

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)
Кафедра безопасности информационных систем (БИС)

К ЗАЩИТЕ ДОПУСТИТЬ

И.о. заведующего кафедрой БИС
Кандидат техн. наук, доцент
_____ Е.Ю. Костюченко
«__» _____ 2019 г.

**ПРИЛОЖЕНИЕ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ОФИСНЫХ
ПАКЕТОВ НА ПРИМЕРЕ MICROSOFT OFFICE**

Дипломная работа по специальности
10.05.04 «Информационно-аналитические системы безопасности»

Пояснительная записка
БИС.502900.007 ПЗ

СОГЛАСОВАНО

Консультант по организационно-
экономической части
ст. преподаватель каф. КИБЭВС
_____ С.В. Глухарева
«__» _____ 2019 г.

Студент гр. 743
_____ Т.С. Койшинов
«__» _____ 2019 г.

Консультант по вопросам охраны
труда и безопасности
жизнедеятельности
доцент каф. КИБЭВС, канд. техн.
наук
_____ Е.М. Давыдова
«__» _____ 2019 г.

Руководитель дипломной работы
к.т.н., доцент каф. КИБЭВС
_____ А.А. Конев
«__» _____ 2019 г.

Томск 2019

Реферат

Дипломная работа, 70 стр., 34 рис., 21 табл., 36 источник, 1 прил.

MICROSOFT OFFICE, ПРИЛОЖЕНИЕ, ЗАЩИЩЕННОСТЬ, CIS, BENCHMARK, ГРУППОВЫЕ ПОЛИТИКИ, РЕЕСТР WINDOWS, DJANGO, PYTHON, VIRTUALBOX, МОДЕЛЬ, ШАБЛОН, ПРЕДСТАВЛЕНИЕ, ТЕСТИРОВАНИЕ.

Цель работы - разработка приложения для анализа защищенности Microsoft Office посредством проверки настроек групповых политик Microsoft Office в соответствии со стандартом безопасности.

В процессе выполнения дипломной работы был проведен обзор стандарта безопасности CIS Microsoft Office 2016, выбраны технологии и средства разработки, подготовлены виртуальные машины для тестирования приложения. Спроектирована инфологическая модель данных, структура приложения.

В результате работы было разработано клиент-серверное приложения с веб-интерфейсом для анализа защищенности Microsoft Office посредством проверки настроек групповых политик Microsoft Office в соответствии со стандартом безопасности CIS Microsoft Office 2016.

Приложение было разработано с помощью среды разработки JetBrains PyCharm, тестировалось с использованием приложения виртуализации Oracle VM VirtualBox, программный код опубликован на сервере Github. Отчет выполнен в текстовом редакторе Microsoft Word 2016.

Abstract

Graduation qualifying work, 70 pp., 34 illustrations, 21 tables, 36 sources, 1 app.

MICROSOFT OFFICE, APPLICATION, SECURITY, CIS, BENCHMARK, GROUP POLICY, WINDOWS REGISTRY, PYTHON. VIRTUALBOX, MODEL, TEMPLATE, VIEW, TESTING.

The purpose of this work is the development of an application for security analysis Microsoft Office through a checking group policy setting in accordance with security benchmark.

In the course of the work, a review was undertaken of CIS Microsoft Office 2016 benchmark, chosen development technologies and means, have been prepared to virtual machines for application testing. Infological model and application structure was designed.

As a result, a client-server application has been developed for security analysis Microsoft Office through a checking group policy setting in accordance with CIS Microsoft Office benchmark.

Application has been developed in JetBrains PyCharm, has been tested with Oracle VM VirtualBox, program code released in Github server. The report is executed in the text editor Microsoft Word 2016.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

УТВЕРЖДАЮ

И.о. заведующего кафедрой БИС

_____ Е.Ю. Костюченко

« ____ » _____ 2019 г.

ЗАДАНИЕ

на дипломную работу студенту Койшинову Тимуру Саматулы
группа 743 факультет безопасности

1. Тема работы: Приложение для анализа защищенности офисных пакетов на примере Microsoft Office.
(утверждена приказом по ВУЗу от 18 декабря 2018 г. № 6036 ст)
2. Исходные данные к работе: стандарт безопасности CIS Microsoft Office 2016; учебно-методическая литература.
3. Содержание пояснительной записки (перечень подлежащих разработке вопросов):
 - обзор стандарта CIS Microsoft Office 2016;
 - описание использованных в работе технологий и средств разработки;
 - настройка виртуальных машин для тестирования приложения;
 - проектирование инфологической модели данных;
 - описание структуры приложения;
 - описание алгоритма проверки настроек групповых политик Microsoft Office 2016;
 - описание пользовательского интерфейса;

- описание интерфейса администратора;
- тестирование приложения.

4. Консультанты по работе:

- консультант по организационно-экономической части: старший преподаватель кафедры КИБЭВС С.В. Глухарева

_____ «__» _____ 2019 г.
(подпись)

- консультант по вопросам охраны труда и безопасности жизнедеятельности: доцент кафедры КИБЭВС, кандидат технических наук Е.М. Давыдова

_____ «__» _____ 2019 г.
(подпись)

5. Задание выдано:

Руководитель: к.т.н., доцент каф. КИБЭВС А.А. Конев

_____ «__» _____ 2019 г.
(подпись)

6. Задание принято к исполнению:

студент группы 743 Т.С. Койшинов

_____ «__» _____ 2019 г.
(подпись)

Содержание

1 Введение.....	8
2 Обзор стандарта безопасности CIS Microsoft Office 2016	9
2.1 Обоснование выбора стандарта.....	9
2.2 Структура стандарта	10
2.3 Аудит настроек Microsoft Office 2016.....	11
2.4 Соответствие настроек групповых политик значениям в реестре Windows.....	14
3 Технологии и средства разработки.....	17
3.1 Система контроля версий.....	17
3.2 Язык программирования и веб-фреймворк	18
3.3 Интегрированная среда разработки	19
3.4 Средства виртуализации для тестирования.....	20
4 Настройка виртуальных машин для тестирования приложения.....	21
5 Разработка приложения для анализа защищенности Microsoft Office	26
5.1 Проектирование инфологической модели данных.....	26
5.2 Структура приложения	30
5.3 Алгоритм проверки настроек Microsoft Office.....	32
5.4 Описание пользовательского интерфейса	38
5.5 Описание интерфейса администратора	41
5.6 Тестирование приложения	46
6 Техничко-экономическое обоснование работы	50
6.1 Обоснование целесообразности работы	50
6.2 Организация и планирование работ	50
6.3 Смета затрат.....	52
6.4 Анализ затрат на выполнение работы.....	57

					БИС.502900.007 ПЗ		
Изм.	Лист	№ докум	Подпись	Дата	Приложение для анализа защищенности офисных пакетов на примере Microsoft Office		
Разраб.	Койцинов Т.С						
Провер.	Конев А.А.						
Реценз.	Мироненко Д.А.						
Н. Контр.	Якимук А.Ю.						
Утверд.	Костюченко Е.Ю.						
					Лит.	Лист	Листов
						6	70
					ТУСУР, ФБ, каф. БИС, гр. 743		

7 Охрана труда и безопасность жизнедеятельности.....	58
7.1 Общие положения	58
7.2 Эргономика рабочего помещения и рабочего места	58
7.3 Общие требования по электробезопасности и пожаробезопасности	65
8 Заключение	66
Список использованных источников	67
Приложение А (справочное) Диаграмма Ганта	71

CD-RW диск

Файлы:

BenchmarkVerification.zip

ПЗ.pdf

Презентация.pptx

В конверте

на обороте обложки

					БИС.502900.007 ПЗ	Лист
Изм	Лист	№ докум.	Подпись	Дата		7

1 Введение

Microsoft Office является самым популярным офисным пакетом, поэтому очень важно обеспечить пользователей безопасной работы с данным продуктом.

Только за первые две недели 2019 года было обнаружено множество уязвимостей в приложениях Outlook, Excel, Word и SharePoint [1]. Постоянно появляющаяся информация о найденных уязвимостях говорит о том, что важно не только устранять известные уязвимости, но и предотвращать атаки до их начала.

Организация «Center for Information Security» подготовила стандарты безопасности с наборами рекомендаций по настройке групповых политик Microsoft Office, которые помогут настроить систему так, чтобы усложнить проведение атаки на приложения пакета.

Проверка соответствия настроек групповых политик может занять большое количество времени, особенно если необходимо проверять несколько компьютеров.

Целью работы является разработка приложения для анализа защищенности Microsoft Office посредством проверки настроек групповых политик Microsoft Office в соответствии со стандартом безопасности.

Для достижения цели были поставлены задачи:

- 1) провести обзор стандарта безопасности CIS Microsoft Office;
- 2) настроить виртуальные машины для тестирования приложения;
- 3) спроектировать инфологическую модель данных;
- 4) разработать приложение для анализа защищенности;
- 5) протестировать приложение.

2 Обзор стандарта безопасности CIS Microsoft Office 2016

2.1 Обоснование выбора стандарта

«Center for Information Security (CIS) – это некоммерческая организация, разрабатывающая стандарты и инструменты в области информационной безопасности» [2].

«Стандарт безопасности CIS – это рекомендации по настройке системы в целях защиты от современных угроз в сфере информационной безопасности. На данный момент доступны стандарты безопасности более чем для 140 различных систем, включая операционные системы, системы управления базами данных и программные обеспечения» [3].

Для офисных пакетов доступны стандарты [4]:

- CIS Microsoft Office 2013;
- CIS Microsoft Office 2016;
- CIS Microsoft Outlook 2010;
- CIS Microsoft Outlook 2013;
- CIS Microsoft Outlook 2016;
- CIS Microsoft Word 2013;
- CIS Microsoft Word 2016;
- CIS Microsoft Access 2013;
- CIS Microsoft Access 2016;
- CIS Microsoft Excel 2013;
- CIS Microsoft Excel 2016;
- CIS Microsoft PowerPoint 2013;
- CIS Microsoft PowerPoint 2016.

Для приложения был выбран стандарт CIS Microsoft Office 2016, т.к. Microsoft Office содержит в себе продукты Outlook, Word, Access, Excel, PowerPoint, а версия 2016 года была выбрана как более новая версия Microsoft Office.

					БИС.502900.007 ПЗ	Лист
Изм	Лист	№ докум.	Подпись	Дата		9

2.2 Структура стандарта

Стандарт [5] состоит из оглавления, обзора и рекомендаций.

В обзоре описано:

- кому стандарт будет полезен;
- кем стандарт разработан;
- типографическое соглашение.

Рекомендации поделены на категории и подкатегории. Каждая из рекомендаций содержит в себе:

- заголовок;
- описание;
- обоснование;
- описание аудита;
- описание настройки;
- последствия.

Обоснование содержит в себе информацию, отвечающую на вопрос: «Почему рекомендация важна и присутствует в стандарте?».

Описание аудита необходимо для того, чтобы знать, как проверять соответствие настроек системы рекомендациям.

Описание настройки содержит в себе информацию, отвечающую на вопрос: «Как настроить систему, чтобы она соответствовала рекомендации?». В соответствии со стандартом CIS Microsoft Office 2016, система настраивается через групповые политики Windows.

В конце рекомендации помещена информация о последствиях, которые могут возникнуть в случае, если она не соблюдена в проверяемой системе.

Также в рекомендации есть «применимость профиля» и «ранжирование», однако в данном стандарте эти части рекомендаций одинаковы между собой и неинформативны.

					БИС.502900.007 ПЗ	Лист
Изм	Лист	№ докум.	Подпись	Дата		10

2.3 Аудит настроек Microsoft Office 2016

Проверка соответствия настроек проходит через системный реестр Windows.

«Системный реестр Windows – это иерархически построенная база данных, включающая всевозможные параметры операционной системы, программного и аппаратного обеспечения ПК, профили пользователей и многое другое» [6].

Проверять рекомендации можно локально и удаленно, через инструментарий WMI.

«Технология WMI - это расширенная и адаптированная под Windows реализация стандарта Web-Based Enterprise Management, принятого многими крупными компаниями в качестве универсального интерфейса мониторинга и управления различными системами и компонентами распределенной информационной среды предприятия с использованием объектно-ориентированных идеологий и протоколов HTML и XML» [7].

Необходимые настройки групповых политик Microsoft Office для проверки стандарта находятся в разделах реестра:

- «HKLM\software\microsoft\internet explorer\main\featurecontrol»;
- «HKLM\software\policies\microsoft\office»;
- «HKU\{SID}\software\policies\microsoft\office».

«Ветка «HKU» содержит подраздел для каждого загруженного профиля пользователя, регистрационную базу данных классов и подраздел «HKU.DEFAULT», связанный с профилем для системы» [8]. Для того, чтобы проверять настройки в данной ветке, сначала нам нужно получить идентификаторы SID всех доступных пользователей, у которых установлен Microsoft Office 2016.

«Идентификатор безопасности (SID) - структура данных переменной длины, которая идентифицирует учётную запись пользователя, группы, службы, домена или компьютера» [9].

