МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ

по дисциплине «Защита информации в профессиональной деятельности»

для студентов специальности 38.05.01 Экономическая безопасность специализация "Экономико-правовое обеспечение экономической безопасности"

Ставрополь,2026

Цель методических указаний - определить единый подход при выполнении студентами самостоятельной работы и в том числе, к подготовке студентами курсовых работ, обязательные требования к их содержанию и оформлению.

Методические указания по организации и проведению самостоятельной работы нацеливают на стимулирование самостоятельной работы студентов с тем, чтобы повысить роль не только в формировании знаний и умений, но и в накоплении навыков научного исследования.

Методические указания содержат общие требования к содержанию и структуре самостоятельной работы по дисциплине «Защита информации профессиональной деятельности», указания по подготовке и защите курсовой работы.

Предназначены в помощь студентам, обучающимся на образовательной программе по специальности 38.05.01 Экономическая безопасность специализация «Экономико-правовое обеспечение экономической безопасности» направленность (профиль) «Экономико-правовое обеспечение экономической безопасности».

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ

Самостоятельная работа студентов является внеаудиторной и предназначена для самостоятельного изучения определенных тем дисциплины по материалам, рекомендованным преподавателем.

Самостоятельная работа студентов в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в технологии обучения.

Целью самостоятельной работы студентов по дисциплине «Защита информации профессиональной деятельности» является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности.

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами самостоятельной работы по дисциплине «Защита информации профессиональной деятельности» являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;

- углубление и расширение теоретических знаний;

- формирование умений использовать нормативную, правовую,

справочную документацию и специальную литературу;

- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

- развитие исследовательских умений;

- использование материала, собранного и полученного в ходе самостоятельных

занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ.

В результате выполнения самостоятельной работы по дисциплине «Защита информации профессиональной деятельности» у обучающийся формируются следующие компетенции:

ПК-4. Способен использовать цифровые средства и информационные технологии для решения задач обеспечения экономической безопасности	
ИД-2 ПК-4.	Способен использовать инструменты цифровизации и автоматизации для решения управленческих задач с учетом требований нормативных правовых актов

План выполнения самостоятельной работы

Код оцениваемой компетенции, индикатора (ов)	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Вид контроля, аттестация *(текущий/промежуточный)*	Тип контроля *(устный, письменный или с использованием технических средств)*	Наименование оценочного средства
ИД-2 ПК-4	1 2 3 4	Зачет	Промежуточный	Устный	Вопросы к экзамену
		Комплект задач	Текущий	Письменный	Зачетное задание
		Собеседование	Текущий	Устный	Вопросы для собеседования

2 ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПРИ САМОСТОЯТЕЛЬНОМ РЕШЕНИИ ЗАДАЧ

2.1 Содержание самостоятельной работы

Для овладения навыками решения практических задач по дисциплине «Защита информации профессиональной деятельности» необходимо выполнить практические работы по темам:

Практическое занятие № 1. Создание кибермира

Практическое занятие № 2. Общение в кибермире

Практическое занятие № 3. Шифрование файлов и данных

Практическое занятие № 4. Проверка целостности файлов и данных

Практическое занятие № 5. WEP/WPA2 PSK/WPA2 RADIUS

Практическое занятие № 6. Настройка транспортного режима VPN

Практическое занятие № 7. Резервирование маршрутизаторов и коммутаторов

Практическое занятие № 8. Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе

2.2 Процедура оценивания результатов самостоятельной работы

Предлагаемые задания позволяют проверить сформированность у студентов общекультурных и профессиональных компетенций. Задания ориентированы на решение конкретных задач с использованием отдельных инструментальных средств для обработки экономических данных, методик анализа экономических и финансовых аспектов деятельности коммерческих и государственных организаций, обобщение результатов расчетов и обоснование выводов, использование полученных сведения для принятия управленческих решений.

При проверке задания, оцениваются правильность решения задач, убедительность аргументации, доказательность выводов и обоснованность рекомендаций.

Компетенции (знания, умения и навыки) студентов оцениваются по пятибалльной системе: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется студенту, если он полностью выполнил задачи, интегрировал знания различных областей, аргументировал собственную точку зрения, последовательно, четко и логически стройно изложил материал, увязал теорию, методологию и практику, правильно обосновал решение, владеет разносторонними навыками и приемами выполнения практических задач и кейсов.

Оценка «хорошо» выставляется студенту, если он в целом выполнил задания, по существу раскрыл вопросы, не допуская существенных неточностей в ответе на них, правильно применил теоретико-методологические положения при решении заданий,

владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется студенту, если он раскрыл только базовые понятия без конкретизации деталей, допустил ошибки и неточности в ходе решения заданий, недостаточно правильные формулировки, нарушил логику последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не выполнил или частично выполнил с ошибками задания, не раскрыл ход решения заданий и практических вопросов, допуская существенные ошибки.

3 ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПРИ САМОСТОЯТЕЛЬНОМ ИЗУЧЕНИИ ЛИТЕРАТУРЫ

3.1 Работа с книгой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса.

Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно.

Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Различают два вида чтения; первичное и вторичное.

Первичное – эти внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятного олова. Содержание не всегда может быть понятно после первичного чтения. Задача вторичного чтения полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

3.2 Правила самостоятельной работы с литературой

Как уже отмечалось, самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие формирования у себя научного способа познания. Основные советы здесь можно свести к следующим: составить перечень книг, с которыми Вам следует познакомиться; сам такой перечень должен быть систематизированным. обязательно выписывать все выходные данные по каждой книге (при написании курсовых и дипломных работ это

позволит очень сэкономить время). разобраться для себя, какие книги (или какие главы книг) следует прочитать более внимательно, а какие – просто просмотреть.

При составлении перечней литературы следует посоветоваться с преподавателями и научными руководителями (или даже с более подготовленными и эрудированными сокурсниками), которые помогут Вам лучше сориентироваться, на что стоит обратить большее внимание, а на что вообще не стоит тратить время...

Все прочитанные книги, учебники и статьи следует конспектировать, но это не означает, что надо конспектировать «все подряд»: можно выписывать кратко основные идеи автора и иногда приводить наиболее яркие и показательные цитаты (с указанием страниц).

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют четыре основные установки в чтении научного текста:

1. Информационно-поисковый (задача – найти, выделить искомую информацию).

2. Усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений).

3. Аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему).

4. Творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

1. Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

2. Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

3. Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

4. Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

5. Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи.

Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

3.3 Методические указания по составлению конспекта

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;

2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

3.4 Шкала и критерии оценивания

Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами при ответе на практикоориентированные вопросы. Компетенции ПК-4 освоены на повышенном уровне.

Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов, владеет необходимыми навыками и приемами ответов на них. Компетенции ПК-4 полностью освоены на базовом уровне.

Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической

последовательности в изложении программного материала, испытывает затруднения при ответе на вопросы. Компетенции ПК-4 частично освоены на базовом уровне.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями отвечает на вопросы. Компетенции ПК-4 не освоены.

4 ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПРИ САМОСТОЯТЕЛЬНОЙ ПОДГОТОВКЕ К зачету

4.1 Методические указания по подготовке к зачету

Процедура проведения зачета осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ.

4.2 Оценочные средства зачета

4.2.1 Вопросы к зачету

Базовый уровень

1. Обеспечение информационной безопасности: содержание и структура понятия.
2. Система обеспечения информационной безопасности.
3. Обеспечение информационной безопасности организации.
4. Обеспечение информационной безопасности Российской Федерации
5. Содержание и структура законодательства. Законодательство об информации, информационных технологиях и о защите информации
6. Термины и определения в области защиты информации

7. Государственной системы защиты информации

8. Задачи органов Государственной системы защиты информации.

9. Административная и уголовная ответственность в сфере защиты информации.

10. Дополнительная и повторная Защита информации профессиональной деятельности.

11. Международная нормативная база обеспечения безопасности.

12. Руководящие документы и методические указания в сфере защиты информации

13. Персональные данных, их классификация

Повышенный уровень

14. Создания и оценка соответствия информационной системы персональных данных

15. Права субъектов персональных данных

16. Обязанности оператора при обработке персональных данных.

17. Порядок отнесения сведений к государственной тайне

18. Порядок засекречивания и рассекречивания сведений, отнесённых к государственной тайне.

19. Порядок распоряжения сведениями, составляющими государственную тайну.

20. Система защиты сведений, составляющих государственную тайну

21. Порядок отнесения информации к коммерческой тайне

22. Порядок охраны коммерческой тайны.

23. Порядок предоставления информации, составляющей коммерческую тайну.

24. Законодательство об электронной цифровой подписи.

25. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи

26. Институты сертификата ключа электронной цифровой подписи и владельца сертификата

27. Институт удостоверяющих центров

28. Особенности использования электронной цифровой подписи

29. Защита прав и законных интересов субъектов информационной сферы.

30. Классы угроз информационной безопасности.

31. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

32. Административный уровень обеспечения информационной безопасности

33. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).

34. Корпоративная нормативная база по защите информации.

35. Комплексная система защиты информации.

36. Организация пропускного режима на предприятии (организации).

37. Методы разграничения доступа

4.5 Критерии оценивания ответов на вопросы экзаменационного билета Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач. Компетенции ПК-4 освоены на повышенном уровне.

Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении

практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Компетенции ПК-4 полностью освоены на базовом уровне.

Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. Компетенции ПК-4 частично освоены на базовом уровне.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические задания. Компетенции ПК-4 не освоены.

5 Учебно-методическое и информационное обеспечение

Перечень основной литературы:

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. - Санкт-Петербург: Лань, 2021. - 324 с. - ISBN 978-5-8114-6738-9.- Текст: электронный //

2. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. - 3-е изд., стер. - СанктПетербург: Лань, 2021. - 108 с. - ISBN 978-5-8114-8370-9. - Текст: электронный //

3. Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. - 4-е изд., стер. - СанктПетербург: Лань, 2022. - 124 с. - ISBN 978-5-507-44201-0. - Текст: электронный//

Перечень дополнительной литературы:

1. Прохорова, О. В. Информационная безопасность и защита информации:

учебник для вузов / О. В. Прохорова. - 3-е изд., стер. - СанктПетербург: Лань, 2021. - 124 с. - ISBN 978-5-8114-7970-2.- Текст: электронный//

2. Фомин, Д. В. Информационная безопасность: учебник / Д. В. Фомин. - Москва: Ай Пи Ар Медиа, 2022. - 222 с. - ISBN 978-5-4497- 1548-7. - Текст: электронный //

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «Защита информации в профессиональной деятельности» для специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности»

Ставрополь
2026

Методические указания к практическим занятиям по информационной безопасности профессиональной деятельности предназначены для формирования у студентов глубоких знаний в области информационной безопасности.

Методические указания предусматривают изучение теоретических вопросов в разрезе тем и выполнение заданий, что позволит закрепить и углубить знания по вопросам защиты информации.

Содержание

1. **Цели и задачи изучения дисциплины**

Целью освоения дисциплины является формирование профессиональной компетенции ПК-4 (способен использовать цифровые средства и информационные технологии для решения задач обеспечения экономической безопасности).

Основными задачами изучения дисциплины являются:

-получение системы знаний о защите информации в профессиональной деятельности, ее целях и задачах;

-ознакомление с методологией и методикой построения систем защиты информации;

-изучение практики реализации систем защиты информации в организации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины обучающийся должен :

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-4. Способен использовать цифровые средства и информационные технологии для решения задач обеспечения экономической безопасности	ИД-2 ПК-4. Способен использовать инструменты цифровизации и автоматизации для решения управленческих задач с учетом требований нормативных правовых актов	Использует инструменты цифровизации и автоматизации для решения управленческих задач с учетом требований нормативных правовых актов

3. Задания к практическим занятиям

Занятие № 1.
Создание кибермира

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь настраивать базовые компоненты сервера.
3. Приобрести навыки развертывания служб FTP, электронной почты, DNS, NTP, AAA и веб-службы на нескольких серверах.
4. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Настройка FTP-сервера
2. Настройка веб-сервера
3. Настройка сервера электронной почты
4. Настройка DNS-сервера
5. Настройка NTP-сервера
6. Настройка сервера AAA

Оборудование и материалы

ПК с установленным Packet Tracer

Общие сведения/сценарий

Выполняя это задание, вы настроите базовые компоненты сервера. Настройка IP-в соответствии с таблицей адресации. Пользуясь вкладкой Services (Службы), вы выполните развертывание служб FTP, электронной почты, DNS, NTP, AAA и веб-службы на нескольких серверах.

Таблица адресации

Устройство	IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	255.255.255.0	Metropolis Bank HQ
Сервер Email/DNS	10.44.1.253	255.255.255.0	Metropolis Bank HQ
Сервер NTP/AAA	10.44.1.252	255.255.255.0	Metropolis Bank HQ
Сервер резервного копирования файлов	10.44.2.254	255.255.255.0	Gotham Healthcare Branch

Учебный вопрос 1: Настройка FTP-сервера

Шаг 1: Активация службы FTP.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **FTP/Web**.

b. Перейдите на вкладку **Services** (Службы) и выберите раздел **FTP**.

c. Включите службу FTP с помощью селективной кнопки, которая находится в верхней части окна.

Шаг 2: Предоставьте пользователям доступ к FTP-серверу.

a. Создайте учетные записи пользователей с именами **bob**, **mary** и **mike**, назначив каждой из них пароль **cisco123**.

b. Каждая учетная запись должна иметь полные разрешения (RWDNL) на доступ к серверу FTP/Web.

Учебный вопрос 2: Настройка веб-сервера

Шаг 1: Активация службы HTTP.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **FTP/Web**.

b. Перейдите на вкладку **Services** (Службы) и выберите **HTTP**.

c. Включите службы HTTP и HTTPS с помощью селективных кнопок, которые находятся в верхней части окна.

Шаг 2: Проверка работоспособности службы HTTP.

a. Выберите компьютер с именем "Sally" и перейдите на вкладку **Desktop** (Рабочий стол).

b. Щелкните значок **Web Browser** (Браузер). Перейдите на веб-сайт **www.cisco.corp**.

c. Пользуясь веб-браузером, перейдите по IP-адресу **10.44.1.254**.

Предположим, переход по IP-адресу происходит корректно, но при этом невозможно выполнить переход с использованием полного доменного имени. В чем может быть причина?

_____

_____

Учебный вопрос 3: Настройка DNS-сервера

Шаг 1: Активация службы DNS.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **Email/DNS**.

b. Перейдите на вкладку **Services** (Службы) и выберите **DNS**.

c. Включите службу DNS с помощью селективной кнопки в верхней части окна.

Шаг 2: Создание записей DNS A.

a. Создайте запись **A email.cisco.corp** с IP-адресом **10.44.1.253**. Нажмите **Add** (Добавить), чтобы сохранить запись.

b. Создайте запись **A www.cisco.corp** с IP-адресом **10.44.1.254**. Нажмите **Add** (Добавить), чтобы сохранить запись.

Шаг 3: Проверка работоспособности службы DNS.

a. Выберите компьютер с именем "Sally" и перейдите на вкладку **Desktop** (Рабочий стол).

b. Щелкните значок **Web Browser** (Браузер). Перейдите на веб-сайт **www.cisco.corp**.

Почему пользователь успешно переходит по указанному полностью квалифицированному имени домена?

Учебный вопрос 4: Настройка сервера электронной почты

Шаг 1: Активация сервисов электронной почты.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **Email/DNS**.

b. Перейдите на вкладку **Services** (Службы) и выберите раздел **EMAIL** (Электронная почта).

c. Включите службы SMTP и POP3 с помощью селективных кнопок, которые находятся в верхней части окна.

Шаг 2: Создайте для пользователей учетные записи электронной почты.

a. Создайте доменное имя **cisco.corp**.

b. Создайте учетные записи пользователей с именами **phil**, **sally**, **bob**, **dave**, **mary**, **tim** и **mike**, назначив каждой учетной записи пароль **cisco123**.

Шаг 3: Настройка пользовательских клиентов электронной почты.

a. Выберите компьютер с именем **Sally** и перейдите на вкладку **Desktop** (Рабочий стол).

b. Щелкните значок **Email** (Электронная почта) и введите следующую информацию.

Name (Имя): **Sally**

Email Address (Адрес электронной почты): **sally@cisco.corp**

Incoming & Outgoing Email Server(s) (сервер (-ы) входящей и исходящей почты): **email.cisco.corp**

Username (имя пользователя): **sally**

Password (пароль): **cisco123**

c. Повторите шаг **3b** на компьютере с именем **Bob**, заменив имя **sally** на **bob**.

Почему для работы сервиса электронной почты необходимо одновременно активировать службы SMTP и POP3?

Учебный вопрос 5: Настройка NTP-сервера

Шаг 1: Активация службы NTP.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.

b. Перейдите на вкладку **Services** (Службы) и выберите **NTP**.

c. Включите службу NTP с помощью селективной кнопки в верхней части окна.

Шаг 2: Защита службы NTP.

a. Включите функцию аутентификации NTP с помощью соответствующей селективной кнопки.

b. Назначьте ключу **Key 1** пароль **cisco123**.

Учебный вопрос 6: Настройка AAA-сервера

Шаг 1: Активация службы AAA.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.

b. Перейдите на вкладку **Services** (Службы) и выберите **AAA**.

c. Включите службу AAA с помощью селективной кнопки в верхней части окна.

Шаг 2: Сетевая конфигурация AAA.

a. Введите имя Client Name (имя клиента) **HQ_Router**, адрес Client IP (IP-адрес клиента) **10.44.1.1** и пароль **cisco123**. Нажмите **Add** (Добавить), чтобы сохранить параметры клиента.

b. Настройте учетную запись пользователя AAA **admin** с паролем **cisco123**. Нажмите **Add** (Добавить), чтобы сохранить информацию о пользователе.

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 2. Настройка веб-сервера	Шаг 2	2	
Вопрос 3. Настройка DNS-сервера	Шаг 3	2	
Вопрос 4. Настройка сервера электронной почты	Шаг 3	2	
Вопросы		**6**	
Балл Packet Tracer		**94**	
Общее число баллов		**100**	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Предположим, переход по IP-адресу происходит корректно, но при этом невозможно выполнить переход с использованием полного доменного имени. В чем может быть причина?

