МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

ФИЛИАЛ ФГБОУ ВО «ЮГУ»
НЕФТЯНОЙ ИНСТИТУТ

МДК 02.03
КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Методические указания к выполнению практических занятий для обучающихся 2 курса всех форм обучения образовательных организаций среднего профессионального образования

Часть 1

Нижневартовск, 2022

ББК 32.81
К 66

РАССМОТРЕНО
На заседании ПЦК «МиЕНД»
Протокол № 9 от 15.10.2022
Председатель Бойко Я.С.

УТВЕРЖДЕНО
Председателем методического совета
НефтИн (филиала) ФГБОУ ВО «ЮГУ»
Хайбулина Р.И.
« 10 » ноября 2022 г.

Методические указания к выполнению практических занятий для обучающихся 2 курса всех форм обучения образовательных организаций среднего профессионального образования по МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ), часть 1, разработаны в соответствии с:

1. Федеральным государственным образовательным стандартом (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденным МИНОБРНАУКИ от 09.12.2016 № 1553.
2. Рабочей программой учебной дисциплины ПМ.01 Эксплуатация автоматизированных (информационных) систем оборудования, утверждённой на методическом совете НефтИн (филиал) ФГБОУ ВО «ЮГУ» протоколом № 4 от 31.08.2022 года.

Разработчик:
1. Бойко Яна Сергеевна, преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ».
2. Баталкина Анастасия Геннадьевна, преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ».

Рецензенты:
1. Валиева Л.Ф., преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ».
2. Фазылова Е.Х., преподаватель БУ «Нижневартовский строительный колледж».

Замечания, предложения и пожелания направлять в Нефтяной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Югорский государственный университет» по адресу: 628615, Тюменская обл., Ханты-Мансийский автономный округ, г. Нижневартовск, ул. Мира, 37.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Основное назначение МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности в средних профессиональных образовательных организациях состоит в формировании у обучающихся общих и профессиональных компетенций:

– выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;

– осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности;

– планировать и реализовывать собственное профессиональное и личностное развитие;

– работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами;

– осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста;

– проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей;

– содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях;

– использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности;

– использовать информационные технологии в профессиональной деятельности;

– пользоваться профессиональной документацией на государственном и иностранном языках;

– осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации;

– обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами;

– осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации;

– осуществлять обработку, хранение и передачу информации ограниченного доступа;

– уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств;

– осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Практическое занятие – это форма организации учебного процесса, предполагающая выполнение обучающимися заданий самостоятельно и под руководством преподавателя. Дидактическая цель практических работ – формирование у обучающихся профессиональных и практических умений, необходимых для изучения последующих учебных дисциплин, а также подготовка к применению этих умений в профессиональной деятельности.

Практические занятия предполагают работу, связанную с криптографической защитой информации.

Структура практических занятий включает в себя:

– теоретические вопросы по изучаемым темам,

– практические задания для решения с помощью программных средств.

Разработано содержание практических занятий, определена их цель, даны методические указания по выполнению заданий и упражнений, указана учебная и справочная литература. Структура рекомендаций соответствует структуре междисциплинарного курса Корпоративная защита от внутренних угроз информационной безопасности.

Правила выполнения практических работ:

В ходе выполнения практических работ обучающийся должен:

✓ выполнять требования по охране труда

✓ соблюдать инструкцию по правилам и мерам безопасности в лаборатории информационных технологий

✓ строго выполнять весь объем работы, указанный в задании

✓ соблюдать требования эксплуатации компьютерной техники (правила включения и выключения)

✓ изучить теоретические вопросы, используя лекционный материал к теме

✓ предоставить отчет о проделанной работе по окончании выполненной работы.

Рекомендации по оформлению практической работы:

✓ при выполнении практической работы в программе MS Word необходимо выбирать гарнитуру и размер шрифтов, выравнивание, отступы и интервалы в соответствии с заданием;

✓ при выполнении в программе MS Word практической работы содержащей таблицы соблюдать структуру и выравнивание ячеек таблиц, цвет границы и заливки фигур;

✓ при выполнении практической работы в программе в MS Excel соблюдать формат и выравнивание ячеек, название листов, точность вычислений в соответствии с заданием.

✓ при выполнении практической работы в программе MS Power Point необходимо выбирать гарнитуру и размер шрифтов, выравнивание, отступы и интервалы, макеты оформления, графические объекты, анимацию и переходы в соответствии с заданием;

✓ при выполнении практической работы в программе MS Access

(создание базы) в таблицы добавлять не менее 10 записей, таблицы переименовывать в соответствии с заданием, отчеты формировать в табличной форме, кнопочная форма обязательна.

Работы проводятся согласно календарно-тематическому планированию, в соответствии с учебной программой. Пропущенные практические работы выполняются обучающимися самостоятельно и сдаются в отведенные на изучение дисциплины сроки.