					БИС.502900.007 ПЗ	Лист
Изм	Лист	№ докум.	Подпись	Дата		11

Для дальнейшего обзора стандарта и разработки присвоим каждой рекомендации идентификаторы (таблица 2.1).

Таблица 2.1 - Присвоение идентификаторов рекомендациям

ID	Раздел в стандарте	Название рекомендации
101	1.2.1.1	Ensure 'Protection From Zone Elevation' is set to Enabled
102	1.2.1.2	Ensure 'Mime Sniffing Safety Feature' is set to Enabled
103	1.2.1.3	Ensure 'Information Bar' is set to Enabled
104	1.2.1.4	Ensure 'Bind to Object' is set to Enabled
105	1.2.1.5	Ensure 'Restrict File Download' is set to Enabled
106	1.2.1.6	Ensure 'Saved from URL' is set to Enabled
107	1.2.1.7	Ensure 'Disable User Name and Password' is set to Enabled
108	1.2.1.8	Ensure 'Scripted Window Security Restrictions' is set to Enabled
109	1.2.1.9	Ensure 'Local Machine Zone Lockdown Security' is set to Enabled
110	1.2.1.10	Ensure 'Object Caching Protection' is set to Enabled
111	1.2.1.11	Ensure 'Consistent Mime Handling' is set to Enabled
112	1.2.1.12	Ensure 'Add-on Management' is set to Enabled
113	1.2.1.13	Ensure 'Navigate URL' is set to Enabled
114	1.2.1.14	Ensure 'Restrict ActiveX Install' is set to Enabled
115	1.3.1	Ensure 'Enable Automatic Updates' is set to Enabled
116	1.3.2	Ensure 'Hide Option to Enable or Disable Updates' is set to Enabled
117	2.7.1	Ensure 'Document Information Panel Beaconsing UI' is set to Enabled (Always show UI)
118	2.11.1.2	Ensure 'Disable UI Extending from Documents and Templates' is set to Enabled
119	2.17.1	Ensure 'Prevent Users From Changing Permissions on Rights Managed Content' is set to Disabled
120	2.17.2	Ensure 'Never Allow Users to Specify Groups When Restricting Permission for Documents' is set to Enabled
121	2.17.3	Ensure 'Always Require Users to Connect to Verify Permission' is set to Enabled
122	2.17.4	Ensure 'Always Expand Groups in Office When Restricting Permission for Documents' is set to Enabled
123	2.17.5	Ensure 'Allow Users With Earlier Versions of Office to Read with Browsers....' is set to Disabled
124	2.21.2	Ensure 'Control Blogging' is set to Enabled (All Blogging Disabled)
125	2.21.3	Ensure 'Block Signing into Office' is set to Enabled (None allowed)

Продолжение таблицы 2.1

ID	Раздел в стандарте	Название рекомендации
126	2.22.1	Ensure 'Block Opening of Pre-Release Versions of File Formats New to PowerPoint Through the Compatibility Pack for Office and PowerPoint Converter' is set to Enabled
127	2.22.2	Ensure 'Block Opening of Pre-release Versions of File Formats New to Excel Through The Compatibility Pack for Office and Excel Converter' is set to Enabled
128	2.24.1.1	Ensure 'Disable Opt-in Wizard on First Run' is set to Enabled
129	2.24.1.2	Ensure 'Enable Customer Experience Improvement Program' is set to Disabled
130	2.24.1.3	Ensure 'Allow including screenshot with Office Feedback' is set to Disabled
131	2.24.1.4	Ensure 'Send Office Feedback' is set to Disabled
132	2.24.1.5	Ensure 'Send personal information' is set to Disabled
133	2.24.1.6	Ensure Set 'Automatically Receive Small Updates to Improve Reliability' is set to Disabled
134	2.25.3.3	Ensure 'Allow Mix of Policy and User Locations' is set to Disabled
135	2.25.4	Ensure 'Suppress Hyperlink Warnings' is set to Disabled
136	2.25.5	Ensure 'Protect Document Metadata for Rights Managed Office Open XML Files' is set to Enabled
137	2.25.6	Ensure 'Protect Document Metadata for Password Protected Files' is set to Enabled
138	2.25.7	Ensure 'Load Controls in Forms3' is set to Disabled
139	2.25.8	Ensure 'Encryption Type for Password Protected Office Open XML Files' is set to Enabled
140	2.25.9	Ensure 'Encryption Type for Password Protected Office 97-2003 files' is set to Enabled
141	2.25.10	Ensure 'Disable Password to Open UI' is set to Disabled
142	2.25.11	Ensure 'Disable All Trust Bar Notifications For Security Issues' is set to Disabled
143	2.25.12	Ensure 'Automation Security' is set to Enabled (Disable Macros by Default)
144	2.25.13	Ensure 'ActiveX Control Initialization' is set to Disabled
145	2.26.2	Ensure 'Disable The Office Client From Polling The SharePoint Server For Published Links' is set to Enabled
146	2.27.1.1	Ensure 'Disable Internet Fax Feature' is set to Enabled
147	2.29.1	Ensure 'Suppress External Signature Service' is set to Enabled
148	2.29.2	Ensure 'Legacy Format Signatures' is set to Disabled
149	2.30.1	Ensure 'Disable Smart Document's Use of Manifests' is set to Enabled

Продолжение таблицы 2.1

ID	Раздел в стандарте	Название рекомендации
150	2.34.2.1	Ensure 'Online Content Options' is set to Enabled (Allow Office to connect to the internet)
151	2.35.1.1	Ensure 'Allow PNG As an Output Format' is set to Disabled
152	2.35.3.1	Ensure 'Open Office Documents as Read/Write While Browsing' is set to Disabled
153	2.36.1.1	Ensure 'Improve Proofing Tools' is set to Disabled

Проверка рекомендаций заключается в сравнении значений реестра требуемым стандартом безопасности. В рекомендациях с идентификаторами 139 и 140 также проверяется корректность типов шифрования, указанных администратором при настройке офисных пакетов.

2.4 Соответствие настроек групповых политик значениям в реестре Windows

В стандарте указаны требуемые значения «Enabled», «Disable» и т.п., а в реестре значения в числовом формате. Для того, чтобы знать, с какими значениями сравнивать содержимое настроек реестра была проведена работа по сопоставлению значений настроек групповых политик значениям в реестре Windows. Результаты отображены в таблице 2.2.

Таблица 2.2 – Соответствие настроек политик значениям в реестре

ID	Значение групповой политики	Параметр (если есть)	Значение реестра
101 - 116; 118 - 123; 126 - 137; 141 - 142; 145 - 149; 151 - 153.	Not cofigured		Null
	Enabled		1
	Disabled		0

Продолжение таблицы 2.2

ID	Значение групповой политики	Параметр (если есть)	Значение реестра
117	Not configured		Null
	Enabled	Never show UI	0
		Always show UI	1
		Show UI if XSN is in Internet Zone	2
	Disabled		Null
124	Not configured		Null
	Enabled	Enabled	0
		Only SharePoint blogs allowed	1
		All blogging disabled	2
	Disabled		Null
125	Not configured		Null
	Enabled	Both IDs allowed	0
		Microsoft Account only	1
		Org ID only	2
		None allowed	3
	Disabled		Null
138	Not configured		Null
	Enabled	1	1
		2	2
		3	3
		4	4
	Disabled		Null
139-140	Not configured		Null
	Enabled	<Encryption type in str format>	<REG_SZ type>
	Disabled		Null

Продолжение таблицы 2.2

ID	Значение групповой политики	Параметр (если есть)	Значение реестра
143	Not cofigured		Null
	Enabled	Macros enabled	1
		Only ShareUse application macro security level	2
		Disable macros by default	3
	Disabled		Null
144	Not cofigured		Null
	Enabled	1	1
		2	2
		3	3
		4	4
		5	5
		6	6
	Disabled		0
150	Not cofigured		Null
	Enabled	Do not allow Office to connect to the Internet	0
		Allow Office to connect to the Internet	2
	Disabled		Null

В процессе работы с редактором групповых политик было обнаружено, что для рекомендаций с идентификаторами 119, 123, 135, 141 и 144 приемлемо несколько значений («Disabled» и «Not configured»).

3 Технологии и средства разработки

3.1 Система контроля версий

«Система контроля версий (СКВ) – это система, регистрирующая изменения в одном или нескольких файлах с тем, чтобы в дальнейшем была возможность вернуться к определённым старым версиям этих файлов» [10].

В качестве системы контроля версий был выбран Git.

«Git - распределенная система контроля версий, разработанная Линусом Торвальдсом» [11]. Программа является свободной и выпущена под лицензией GNU GPL. Особенностью Git, которая выделяет его из большинства СКВ, является модель ветвления.

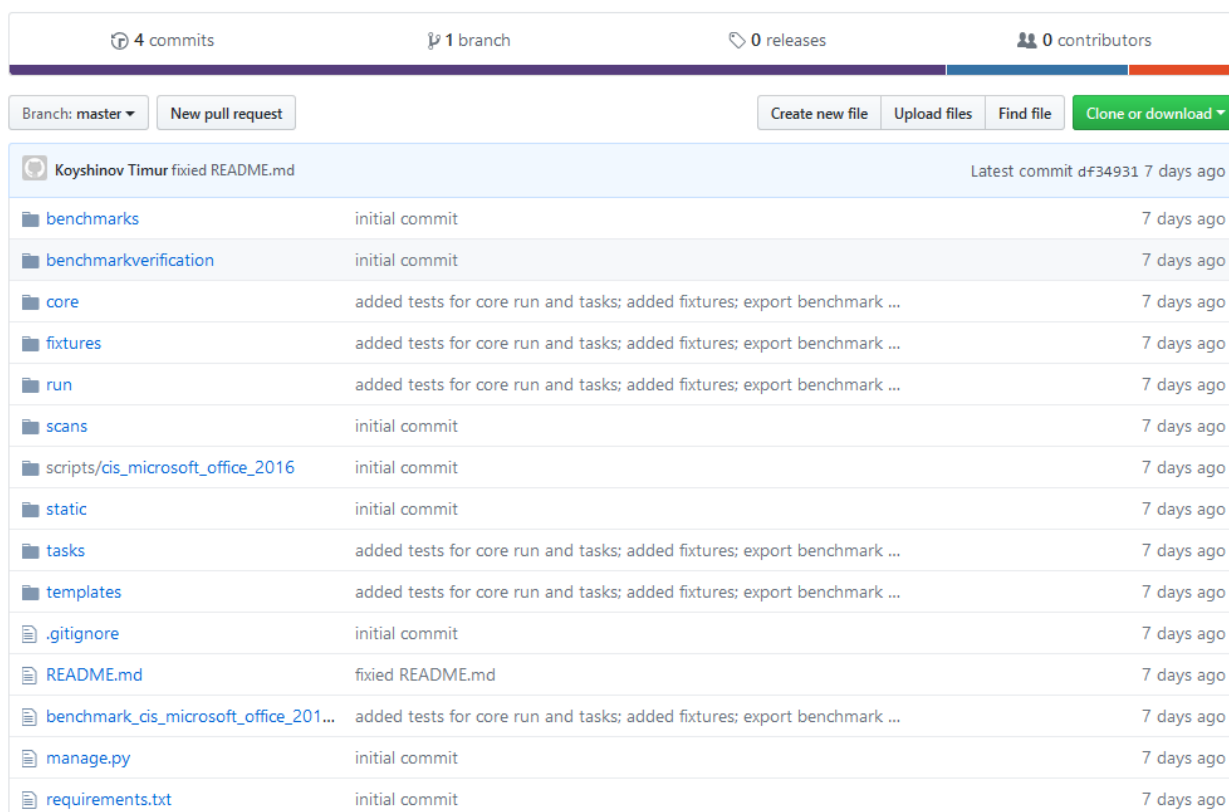


Рисунок 3.1 – Веб-интерфейс репозитория на github

Рабочий Git-репозиторий приложения размещен на сервере Github по адресу <https://github.com/koyshinov/BenchmarkVerification>. На сервере проект доступен для просмотра и скачивания (рис. 3.1).

3.2 Язык программирования и веб-фреймворк

В качестве языка программирования был выбран Python версии 3.7.

«Python – высокоуровневый язык программирования общего назначения, ориентированный на повышение производительности разработчика и читаемости кода» [12].

«Python поддерживает несколько парадигм программирования, в том числе структурное, объектно-ориентированное, функциональное, императивное и аспектно-ориентированное. Основные архитектурные черты – динамическая типизация, автоматическое управление памятью, полная интроспекция, механизм обработки исключений, поддержка многопоточных вычислений и удобные высокоуровневые структуры данных. Код в Python организовывается в функции и классы, которые могут объединяться в модули (они, в свою очередь, могут быть объединены в пакеты)» [12].

Для разработки приложения было решено использовать веб-фреймворк Django, который придерживается концепции MTV (Model - Template - View).

«Модель (Model) – слой доступа к данным. Этот слой знает все о данных: как получить к ним доступ, как проверить их, как с ними работать и как данные связаны между собой» [13].

Для работы с базой данных Django использует технологию ORM, в которой модель данных описывается с помощью классов, на их основе генерируется схема базы данных.