2. Почему пользователь успешно переходит по указанному полностью квалифицированному имени домена?

3. Почему для работы сервиса электронной почты необходимо одновременно активировать службы SMTP и POP3?

Занятие № 2.
Общение в кибермире

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь передавать электронные сообщения от пользователя к пользователю.
3. Приобрести навыки выгрузки файлов на сервер / с сервера по протоколу FTP.
4. Уметь осуществлять удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet.
5. Уметь осуществлять удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH.
6. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Передача электронных сообщений от пользователя к пользователю.
2. Выгрузка файлов на сервер / с сервера по протоколу FTP.
3. Удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet.
4. Удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH.

Оборудование и материалы

ПК с установленным Packet Tracer

Общие сведения

Выполняя это задание, вы обеспечите общение через удаленные сети с помощью общих сетевых сервисов. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Вы будете пользоваться клиентскими устройствами, которые находятся в различных географических регионах. С этих устройств вы будете подключаться к другим клиентским устройствам и серверам.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Сервер Email/DNS	10.44.1.253	209.165.201.4	255.255.255.0	Metropolis Bank HQ
Сервер NTP/AAA	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ
Сервер резервного копирования файлов	10.44.2.254	—	255.255.255.0	Gotham Healthcare Branch

Учебный вопрос 1: Передача электронного сообщения от пользователя к пользователю

Шаг 1: Откройте клиент электронной почты на компьютере пользователя Mike.

d. Откройте объект **Gotham Healthcare Branch** и выберите компьютер с именем **Mike**.

e. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).

Шаг 2: Отправка электронного сообщения пользователю Sally.

a. Нажмите кнопку **Compose** (Создать), чтобы создать электронное сообщение.

b. В поле **To:** (Кому:) введите адрес **sally@cisco.corp**.

В поле **Subject:** (Тема:) введите текст "**Urgent- Call me**".

В поле **Message** (Сообщение) введите следующий текст. "**Call me when you are free today to discuss the new sale.**"

c. Нажмите кнопку **Send** (Отправить), чтобы отправить электронное сообщение.

По какому протоколу письмо было отправлено на сервер электронной почты?

_____

Шаг 3: Проверка почты пользователем Sally.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер с именем **Sally**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).

c. Нажмите кнопку **Receive** (Получить), чтобы получить письмо, отправленное пользователем Mike.

По какому протоколу письмо было получено с сервера электронной почты?

_____

Учебный вопрос 2: Загрузка файлов на сервер по протоколу FTP

Шаг 1: Настройка анализатора пакетов на перехват трафика соответствующего порта.

d. Перейдите к географическому (корневому) виду, чтобы просмотреть все три удаленных объекта.

e. Выберите анализатор трафика **Cyber Criminals Sniffer**.

f. Выберите порт **Port1**, чтобы перехватывать пакеты на этом порте.

g. Оставьте анализатор трафика **Cyber Criminals Sniffer** открытым и видимым до конца этой части работы.

Шаг 2: Удаленное подключение к FTP-серверу.

a. Откройте объект **Healthcare at Home** и выберите компьютер с именем **Mary**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

c. Подключитесь к серверу **FTP/Web** объекта **Metropolis Bank HQ**. Для этого введите команду **ftp 209.165.201.3** в командной строке.

d. Введите имя пользователя **mary** и пароль **cisco123**.

Шаг 3: Загрузите файл на FTP-сервер.

d. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.

e. У пользователя Mary имеется файл с конфиденциальной информацией о новых клиентах медицинского учреждения.

Загрузите файл **newclients.txt** на FTP-сервер. Для этого введите команду **put newclients.txt**.

f. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы убедиться в том, что файл **newclients.txt** теперь находится на FTP-сервере.

Почему загрузка по протоколу FTP считается небезопасным способом передачи файлов?

_____

Шаг 4: Анализ FTP-трафика.

a. Перейдите к географическому (корневому) виду, чтобы просмотреть все три удаленных объекта.

b. Выберите анализатор трафика **Cyber Criminals Sniffer**.

c. На вкладке GUI (Графический интерфейс) слева выберите первый доступный FTP-пакет. После этого полностью прокрутите вниз содержимое окна, отображаемого справа.

Какая информация из FTP-заголовка отображается в виде открытого текста?

_____

d. Слева выберите второй доступный FTP-пакет. После этого полностью прокрутите вниз содержимое окна, отображаемого справа. Повторите те же действия с третьим FTP-пакетом.

e. Какая конфиденциальная информация из FTP-заголовка (помимо имени пользователя) отображается в виде отрытого текста?

_____

Учебный вопрос 3: Удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet

Шаг 1: Удаленное подключение к маршрутизатору корпоративной сети.

d. Откройте объект **Healthcare at Home** и выберите компьютер с именем **Dave**.

e. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

f. Отправьте ping-запрос на маршрутизатор корпоративной сети, чтобы убедиться в наличии связи с маршрутизатором. Для этого введите команду **ping 209.165.201.2**.

g. С помощью команды **telnet 209.165.201.2** установите соединение по протоколу Telnet с маршрутизатором корпоративной сети, которому назначен указанный IP-адрес.

h. Выполните аутентификацию на маршрутизаторе корпоративной сети, используя имя пользователя **admin** и пароль **cisco123**.

i. Введите команду **show users**, чтобы отобразить информацию об активном Telnet-соединении с маршрутизатором корпоративной сети.

Почему протокол Telnet считается небезопасным средством удаленного управления устройствами?

_____

Учебный вопрос 4: Удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH

Шаг 1: Удаленное подключение к маршрутизатору корпоративной сети.

a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер с именем **Tim**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

c. Отправьте ping-запрос на маршрутизатор корпоративной сети, чтобы убедиться в наличии связи с маршрутизатором. Для этого введите команду **ping 209.165.201.2**.

d. С помощью команды **ssh -l admin 209.165.201.2** установите соединение по протоколу SSH с маршрутизатором корпоративной сети, которому назначен указанный IP-адрес.

e. Выполните аутентификацию на маршрутизаторе корпоративной сети, используя пароль **cisco123**.

f. Введите команду **show users**, чтобы отобразить информацию об активном SSH-соединении с маршрутизатором корпоративной сети.

Почему протокол SSH считается безопасным средством для удаленного управления устройствами?

_____

g. Перейдите в режим глобальной настройки. Для этого введите команду **configure terminal**.

h. С помощью команды **enable secret** создайте пароль **cisco**. Для этого введите команду **enable secret cisco**.

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Передача электронных сообщений от пользователя к пользователю	Шаг 2	2	
	Шаг 3	2	
Вопрос 2. Выгрузка файлов на сервер /с сервера по протоколу FTP	Шаг 2	2	
	Шаг 3d	2	
	Шаг 3e	2	
Вопрос 3. Удаленный доступ к маршрутизатору корпоративной сети по протоколу Telnet	Шаг 1	2	
Вопрос 4. Удаленный доступ к маршрутизатору корпоративной сети по протоколу SSH	Шаг 1	2	
Вопросы		**14**	
Балл Packet Tracer		**86**	
Общее число баллов		**100**	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. По какому протоколу письмо отправляется на сервер электронной почты??
2. По какому протоколу письмо принимается с сервера электронной почты?
3. Почему загрузка по протоколу FTP считается небезопасным способом передачи файлов?
4. Какая информация из FTP-заголовка отображается в виде открытого текста?
5. Какая конфиденциальная информация из FTP-заголовка (помимо имени пользователя) отображается в виде отрытого текста?
6. Почему протокол SSH считается безопасным средством для удаленного управления устройствами?

Занятие № 3.
Шифрование файлов и данных

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь осуществлять поиск данных учетной записи FTP.
3. Уметь осуществлять выгрузку конфиденциальных данных на сервер по протоколу FTP.
4. Уметь осуществлять загрузку конфиденциальных данных на сервер по протоколу FTP.
5. Приобрести навыки расшифровки содержимого файла.
6. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Поиск данных учетной записи FTP для ноутбука пользователя Mary.
2. Выгрузка конфиденциальных данных на сервер по протоколу FTP.
3. Поиск данных учетной записи FTP для компьютера пользователя Bob.
4. Загрузка конфиденциальных данных с сервера по протоколу FTP.
5. Расшифровка содержимого файла clientinfo.txt.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это задание, вы получите доступ к зашифрованному содержимому нескольких файлов и передадите файл через Интернет на центральный FTP-сервер. Затем другой пользователь загрузит файл с FTP-сервера и расшифрует содержимое файла. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Пользуясь клиентскими устройствами, которые находятся в различных географических регионах, вы передадите файл с зашифрованными данными с одного устройства на другое.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Mary	10.44.3.101	—	255.255.255.0	Healthcare at Home
Боб	10.44.1.3	—	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Поиск данных учетной записи FTP для ноутбука пользователя Mary

Шаг 1: Получение доступа к текстовому документу на ноутбуке пользователя Mary.

a. Откройте объект **Healthcare at Home** и выберите ноутбук **Mary**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).

c. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).

d. Выберите документ **ftplogin.txt** и нажмите кнопку **ОК**.

