ПРОФЕССИОНАЛИТЕТ, 2024, № 1 (001)

***УДК** 378.1*

М.А. Алькова[1], А.М. Вернигора[1]

[1]*ОГБПОУ «Томский индустриальный техникум», г. Томск, Российская Федерация*

БАЗОВАЯ ПОДГОТОВКА К ДЕМОНСТРАЦИОННОМУ ЭКЗАМЕНУ ДЛЯ СТУДЕНТОВ IT-СПЕЦИАЛЬНОСТЕЙ

Аннотация: *В статье представлен опыт разработки учебных занятий для студентов первого курса IT-специальностей, направленных на базовую подготовку к демонстрационному экзамену по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Описана методика проведения демонстрационного экзамена в формате учебного занятия по дисциплине «Информатика», реализованная осенью 2021 года на базе Томского техникума информационных технологий в рамках открытого мероприятия «Педагог года». Практическое задание предполагало создание схемы с использованием графического элемента SmartArt в Word на основе аналитического текста о статистике операционных систем. Экзамен был организован в двухчастной форме: самостоятельное выполнение задания подгруппой в течение фиксированного времени и последующее оценивание результатов другой подгруппой по установленным критериям. Рассмотрены критерии оценивания, включающие наличие названия схемы, полноту текстовой и цифровой информации, корректность соответствия данных и оформление работы. Показано использование цифровых инструментов, в том числе файловой структуры и облачных форм для интерактивного контроля результатов. Представлен фрагмент методических указаний по модулям демонстрационного экзамена, включающий установку и конфигурирование компонентов DLP-системы, технологии агентского мониторинга, разработку и применение политик безопасности. Описаны практические задачи по настройке контроллера домена Active Directory, конфигурированию DLP-сервера, установке сервера агентского мониторинга и синхронизации каталогов пользователей. Представленные методические материалы способствуют формированию у студентов практических навыков работы с операционными системами Windows и Linux, сетевыми параметрами и современными средствами защиты корпоративных данных, обеспечивая базовую подготовку к профессиональной деятельности в сфере информационной безопасности.*

Ключевые слова: *демонстрационный экзамен, критерии оценки, компетенция, корпоративная защита.*

Введение

Авторами статьи разработаны занятия для студентов первого курса IT-специальностей, ориентированные на базовую подготовку к демонстрационному экзамену по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Кроме того, представлен фрагмент сборника методических указаний по выполнению модулей в рамках данной компетенции.

Демонстрационный экзамен по стандартам WorldSkills Russia проводится с целью определения уровня знаний, умений и навыков студентов и выпускников, необходимых для осуществления профессиональной деятельности в определенной сфере и выполнения работ по конкретным профессиям. Вместе с тем для результативной подготовки к данному формату аттестации требуется не только освоение содержания соответствующей компетенции, но и понимание регламента проведения экзамена, его правил и критериев оценивания.

В связи с этим в статье представлен авторский вариант организации учебного занятия, разработанный для развития и проверки ряда навыков в рамках дисциплины «Информатика» у студентов первого курса среднего профессионального образования, а также ознакомительный фрагмент задания по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

Основной формой, рассматриваемой в статье, является демонстрационный экзамен, проведенный в формате учебного занятия по теме «Создание графического элемента SmartArt в Word». Цель статьи состоит в представлении опыта проведения такого демонстрационного экзамена по дисциплине «Информатика» на базе Томского техникума информационных технологий для студентов первого курса IT-специальностей. Указанное занятие было реализовано осенью 2021 года в рамках открытого урока «Педагог года -2021».

В ходе экзамена проверялись знания студентов по дисциплине «Информатика», навыки практической работы с инструментами Word, умение работать в команде, выполнять задание

в условиях ограниченного времени и оценивать результат по установленным критериям. Одновременно обеспечивалось знакомство студентов со структурой IP-адреса, программным обеспечением, серверными и клиентскими операционными системами Windows и Linux, что в дальнейшем способствует выполнению базовой настройки заданий демонстрационного экзамена.