«Шаблон (Template) – слой представления данных. Этот слой принимает решения относительно представления данных: как и что должно отображаться на странице или в другом типе документа» [13].

Шаблоны содержат в себе статические HTML-коды с динамическими данными, генерация которых возможна с помощью специальных конструкций шаблонизатора Django.

«Представление (View) – слой бизнес-логики. Этот слой содержит логику, как получать доступ к моделям и применять соответствующий шаблон. Можно рассматривать его как мост между моделями и шаблонами» [13].

3.3 Интегрированная среда разработки

В качестве интегрированной среды разработки был выбран PyCharm (рис. 3.2), разработанный компанией JetBrains.

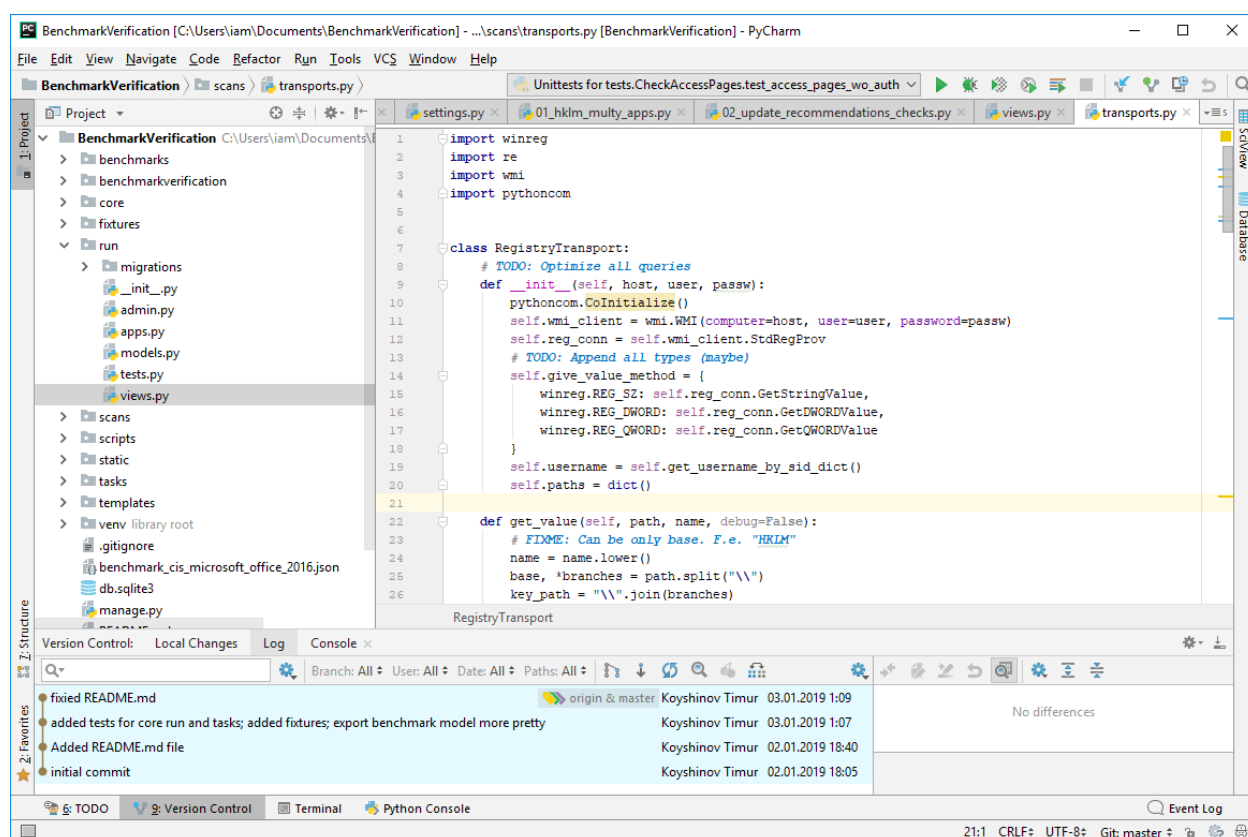


Рисунок 3.2 – Интегрированная среда разработки PyCharm

Основные возможности PyCharm [14]:

- полнофункциональная IDE для разработки на Python, в том числе для многоязычных веб-приложений с фреймворками;
- поддержка фреймворков Django, Flask, Google App Engine, Pyramid, web2py;
- поддержка языков JavaScript, CoffeeScript, TypeScript, CSS;
- удаленная разработка, поддержка работы с базой данных;

- обнаружение дублирующегося кода;
- диаграммы UML & SQLAlchemy;
- профилирование кода Python.

3.4 Средства виртуализации для тестирования

Для тестирования приложения необходимы машины с операционной системой Windows и возможностью подключения к удаленному рабочему столу. Целесообразно использовать виртуальные машины (ВМ) с установленной операционной системой Microsoft Windows (рис. 3.3).

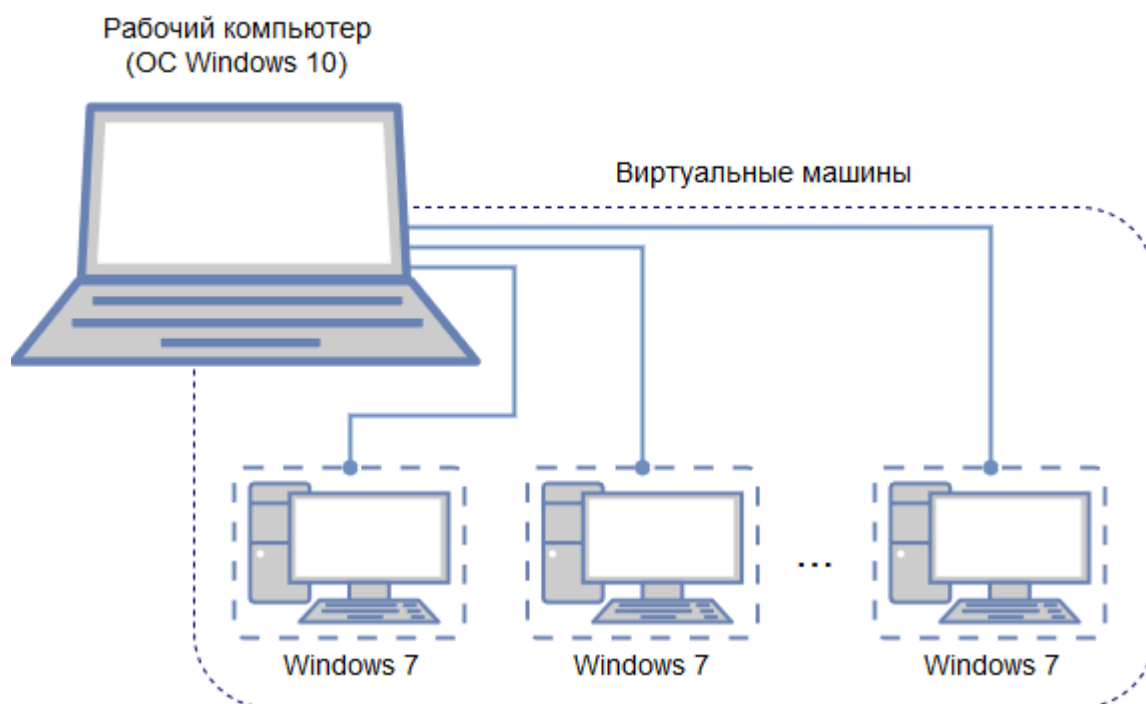


Рисунок 3.3 – Схема виртуальных машин для тестирования приложения

В качестве программы для виртуализации был выбран Oracle VM VirtualBox.

«Oracle VM VirtualBox – кроссплатформенное программное обеспечение для виртуализации, которое позволяет запускать несколько операционных систем одновременно» [15].

В качестве операционной системы для виртуальных машин была выбрана Microsoft Windows 7, так как требует меньше системных ресурсов, чем Microsoft Windows 8.1 или Microsoft Windows 10.

4 Настройка виртуальных машин для тестирования приложения

Для тестирования приложения необходимы виртуальные машины. Т.к. на рабочем компьютере 4 ГБ оперативной памяти, а для работы Windows 7 нужен 1 ГБ [16], то целесообразно использовать для тестирования три виртуальные машины, на которых будут установлены операционные системы с различной настройкой групповых политик Microsoft Office. Характер настроек виртуальных машин отображен в таблице 4.1.

Таблица 4.1 – Виртуальные машины для тестирования

Название	IP адрес	Настройки безопасности
All Good Stand	192.168.1.101	Виртуальная машина должна быть настроена в соответствии с рекомендациями стандарта безопасности.
All Bad Stand	192.168.1.102	Виртуальная машина должна быть настроена так, чтобы никакие рекомендации стандарта безопасности не соблюдались.
Not Configured Stand	192.168.1.103	Виртуальная машина должна быть без настроек групповых политик Microsoft Office

Первоначально нужно создать виртуальные машины в VirtualBox.

Далее необходимо установить:

- операционную систему Microsoft Windows 7;
- офисные пакеты Microsoft Office 2016;
- шаблоны групповых политик Microsoft Office 2016.

В виртуальных машинах в программе VirtualBox в качестве настройки сети указываем «Сетевой мост» (рис. 4.1). Благодаря настройке «Сетевой мост» виртуальные машины получают IP-адреса той же подсети, что и рабочий компьютер [17]. Структура сети будет выглядеть как на рисунке 4.2. Для удобства пропишем статические IP-адреса (рис.4.3) согласно таблице 4.1.