Шаг 2: Расшифровка данных учетной записи FTP пользователя Mary.

a. Выделите весь текст, содержащийся в файле **ftplogin.txt**, и скопируйте его.

b. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://encipher.it.

c. Поместите курсор в **белое поле, которое находится в правой части веб-сайта, и вставьте зашифрованный текст**.

Чтобы расшифровать текст, нажмите кнопку **Decipher It** (Расшифровать) и введите пароль расшифровки **maryftp123**. Нажмите **Decrypt** (Расшифровать).

Какие идентификационные данные (имя пользователя и пароль) соответствуют учетной записи FTP пользователя Mary?

_____

Учебный вопрос 2: Загрузка конфиденциальных данных на сервер по протоколу FTP

Шаг 1: Просмотр конфиденциального документа на ноутбуке пользователя Mary.

a. Откройте объект **Healthcare at Home** и выберите ноутбук **Mary**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).

c. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).

d. Выберите документ **clientinfo.txt** и нажмите кнопку **ОК**.

В какой форме представлены данные?

_____

Шаг 2: Удаленное подключение к FTP-серверу.

a. Откройте объект **Healthcare at Home** и выберите ноутбук **Mary**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

c. Подключитесь к серверу **FTP/Web** объекта **Metropolis Bank HQ**. Для этого введите команду **ftp 209.165.201.3** в командной строке.

d. Введите имя пользователя и пароль, найденные на Шаге 2 в Части 1.

Шаг 3: Загрузите файл на FTP-сервер.

a. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.

b. У пользователя Mary имеется файл с зашифрованной информацией о клиентах медицинского учреждения. Загрузите файл **clientinfo.txt** на FTP-сервер. Для этого введите команду **put clientinfo.txt**.

c. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы убедиться в том, что файл **clientinfo.txt** находится на FTP-сервере.

Если киберпреступники перехватят файл при его передаче через Интернет, то какую информацию они смогут получить в виде открытого текста?

_____

Учебный вопрос 3: Поиск данных учетной записи FTP для компьютера пользователя Bob

Шаг 1: Получение доступа к текстовому документу на компьютере пользователя Bob.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).

c. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).

d. Выберите документ **ftplogin.txt** и нажмите кнопку **ОК**.

Шаг 2: Расшифровка данных учетной записи FTP пользователя Bob.

a. Выделите весь текст, содержащийся в файле **ftplogin.txt**, и скопируйте его.

b. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://encipher.it.

c. Поместите курсор в **белое поле, которое находится в правой части веб-сайта, и вставьте зашифрованный текст**.

d. Чтобы расшифровать текст, нажмите кнопку **Decipher It** (Расшифровать) и введите пароль расшифровки **bobftp123**. Нажмите **Decrypt** (Расшифровать).

Какие идентификационные данные (имя пользователя и пароль) соответствуют учетной записи FTP пользователя Bob?

_____

Учебный вопрос 4: Загрузка конфиденциальных данных с сервера по протоколу FTP

Шаг 1: Удаленное подключение к FTP-серверу.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

c. Подключитесь к серверу **FTP/Web** объекта **Metropolis Bank HQ**. Для этого введите в командной строке команду **ftp 10.44.1.254**.

d. Введите имя пользователя и пароль, найденные на Шаге 2 в Части 3.

Шаг 2: Загрузите файл на компьютер пользователя Bob.

a. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.

b. Пользователь Mary загрузила на сервер файл clientinfo.txt с зашифрованной информацией о клиентах медицинского учреждения.

Загрузите файл **clientinfo.txt** на компьютер пользователя Bob. Для этого введите команду **get clientinfo.txt**.

c. В командную строку с подсказкой **ftp>** введите команду **quit**.

d. В командную строку с подсказкой **PC>** введите команду **dir**, чтобы убедиться в том, что файл **clientinfo.txt** находится на компьютере пользователя Bob.

Если киберпреступники перехватят файл при его передаче через Интернет, то какую информацию они смогут получить в виде открытого текста?

_____

Учебный вопрос 5: Расшифровка содержимого файла clientinfo.txt

Шаг 1: Получение ключа расшифровки от пользователя Mary.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).

c. В окне приложения Email (Электронная почта) нажмите кнопку **Receive** (Получить).

d. Выберите электронное сообщение с темой "Decryption Key" («Ключ расшифровки») и запишите ключ расшифровки ниже.

Какой ключ расшифровки необходим для доступа к конфиденциальной информации, содержащейся в файле clientinfo.txt?

_____

Шаг 2: Расшифровка содержимого файла clientinfo.txt.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).

c. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).

d. Выберите документ **clientinfo.txt** и нажмите кнопку **ОК**.

e. Выделите весь текст, содержащийся в файле **clientinfo.txt**, и скопируйте его.

f. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://encipher.it.

g. Поместите курсор в **белое поле, которое находится в правой части веб-сайта, и вставьте зашифрованный текст**.

Чтобы расшифровать текст, нажмите кнопку **Decipher It** (Расшифровать) и введите пароль расшифровки, полученный в электронном сообщении от пользователя Mary. Нажмите **Decrypt** (Расшифровать).

Каково имя первой учетной записи в файле clientinfo.txt?

_____

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Поиск данных учетной записи FTP для ноутбука пользователя Mary	Шаг 2	2	
Вопрос 2. Выгрузка конфиденциальных данных на сервер по протоколу FTP	Шаг 1	2	
	Шаг 3	2	

Вопрос 3. Поиск данных учетной записи FTP для компьютера пользователя Bob	Шаг 2	2	
Вопрос 4. Загрузка конфиденциальных данных с сервера по протоколу FTP	Шаг 2	2	
Вопрос 5. Расшифровка содержимого файла clientinfo.txt	Шаг 1	2	
	Шаг 2	2	
Вопросы		**14**	
Балл Packet Tracer		**86**	
Общее число баллов		**100**	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Какие идентификационные данные (имя пользователя и пароль) соответствуют учетной записи FTP пользователя Mary?

2. Если киберпреступники перехватят файл при его передаче через Интернет, то какую информацию они смогут получить в виде открытого текста?

3. Какие идентификационные данные (имя пользователя и пароль) соответствуют учетной записи FTP пользователя Bob?

4. Какой ключ расшифровки необходим для доступа к конфиденциальной информации, содержащейся в файле clientinfo.txt?

5. Каково имя первой учетной записи в файле clientinfo.txt?

Занятие № 4.
Проверка целостности файлов и данных

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь проверять целостность файлов с помощью хеширования.
3. Приобрести навыки проверки целостности критически важных файлов с помощью механизма HMAC.

Учебные вопросы занятия

1. Загрузка файлов с информацией о клиентах на компьютер пользователя Mike.
2. Загрузка файлов с информацией о клиентах на компьютер пользователя Mike с резервного файлового сервера Backup File.
3. Проверка целостности файлов с информацией о клиентах с помощью хеширования.
4. Проверка целостности критически важных файлов с помощью механизма HMAC.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это задание, вы будете проверять целостность файлов с помощью хеш-сумм, чтобы убедиться в том, что содержимое файлов не было искажено. Файлы, целостность которых вызовет сомнение, следует передать на компьютер пользователя Sally для дальнейшего анализа. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Вы будете проверять и пересылать подозрительные файлы с помощью клиентских устройств, которые находятся в различных географических регионах.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер FTP/Web	10.44.1.254	209.165.201.3 http://www.cisco.corp	255.255.255.0	Metropolis Bank HQ
Резервный файловый сервер Backup File	—	209.165.201.10 https://www.cisco2.corp	255.255.255.248	Интернет
Mike	10.44.2.101	—	255.255.255.0	Healthcare at Home
Sally	10.44.1.2	—	255.255.255.0	Metropolis Bank HQ
Боб	10.44.1.3	—	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike

Шаг 1: Получение доступа к FTP-серверу с компьютера пользователя Mike.

a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер с именем **Mike**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).

c. Введите URL-адрес **http://www.cisco.corp** и нажмите кнопку **Go** (Перейти).

d. Перейдите по ссылке, чтобы загрузить новейшие версии файлов.

По какому протоколу был предоставлен доступ к этой веб-странице на резервном файловом сервере Backup File?

_____

Шаг 2: Файловый сервер взломан. Об этом необходимо уведомить пользователя Sally.

a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер **Mike**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Email** (Электронная почта).

c. Создайте электронное сообщение с сообщением о взломе файлового сервера и отправьте это письмо на адрес Sally@cisco.corp.

Учебный вопрос 2: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike с резервного файлового сервера Backup File

Шаг 1: Получение доступа к внешнему FTP-серверу с компьютера пользователя Mike.

a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер **Mike**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).

c. Введите URL-адрес **https://www.cisco2.corp** и нажмите кнопку **Go** (Перейти).

d. Перейдите по ссылке, чтобы просмотреть список новейших файлов и соответствующих хеш-сумм.

По какому протоколу был предоставлен доступ к этой веб-странице на резервном файловом сервере Backup File?

_____

Каковы имена и хеш-суммы файлов на резервном файловом сервере?