Организация демонстрационного экзамена в формате урока

Экзамен состоял из двух основных частей: самостоятельного выполнения задания одной подгруппой и последующего оценивания выполненной работы другой подгруппой по установленным критериям. На выполнение задания отводилось фиксированное время — 25 минут. По истечении указанного времени студенты должны были представить результаты своей работы аудитории.

Практическое задание предполагало создание схемы по предложенному кейсу с использованием графического элемента SmartArt в Word на базе операционной системы Windows.

Текст задания

«Статистика операционных систем в мире в 2020 году.

Общий рейтинг операционных систем, включая компьютеры, ноутбуки, смартфоны показывает, что лидером является Android, который установлен на 39,77% приборах, что свидетельствует о росте количества мобильных гаджетов в мире. Если брать отдельно операционные системы, установленные на компьютерах, то тут лидирует Windows — 76,58% всех компьютеров, OS X — 18,93% и Linux — 1,62%. Среди мобильных телефонов лидером остается Android — 70,43%, мобильная операционная система iOS — 29,06% — практически каждый третий смартфон. На планшетах iOS: 59,97%, а у Android 39,79% всех планшетов».

Алгоритм работы

- Прочитать текст.
- Выделить главную суть информации.
- На листе начертить примерную схему, применяя любой вид рисунка для SmartArt (этот пункт по желанию).
- Создать файл Word на рабочем столе.
- Создать схему в текстовом документе Word, используя инструмент SmartArt.
- Заполнить блоки схемы текстовой и цифровой информацией. Для ускорения работы текст можно скопировать из файла «УРОК_2024», расположенного на рабочем столе компьютера.
- Выполнить задание с учетом критериев оценивания.
- Сохранить файл на общем диске.

Критерии оценивания

Итоговая оценка за экзамен формировалась на основе следующих критериев:

– название схемы — 1 балл;
– представлена вся текстовая информация (8 элементов) — 1 балл;
– представлена вся цифровая информация (8 элементов) — 1 балл;
– соответствие текстовой и цифровой информации — 1 балл;
– наличие дизайна, включая применение различной цветовой гаммы, заливки фигуры или различных цветов линий — 1 балл.

Итоговый максимальный результат составлял 5 баллов, что соответствовало оценке «5». Для интерактивного наблюдения результатов экзамена использовались цифровые инструменты: файловая структура и ссылка на Google-форму для оценивания. Такой подход обеспечивал наглядность и оперативность процедуры контроля.

Связь урока с подготовкой к демонстрационному экзамену по компетенции

В серии подобных занятий студенты участвуют в практическом выполнении базовых настроек операционных систем, используемых в модулях демонстрационного экзамена по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

Специалист в области корпоративной безопасности должен обладать теоретическими знаниями по обеспечению защиты от внутренних угроз, понимать аспекты применения нормативно-правовой базы для классификации и расследования инцидентов, а также владеть системами и технологиями, направленными на достижение целей защиты.

Компетенция «Корпоративная защита от внутренних угроз информационной безопасности» включает реализацию профессиональных мер и действий, связанных с защитой предприятия от внутренних угроз информационной безопасности. Студенты, сдающие демонстрационный экзамен по данной компетенции, должны знать основы корпоративной защиты от внутренних угроз, понимать принципы применения нормативно-правовой базы для классификации и расследования инцидентов, а также уметь использовать системы и методы, предназначенные для защиты данных.

Данная компетенция включает три модуля:

– установка и конфигурирование компонентов DLP-системы;

– технологии агентского мониторинга;

– разработка и применение политик, анализ выявленных инцидентов.

Для наглядности в статье представлен фрагмент задания из методического пособия, разработанного для подготовки студентов по указанной компетенции.

Фрагмент методических указаний

Модуль 1. Установка и конфигурирование компонентов DLP-системы

В компании «Демо Лаб» возникла необходимость внедрения DLP-системы для повышения уровня защиты разработок и предотвращения утечек иной информации. В соответствии с выданным заданием необходимо установить и настроить компоненты системы. В качестве основных каналов потенциальной утечки рассматриваются носители информации, электронная почта и различные интернет-ресурсы. Серверные компоненты устанавливаются в виртуальной среде. Сетевые интерфейсы уже настроены, однако IP-адреса должны быть назначены согласно прилагаемой карточке.

