необходимые примеры. Изложение материала последовательно и правильно.
7-8	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
5-6	«удовлетворительно»		Студент обнаруживает знание и понимание основных положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.
0-4	«неудовлетвори-тельно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий

включает 30 вопросов.

Методика оценивания выполнения тестов

Баллы	Оценка	Показатели	Критерии
18-20	«отлично»	1. Полнота выполнения тестовых заданий; 2. Своевременность выполнения; 3. Правильность ответов на вопросы.	Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос
14-17	«хорошо»		Выполнено более 70 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др.
11-13	«удовлетворительно»		Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.
0-10	«неудовлетвори-тельно»		Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Тема реферата выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На написание реферата отводится одна неделя. Реферат оформляется согласно действующим в Дагестанском государственном университете народного хозяйства требованиям к оформлению письменных работ. Объем представленного реферата должен быть не менее 10 страниц машинописного текста без учета титульного листа.

Публичная защита реферата проводится в присутствии остальных студентов, защищающих рефераты. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель реферата, а также цельно сформулировать базовую идею, отраженную в реферате.

Методика оценивания выполнения рефератов

Баллы	***Оценка***	***Показатели***	***Критерии***
9-10	«отлично»	1. Полнота выполнения рефератов; 2. Своевременность выполнения; 3. Четкость изложения идеи реферата во время	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены

		защиты.	требования к внешнему оформлению, четкое и последовательное выступление во время защиты.
7-8	«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; выступление во время защиты требует дополнительных вопросов.
5-6	«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 во время выступления.
0-4	«неудовлетвори-тельно»		Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы, не проведена защита реферата.

Лабораторные работы выполняются в специализированной аудитории во время лабораторных занятий. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения лабораторных работ

Баллы	***Оценка***	***Показатели***	***Критерии***
18-20	«отлично»	1. Полнота выполнения задания лабораторной работы; 2. Своевременность выполнения задания лабораторной работы; 3. Самостоятельность решения.	Основные требования к выполнению задания лабораторной работы выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели
14-17	«хорошо»		Основные требования к выполнению задания лабораторной работы реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых

			решений
11-13	«удовлетворительно»		Имеются существенные отступления от выполнения лабораторной работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
0-10	«неудовлетвори-тельно»		Шаги выполнения лабораторной работы не выполнены, обнаруживается существенное непонимание проблемы.

В экзаменационный билет включено два теоретических вопроса. Экзамен проводится в виде письменного ответа на вопрос билета. При оценке ответа на вопрос оценивается полнота ответа, точность формулировок, правильное цитирование соответствующих законодательных актов, наличие иллюстративных примеров. Время подготовки ответа при сдаче экзамена составлять 60 минут. Оценка ответов, подготовленных студентами объявляется обучающимся в день проведения экзамена.

Методика оценивания ответа на экзамене

Баллы	Оценка	Показатели	Критерии
18-20	«отлично»	1. Полнота и последовательность ответа на поставленные вопросы; 2. Логичность и аргументированность изложения; 3. Наличие практических примеров.	Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать и систематизировать материал.
14-17	«хорошо»		Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по дисциплине компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примера-ми; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала.
11-13	«удовлетворительно»		Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме.
0-10	«не удовлетворительно»		Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы.

Лист актуализации оценочных материалов по дисциплине

«Безопасность вычислительных сетей»

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____