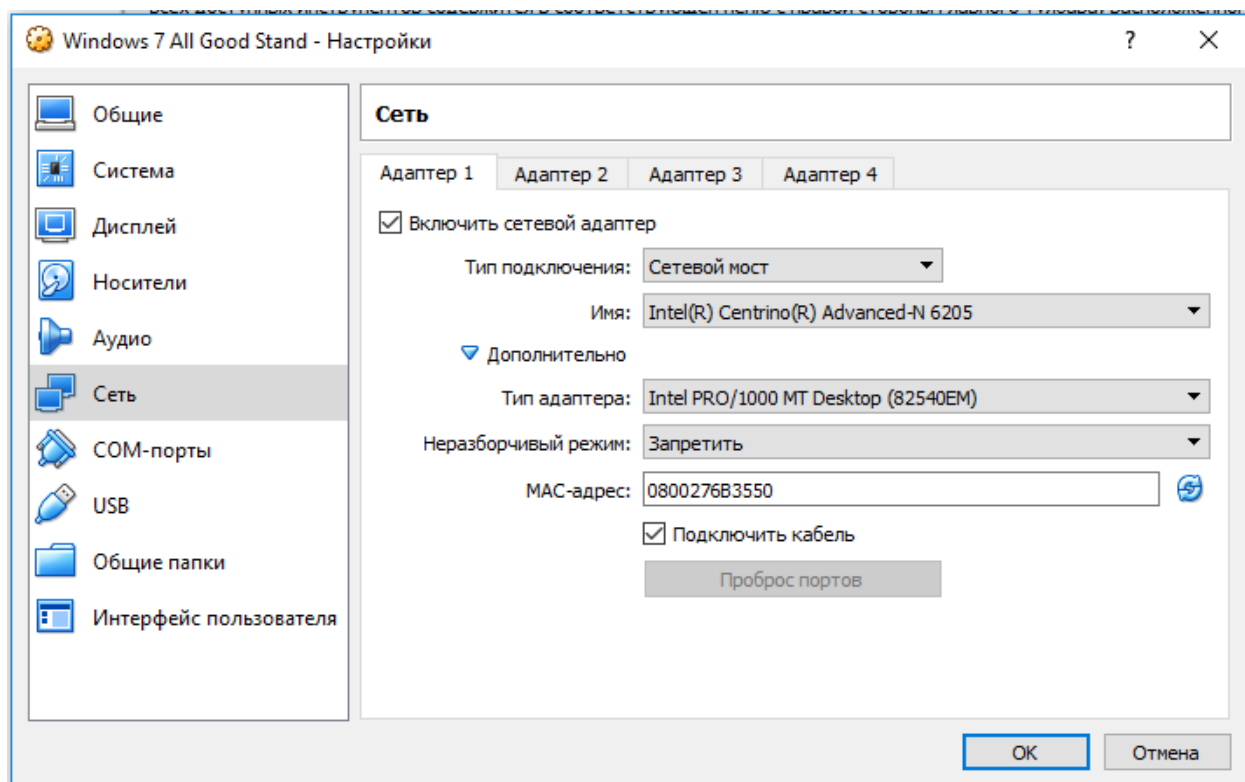


Рисунок 4.1 – Настройки сети виртуальной машины

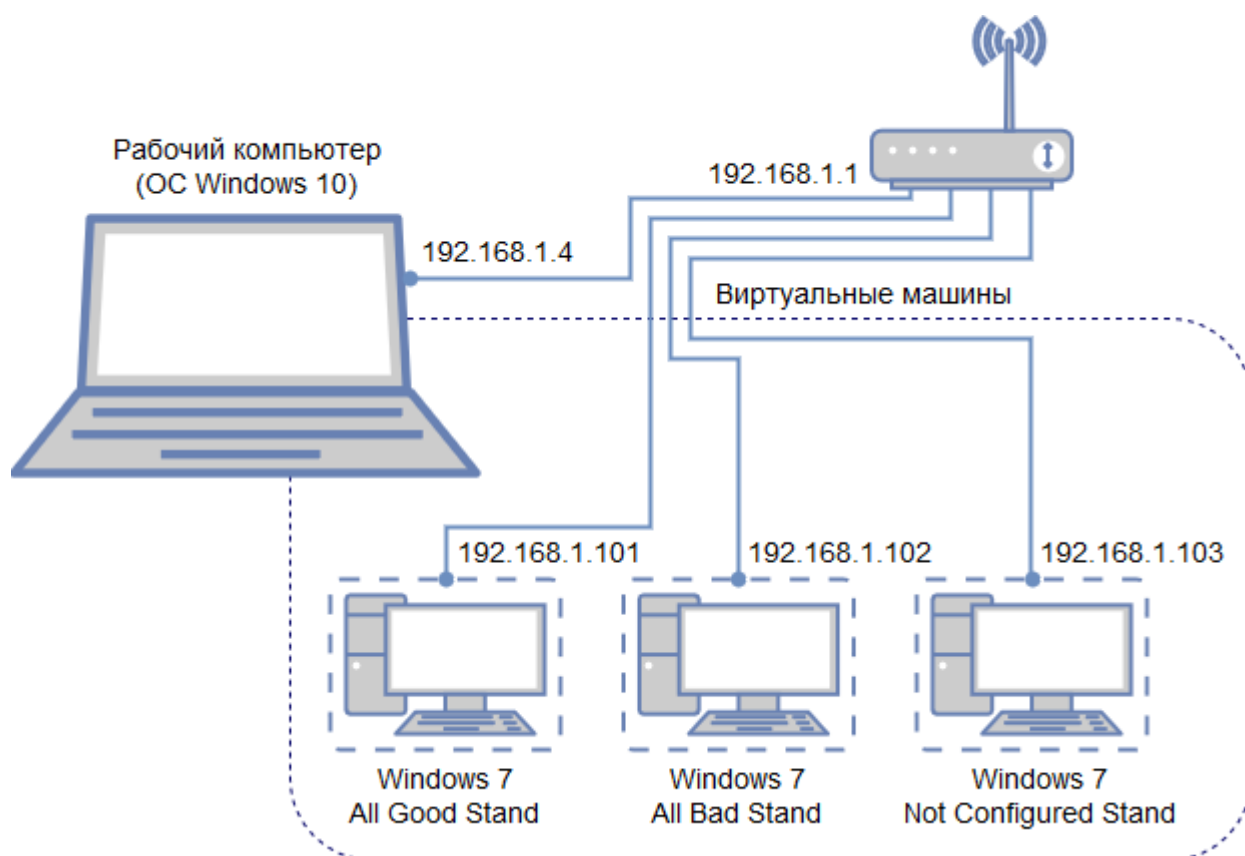


Рисунок 4.2 – Структура сети

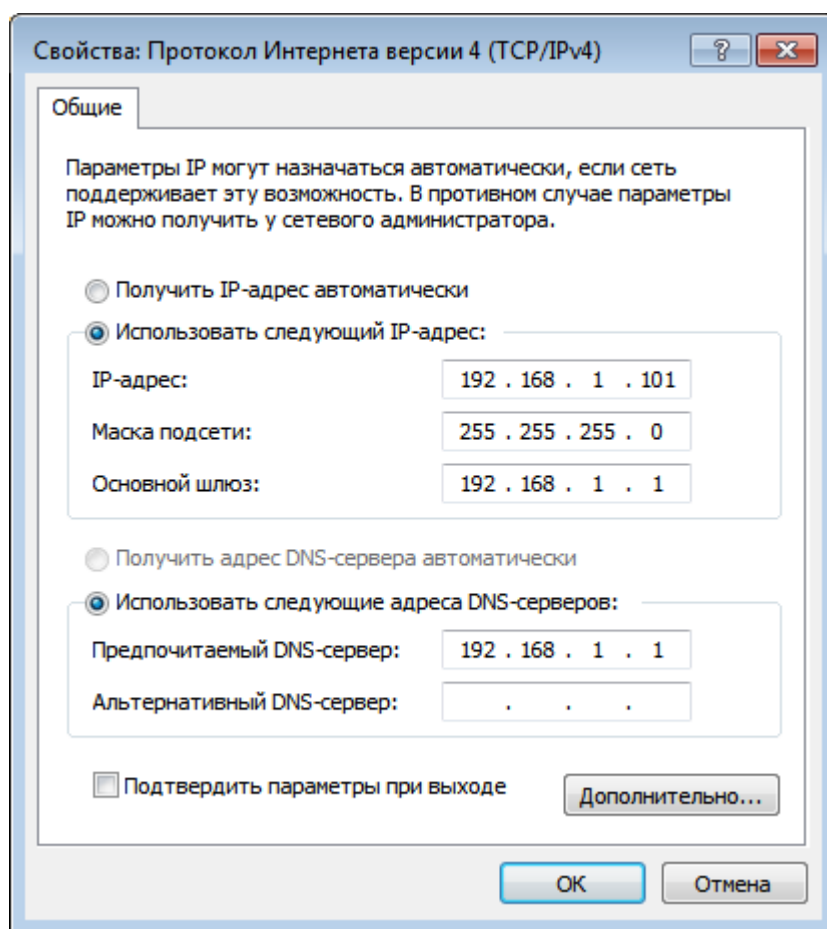


Рисунок 4.3 – Настройка статического IP адреса

Разрешаем удаленный доступ к рабочему столу и настраиваем брандмауэр на виртуальных машинах в командной строке. Вводим «netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow» для того, чтобы брандмауэр пропускал пакеты утилиты «ping». Вводим «netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes», чтобы брандмауэр пропускал трафик библиотеки Python «wmi» [18].

Шаблоны групповых политик для Microsoft Office 2016 скачиваем с официального сайта Microsoft [19]. В распакованном архиве будет папка «admx». Содержимое папки «admx» копируем в папку «C:\Windows\Policy Definition». После копирования в групповых политиках появятся настройки Microsoft Office 2016 (рис. 4.4).

Настройка параметров групповых политик (рис. 4.5) проходит согласно стандарту безопасности в соответствии с виртуальной машиной.

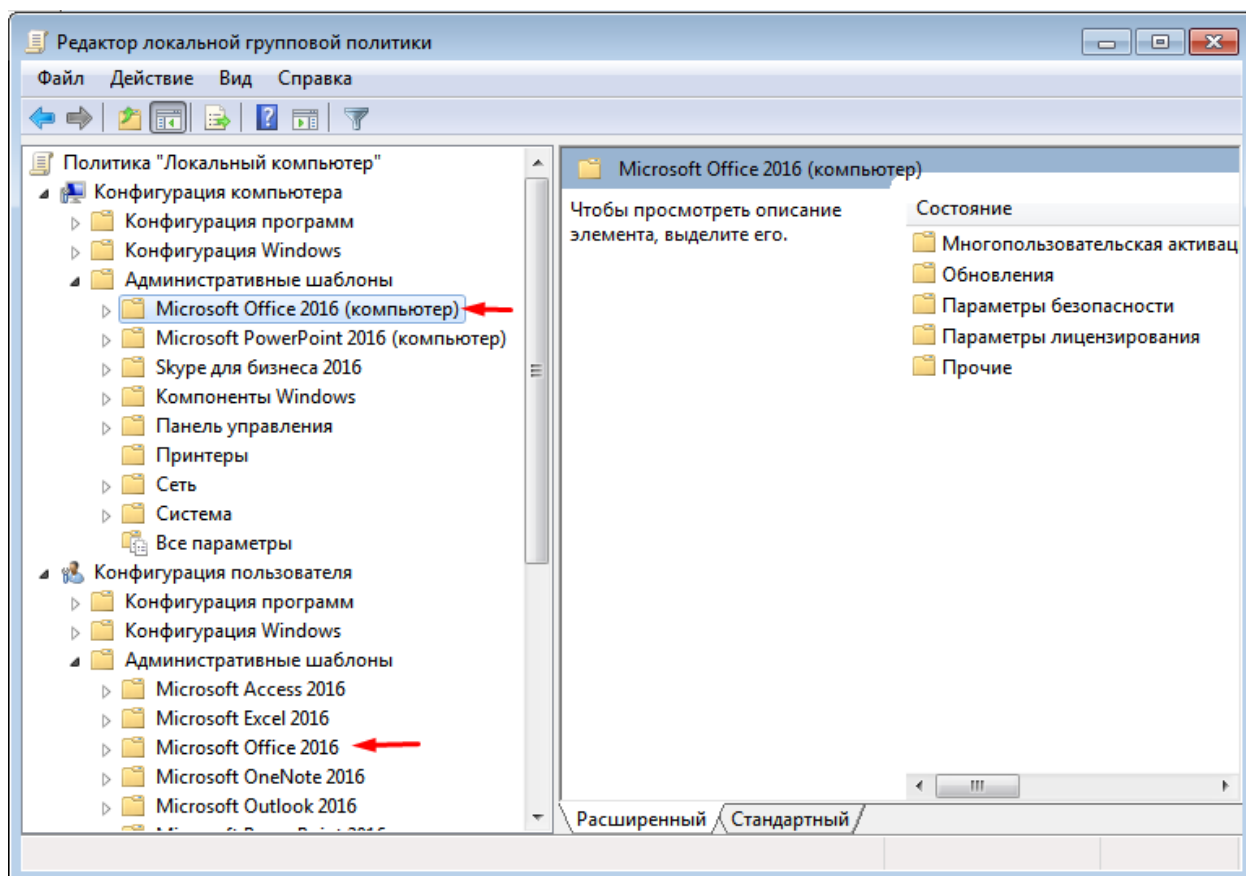


Рисунок 4.4 – Настройки групповых политик для Microsoft Office 2016

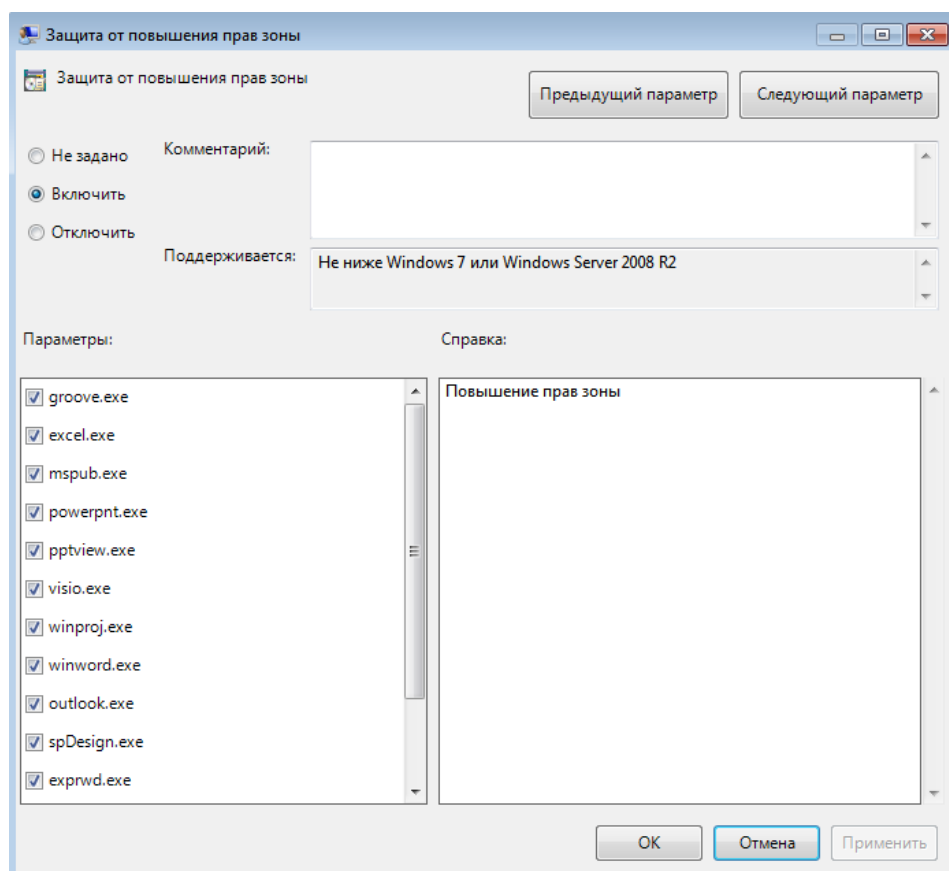
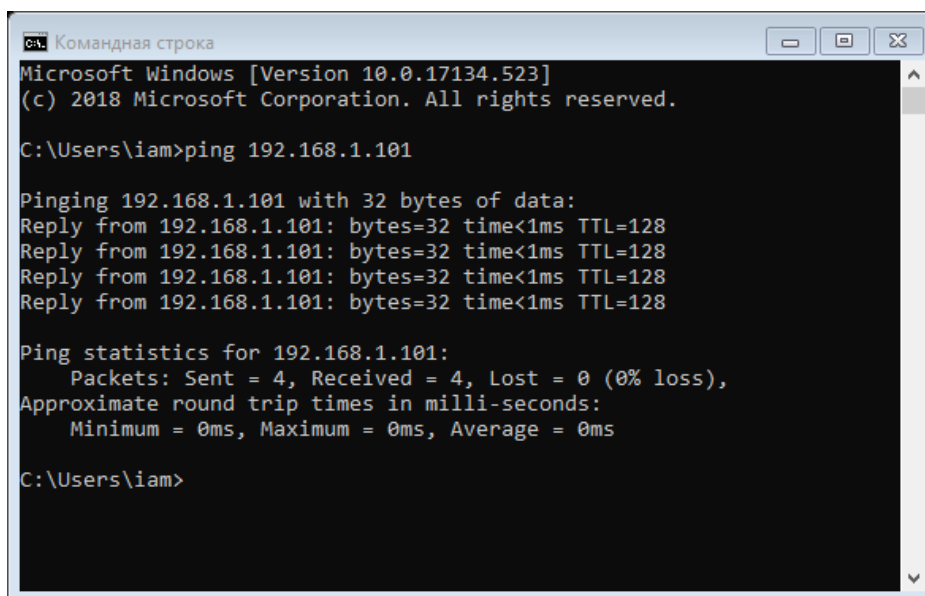