Критерии оценивания:

Оценка «Отлично» - полно раскрыто содержание материала в объеме, предусмотренном программой, практическая работа выполнена правильно, в полном объеме и защищена.

Оценка «Хорошо» - в изложении материала допущены небольшие пробелы, не исказившие логического и информационного содержания ответа; допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; в выполненной практической работе допущены в ответах отдельные неточности, исправленные с помощью преподавателя.

Оценка «Удовлетворительно» - неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии; практическая работа выполнена частично, допущены ошибки и неточности, которые не всегда исправляются с помощью преподавателя.

Оценка «Неудовлетворительно» - не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала; практическая работа носит трафаретный характер, выполнена неправильно или не выполнена вовсе.

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Номер темы	Номер и наименование работы (занятия)	Количество аудиторных часов	Формируемые компетенции
1	2	3	4
1.1	Практическое занятие № 1-2. Организация безопасной, аккуратной и эффективной рабочей зоны	4	ПК 2.6, ОК 1– ОК 10
1.1	Практическое занятие № 3-4. Планирование работы специалиста по информационной безопасности в соответствии с изменяющимися приоритетами	4	ПК 2.6, ОК 1– ОК 10

1	2	3	4
2.1	Практическое занятие № 5-6. Конфигурация сетевой инфраструктуры: настройка хост – машины, сетевого окружения, виртуальных машин	4	ПК 2.6, ОК 1– ОК 10

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1-2

ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ, АККУРАТНОЙ И ЭФФЕКТИВНОЙ РАБОЧЕЙ ЗОНЫ

Цель: изучить общие требования к организации рабочего места, изучить требования к безопасному содержанию рабочего места, составить рабочую зону для предприятия.

Теоретическая часть: (изучить)

Общие требования к организации безопасного рабочего места

I. Общие положения

1. Общие требования к организации безопасного рабочего места (далее – Требования) разработаны в целях обеспечения выполнения требований охраны труда работниками, занятыми на своих рабочих местах. Для рабочих мест с территориально меняющимися рабочими зонами, где рабочей зоной считается оснащенная необходимыми средствами производства часть рабочего места, в которой один работник или несколько работников выполняют схожие работы или технологические операции 1 положения Требований распространяются на каждую рабочую зону.

2. Рабочее место, его оборудование и оснащение, применяемые в соответствии с особенностями выполняемых работ, должны обеспечивать безопасность, охрану здоровья и работоспособность занятых на нем работников.

3. На рабочем месте (в рабочей зоне) должны быть приняты меры по снижению, по возможности, до установленных предельно допустимых значений уровней воздействия (концентрации) вредных и (или) опасных производственных факторов на занятых на данном рабочем месте работников с учетом применения ими средств индивидуальной (коллективной) защиты.

4. Рабочее место (рабочая зона), его размеры, взаимное расположение органов управления, средств отображения информации, размещение вспомогательного оборудования и инструментов должны соответствовать антропометрическим, физиологическим и психофизиологическим свойствам занятых на нем работников и особенностям выполняемой работы.

II. Требования к организации рабочего места

5. При организации рабочего места (рабочей зоны) должна быть обеспечена возможность смены рабочей позы занятыми на нем работниками.

6. В зависимости от особенностей выполняемой работы рабочая поза работника «сидя» является более удобной, чем рабочая поза «стоя». Если основной рабочей позой работника является положение «стоя», необходимо обеспечить периодическое чередование данной рабочей позы с положением «сидя», в том числе посредством организации места для сидения.

7. Удобство рабочей позы работника в положении «сидя» достигается регулированием взаимного положения места для сидения и рабочей поверхности, в том числе ее высоты и размеров, а также высоты и угла наклона подставки для ног при ее применении. При невозможности обеспечения указанного выше регулирования рабочей позы допускается использование рабочего места с нерегулируемыми параметрами. В этом случае высоту рабочей поверхности устанавливают, исходя из особенностей выполнения работы, требований к сенсорному контролю и обеспечению требуемой точности действий, среднего роста работающих (мужчин - если работают только мужчины, женщин - если работают только женщины, по-отдельности мужчин и женщин - если работают и мужчины, и женщины).

8. При организации рабочего места (рабочей зоны) должно быть обеспечено выполнение трудовых операций в зонах «моторного поля» - зонах оптимальной, легкой досягаемости и возможной досягаемости, в зависимости от требуемой точности и частоты действий.

9. При организации рабочего места (рабочей зоны) должно быть обеспечено устойчивое положение и свобода движений занятого на нем работника, сенсорный контроль деятельности и безопасность выполнения трудовых операций.

10. При организации рабочего места (рабочей зоны) должны быть исключена или снижена до минимума продолжительность выполнения работы в неудобных 2 и вынужденных 3 позах (характеризующихся, например, необходимостью сильно наклоняться вперед или в стороны, приседать, работать с вытянутыми или высоко поднятыми руками, закинув голову назад), вызывающих повышенную утомляемость.