_____

_____

_____

Шаг 2: Загрузка файлов с информацией о клиентах на компьютер пользователя Mike.

a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер **Mike**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

c. Установите соединение с резервным файловым сервером **Backup File**. Для этого введите в командную строку команду **ftp www.cisco2.corp**.

d. Введите имя пользователя **mike** и пароль **cisco123**.

e. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.

f. Загрузите шесть файлов с информацией о клиентах (NEclients.txt, NWclients.txt, Nclients.txt, SEclients.txt, SWclients.txt, Sclients.txt) на компьютер пользователя Mike с помощью команды **get FILENAME.txt**, где "FILENAME" — имя загружаемого файла.

ftp> **get NEclients.txt**

Чтение файла NEclients.txt с www.cisco2.corp:
File transfer in progress...

[Передача завершена — 584 байта]

584 bytes copied in 0.05 secs (11680 bytes/sec)

g. Загрузив все файлы, введите команду **quit** в командную строку с подсказкой **ftp>**.

h. В командную строку с подсказкой **PC>** введите команду **dir**, чтобы убедиться в том, что файлы с информацией о клиентах действительно находятся на компьютере пользователя Mike.

Учебный вопрос 3: Проверка целостности файлов с информацией о клиентах с помощью хеширования

Шаг 1: Проверка хеш-сумм на компьютере пользователя Mike.

a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер **Mike**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).

c. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).

d. Выберите документ **NEclients.txt** и нажмите кнопку **ОК**.

e. Полностью скопируйте содержимое текстового документа.

f. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт https://www.tools4noobs.com/online_tools/hash/.

g. Поместите курсор в белое поле ввода и вставьте содержимое текстового документа. Убедитесь в том, что выбран алгоритм md2. Нажмите кнопку **Hash this!** (Вычислить хеш-сумму).

h. Чтобы удостовериться в том, что содержимое файла не было искажено, сравните полученную хеш-сумму с соответствующей хеш-суммой из списка файлов, который вы получили на шаге 1 в части 2.

i. Повторите шаги d–h для каждого файла с информацией о клиентах и сравните полученные хеш-суммы с первоначальными хеш-суммами из списка файлов, который вы получили на шаге 1 в части 2.

Какой из файлов имеет некорректную хеш-сумму (то есть был искажен)?

_____

Шаг 2: Загрузка подозрительного файла на компьютер пользователя Sally.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Sally**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

c. Установите соединение с резервным файловым сервером **Backup File**. Для этого введите в командную строку команду **ftp www.cisco2.corp**.

d. Введите имя пользователя **sally** и пароль **cisco123**.

e. В командную строку с подсказкой **ftp>** введите команду **dir**, чтобы просмотреть список файлов, хранящихся на удаленном FTP-сервере.

f. Загрузите с сервера искаженный файл, выявленный на шаге 1 в части 3.

g. В командную строку с подсказкой **ftp>** введите команду **quit**.

h. В командную строку с подсказкой **PC>** введите команду **dir**, чтобы удостовериться в том, что искаженный файл успешно загружен на компьютер пользователя Sally для последующего анализа.

Учебный вопрос 4: Проверка целостности критически важных файлов с помощью механизма HMAC

Шаг 1: Расчет HMAC-суммы критически важного файла.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

c. В командную строку с подсказкой **PC>** введите команду **dir**, чтобы убедиться в том, что критически важный файл **income.txt** находится на компьютере пользователя Bob.

d. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Text Editor** (Текстовый редактор).

e. В окне приложения Text Editor (Текстовый редактор) выберите пункты меню **File** (Файл) > **Open** (Открыть).

f. Выберите документ **income.txt** и нажмите кнопку **ОК**.

g. Полностью скопируйте содержимое текстового документа.

h. Откройте веб-браузер на вашем персональном компьютере и перейдите на веб-сайт http://www.freeformatter.com/hmac-generator.html.

i. Поместите курсор в белое поле ввода и вставьте содержимое текстового документа. Введите секретный ключ **cisco123**. Убедитесь в том, что выбран алгоритм **SHA1**. Нажмите кнопку **Compute HMAC** (Рассчитать HMAC).

   Какова HMAC-сумма содержимого файла?

   _____

   Почему механизм HMAC безопаснее обычного хеширования?

   _____

Шаг 2: Проверьте полученную HMAC-сумму.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).

c. Введите URL-адрес **https://www.cisco2.corp** и нажмите кнопку **Go** (Перейти).

d. Перейдите по ссылке, чтобы просмотреть список новейших файлов и соответствующих хеш-сумм.

   Совпадает ли полученная хеш-сумма HMAC файла income.txt с хеш-суммой в списке?

   _____

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Загрузка файлов с информацией о клиентах на компьютер пользователя Mike	Шаг 1	2	
Вопрос 2. Загрузка файлов с информацией о клиентах на компьютер пользователя Mike с резервного файлового сервера Backup File	Шаг 1	2	
	Шаг 1	6	
Вопрос 3. Проверка целостности файлов с информацией о клиентах с помощью хеширования	Шаг 1	5	
Вопрос 4. Проверка целостности критически важных файлов с помощью механизма HMAC	Шаг 1	5	
	Шаг 1	5	
	Шаг 2	5	
Вопросы		**30**	
Балл Packet Tracer		**70**	
Общее число баллов		**100**	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. По какому протоколу был предоставлен доступ к веб-странице на резервном файловом сервере Backup File?
2. Каковы имена и хеш-суммы файлов на резервном файловом сервере?
3. Какой из файлов имеет некорректную хеш-сумму (то есть был искажен)?
4. Какова HMAC-сумма содержимого файла?
5. Почему механизм HMAC безопаснее обычного хеширования?
6. Совпадает ли полученная хеш-сумма HMAC файла income.txt с хеш-суммой в списке?

Занятие № 5.
WEP/WPA2 PSK/WPA2 RADIUS

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь настраивать WEP на объекте.
3. Уметь настраивать WPA2 PSK на объекте.
4. Уметь настраивать WPA2 RADIUS.
5. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Настройка WEP на объекте Healthcare at Home.
2. Настройка WPA2 PSK на объекте Gotham Healthcare Branch.
3. Настройка WPA2 RADIUS на объекте Metropolis Bank HQ.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это задание, вы настроите сети Wi-Fi на всех трех объектах. В этом упражнении вы будете работать с защитой WEP, WPA2 PSK и WPA2 RADIUS. Таким образом, вы познакомитесь с различными конфигурациями сетей Wi-Fi и особенностями обеспечения их безопасности. На объекте Healthcare at Home вы настроите защиту WEP. На объектах Gotham Healthcare Branch и Metropolis Bank HQ нужно будет настроить защиту WPA2 PSK и WPA2 Radius соответственно. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Вы настроите несколько безопасных беспроводных сетей, пользуясь беспроводными маршрутизаторами и клиентскими устройствами, которые находятся в различных географических регионах.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Сервер NTP/AAA	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Настройка WEP на объекте Healthcare at Home

Шаг 1: Настройка идентификатора SSID беспроводной сети.

a. Откройте объект **Healthcare at Home** и выберите **PC0**.

b. Выберите вкладку **Desktop**. Щелкните **Командная строка**. Введите в командную сроку команду **ipconfig**.

PC> **ipconfig**

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::20B:BEFF:FEB4:1262
IP Address.....: 10.44.3.100
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 10.44.3.1

Какой IP-адрес назначен шлюзу по умолчанию?

_____

c. Перейдите в приложение **Web Browser** (Браузер) и введите IP-адрес шлюза по умолчанию. Введите **admin** в качестве имени пользователя и пароля. Щелкните **OK**.

d. В этой сетевой инфраструктуре шлюзом по умолчанию является беспроводной маршрутизатор **Wireless Router**. Перейдите на вкладку **Wireless** (Беспроводная сеть).

e. Измените идентификатор **SSID** с **DefaultWIFI** на **Home**.

f. Включите передачу идентификатора SSID. Для этого выберите вариант **Broadcast** (Передавать).

g. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 2: Настройка защиты беспроводной сети.

a. Выберите беспроводной маршрутизатор Wireless Router и перейдите в раздел **Wireless** (Беспроводная сеть) > **Wireless Security** (Защита беспроводной сети).

b. В раскрывающемся меню Security Mode (Режим защиты) выберите **WEP**.

c. Параметр Encryption (Шифрование) имеет значение по умолчанию 40/64-bits (40/64 бита). Не меняйте это значение. В качестве ключа Key 1 введите **0123456789**.

d. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Защита WEP и ключ 0123456789 ненадежны. Почему алгоритм WEP считается недостаточно безопасным?

_____

_____

Шаг 3: Подключение клиентских устройств.

a. Откройте объект **Healthcare at Home** и выберите ноутбук **Dave**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **PC Wireless** (Беспроводная связь).

c. Перейдите на вкладку **Connect** (Подключиться) и нажмите кнопку **Refresh** (Обновить).

d. Выберите название беспроводной сети **Home** и нажмите кнопку **Connect** (Подключиться).

e. В качестве ключа WEP Key 1 введите ключ **0123456789** и нажмите кнопку **Connect** (Подключиться).

f. Повторите шаги **a–e** на ноутбуке **Mary**.