Для дальнейшей работы подготовлены следующие виртуальные машины:

– AD-сервер с контроллером домена;

– DLP-сервер, установленный, но не настроенный, с активированной лицензией;

– виртуальная машина для установки сервера агентского мониторинга;

– виртуальные машины «нарушителей» для установки агентов.

Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Таблица 1. Преднастройка виртуальных машин

Наименование виртуальной машины	IP адрес	Маска подсети	DNS
Demo.lab	172.16.X.2	255.255.255.248	127.0.0.1
IWTM	172.16.X.3 (Linux)	255.255.255.248	172.16.X.2
IWDM	172.16.X.4	255.255.255.248	172.16.X.2
W10-agent	172.16.X.5	255.255.255.248	172.16.X.2

где X — номер варианта по жеребьевке.

После выполнения преднастройки необходимо провести проверку. Для этого требуется перейти на виртуальную машину Demo.lab, открыть браузер Google и ввести IP-адрес 172.16.X.3 (Linux). Если открывается сайт для входа в DLP-систему, настройка выполнена корректно.

Задание 1. Настройка контроллера домена

Необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

– логин: user1, пароль: 12345678, запретить локальный вход в систему;

– логин: user2, пароль: 12345678, запретить локальный вход в систему;

– логин: user3, пароль: 12345678, права администратора домена и локального администратора;

– логин: user4, пароль: 12345678, права пользователя домена.

Создание пользователей осуществляется в службе каталогов Active Directory: Пользователи и компьютеры — Users.

Пароль 12345678 по заданию не может быть задан стандартным образом, поскольку его не допускает политика безопасности. В связи с этим возможны два варианта решения: изменить политику безопасности либо установить пароль P@ssw0rd и зафиксировать его в документе для экспертов.

User1 и User2.

Необходимо создать новую групповую политику в домене demo.lab с именем политики «запрет анимации». Далее требуется перейти во вкладку «прошедшие проверку» и последовательно добавить user1, user2 и domain computers с проверкой имен. После этого следует открыть созданную групповую политику и перейти: Конфигурация ПК — Политики — Конфигурация Windows — Параметры безопасности — Локальные политики — Назначение прав пользователя — Запретить локальный вход. В политике безопасности необходимо определить соответствующий параметр и добавить пользователей user1 и user2.

User3.

Следует добавить пользователя в члены группы Domain Admins.

User4.

Необходимо проверить включение пользователя в группу Domain users.

Задание 2. Настройка DLP-сервера

DLP-сервер контроля сетевого трафика уже предустановлен, однако не настроен. Требуется определить IP-адрес сервера через локальную консоль виртуальной машины, настроить DNS для корректной работы, проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам. Далее необходимо синхронизировать каталог пользователей и компьютеров LDAP с доменом с использованием ранее созданного пользователя.

Для входа в веб-консоль следует использовать ранее созданного доменного пользователя с полными правами администрирования системы и полным доступом ко всем областям видимости.

Настройка DLP-сервера включает следующие действия.

Прежде всего необходимо добавить машины IWDM и W10-agent в домен Demo.lab, изменив имя ПК и используя пользователя demo\user3. Затем требуется перейти на виртуальную машину Demo.lab, выполнить вход в систему, открыть браузер и ввести IP-адрес 176.16.X3.

Логин: officer.

Пароль: xxXX1234.

Шаг 1. Проверить наличие активной лицензии: Управление — Лицензии — Статус — Активная.

Шаг 2. Перейти: Управление — LDAP синхронизация — Серверы — Добавить LDAP сервер.

Необходимо задать следующие параметры:

- имя: demo.lab;
- тип: AD;
- ежеминутно — 15 минут;

- LDAP-сервер: 172.16.X.2;
- использовать глобальный каталог;
- LDAP-запрос: DC=demo,DC=lab;
- логин: demo\user3;
- пароль: от пользователя user3.

После ввода параметров необходимо проверить соединение, сохранить настройки и повторно выполнить проверку соединения.

Шаг 3. Перейти: Пользователи — Управление доступом — Роли — Область видимости — Пользователи — Добавить из LDAP — user3 — Сохранить.