11. При организации рабочего места (рабочей зоны) необходимо обеспечить необходимый обзор наблюдения с места выполнения работ зоны информационного поля, визуальных средств отображения информации, знаков безопасности.

12. Средства отображения информации должны быть размещены в зонах информационного поля рабочего места с учетом частоты и значимости поступающей информации, типа средства отображения информации, точности и скорости слежения и считывания.

13. Визуальные средства отображения информации должны быть освещены в соответствии с нормативами и достаточно для восприятия отображаемой информации с места выполнения работ.

14. Органы управления машинами и оборудованием должны быть размещены на рабочем месте (в рабочей зоне) с учетом рабочей позы работника, функционального назначения органа управления, частоты

применения, последовательности использования, функциональной связи с соответствующими средствами отображения информации.

15. Расстояние между органами управления машинами и оборудованием должно исключать возможность произвольного изменения положения не задействованного органа управления при манипуляции с иным смежным органом управления.

16. Участки и зоны, где возможно травмирование работника, должны быть обозначены сигнальными цветами и знаками безопасности.

17. Применение знаков безопасности не заменяет необходимости информирования работника всеми доступными способами, которые могут предупредить или уменьшить вредное, или опасное воздействие на работников.

18. Рабочее место (рабочая зона), при необходимости, оснащается вспомогательным подъемно-транспортным оборудованием (средствами).

19. Цветовое оформление зон рабочего места должно соответствовать требованиям технической эстетики.

20. При организации рабочих мест их взаимное расположение и компоновка должны обеспечивать безопасный доступ занятых на них работников на каждое рабочее место и возможность быстрой эвакуации работников при возникновении аварийной или иной чрезвычайной ситуации. Пути эвакуации и проходы должны быть обозначены соответствующими указателями и иметь достаточную освещенность.

III. Требования к безопасному содержанию рабочего места

21. Рабочее место (рабочая зона) и взаимное расположение его элементов должны обеспечивать безопасное и удобное содержание, в том числе техническое обслуживание, уборку и чистку используемых на рабочем месте машин и оборудования, инструментов и мебели.

22. Организация и содержание рабочих мест, а также расстояния между рабочими местами должны обеспечивать безопасное передвижение работников и транспортных средств, удобные и безопасные действия с сырьем, материалами, заготовками, полуфабрикатами.

23. Работники должны выполнять следующие процедуры по содержанию своих рабочих мест (рабочих зон): - сортировку; - самоорганизацию; - систематическую уборку (содержание в чистоте).

24. При сортировке выполняется разделение предметов, включая инструменты, сырье и материалы, на являющиеся и не являющиеся источниками опасностей, на необходимые при выполнении конкретных работ на рабочем месте (в рабочей зоне) и не требующиеся при выполнении этих работ с последующей уборкой с рабочего места инструментов, сырья и материалов, не требующихся при выполнении указанных работ перед началом их выполнения.

25. При самоорганизации рабочего места (рабочих зон) обеспечивается соблюдение порядка на нем путем размещения на рабочем месте или в рабочей зоне при выполнении конкретных работ только необходимых для

этого предметов, включая инструменты, сырье и материалы, таким образом, чтобы максимально снизить риски реализации опасностей и получения микротравм при их использовании. При хранении предметов, включая инструменты сырье и материалы, на рабочем месте необходимо обязательно применять различные методы визуализации, такие как оконтуривание, маркировка, разметка, цветовое кодирование и другие аналогичные методы.

26. При систематической уборке (содержании в чистоте) обеспечивается постоянное поддержание рабочих мест (рабочих зон) с расположенными в них машинами, оборудованием, иными предметами, включая инструменты, сырье и материалы, в чистоте и постоянной готовности к использованию путем удаления отходов производства, например, стружки, опилок, окалины, пролитых технологических жидкостей и реагентов, пыли, мусора, использованной упаковки с рабочего места, а также размещения отходов в предназначенные для этого контейнеры.

27. Процедуры по содержанию рабочего места (рабочих зон) в соответствии с пунктом 23 Требований следует документировать в локальных нормативных актах работодателя в рамках Системы управления охраной труда (при наличии) или иных документах работодателя, например, инструкциях по охране труда.

28. Работодатель должен обеспечить процесс непрерывного совершенствования, поддержания и развития результатов, достигнутых при выполнении пунктов 23 и 27 Требований.

Практическое задание:

На основе изученных выше требований к безопасному содержанию рабочего места, составить рабочую зону для предприятия.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3-4

ПЛАНИРОВАНИЕ РАБОТЫ СПЕЦИАЛИСТА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ИЗМЕНЯЮЩИМИСЯ ПРИОРИТЕТАМИ

Цель: изучить проблемы информационной безопасности, разработать план мероприятий, обеспечивающий минимизацию информационных рисков по направлениям.