Учебный вопрос 2: Настройка WPA2 PSK на объекте Gotham Healthcare Branch

Шаг 1: Настройка идентификатора SSID беспроводной сети.

a. Откройте объект **Gotham Healthcare Branch** и выберите **PC1**.

b. Выберите вкладку **Desktop**. Щелкните **Командная строка**. Введите в командную сроку команду **ipconfig**.

Запишите IP-адрес шлюза по умолчанию.

_____

c. Перейдите в приложение **Web Browser** (Браузер) и введите IP-адрес шлюза по умолчанию. Введите **admin** в качестве имени пользователя и пароля. Щелкните **ОК**.

d. Перейдите на вкладку **Wireless** (Беспроводная сеть).

e. Измените идентификатор **SSID** с **DefaultWIFI** на **BranchSite**.

f. Измените значение параметра Standard Channel (Стандартный канал) на **6 — 2.437GHz**.

g. Включите передачу идентификатора SSID. Для этого выберите вариант **Broadcast** (Передавать).

h. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 2: Настройка защиты беспроводной сети.

a. Выберите беспроводной маршрутизатор Wireless Router и перейдите в раздел **Wireless** (Беспроводная сеть) > **Wireless Security** (Защита беспроводной сети).

b. В раскрывающемся меню Security Mode (Режим защиты) выберите **WPA2 Personal**.

c. Параметр Encryption по умолчанию имеет значение **AES**. Не меняйте это значение. В качестве фразы-пароля введите **ciscosecure**.

d. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 3: Подключение клиентских устройств.

a. Откройте объект **Gotham Healthcare Branch** и выберите компьютер **Tim**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **PC Wireless** (Беспроводная связь).

c. Перейдите на вкладку **Connect** (Подключиться) и нажмите кнопку **Refresh** (Обновить).

d. Выберите название беспроводной сети **BranchSite** и нажмите кнопку **Connect** (Подключиться).

e. Введите PSK-ключ **ciscosecure** и нажмите кнопку **Connect** (Подключиться).

f. Повторите шаги **a–e** на компьютере **Mike**.

Учебный вопрос 3: Настройка WPA2 RADIUS на объекте Metropolis Bank HQ

Шаг 1: Настройка идентификатора SSID беспроводной сети.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Sally**.

b. Перейдите в приложение **Web Browser** (Браузер) и введите IP-адрес беспроводного маршрутизатора (**10.44.1.251**). Введите **admin** в качестве имени пользователя и пароля. Щелкните **ОК**.

c. Перейдите на вкладку **Wireless**. Измените идентификатор **SSID** с **DefaultWIFI** на **HQ**.

d. Измените значение параметра Standard Channel (Стандартный канал) на **11 — 2.462GHz**.

e. Включите передачу идентификатора SSID. Для этого выберите вариант **Broadcast** (Передавать).

f. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 2: Настройка защиты беспроводной сети.

a. Выберите беспроводной маршрутизатор **Wireless Router** и перейдите в раздел **Wireless** (Беспроводная сеть) > **Wireless Security** (Защита беспроводной сети).

b. В раскрывающемся меню Security Mode (Режим защиты) выберите **WPA2-Enterprise**.

c. Параметр Encryption по умолчанию имеет значение **AES**. Не меняйте это значение. Введите следующие параметры сервера RADIUS:

RADIUS SERVER IP (IP-адрес сервера RADIUS): **10.44.1.252**

Shared Secret (Общий секретный ключ): **ciscosecure**

d. Нажмите кнопку **Save Settings** (Сохранить параметры). Щелкните **Continue**.

Шаг 3: Настройка сервера RADIUS.

a. Откройте объект **Metropolis Bank HQ** и выберите сервер **NTP/AAA**.

b. Перейдите на вкладку **Services** (Службы) и выберите раздел **AAA**.

c. Введите следующую информацию в области **Network Configuration** (Конфигурация сети):

Client Name (Имя клиента).....**HQ**

Client IP (IP-адрес клиента):.....**10.44.1.251**

Secret (Ключ):.....**ciscosecure**

ServerType (Тип сервера):.....**Radius**

d. Нажмите **Добавить**.

e. Введите указанные ниже данные в области **User Setup** (Параметры пользователей) и нажмите кнопку **Add** (Добавить), чтобы добавить новое имя пользователя.

Username (Имя пользователя):	**bob**	Password (Пароль):	**secretninjabob**
Username (Имя пользователя):	**phil**	Password (Пароль):	**philwashere**

Шаг 4: Подключение клиентских устройств.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Bob**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **PC Wireless** (Беспроводная связь).

c. Перейдите на вкладку **Profiles** (Профили) и нажмите кнопку **New** (Создать).

d. Введите имя профиля **RADIUS** и нажмите кнопку **OK**.

e. Нажмите **Advanced Setup** (Расширенная настройка).

f. В поле Wireless Network Name (Название беспроводной сети) введите **HQ** и нажмите **Next** (Далее).

g. Не меняя сетевые настройки, вновь нажмите **Next** (Далее).

h. В раскрывающемся меню Wireless Security (Режим защиты) выберите **WPA2-Enterprise** и нажмите **Next** (Далее).

i. Введите имя пользователя **bob** и пароль **secretninjabob**. Нажмите **Next** (Далее).

j. Нажмите **Save** (Сохранить), затем нажмите **Connect to Network** (Подключиться к сети).

k. Подключение компьютера **Bob** будет выполнено автоматически.

l. Повторите шаги **a–j** на ноутбуке **Phil**, используя аутентификационную информацию, указанную в описании шага 3e.

Почему в крупной организации разумнее применить режим WPA2 RADIUS вместо WPA2 PSK?

_____

_____

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Настройка WEP на объекте Healthcare at Home	Шаг 2	5	
Вопрос 3. Настройка WPA2 RADIUS на объекте Metropolis Bank HQ	Шаг 4	5	
Вопросы		**10**	
Балл Packet Tracer		**90**	
Общее число баллов		**100**	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Какой IP-адрес назначен шлюзу по умолчанию?

2. Защита WEP и ключ 0123456789 ненадежны. Почему алгоритм WEP считается недостаточно безопасным?

3. Запишите IP-адрес шлюза по умолчанию.

4. Почему в крупной организации разумнее применить режим WPA2 RADIUS вместо WPA2 PSK?

Занятие № 6.
Настройка транспортного режима VPN

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь передавать незашифрованный FTP-трафик.
3. Уметь передавать зашифрованный FTP-трафик.
4. Приобрести способность настраивать VPN-клиента на объекте.
5. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Передача незашифрованного FTP-трафика.
2. Настройка VPN-клиента на объекте Metropolis.
3. Передача зашифрованного FTP-трафика.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

Выполняя это задание, вы будете отслеживать передачу незашифрованного FTP-трафика между клиентом и удаленным объектом. Затем вы настроите VPN-клиент для подключения к объекту Gotham Healthcare Branch и начнете передачу зашифрованного FTP-трафика. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Передачу зашифрованных и незашифрованных FTP-данных вы будете выполнять с помощью клиентского устройства, которое находится в пределах объекта Metropolis Bank HQ.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Private_FTP server	10.44.2.254	—	255.255.255.0	Gotham Healthcare Branch
Public_FTP server	10.44.2.253	209.165.201.20	255.255.255.0	Gotham Healthcare Branch
Branch_Router	—	209.165.201.19	255.255.255.248	Gotham Healthcare Branch
Компьютер Phil's	10.44.0.2	—	255.255.255.0	Metropolis Bank HQ

Учебный вопрос 1: Передача незашифрованного FTP-трафика

Шаг 1: Получение доступа к анализатору трафика Cyber Criminals Sniffer.

a. Выберите анализатор трафика **Cyber Criminals Sniffer** и перейдите на вкладку **GUI** (Графический интерфейс).

b. Нажмите кнопку **Clear** (Очистить), чтобы удалить все собранные ранее записи с информацией о трафике.

c. Сверните окно анализатора трафика **Cyber Criminals Sniffer**.

Шаг 2: Установите небезопасное FTP-соединение с сервером Public_FTP.

a. Откройте объект **Metropolis Bank HQ** и выберите ноутбук **Phil**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **Command Prompt** (Командная строка).

c. Введите команду **ipconfig**, чтобы отобразить текущий IP-адрес компьютера **Phil**.

d. Установите соединение с сервером **Public_FTP** объекта **Gotham Healthcare Branch**. Для этого введите в командную строку команду **ftp 209.165.201.20**.

e. Введите имя пользователя **cisco** и пароль **publickey**, чтобы войти на сервер **Public_FTP**.

f. С помощью команды **put** выгрузите файл **PublicInfo.txt** на сервер **Public_FTP**.

Шаг 3: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer.

a. Разверните свернутое ранее окно анализатора трафика **Cyber Criminals Sniffer**.

b. В анализаторе трафика выберите сообщения **FTP** и полностью прокрутите содержимое каждого из сообщений.

Какая информация отображается в виде открытого текста?

_____

c. Введите **quit**, чтобы завершить сеанс на сервере **Public_FTP**.