Рисунок 4.5 – Настройка параметра «Protection From Zone Elevation»

Для того, чтобы убедиться в готовности использования виртуальных машин, сделаем следующие действия:

- проверим соединение с виртуальными машинами с помощью программной утилиты «ping» (рис. 4.6);
- доступность подключений к удаленным рабочим столам виртуальных машин;
- доступность подключений через библиотеку Python «wmi» (рис. 4.7).



```
Ca\ Командная строка
Microsoft Windows [Version 10.0.17134.523]
(c) 2018 Microsoft Corporation. All rights reserved.

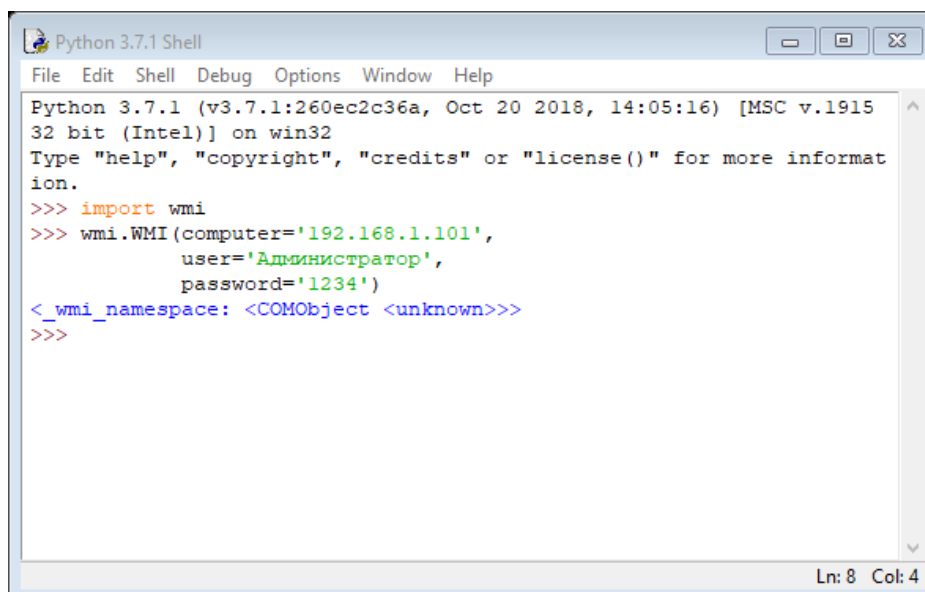
C:\Users\iam>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\iam>
```

Рисунок 4.6 – Проверка соединения



```
Python 3.7.1 Shell
File Edit Shell Debug Options Window Help
Python 3.7.1 (v3.7.1:260ec2c36a, Oct 20 2018, 14:05:16) [MSC v.1915
32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license()" for more informat
ion.
>>> import wmi
>>> wmi.WMI(computer='192.168.1.101',
            user='Администратор',
            password='1234')
<wmi_namespace: <COMObject <unknown>>>
>>>
```

Рисунок 4.7 – Проверка подключения

5 Разработка приложения для анализа защищенности Microsoft Office

5.1 Проектирование инфологической модели данных

Цель – анализ защищенности Microsoft Office 2016 с помощью проверки соблюдения рекомендаций стандарта безопасности CIS Microsoft Office 2016.

Возможные варианты результата проверки отображены в таблице 5.1.

Таблица 5.1 – Значения возможных вариантов результатов проверки

Результат проверки	Сообщение для пользователя	Значение
Соответствует	Compliant (Зеленый)	Настройка групповой политики совпадает с рекомендуемой
Не соответствует	Not Compliant (Красный)	Настройка групповой политики не совпадает с рекомендуемой
Неприменимо	Not Applicable (Синий)	Нет необходимой информации для того, чтобы определить, соответствует ли настройка групповой политики рекомендуемой
Неизвестно	Unknown (Желтый)	Во всех других (не предвиденных случаях)

Защищенность Microsoft Office будет определяться, как соответствие настроек групповых политик рекомендуемым. Данная оценка будет выражена в процентах с минимальным значением 0, максимальным 100.

Оценка защищенности будет рассчитываться по формуле (5.1):

$$\text{Защищенность} = \frac{C}{C+HC}, \quad (5.1)$$

где C – количество проверок с результатом «соответствует»;

HC – количество проверок с результатом «не соответствует».

Для анализа защищенности офисных пакетов необходимо использовать базы данных (БД).

Основными пользователями БД являются аудитор и администратор.

Аудитор – тот, кто проверяет на защищенность офисные пакеты. Администратор нужен будет для того, чтобы создавать или удалять пользователей, а также для более гибкой работы с данными.

Основные бизнес-процессы:

- авторизация пользователя;
- просмотр требований стандарта;
- создание и просмотр конфигураций сканирования;
- сканирования целевых удаленных систем;
- подсчет оценки защищенности;
- просмотр общих результатов сканирования;
- просмотр подробных результатов сканирования по каждой рекомендации.

Бизнес-правила:

- для того, чтобы получить доступ к функционалу приложения, нужно авторизоваться;
- для сканирования систем доступен только один стандарт безопасности CIS Microsoft Office 2016;
- стандарт состоит из 53 рекомендаций;
- можно проверить на соответствие стандарту несколько целевых систем;
- для того, чтобы начать сканирование целевых систем, нужно создать конфигурацию или использовать существующую;
- результат проверки должен содержать статус («соответствует», «не соответствует» и т.п.) и подробную информацию по проверяемой настройке групповой политики;
- в случае, если удаленная система не доступна, или логин-пароль не совпадают, сканирование завершается с соответствующим сообщением;
- результат каждой проверки должен содержать описание и рекомендацию исправления в соответствии со стандартом.

Описание сущностей отображено в таблице 5.2, а атрибуты сущностей – в таблице 5.3.

Таблица 5.2 – Описание сущностей

Имя сущности	Определение
User	Пользователь приложением
Task configuration	Конфигурация настроек сканирования (ip адреса, логин и пароль)
Benchmark	Стандарт безопасности
Control	Рекомендация стандарта безопасности
Total scan	Сканирование удаленных машин
Host scan	Сканирование определенной удаленной машины
Bench scan	Сканирование определенного стандарта на удаленной машине
Control scan	Сканирование рекомендации определенного стандарта на удаленной машине

Таблица 5.3 – Определение основных атрибутов сущностей

Имя атрибута	Владелец	Ограничения
Username	User	Идентификатор, обязательный
Password	User	Обязательный
Superuser status	User	Обязательный
Id	Task configuration	Идентификатор, обязательный
User	Task configuration	Обязательный
Host	Task configuration	Обязательный
WMI login	Task configuration	Обязательный
WMI password	Task configuration	Обязательный
Id	Control	Идентификатор, обязательный
Benchmark	Control	Обязательный
Name	Control	Обязательный
Information	Control	Обязательный, в формате yaml
Id	Benchmark	Идентификатор, обязательный
Name	Benchmark	Обязательный

Продолжение таблицы 5.3

Id	Total scan	Идентификатор, обязательный
User	Total scan	Обязательный
Name	Total scan	Обязательный
Configuration	Total scan	Обязательный
Id	Host scan	Идентификатор, обязательный
Host	Host scan	Обязательный
Total scan	Host scan	Обязательный
Id	Bench scan	Идентификатор, обязательный
Host scan	Bench scan	Обязательный
Benchmark	Bench scan	Обязательный
Id	Control scan	Идентификатор, обязательный
Bench Scan	Control scan	Обязательный
Control	Control scan	Обязательный
Status	Control scan	Обязательный
Result	Control scan	В формате json

Связи между сущностями:

- User и Total scan – 1:M;
- User и Task configuration – 1:M;
- Task configuration и Total scan – 1:M;
- Task configuration и Benchmark – M:M;
- Benchmark и Control – 1:M;
- Benchmark и Bench scan – 1:M;
- Control и Control scan – 1:M;
- Total scan и Host scan – 1:M;
- Host scan и Bench scan – 1:M;
- Control scan и Bench scan – 1:M.

Структура спроектированной базы данных отображена на рисунке 5.1.

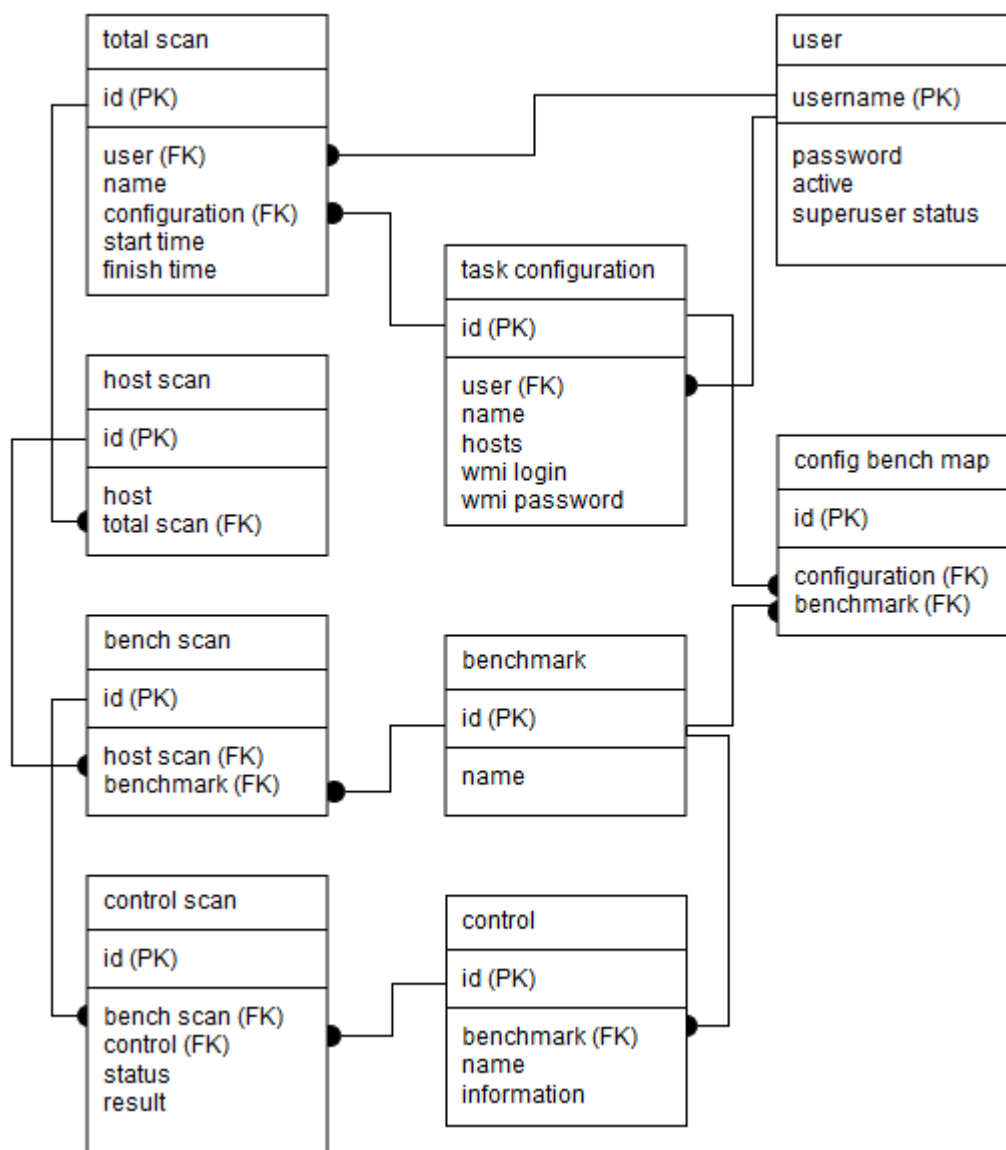


Рисунок 5.1 – Структура базы данных

5.2 Структура приложения

Проект состоит из:

- файла настройки;
- url диспетчера;
- данных для тестирования;
- статических файлов (html, css, js);
- файлов проверки стандарта безопасности;

- данные стандарта CIS Microsoft Benchmark для импорта в базу данных;
- диспетчер проекта Django;
- файл зависимостей;
- модули приложения.