Теоретическая часть:

Проблемы информационной безопасности: алгоритм построения системы ИБ с нуля.

1. Заручиться поддержкой руководства.

Если отдел информационной безопасности создан по инициативе руководства компании, то проблема решена. Однако в реальности часто ИБ-отдел создается стихийно, при этом существует служба безопасности,

которая не очень понимает, что такое технические меры защиты, есть также ИТ-служба, которая воспринимает ИБ-отдел как помеху и т д.

Организация защиты информации на практике ведется одним из способов: «снизу вверх» либо «сверху вниз».

Подход «снизу вверх» наиболее распространен. В данном случае инициатива по всем ИБ-мероприятиям исходит от рядовых специалистов или линейных руководителей. Подход включает в себя написание служебных записок, доведение до руководства информации об инцидентах и прочее. Такой подход малоэффективен, так как высшее руководство компании не до конца понимает целесообразность и необходимость проведения большинства работ по информационной безопасности. В итоге информационной безопасности уделяется малое внимание, ей занимаются по остаточному принципу, работы зачастую носят несистемный характер.

Подход «сверху вниз» предполагает вовлеченность топ-менеджмента и владельцев бизнеса в проблематику информационной безопасности. Данный подход считается более эффективным, поскольку руководство смотрит на информационную безопасность с позиции бизнеса, ведется оценка рисков. Подход позволяет получать требуемые ресурсы и принимать необходимые меры, так как комплексная защита информации на предприятии — инициатива руководства.

На первом этапе следует заручиться поддержкой руководства, а в организации работ придерживаться подхода «сверху вниз».

2. Определить состав рабочей группы.

Важно определить, какие специалисты будут принимать активное участие в работах по информационной безопасности.

Есть мнение, что можно отдать работы по ИБ на аутсорсинг и полностью сосредоточиться на текущих задачах. Это верно лишь отчасти, поскольку никакие внешние эксперты не смогут оценить реальную важность и ценность информационных ресурсов компании, они могут лишь привнести объективный взгляд со стороны. Поэтому в рабочей группе обязательно должен быть представитель владельца информационных ресурсов.

3. Определить риски.

После того как сформирована рабочая группа и получена поддержка действий от руководства, переходим к этапу управления рисками. На этом этапе необходимо:

- идентифицировать информационные активы, представляющие ценность;
- провести анализ информационных ресурсов, к защите которых предъявляются требования со стороны законодательства/отрасли;
- провести анализ информационных ресурсов на существующие уязвимости с точки зрения информационной безопасности;
- провести анализ источников угроз;
- проанализировать сами угрозы;

- оценить возможный ущерб;
- подготовить отчет для презентации руководству.

После проведения этапа должен быть составлен список определенных угроз и оценен ущерб, который может быть потенциально нанесен компании при реализации этих угроз. При расчете ущерба следует учитывать вероятность наступления тех или иных угроз.

После оценки возможного ущерба необходимо проработать риски по каждой актуальной угрозе.

4. Принять организационные меры.

На данном этапе разрабатываются политики, стандарты, руководства и инструкции, направленные на поддержание системы ИБ. Фиксируется ответственность сотрудников за нарушение требований ИБ, разглашение и нарушение конфиденциальности информации. Важно понимать, что эффективная система ИБ не может существовать без регламентов, инструкций, документов, направленных на ее поддержание.

5. Выбрать и внедрить меры и средства защиты информации.

На этом этапе осуществляется выбор средств защиты информации и оценка их эффективности. Оценка эффективности нужна для понимания, окупятся ли затраты, потраченные на СЗИ. Прибыль здесь косвенная — минимизация рисков, которые были определены ранее.

При выборе мер и средств защиты необходимо руководствоваться правилом: затраты на приобретение, внедрение, настройку, обучение специалистов, сопровождение средств защиты не должны превышать ущерба от реализации угрозы, на защиту от которой эти средства направлены.

6. Довести информацию до заинтересованных лиц.

Важно донести до пользователей необходимую информацию по ИБ доступными для них способами. Сотрудникам лучше всего показать на практике, как безопасно работать и взаимодействовать, провести презентацию или обучение. Руководству полезно будет показать убытки, которые может получить компания в случае невыполнения мер по информационной безопасности. Специалистам нужно показать, какими средствами можно пользоваться, а какими нет и почему, а также озвучить ответственность за нарушения этих мер.

7. Провести мониторинг и оценку.

После проведения всех этапов необходимо провести мониторинг и оценку результатов работ. Важно понять, насколько изменилось состояние ИБ.

Например, хорошим показателем будет появление инцидентов или вопросов по ИБ после проведения обучения сотрудников. Если до обучения обращений по инцидентам не возникало, а после обучения стали появляться инциденты, значит, оно прошло не зря.