Дополнительно следует указать:

- роль: администратор, офицер безопасности;
- область видимости: постоянный доступ;
- e-mail: задать самостоятельно.

Задание 3. Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен с использованием ранее созданного пользователя, после перезагрузки войти в систему от имени этого пользователя и продолжить работу в домене.

Далее требуется установить базу данных с паролем суперпользователя 12345678, установить сервер агентского мониторинга с параметрами по умолчанию. В процессе установки необходимо установить соединение с DLP-сервером контроля сетевого трафика по IP-адресу и токену, однако это можно выполнить и после установки сервера агентского мониторинга.

Также необходимо настроить пользователя консоли управления:

логин — officer, пароль — 12345678.

После этого требуется синхронизировать каталог пользователей и компьютеров с Active Directory.

После синхронизации следует настроить вход в консоль управления от имени ранее созданного пользователя, предоставить полный доступ к системе и установить все области видимости.

Для выполнения задания необходимо перейти на виртуальную машину IWDM под пользователем user3.

Шаг 1. Установить базу данных PostgreSQL с паролем 12345678.

Шаг 2. Установить сервер агентского мониторинга InfoWatch Device Monitor. В процессе установки необходимо выбрать: и сервер, и консоль; основной сервер; сервер БД 127.0.0.1; имя: IWDM; имя пользователя: postgres; пароль: 12345678.

Необходимо создать новый ключ и сохранить его в каталоге, где размещены установщики. По заданию требуется настроить учетную запись: имя — officer, пароль — 12345678.

Шаг 3. На рабочем столе появляется ярлык «консоль управления».

Адрес: 127.0.0.1.

Логин: officer.

Пароль: 12345678.

Далее следует перейти: Инструменты — Настройки — Синхронизация политик.

Адрес: 172.16.X.1.

Затем требуется ввести токен. Для его получения необходимо перейти на виртуальную машину Demo.lab, открыть DLP-систему и выбрать: Управление — Плагины — Токены — Содержание. После этого следует применить и сохранить изменения.

Шаг 4. Перейти: Инструменты — Настройки — Интеграция AD.

Необходимо выбрать домен из леса, выполнить проверку соединения, указав логин demo\user3, после чего синхронизировать директорию, выбрать весь домен и запустить процесс.

Заключение

Представленная методика демонстрирует эффективность ранней интеграции форматов демонстрационного экзамена в учебный процесс первого курса. Поэтапное включение студентов в практические задачи — от базовой работы с офисными инструментами до конфигурирования DLP-систем и настройки доменной среды — способствует формированию профессиональных компетенций до начала итоговой аттестации.

Сочетание индивидуальной деятельности, командного взаимодействия и критериального оценивания с использованием цифровых инструментов повышает качество подготовки, а также развивает навыки самоконтроля и объективной экспертизы. Разработанные уроки и фрагменты методических указаний могут рассматриваться как тиражируемый ресурс для образовательных организаций, реализующих программы по информационной безопасности в рамках стандартов WorldSkills Russia.

Список литературы

1. Актуальные проблемы и инновационные подходы в образовании: Материалы научно-практической конференции: сборник /Редакционная коллегия: Никифорова Е.П., Васильева С.Г. Сергеева Ю.А. — Томск: Изд-во ОГБПОУ «ТГПК», 2019. — 968 с.
2. Методика организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия: Москва: Союз «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы (Ворлдскиллс Россия)» [Электронный ресурс]. — 2019. — Режим доступа: http://www.esat.worldskills.ru (дата обращения 10.04.2024).
3. Ефанов, Н.Н. О некоторых комбинаторных свойствах деревьев процессов LINUX. Чебышевский сборник. 2018. 19(2). 151-162с.
4. Лунгу К.Н., Макаров Е.В., Нефедова И.В. Основы проектирования учебно-методического комплекса по математике для студентов технических специальностей // Наука и современность. — 2014. — № 27. — С. 70-74.
5. Гончарук С.В. Администрирование ОС Linux [Электронный ресурс] / С.В. Гончарук. — Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 164 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52142.html
6. G. Basler, A. Donaldson, A. Kaiser, D. Kröning, M. Tautschnig, T. Wahl. (2012) SATABS: *A Bit-Precise Verifier for C Programs* // C. Flanagan, B. König (eds.). TACAS 2012. LNCS, vol. 7214, pp. 552-555. Springer, Heidelberg.
7. D. Beyer. (2012) *Competition on Software Verification* // C. Flanagan, B. König (eds.). TACAS 2012. LNCS, vol. 7214, pp. 504-524. Springer, Heidelberg.