Краткое описание модулей отображено в таблице 5.4.

Таблица 5.4 – Краткое описание модулей приложения

Название модуля	Описание	Содержание
benchmark	Модуль, отвечающий за отображение рекомендаций стандарта безопасности	модели; url-диспетчер; представления; настройки админ-панели.
core	Модуль, отвечающий за авторизацию	url-диспетчер; представления; тесты.
tasks	Модуль, отвечающий за конфигурации сканирований	модель; url-диспетчер; представления; настройки админ-панели; тесты.
scans	Модуль, отвечающий за отображения результатов сканирований, а также за вспомогательные функции и классы для модуля run	модели; url-диспетчер; представления; настройки админ-панели; функции работы с yaml; WMI транспорт.
run	Модуль, отвечающий за запуск и проведение сканирований	представления; тесты.

Модели в модулях отражают информацию об объектах, с которыми мы работаем. В нашем случае каждая модель представляет собой одну таблицу базы данных.

Url-диспетчер проекта получает запрашиваемый пользователем url страницы и перенаправляет его на url-диспетчер соответствующего модуля, тот в свою очередь определяет какое представление запустить.

Представления приложения обрабатывают данные от пользователя и возвращает соответствующий результат.

Через настройки админ-панели можно гибко сконфигурировать особенности работы администратора с моделями.

5.3 Алгоритм проверки настроек Microsoft Office

Проверка целевых систем начинается с того момента, когда пользователь запустит сканирование с конфигурацией.

Алгоритм анализа на защищенность целевых систем представлен на рисунке 5.3.

Проверки стандарта CIS Microsoft Office 2016 очень похожи друг на друга, поэтому было решено вынести особенности проверок в конфигурационный файл формата yaml. Конфигурационный файл содержит в себе тип проверки, ветку и ключ реестра, а также список приемлемых значений (рис. 5.2).

```
236
237 143:
238   type: users_sid_many_enabled_check
239   path: HKEY_USERS\{sid}\software\policies\microsoft\office\common\security
240   name: automationsecurity
241   compliant_values: [3]
242
243 144:
244   type: users_sid_single_enabled_check
245   path: HKEY_USERS\{sid}\software\policies\microsoft\office\common\security
246   name: uficontrols
247   compliant_values: [0, Null]
248
249 145:
250   type: users_sid_single_enabled_check
251   path: HKEY_USERS\{sid}\software\policies\microsoft\office\16.0\common\portal
252   name: linkpublishingdisabled
253   compliant_values: [1]
254
```

Рисунок 5.2 – Часть конфигурационного файла

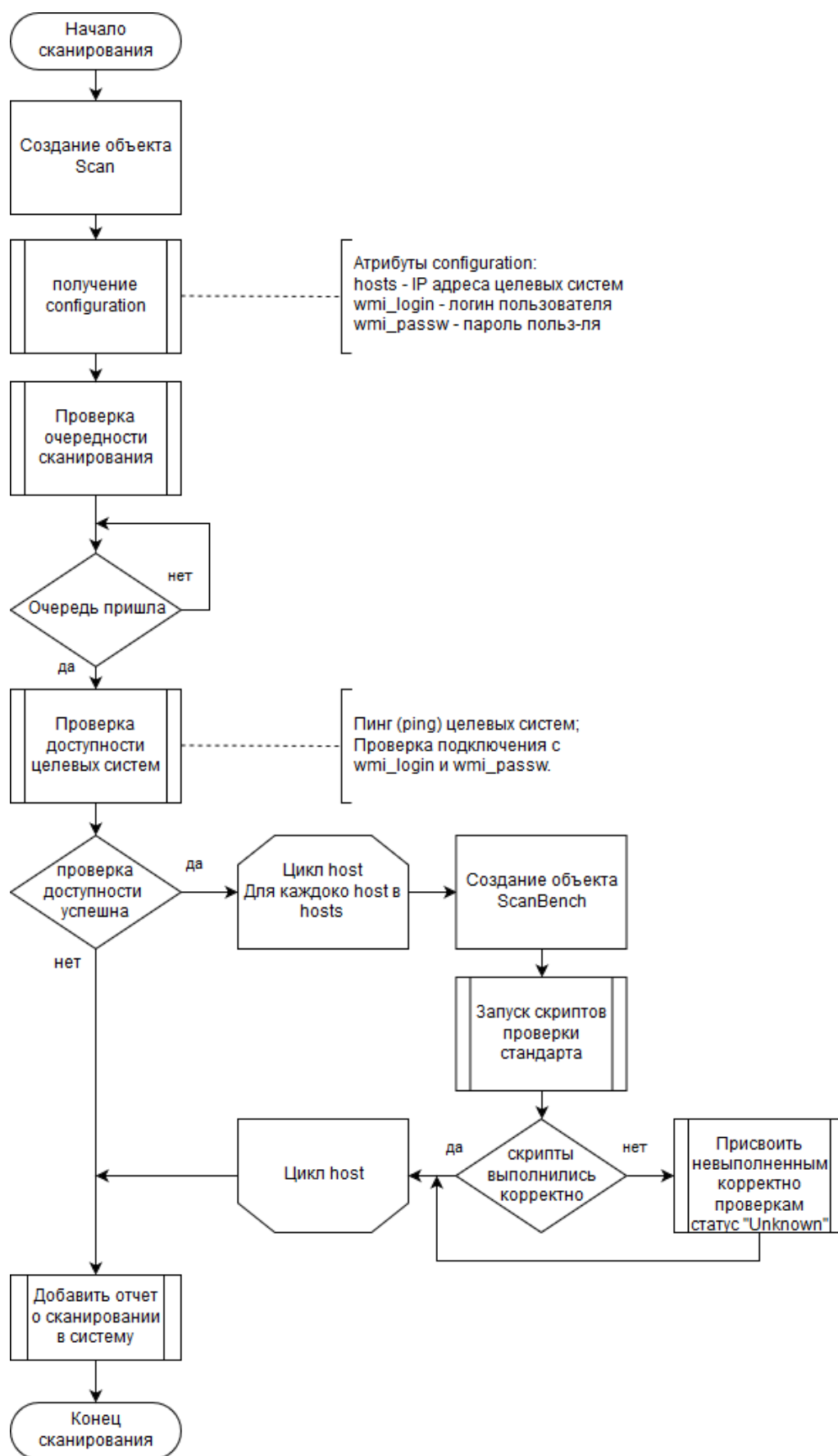


Рисунок 5.3 – Алгоритм проверки целевых систем

Есть шесть типовых видов проверок:

- проверка обновлений Microsoft Office (рис. 5.4);
- проверка настроек безопасности категории «IE Security» (рис. 5.5);
- проверка пользовательских групповых политик (рис. 5.6);
- проверка типов шифрования для защищенный паролем файлов (рис.5.7).

Особенностью последних двух видов проверок является то, что параметры нужно проверять для каждого пользователя, у которого установлен Microsoft Office 2016.

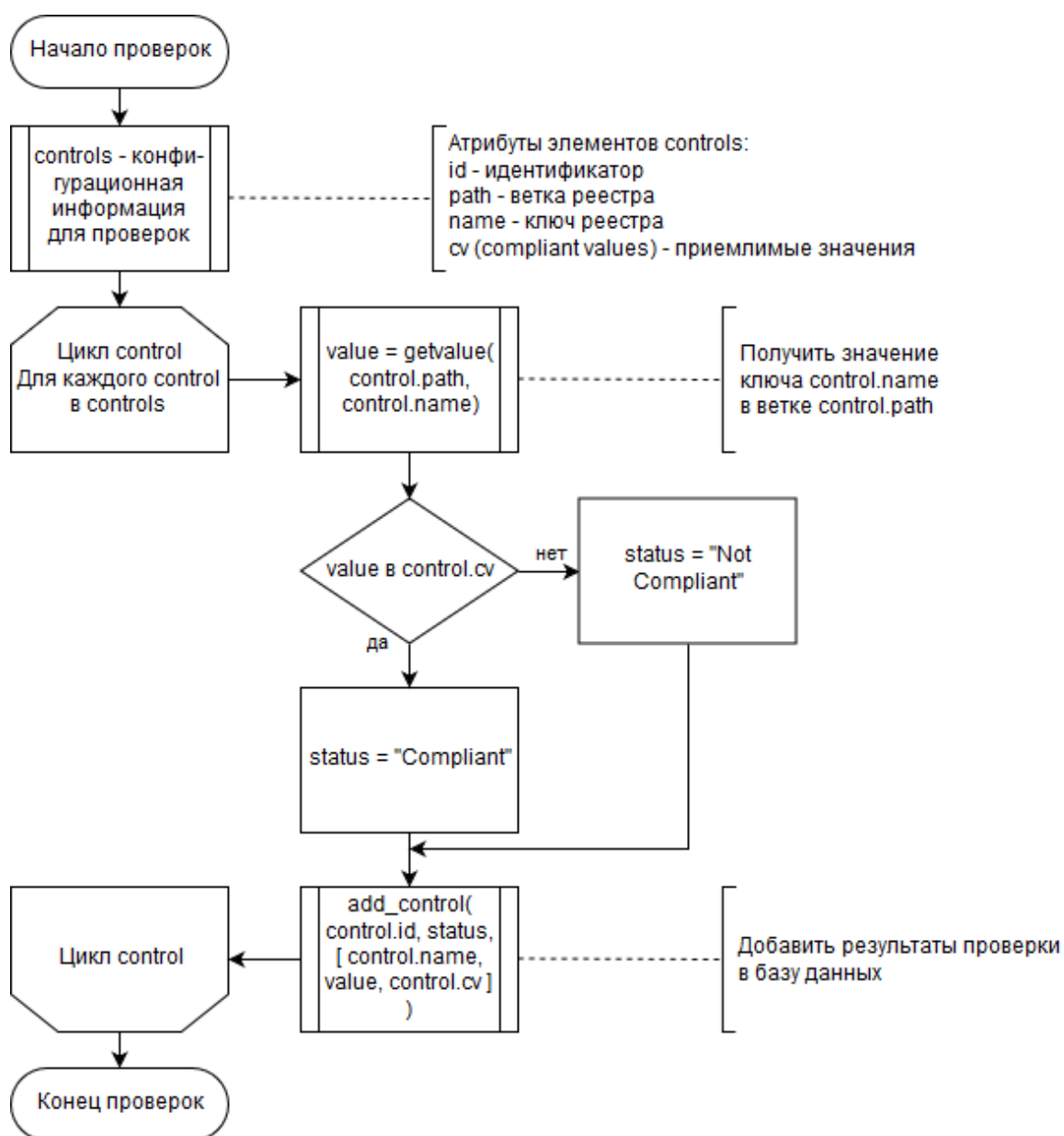


Рисунок 5.4 – Проверки обновлений

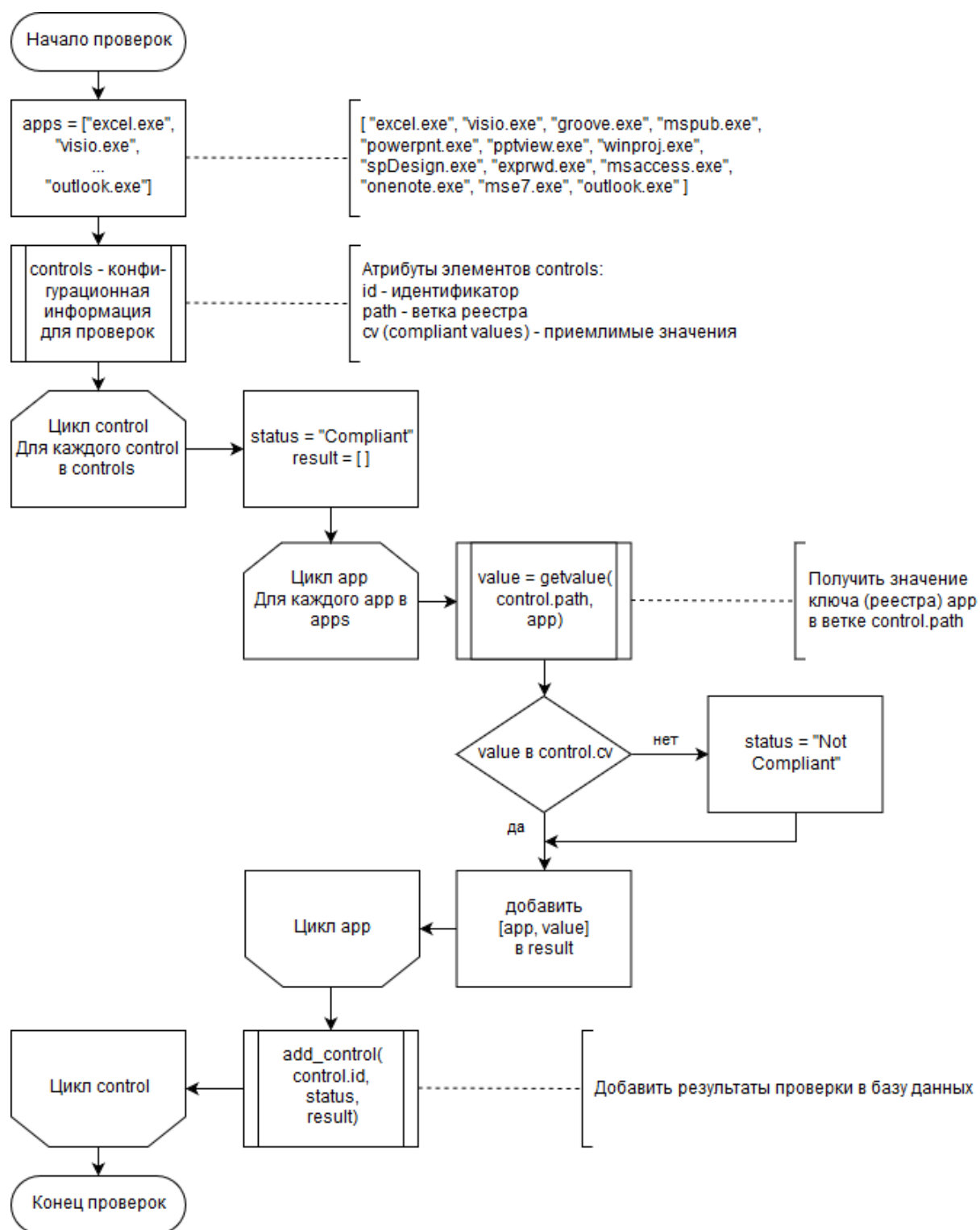


Рисунок 5.5 – Проверки параметров категории «IE Security»