Но на этом работа не заканчивается. Цикличность работ по ИБ связана с тем, что информационная среда очень изменчива. Происходят изменения

внутри самих информационных активов, изменения в информационных технологиях, в способах обработки информации, а значит, нужно снова возвращаться к анализу рисков и актуализации системы ИБ.

Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

Организация просвещения сотрудников Департамента и подведомственных учреждений в области информационной безопасности возлагается на администратора информационной безопасности. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности». Обучение сотрудников Департамента правилам обращения с конфиденциальной информацией, проводится путем:

- проведения администратором информационной безопасности инструктивных занятий с сотрудниками, принимаемыми на работу в Департамент;
- самостоятельного изучения сотрудниками внутренних нормативных документов Департамента.

Допуск сотрудников к работе с защищаемыми информационными ресурсами Департамента осуществляется только после его ознакомления с настоящими Регламентом. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками Департамента, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

Практическое задание:

«Разработка плана мероприятий по защите информации на предприятии»

Разработать план мероприятий, обеспечивающий минимизацию информационных рисков по трём направлениям:

- организационно-правовые мероприятия;
- обеспечение физической защиты информации;
- внедрение программно - аппаратных средств защиты информации.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5-6

КОНФИГУРАЦИЯ СЕТЕВОЙ ИНФРАСТРУКТУРЫ: НАСТРОЙКА ХОСТ – МАШИНЫ, СЕТЕВОГО ОКРУЖЕНИЯ, ВИРТУАЛЬНЫХ МАШИН

Цель: научиться включать на сервере программу Удаленный рабочий стол для администрирования; включать пользователей в соответствующую

группу, чтобы разрешить им удаленно администрировать сервер; подключаться к серверу с помощью программы Удаленный рабочий стол для администрирования.

Теоретическая часть:

В семействе Windows Server был впервые реализован тесно интегрированный набор программных средств и технологий, позволяющих выполнять удаленное администрирование и совместно использовать приложения с помощью Служб терминалов (Terminal Services).

Эволюция продолжилась: отныне службы терминалов — неотъемлемый компонент семейства Windows Server, а инструмент Дистанционное управление рабочим столом (Remote Desktop) усовершенствован и позиционируется как стандартная функция. Так что теперь достаточно одного щелчка мыши, и компьютер с Windows Server будет параллельно обрабатывать до двух подключений удаленного администрирования. Добавив компонент Сервер терминалов (Terminal Server) и настроив соответствующую лицензию, администратор добьется еще большего эффекта: множество пользователей смогут запускать приложения на сервере. На этом занятии вы научитесь работать со служебной программой Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

Включение и конфигурирование программы Удаленный рабочий стол для администрирования.

Службы терминалов позволяют совместно использовать приложения с помощью таких инструментов, как Дистанционное управление рабочим столом (Remote Desktop), Удаленный помощник (Remote Assistance) и Сервер терминалов (Terminal Server). По умолчанию служба устанавливается вместе с Windows Server и настраивается в программе Дистанционное управление рабочим столом для работы в режиме удаленного администрирования: допускает только два параллельных удаленных подключения и не содержит компоненты для совместного использования приложений из состава Сервера терминалов. Следовательно, Дистанционное управление рабочим столом создает очень небольшую дополнительную нагрузку на систему, причем не требует дополнительного лицензирования.

Примечание Поскольку Службы терминалов и Дистанционное управление рабочим столом являются стандартными компонентами Windows Server, каждый сервер способен поддерживать удаленные подключения к своей консоли. Термин «сервер терминалов», таким образом, теперь по праву можно применить к любому компьютеру под управлением Windows Server, обеспечивающему совместное использование приложений несколькими клиентами за счет добавления компонента Службы терминалов.

Другие компоненты — Сервер терминалов и службу Лицензирование сервера терминалов (Terminal Server Licensing) — нужно добавлять с

помощью функции Установка и удаление программ (Add Or Remove Programs). Тем не менее, все средства администрирования для настройки и поддержки клиентских подключений и управления сервером терминалов устанавливаются по умолчанию на все компьютеры с Windows Server.

Эти средства и их функции описаны в таблице 1.

Таблица 1 – Стандартные компоненты *Сервер терминалов* и *Подключение к удаленному рабочему столу*

Установленное ПО	Назначение
Настройка служб терминалов (Terminal Services Configuration)	Настройка свойств сервера терминалов, в том числе параметров сеанса, сети, клиентского рабочего стола и удаленного управления клиентом
Диспетчер служб терминалов (Terminal Services Manager)	Отправка сообщений клиентам, подключенным к серверу терминалов, отключение или завершение сеансов, а также инициирование удаленного управления или маскировки сеансов
Подключение к удаленному рабочему столу (Установочные файлы клиента Remote Desktop Connection)	Установка клиентского приложения *Дистанционное управление рабочим столом* (Remote Desktop) для Windows Server 2003 или Windows XP. 32_разрядное клиентское ПО *Дистанционное управление рабочим столом* устанавливается в папку %Systemroot%\System32\Clicnts\Tsclicnt\Win32 на сервере терминалов
Лицензирование служб терминалов (Terminal Services Licensing)	Настройка лицензий для клиентских подключений к серверу терминалов. Это средство не подходит для сред, где используется только *Удаленный рабочий стол для администрирования*

Чтобы разрешить подключения Дистанционное управление рабочим столом (Remote Desktop) на компьютере под управлением Windows Server, в Панели управления выберите Система (System Properties). На вкладке Удаленное использование (Remote) выберите Разрешить удаленный доступ к этому компьютеру (Allow Users To Connect Remotely To This Computer).