Учебный вопрос 2: Настройка VPN-клиента на компьютере пользователя Phil

a. На компьютере **Phil's** выполните команду **ping**, указав IP-адрес маршрутизатора **Branch_Router**. Первые несколько ping-запросов могут остаться без ответа из-за превышения времени ожидания. Введите команду **ping**. Вы должны получить ответы на четыре ping-запроса.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **VPN**

c. В окне **VPN Configuration** (Настройка VPN) введите следующие параметры:

GroupName (Имя группы)..... **VPNGROUP**

Group Key (Ключ группы)..... **123**

Host IP (Server IP) (IP-адрес хоста (IP-адрес сервера)):..... **209.165.201.19**

Username (Имя пользователя):..... **phil**

Password (Пароль)..... **cisco123**

d. Нажмите кнопку **Connect** (Подключиться) и затем кнопку **ОК** в следующем окне.

Какой IP-адрес клиента применяется для установки VPN-соединения «клиент-объект»?

_____

Учебный вопрос 3: Передача зашифрованного FTP-трафика

Шаг 1: Просмотр текущих параметров IP-адресации на компьютере пользователя Phil.

a. Откройте объект **Metropolis Bank HQ** и выберите компьютер **Phil**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и нажмите значок **Command Prompt** (Командная строка).

c. С помощью команды **ipconfig** отобразите текущий IP-адрес компьютера **Phil**.

Видите ли вы дополнительный IP-адрес, который не отображался ранее на шаге 2c в части 1? Какой это адрес?

_____

Шаг 2: Передача зашифрованного FTP-трафика с компьютера пользователя Phil на сервер Private_FTP.

a. Установите соединение с сервером **Private_FTP** объекта **Gotham Healthcare Branch**. Для этого введите команду **ftp 10.44.2.254** в командную строку.

b. Введите имя пользователя **cisco** и пароль **secretkey**, чтобы войти на сервер **Private_FTP**.

c. Выгрузите файл **PrivateInfo.txt** на сервер **Private_FTP**.

Шаг 3: Просмотр информации о трафике с помощью анализатора трафика Cyber Criminals Sniffer

a. Разверните свернутое ранее окно анализатора трафика **Cyber Criminals Sniffer**.

b. Выберите сообщения **FTP** в окне анализатора трафика.

Есть ли среди них FTP-сообщения, в которых отображается внутренний пароль или информация о выгрузке файла PrivateInfo.txt на сервер? Дайте пояснение.

_____

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Передача незашифрованного FTP-трафика	Шаг 3	20	
Вопрос 2. Настройка VPN-клиента на компьютере пользователя Phil	Шаг 1	10	
Вопрос 3. Передача зашифрованного FTP-трафика	Шаг 1	10	
	Шаг 3	20	
Вопросы		**60**	
Балл Packet Tracer		**40**	
Общее число баллов		**100**	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Какая информация отображается в виде открытого текста?

2. Какой IP-адрес клиента применяется для установки VPN-соединения «клиент-объект»?

3. Видите ли вы дополнительный IP-адрес, который не отображался ранее на шаге 2c в части 1? Какой это адрес?

4. Есть ли среди FTP-сообщений FTP-сообщения, в которых отображается внутренний пароль или информация о выгрузке файла PrivateInfo.txt на сервер? Дайте пояснение.

Занятие № 7.
Резервирование маршрутизаторов и коммутаторов

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Приобрести способность наблюдения за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов.
3. Приобрести способность наблюдения за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов.
4. Приобрести навыки анализа и обобщения полученных результатов.

Учебные вопросы занятия

1. Наблюдение за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов.
2. Наблюдение за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

В этом задании вы будете наблюдать за успешным переключением при отказе сетевой инфраструктуры Metropolis. Для резервирования шлюза по умолчанию используются несколько маршрутизаторов. Затем будет проведено успешное переключение при отказе сетевой инфраструктуры Gotham. Резервирование сетевых маршрутов будет обеспечиваться с помощью нескольких коммутаторов. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. Для тестирования маршрутов до и после успешного переключения при отказе сетевой инфраструктуры вы будете использовать клиентские устройства в различных географических регионах.

Таблица адресации

Устройство	IP-адрес	Маска подсети	Шлюз по умолчанию	Сайт
Внешний веб-сервер	209.165.201.10	255.255.255.0	—	Интернет
R1	10.44.1.2	255.255.255.0	—	Metropolis Bank HQ
R2	10.44.1.3	255.255.255.0	—	Metropolis Bank HQ
Компьютер Phil's	10.44.1.12	255.255.255.0	10.44.1.1	Metropolis Bank HQ
Компьютер Tim's	10.44.2.11	255.255.255.0	10.44.2.1	Gotham Healthcare Branch

Учебный вопрос 1: Понаблюдайте за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов.

Шаг 1: Откройте командную строку на компьютере пользователя Phil.

a. Выберите узел **Metropolis Bank HQ** и выберите ноутбук **Phil**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

Шаг 2: Проследите маршрут к внешнему веб-серверу.

a. Отправьте ping-запрос к серверу **External Web** в **Интернете**. Для этого в командной строке введите **ping 209.165.201.10**.

b. Проследите маршрут к серверу **External Web** в **Интернете**. Для этого в командной строке введите **tracert 209.165.201.10**.

c. IP-адреса в выводе команды **tracert** представляют сетевые устройства, через которые проходит сетевой трафик.

Укажите IP-адреса устройств, через которые проходит трафик от ноутбука пользователя Phil до внешнего веб-сервера.

_____

Первый адрес, который выводит команда **tracert**, — это сетевой шлюз (точка выхода) по умолчанию.

d. Сравните вывод команды **tracert** с таблицей адресации, приведенной в начале лабораторной работы. Какой маршрутизатор в данный момент является текущим шлюзом по умолчанию?

_____

Шаг 3: Запустите переключение при отказе сетевой инфраструктуры.

a. В узле **Metropolis Bank HQ** нажмите коммутатор **HQ_S1**.

b. Щелкните вкладку **«Интерфейс командной строки» (CLI)**.

c. Введите следующие команды, чтобы отключить порт каскадирования Gig0/2:

```
enable
configure terminal
interface GigabitEthernet0/2
shutdown
```

Шаг 4: Снова проследите маршрут к внешнему веб-серверу.

a. В узле **Metropolis Bank HQ** нажмите ноутбук **Phil**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

c. Отправьте ping-запрос к серверу **External Web** в **Интернете**. Для этого в командной строке введите **ping 209.165.201.10**.

d. Проследите маршрут к серверу **External Web** в **Интернете**. Для этого в командной строке введите **tracert 209.165.201.10**.

IP-адреса в выводе команды **tracert** представляют сетевые устройства, через которые проходит сетевой трафик.

Укажите IP-адреса устройств, через которые проходит трафик от ноутбука пользователя Phil до внешнего веб-сервера.

_____

e. Первый адрес, который выводит команда **tracert**, — это сетевой шлюз (точка выхода) по умолчанию.

Какой маршрутизатор теперь работает как шлюз по умолчанию?

_____

f. В появившейся **командной строке** введите команду **ipconfig**. Для шлюза по умолчанию показан IP-адрес 10.44.1.1, который не совпадает ни с первым (10.44.1.2), ни со вторым (10.44.1.3) выводом команды tracert. Это указывает на то, что маршрутизация трафика шлюза по умолчанию 10.44.1.1 фактически выполняется через резервные маршрутизаторы с различными IP-адресами: R1 с адресом 10.44.1.2 или R2 с адресом 10.44.1.3, если маршрутизатор R1 недоступен.

Учебный вопрос 2: Понаблюдайте за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов.

Шаг 1: Откройте командную строку на компьютере Tim's.

a. Выберите узел **Gotham Healthcare Branch** и выберите компьютер **Tim**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

Шаг 2: Проследите маршрут к внешнему веб-серверу.

a. Отправьте ping-запрос к серверу **External Web** в **Интернете**. Для этого в командной строке введите **ping 209.165.201.10**.

b. Для наблюдения за переключением при отказе сетевой инфраструктуры можно использовать команду constant ping.

Выполните команду constant ping для сервера **External Web**. Для этого в командной строке введите **ping -t 209.165.201.10**.

Сверните окно для компьютера пользователя Tim.

Шаг 3: Запустите переключение при отказе сетевой инфраструктуры.

a. В узле **Gotham Healthcare Branch** нажмите коммутатор **S3**.

b. Перейдите на вкладку **CLI**.

c. Введите следующие команды, чтобы отключить порт каскадирования Gig0/2:

enable
configure terminal
interface GigabitEthernet0/2
shutdown

Шаг 4: Снова проследите маршрут к внешнему веб-серверу.

a. В узле **Gotham Healthcare Branch** разверните окно, отображающее компьютер пользователя Tim.

b. Подождите 30–60 секунд. Также можно наблюдать за индикаторами соединений коммутационного порта в сетевой инфраструктуре Gotham Healthcare Branch.

c. Вывод результатов выполнения команды на компьютере пользователя Tim должен быть аналогичен следующему:

PC> **ping -t 209.165.201.10**
Pinging 209.165.201.10 with 32 bytes of data:

Reply from 209.165.201.10: bytes=32 time=47ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126

Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
Reply from 209.165.201.10: bytes=32 time=43ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 209.165.201.10: bytes=32 time=41ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126

d. Закройте окно.

По какому кабелю передавались данные при получении ответов на ping-запросы **до** появления сообщения "Request timed out" (Время ожидания запроса истекло)?