В случае, если пользователь не активен, то соответствующая пользовательская ветка недоступна. Поэтому может возникнуть ситуация, что проверки 117-153 завершатся со статусом «Not Applicable».

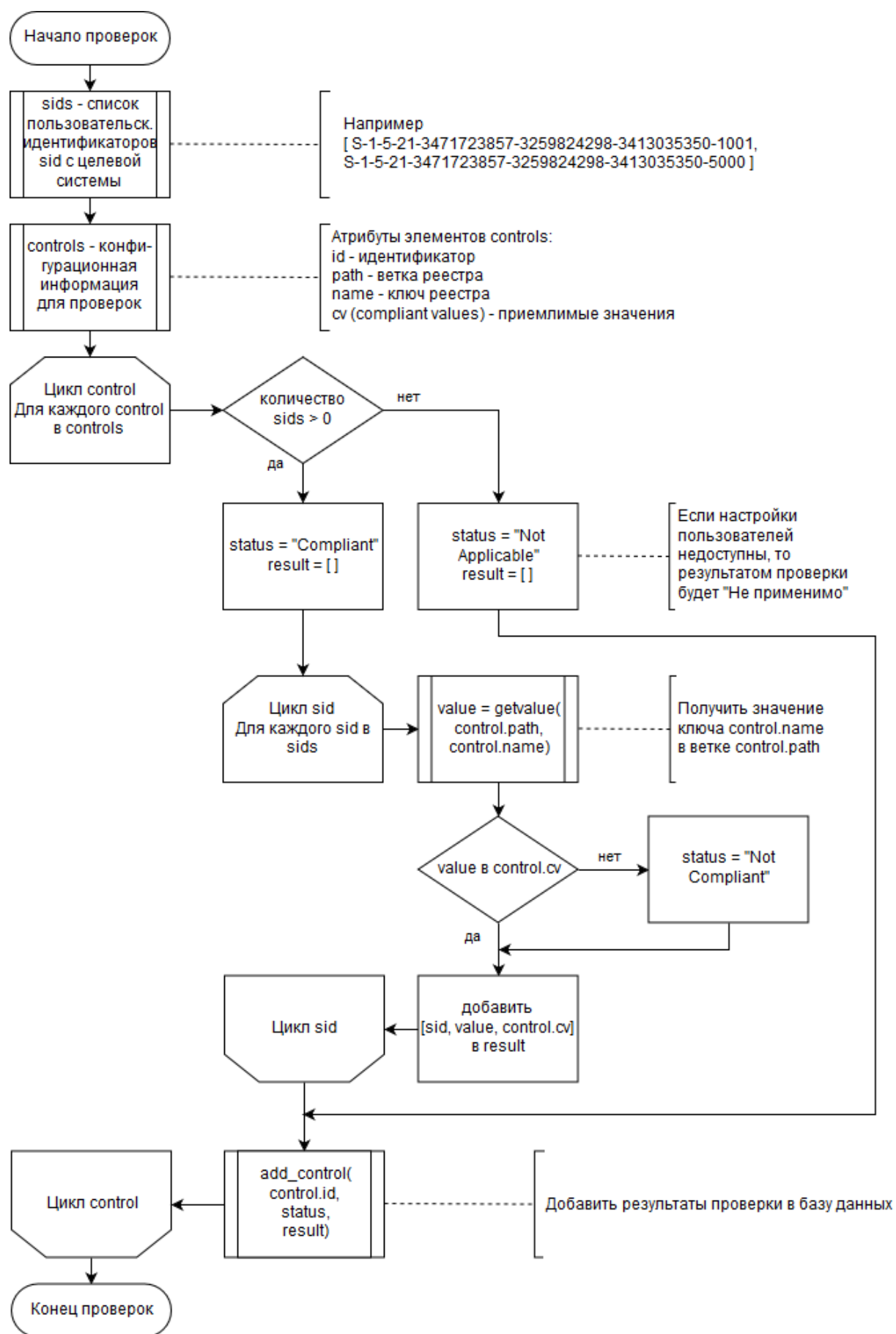


Рисунок 5.6 – Проверки пользовательских параметров

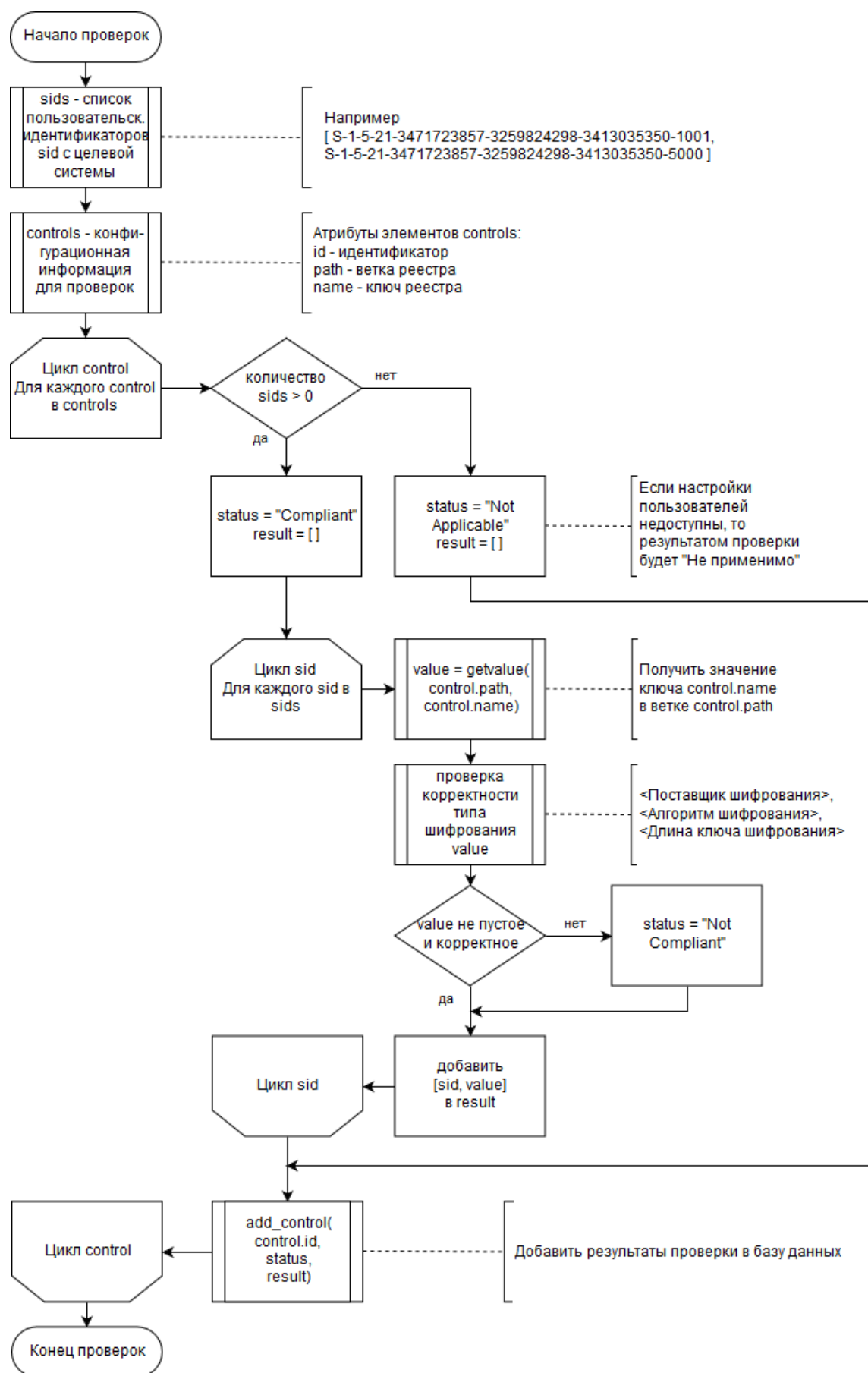


Рисунок 5.7 – Проверки типов шифрования

5.4 Описание пользовательского интерфейса

Работа с приложением происходит через веб-браузер. Для того, чтобы был доступен функционал приложения, нужно пройти авторизацию (рис. 5.8).

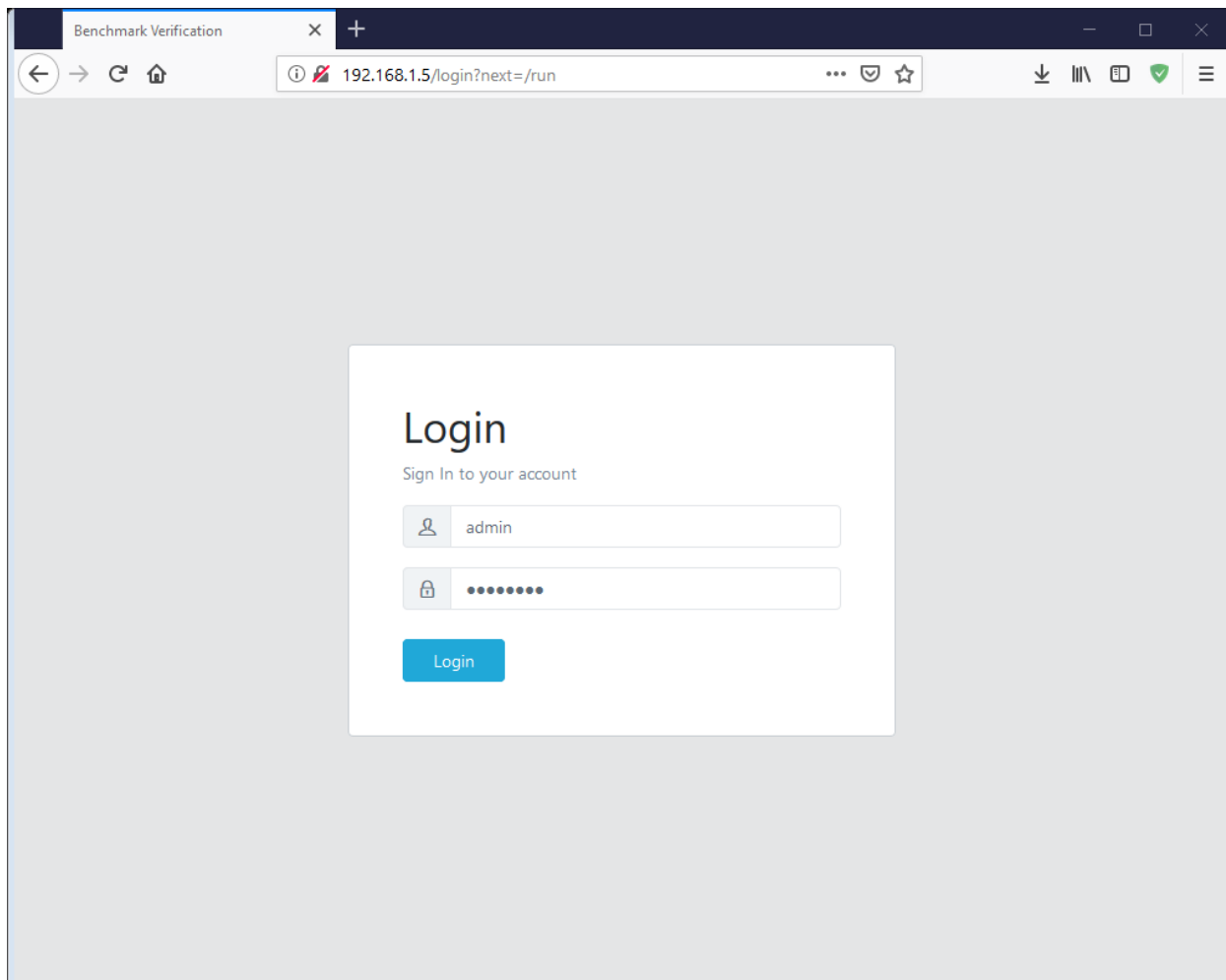


Рисунок 5.8 – Форма авторизации пользователя

После авторизации будут доступны страницы:

- описания стандарта CIS Microsoft Office 2016 (рис. 5.9);
- создания и просмотра конфигураций (рис. 5.10);
- запуска сканирования с выбором конфигурации (рис. 5.11);
- результатов сканирования (рис. 5.12-5.14).