Примечание: если сервер терминалов является контроллером домена, необходимо

также настроить групповую политику контроллера, чтобы разрешить группе Пользователи удаленного рабочего стола (Remote Desktop Users) подключение посредством служб терминалов. На серверах, не являющихся контроллерами домена, подключение через службы терминалов пользователям из этой группы разрешено по умолчанию.

Подключение к удаленному рабочему столу.

Подключение к удаленному рабочему столу (Remote Desktop Connection) — это клиентское приложение, используемое для подключения к серверу в контексте режима Дистанционное управление рабочим столом (Remote Desktop) или Сервер терминалов (Terminal Server). Для клиента нет функциональных различий между этими двумя конфигурациями сервера.

На компьютерах с Windows XP и Windows Server 2003 программа

Подключение к удаленному рабочему столу установлена по умолчанию, но глубоко запрятана:

Пуск (Start)\Все программы (All Programs)\Стандартные (Accessories)\Связь

(Communications)\Подключение к удаленному рабочему столу (Remote Desktop Connection).

На других платформах программу Подключение к удаленному рабочему столу можно установить с компакт_диска Windows Server либо из установочной папки клиента (%Systemroot%\System32\Clients \Tsclient\Win32) на любом из компьютеров под управлением Windows Server. Установочный пакет MSI можно распространять на системы Windows с помощью групповой политики или средствами SMS (Systems Management Server).

Совет: рекомендуется обновить предыдущие версии клиента Служб терминалов, установив последнюю версию Подключение к удаленному рабочему столу, чтобы обеспечить наиболее оптимальную, безопасную и стабильную среду, поскольку в этом случае будет доступен улучшенный пользовательский интерфейс, 128_битное шифрование и выбор альтернативных портов.

Настройка клиента удаленного подключения к рабочему столу.

Вы можете управлять множеством аспектов дистанционного подключения как со стороны клиента, так и со стороны сервера. В таблице 2 перечислены конфигурационные параметры и их назначение.

Таблица 2 – Параметры программы *Удаленное подключение к рабочему столу*

Параметры	Назначение
1	2
Параметры клиента	
Общие (General)	Параметры выбора компьютера, к которому необходимо подключаться. настройка статических реквизитов для входа в систему, а также сохранение параметров для данного подключения
Экран (Display)	Задает размер окна клиента, глубину цвета, а также доступность панели подключений при работе в полноэкранном режиме
Программы (Programs)	Задает путь и папки расположения для любых программ. которые необходимо запустить после установки соединения
Дополнительно (Experience)	Категории функций экрана можно включать или отключать в зависимости от пропускной способности канала связи между локальным и удаленными компьютерами. Предусмотрены параметры для отображения фона рабочего стола, содержимого окна при перетаскивании. визуальных эффектов при прорисовке меню и окон, тем рабочего стола; также вы можете активировать режим кэширования растровой графики, при котором после каждого интервала обновления передаются только изменения, а не весь экран целиком
Параметры сервера	
Параметры входа (Logon Settings)	Позволяет задать статические реквизиты для подключения вместо реквизитов, предоставляемых клиентом

1	2
Сеансы (Sessions)	Чтобы перекрыть настройки клиента, задайте здесь параметры завершения прерванного сеанса, ограничения длительности сеанса и времени его простоя, а также допустимость повторного подключения
Среда (Environment)	Перекрывает настройки из профиля пользователя для данного подключения в отношении запуска программы: здесь вы можете переопределить запускаемую при подключении программу. Заданный здесь путь и папка запуска приоритетнее настроек, сделанных программой *Подключение к удаленному рабочему столу*
Разрешения (Permissions)	Позволяет задавать дополнительные разрешения для данного подключения
Удаленное управление (Remote Control)	Указывает, можно ли удаленно управлять сеансом *Подключение к удаленному рабочему столу*, и если так, то должен ли пользователь выдавать разрешение на инициализацию сеанса удаленного управления. Дополнительные параметры позволяют ограничить сеанс удаленного управления только функцией просмотра либо разрешить полную интерактивность с сеансом клиента *Дистанционное управление рабочим столом*
Параметры клиента (Client Settings)	Позволяют перекрыть параметры из конфигурации клиента, изменить глубину цвета и отключить различные коммуникационные порты (порты ввода-вывода)
Сетевой адаптер (Network Adapters)	Указывает, какие сетевые платы на сервере будут принимать удаленные подключения для администрирования
Общие (General)	Задает уровень шифрования и механизм проверки подлинности для подключений к этому серверу

Устранение неполадок при работе со службами терминалов.