_____

По какому кабелю передавались данные при получении ответов на ping-запросы **после** появления сообщения "Request timed out" (Время ожидания запроса истекло)?

_____

e. О какой особенности резервирования коммутаторов для переключения при отказе гигабитного Ethernet-порта свидетельствует этот сценарий?

_____

_____

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Наблюдение за переключением при отказе сетевой инфраструктуры с использованием резервных маршрутизаторов	Шаг 2	10	
	Шаг 2	10	
	Шаг 4	10	
	Шаг 4	10	
Вопрос 2. Наблюдение за переключением при отказе сетевой инфраструктуры с использованием резервных коммутаторов	Шаг 4	5	
	Шаг 4	5	
	Шаг 4	10	
Вопросы		**60**	
Балл Packet Tracer		**40**	
Общее число баллов		**100**	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Укажите IP-адреса устройств, через которые проходит трафик от ноутбука пользователя Phil до внешнего веб-сервера.

2. Укажите IP-адреса устройств, через которые проходит трафик от ноутбука пользователя Phil до внешнего веб-сервера.

3. Какой маршрутизатор работает как шлюз по умолчанию?

4. По какому кабелю передавались данные при получении ответов на ping-запросы до появления сообщения "Request timed out" (Время ожидания запроса истекло)?

5. По какому кабелю передавались данные при получении ответов на ping-запросы после появления сообщения "Request timed out" (Время ожидания запроса истекло)?

6. О какой особенности резервирования коммутаторов для переключения при отказе гигабитного Ethernet-порта свидетельствует этот сценарий?

Занятие № 8.
Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе

Цели занятия

В результате настоящего занятия и последующей самостоятельной работы студенты должны:

1. Закрепить материал, полученный на лекционных занятиях.
2. Уметь осуществлять подключение к веб-серверу.
3. Уметь осуществлять предотвращение незашифрованных сеансов HTTP.
4. Приобрести навыки доступа к межсетевому экрану на сервере электронной почты.
5. Приобрести способность формировать процедуры для управления информационной безопасностью.

Учебные вопросы занятия

1. Подключение к веб-серверу.
2. Предотвращение незашифрованных сеансов HTTP.
3. Доступ к межсетевому экрану на сервере электронной почты.

Оборудование и материалы

ПК с установленным Packet Tracer.

Общие сведения

В этом задании вы получите доступ к пользователю в узле Metropolis и подключитесь по протоколам HTTP и HTTPS к удаленному веб-серверу. Настройка IP-адресации, сети и сервисов в соответствии с таблицей адресации. С помощью клиентского устройства в узле Metropolis вы протестируете подключение к удаленному веб-серверу. Чтобы обеспечить защиту узла Metropolis, вы запретите незашифрованное соединение с внешними веб-сеансами.

Таблица адресации

Устройство	Частный IP-адрес	Общедоступный IP-адрес	Маска подсети	Сайт
Веб-сервер	—	209.165.201.10	255.255.255.0	Интернет

Учебный вопрос 1: Подключение к веб-серверу.

Шаг 1: Установите доступ к веб-серверу HQ Internet с ПК пользователя Sally по протоколу HTTP.

a. Выберите узел **Metropolis Bank HQ** и выберите ПК **Sally**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).

c. Введите URL-адрес **http://www.cisco.corp** и нажмите **Go** (Начать).

d. Щелкните ссылку **Login Page** (Страница входа).

Почему пользователь должен быть обеспокоен при отправке информации через этот веб-сайт?

_____

Шаг 2: Установите доступ к веб-серверу HQ Internet с компьютера пользователя Sally по протоколу HTTPS.

a. Откройте **веб-обозреватель** на компьютере Sally's.

b. Введите URL-адрес **https://www.cisco.corp** и нажмите Go (Начать).

c. Щелкните ссылку **Login Page** (Страница входа).

У пользователя меньше поводов для беспокойства при отправке информации через этот веб-сайт. Почему?

_____

d. Закройте компьютер пользователя **Sally**.

Учебный вопрос 2: Запрет незашифрованных сеансов HTTP.

Шаг 1: Настройте маршрутизатор HQ_Router.

a. Откройте объект **Metropolis Bank HQ** и выберите маршрутизатор **HQ_Router**.

b. Нажмите вкладку **CLI** и нажмите **Enter**.

c. Для входа в систему маршрутизатора используйте пароль **cisco**.

d. Введите команду **enable**, а затем **configure terminal** для доступа к режиму глобальной настройки.

Чтобы предотвратить передачу незашифрованного HTTP-трафика через головной маршрутизатор, сетевые администраторы могут создать и развернуть списки контроля доступа (ACL).

Следующие команды выходят за рамки этого курса. Они используются для демонстрации возможности предотвращения передачи незашифрованного трафика через маршрутизатор HQ_Router.

e. В командной строке **HQ_Router**(config)# в режиме глобальной настройки скопируйте и вставьте показанную ниже конфигурацию списка контроля доступа в **HQ_Router**.

```
!
access-list 101 deny tcp any any eq 80
access-list 101 permit ip any any
!
int gig0/0
ip access-group 101 in
!
end
```

f. Закройте маршрутизатор **HQ_Router**.

Шаг 2: Установите доступ к веб-серверу HQ Internet с ПК пользователя Sally по протоколу HTTP.

a. В узле **Metropolis Bank HQ** нажмите ПК пользователя **Sally**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Web Browser** (Браузер).

c. Введите URL-адрес **http://www.cisco.corp** и нажмите **Go** (Начать).

Может ли компьютер пользователя **Sally** получить доступ к веб-серверу HQ Internet по протоколу HTTP?

_____

Шаг 3: Установите доступ к веб-серверу HQ Internet с компьютера пользователя Sally по протоколу HTTPS.

a. Откройте **веб-обозреватель** на компьютере Sally's.

b. Введите URL-адрес **https://www.cisco.corp** и нажмите Go (Начать).

Может ли компьютер пользователя "Sally" получить доступ к веб-серверу HQ Internet по протоколу HTTP?

_____

c. Закройте компьютер пользователя **Sally**.

Учебный вопрос 3: Доступ к межсетевому экрану на сервере электронной почты.

a. В узле **Metropolis Bank HQ** нажмите сервер **Email**.

b. Нажмите вкладку **Desktop** (Рабочий стол) и выберите **Firewall** (Межсетевой экран). Правила межсетевого экрана не заданы.

Чтобы предотвратить отправку или получение через сервер электронной почты трафика, не связанного с ней, сетевые администраторы могут создавать правила межсетевого экрана непосредственно на сервере. Либо, как показано ранее, можно использовать списки контроля доступа (ACL) на сетевом устройстве, например, маршрутизаторе.

Предлагаемый способ подсчета баллов

Вопросы занятия	Шаги вопроса	Максимальное количество баллов	Заработанные баллы
Вопрос 1. Подключение к веб-серверу	Шаг 1	15	
	Шаг 2	15	
Вопрос 2. Предотвращение незашифрованных сеансов HTTP	Шаг 2	15	
	Шаг 3	15	
Вопросы		**60**	
Балл Packet Tracer		**40**	
Общее число баллов		**100**	

Содержание отчета

Отчет по практическому занятию должен содержать:

1. Структуру исходных данных в Packet Tracer с IP-адресацией устройств.
2. Ответы на вопросы, поставленные в ходе выполнения практических заданий.
3. Выводы о проделанной работе и полученных результатах.

Результаты работы должны быть отражены в рабочей тетради и защищены устно каждым студентом.

Контрольные вопросы

1. Почему пользователь должен быть обеспокоен при отправке информации через этот веб-сайт?

2. У пользователя меньше поводов для беспокойства при отправке информации через веб-сайт https://www.cisco.corp. Почему?

3. Может ли компьютер пользователя **Sally** получить доступ к веб-серверу HQ Internet по протоколу HTTP?

4. Может ли компьютер пользователя "**Sally**" получить доступ к веб-серверу HQ Internet по протоколу HTTP?

5 Учебно-методическое и информационное обеспечение

Перечень основной литературы:

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. - Санкт-Петербург: Лань, 2021. - 324 с. - ISBN 978-5-8114-6738-9.- Текст: электронный //

2. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. - 3-е изд., стер. - СанктПетербург: Лань, 2021. - 108 с. - ISBN 978-5-8114-8370-9. - Текст: электронный //

3. Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. - 4-е изд., стер. - СанктПетербург: Лань, 2022. - 124 с. - ISBN 978-5-507-44201-0. - Текст: электронный//

Перечень дополнительной литературы:

Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. - 3-е изд., стер. - СанктПетербург: Лань, 2021. - 124 с. - ISBN 978-5-8114-7970-2.- Текст: электронный//

2. Фомин, Д. В. Информационная безопасность: учебник / Д. В. Фомин. - Москва: Ай Пи Ар Медиа, 2022. - 222 с. - ISBN 978-5-4497- 1548-7. - Текст: электронный //

Перечень учебно-методического обеспечения по дисциплине

1.Курс лекций по дисциплине "Защита информации профессиональной деятельности"

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1.Информационная справочная система КонсультантПлюс. // Режим доступа: http://www.consultant.ru

2.Профессиональная база данных Росстата // Режим доступа: Росстат — Базы данных (https://rosstat.gov.ru)