References

1. Nikiforova, E.P., Vasilyeva, S.G., Sergeeva, U.A. (2019). *Current problems and innovative approaches in education.* Materials of the scientific and practical conference: collection. 968.
2. Union "Agency for the Development of Professional Communities and workers "Young Professionals (Worldskills Russia)". (2019) *The methodology of organization and conduct of the demonstration exam according to the standards of Worldskills Russia.* — URL: http://www.esat.worldskills.ru
3. Efanov, N.N. (2018) *On some combinatorial properties of LINUX process trees.* Chebyshev collection. 151-162.
4. Lungu, K.N., Makarov, E.V., Nefedova, I.V. (2014) *Fundamentals of designing an educational and methodological complex in mathematics for students of technical specialties* // Science and modernity. 70-74.
5. Goncharuk, S.V. (2016) *Linux OS Administration*. Internet University of Information Technology (INTUIT). 164. — URL: http://www.iprbookshop.ru/52142.html
6. G. Basler, A. Donaldson, A. Kaiser, D. Kröning, M. Tautschnig, T. Wahl. (2012) SATABS: *A Bit-Precise Verifier for C Programs* // C. Flanagan, B. König (eds.). TACAS 2012. LNCS, vol. 7214, pp. 552-555. Springer, Heidelberg.
7. D. Beyer. (2012) *Competition on Software Verification* // C. Flanagan, B. König (eds.). TACAS 2012. LNCS, vol. 7214, pp. 504-524. Springer, Heidelberg.

Информация об авторах

Алькова М. А. — преподаватель, ОГБПОУ «Томский индустриальный техникум», г. Томск, Российская Федерация, e-mail: alkovama@tomintech.ru

Вернигора А. М. — преподаватель, ОГБПОУ «Томский индустриальный техникум», г. Томск, Российская Федерация, e-mail: alkovama@tomintech.ru

BASIC PREPARATION FOR THE DEMONSTRATION EXAM FOR IT STUDENTS

M.A. Alkova[1], A.M. Vernigora[1]

[1]Regional State Budgetary Professional Educational Institution "Tomsk Industrial Technical College"

Abstract. *The article presents the experience of developing lessons for first-year students of IT specialties aimed at basic preparation for the demonstration exam in the competence "Corporate protection against internal threats to information security". The methodology of conducting a demonstration exam in the format of a lesson in the subject "Informatics" on the basis of the Tomsk College of Information Technology, implemented in the fall of 2021 as part of the open event "Teacher of the Year", is described. The practical task included creating a diagram using the SmartArt graphical element in Word based on an analytical text about operating system statistics. The exam consisted of two parts: the independent completion of the task by a subgroup in a fixed time and the subsequent assessment of the work by another subgroup according to established criteria. The evaluation criteria are considered: the name of the scheme, the completeness of textual and digital information, the correspondence of the data, the availability of design. The use of digital tools is demonstrated: a file structure, cloud forms for interactive control of results. A fragment of methodological guidelines on the modules of the demo exam is presented: installation and configuration of DLP system components, agent monitoring technologies, development and application of security policies. The practical tasks of setting up an Active Directory domain controller, configuring a DLP server, installing an agent monitoring server, and synchronizing user directories are described. The presented methodological materials contribute to the formation of students' practical skills in working with Windows and Linux operating systems, network parameters, and modern corporate data protection tools, providing effective training for professional activities in the relevant field of information security.*

Keywords: *demonstration exam, assessment criteria, competence, corporate protection.*

Information about the authors

Alkova M. A. — Teacher, Tomsk Industrial College, Tomsk, Russian Federation, e-mail: alkovama@tomintech.ru

Vernigora A. M. — Teacher, Tomsk Industrial College, Tomsk, Russian Federation, e-mail: alkovama@tomintech.ru