При использовании программы Удаленный рабочий стол для администрирования (Remote Desktop for Administration) создается подключение к консоли сервера. Есть несколько потенциальных причин неудачных подключений или сеансов с ошибками.

• Сбои сети. Ошибки в работе стандартной TCP/IP_сети могут вызывать сбои или разрывы подключений Дистанционное подключение к рабочему столу (Remote Desktop). Если не функционирует служба DNS, клиент не сможет найти сервер по имени. Если не функционирует маршрутизация либо неверно настроен порт Служб терминалов (Terminal Services) (по умолчанию это порт 3389) на клиенте или сервере, соединение установить не удастся.

• Реквизиты входа. Для успешного подключения к серверу средствами программы

Удаленный рабочий стол для администрирования пользователи должны быть включены в

группу Администраторы (Administrators) или Пользователи удаленного рабочего стола (Remote Desktop Users). Подготовка к экзамену Если подключиться через Удаленный рабочий стол для администрирования не удается из_за запрета доступа, проанализируйте членство в группах. В

предыдущих версиях Сервера терминалов (Terminal Server) для подключения к серверу требовалось быть участником группы Администраторы (Administrators), хотя специальные разрешения можно было выдать вручную. Сервер терминалов поддерживает только два удаленных подключения.

• Политика. Только администраторам разрешено подключаться средствами программы Дистанционное подключение к рабочему столу (Remote Desktop) к контроллерам доменов. Чтобы разрешить подключаться остальным пользователям, нужно настроить политику безопасности на контроллере домена.

• Слишком много параллельных подключений. Если сеансы прерывались без выхода из системы, сервер может посчитать, что достигнут предел, одновременно обрабатываемых подключений, даже если в данный момент к серверу не подключены два пользователя.

Например, администратор может завершить сеанс без выхода из системы. Если еще два администратора попытаются подключиться к серверу, это удастся только одному из них.

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

2. Запишите в тетрадь для лабораторных работ основные команды для работы с протоколом TCP/IP;

3. Выполните задания. На этой лабораторной работе вы настроите на сервере Server01 подключения через Удаленный рабочий стол для администрирования (Remote Desktop for Administration). Затем вы оптимизируете Server01, чтобы обеспечить доступность неиспользуемого подключения и разрешить лишь одно подключение в любой момент времени. После этого вы установите сеанс удаленного администрирования с ПК 2 (либо с другого удаленного компьютера).

Если в вашем распоряжении только один компьютер, можно использовать клиент программы Дистанционное подключение к рабочему столу (Remote Desktop) для подключения к службам терминалов на том же компьютере. В этом случае ссылки на удаленный компьютер на этой лабораторной работе будут относится к локальному компьютеру.

Упражнение 1. Настройка удаленного подключения к рабочему столу

В этом упражнении вы активируете удаленное подключение к рабочему столу, измените число разрешенных одновременных подключений на сервере и настроите параметры завершения подключения.

1. Войдите на Server01 как Администратор (Administrator).

2. В Панели управления выберите Система (System Properties).

3. На вкладке Remote включите Remote Desktop. Закройте окно Система (System Properties).

4. Откройте консоль Настройка служб терминалов (Terminal Services Configuration) из группы программ Администрирование (Administrative

Tools).

5. В консоли tscc (Terminal Services Configuration\Connections) на правой панели щелкните правой кнопкой подключение RDP_tcp и выберите Свойства (Properties).

6. На вкладке Сетевой адаптер (Network Adapter) установите значение параметра Максимальное число подключений (Maximum Connections) равным 1.

7. На вкладке Сеансы (Sessions) установите оба флажка Заменить параметры пользователя (Override User Settings) и измените настройки следующим образом: все прерванные любыми способами (или по любой причине) сеансы пользователей закрываются через 15 минут, активный сеанс не ограничивается по времени, сеансы завершаются после 15 минут бездействия.

• Завершение отключенного сеанса (End a disconnected session): 15 минут,

• Ограничение активного сеанса (Active session limit): никогда (never),

• Ограничение активного сеанса (Active session limit): 15 минут.

• При превышении ограничений или разрыве подключения (When session limit is reached or connection is broken): Отключить сеанс (Disconnect from session).

Такая конфигурация обеспечивает следующее: только один пользователь одновременно подключен к серверу терминалов, любой прерванный сеанс закроется через 15 минут и неактивный сеанс прервется через 15 минут. Эти параметры позволяют избежать ситуации, когда прерванный или бездействующий сеанс мешает подключаться средствами программы Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

Упражнение 2. Подключение к серверу с помощью клиента удаленного подключения к рабочему столу

1. На ПК 2 (или на другом удаленном компьютере либо прямо с ServerOl, если удаленного компьютера нет) в группе Стандартные\Связь (Accessories\Communications) щелкните Подключение к удаленному рабочему столу (Remote Desktop Connection), подключитесь к Server01 и войдите в его систему.

2. На сервере Server01 откройте консоль tscc.msc: Администрирование (Administrative tools)\Настройка служб терминалов (Terminal Services Configuration). В открывшейся консоли выберите Подключения (Connections). Вы должны увидеть сведения о сеансе удаленного подключения к Server01.

3. Не выполняйте никаких действий в этом сеансе 15 минут либо закройте клиент программы Удаленное подключение к рабочему столу (Remote Desktop), не завершив сеанс Сервера терминалов (Terminal Server) явно: сеанс должен будет завершиться автоматически через 15 минут.

В данный момент вы подключены к ServerOl удаленно и можете

выполнять на нем любые задачи, допустимые в интерактивном режиме на консоли.

Контрольные вопросы:

1. Сколько одновременных подключений разрешено к серверу терминалов, работающему в режиме удаленного администрирования? Почему?

2. Как оптимальным образом предоставить администраторам возможность удаленного управления сервером через службы терминалов?

a. Не выполнять никаких действий; они уже имеют доступ, поскольку являются администраторами.

b. Удалить группу Администраторы (Administrators) из списка разрешений в подключении к серверу терминалов и поместить их административную учетную запись в группу Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

c. Создать отдельную пользовательскую учетную запись с более низким уровнем авторизации для повседневного использования группой Администраторы и поместить ее в группу Удаленный рабочий стол для администрирования.

3. Какое программное средство используется на сервере для включения удаленного подключения к рабочему столу?

a. Диспетчер служб терминалов (Terminal Services Manager).

b. Настройка служб терминалов (Terminal Services Configuration).

c. Система (System Properties) из Панели управления.

d. Лицензирование служб терминалов (Terminal Services Licensing).

Сделайте выводы.

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основные источники:

1. Белов Е. Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования – М.: Издательский центр «Академия», 2017. – 336 с.

2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2019. [Электронный ресурс; Режим доступа http://znanium.com]

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2019. — 325 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

4. Ковалев Д. Р. МДК 02.01 Программные и программно-аппаратные

средства защиты информации Методические указания по выполнению практических занятий для обучающихся всех форм обучения образовательных учреждений среднего профессионального обучения специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ) – г. Нижневартовск: ННТ (филиал) ФГБОУ ВО «ЮГУ», 2020 [Электронный ресурс; Режим доступа: Полнотекстовая коллекция учебно-методических изданий ЮГУ]

5. Ковалев Д.Р. МДК 02.02 Криптографические средства защиты информации Методические указания по выполнению практических занятий для обучающихся всех форм обучения образовательных учреждений среднего профессионального обучения специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ) – г. Нижневартовск: ННТ (филиал) ФГБОУ ВО «ЮГУ», 2020 [Электронный ресурс; Режим доступа: Полнотекстовая коллекция учебно-методических изданий ЮГУ]

6. Ковалев Д. Р. МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности Методические указания по выполнению практических занятий для обучающихся всех форм обучения образовательных учреждений среднего профессионального обучения специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ) – г. Нижневартовск: ННТ (филиал) ФГБОУ ВО «ЮГУ», 2020 [Электронный ресурс; Режим доступа: Полнотекстовая коллекция учебно-методических изданий ЮГУ]

Периодические издания:

1. Теоретический и научно-методический журнал «Среднее профессиональное образование» + Приложение

2. Вопросы кибербезопасности. Научный, периодический, информационно- методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

3. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

Электронные ресурсы:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru Справочно-правовая система «Гарант» www.garant.ru

5. Федеральный портал «Российское образование www.edu.ru

6. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru Российский биометрический портал www.biometrics.ru

7. Федеральный портал «Информационно- коммуникационные технологии в образовании» http://www.ict.edu.ru

8. Сайт Научной электронной библиотеки www.elibrary.ru

9. Сайт МКИТ https://mkit.online/eios/

СОДЕРЖАНИЕ

МДК 02.03
КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Методические указания к выполнению практических занятий для обучающихся 2 курса всех форм обучения образовательных организаций среднего профессионального образования

Часть 1

Методические указания
разработали преподаватели:
Бойко Яна Сергеевна, Баталкина Анастасия Геннадьевна

Подписано к печати ***10.11.2022 г.*** Объем ***1,4*** п.л.
Формат 60х84/16 Заказ
Тираж ***1*** *экз.*

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
628615 Тюменская обл., Ханты-Мансийский автономный округ,
г. Нижневартовск, ул. Мира, 37.