Описание стандарта соответствует исходному. Данная страница предназначена для работы со стандартом перед сканированием целевой системы.

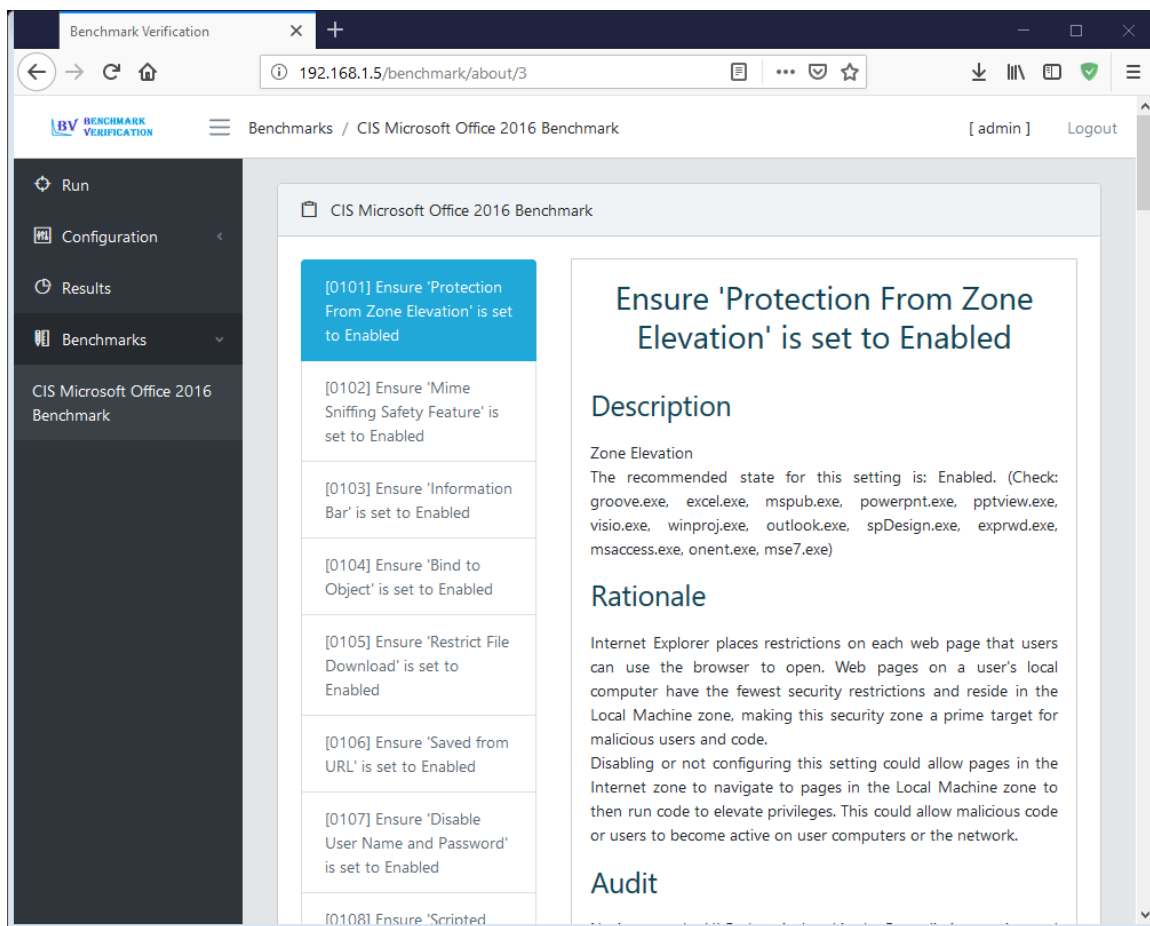


Рисунок 5.9 – Страница описания стандарта

Create Configuration

Name

Scan Virtual Machines

Benchmarks

CIS Microsoft Office 2016 Benchmark

Hosts

192.168.1.101
192.168.1.102
192.168.1.103

WMI Login

Администратор

WMI Password

••••

Repeat WMI Password

••••

Create

Рисунок 5.10 – Окно создания конфигурации

Изм	Лист	№ докум.	Подпись	Дата

БИС.502900.007 ПЗ

Лист

39

Run scanning

Name

Test scanning...

Configuration

Scan Virtual Machines

▼

Run

Рисунок 5.11 - Окно запуска сканирования

Configurations Table				
Scan Name	Finish Time	Configuration	Status	Results
Test scanning...	2019-01-14 19:04:05	Scan Virtual Machines	Complete	192.168.1.101: <Full Info> <div></div>
				192.168.1.102: <Full Info> <div></div>
				192.168.1.103: <Full Info> <div></div>

Рисунок 5.12 – Таблица результата сканирования

Host scan result						
Scan Name: Test scanning... Hostname: 192.168.1.103 Username: Администратор Start Time: 14.01.2019 19:02:57 Finish Time: 14.01.2019 19:04:05						
Benchmark	Compliant	Not compliant	Not applicable	Unknown	Safety	Detail
CIS Microsoft Office 2016 Benchmark	6 / 53	47 / 53	0 / 53	0 / 53	11 %	<Full Info>

Рисунок 5.13 – Подробная информация по сканированию

Not coml

Ensure 'Protection From Zone Elevation' is set to Enabled

Not coml

Ensure 'Mime Sniffing Safety Feature' is set to Enabled

Not coml

Ensure 'Information Bar' is set to Enabled

Not coml

Ensure 'Bind to Object' is set to Enabled

Not coml

Ensure 'Restrict File Download' is set to Enabled

Not coml

Ensure 'Saved from URL' is set to Enabled

Not coml

Ensure 'Disable User Name and Password' is set to Enabled

Not coml

Ensure 'Scripted Window Security Restrictions' is set to Enabled

Not coml

Ensure 'Local Machine Zone Lockdown Security' is set to

[116] Ensure 'Hide Option to Enable or Disable Updates' is set to Enabled

Status

Not compliant

Description

This policy setting allows you to hide the user interface (UI) options to enable or disable Office automatic updates from users. These options are found in the Product Information area of all Office applications installed via Click-to-Run. This policy setting has no effect on Office applications installed via Windows Installer. The recommended state for this setting is: Enabled.

Rationale

Security updates help prevent malicious attacks on Office applications. Timely application of Office updates helps ensure the security of devices and the applications running on the devices. Without these updates, devices and the applications running on those devices are more susceptible to security attacks. Enabling this policy setting helps prevent users from disabling automatic updates for Office.

Result

Name	System	Compliant values	Status
hideenabledisableupdates	None	1	Not compliant

Рисунок 5.14 – Результаты сканирования проверок стандарта

5.5 Описание интерфейса администратора

Если пользователь обладает правами администратора, то он может воспользоваться панелью администратора (рис. 5.15).

В панели администратора можно неограниченно работать с такими объектами, как:

- пользователи;
- стандарты;
- рекомендации стандарта;
- очередь сканирований;
- сканирования;
- конфигурации.

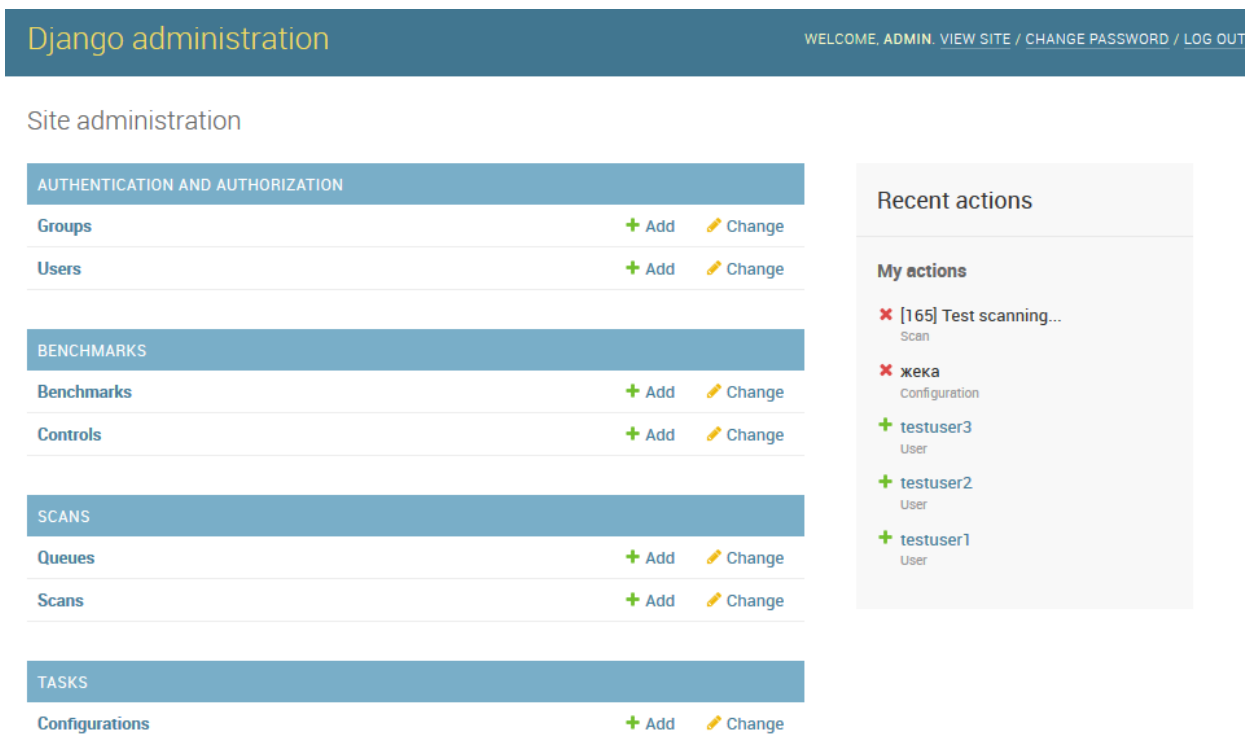


Рисунок 5.15 – Панель администратора

Для создания пользователя нужно нажать на кнопку «Add» напротив модели «Users». В появившемся окне ввести логин и пароль (рис. 5.16). Требования к паролю:

- пароль не должен совпадать с логином;
- пароль должен состоять минимум из 8 символов;
- пароль не должен состоять только из чисел.

Чтобы предоставить пользователю возможность управления данными через панель администратора необходимо поставить галочку рядом с полями «Staff status» и «Superuser status» (рис. 5.17). Для того чтобы лишить пользователя этой возможности, соответствующие галочки нужно убрать.

Пользователя можно заблокировать, если снять галочку с полем «Active». Все данные останутся, но пользователь не сможет авторизоваться и работать с приложением.

Add user

First, enter a username and password. Then, you'll be able to edit more user options.

Username:

Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Password:

Your password can't be too similar to your other personal information.

Your password must contain at least 8 characters.

Your password can't be a commonly used password.

Your password can't be entirely numeric.

Password confirmation:

Enter the same password as before, for verification.

[Save and add another](#)[Save and continue editing](#)[SAVE](#)

Рисунок 5.16 – Создание пользователя

Permissions

☒ **Active**

Designates whether this user should be treated as active. Unselect this instead of deleting accounts.

☒ **Staff status**

Designates whether the user can log into this admin site.

☒ **Superuser status**

Designates that this user has all permissions without explicitly assigning them.

Рисунок 5.17 – Добавление прав администратора

В случае необходимости можно отредактировать информацию по определенной рекомендации стандарта безопасности во вкладке «Controls» (рис. 5.18). Для этого выбираем необходимую рекомендацию и нажимаем на значение поля «ID» (выделено синим, полужирным). Информация по рекомендации хранится в текстовом yaml формате (5.19).

Select control to change

ADD CONTROL +

Action: 0 of 53 selected

<input type="checkbox"/>	ID	NAME	BENCHMARK	COMMENT
<input type="checkbox"/>	153	Ensure 'Improve Proofing Tools' is set to Disabled	CIS Microsoft Office 2016 Benchmark	-
<input type="checkbox"/>	152	Ensure 'Open Office Documents as Read/Write While Browsing' is set to Disabled	CIS Microsoft Office 2016 Benchmark	-
<input type="checkbox"/>	151	Ensure 'Allow PNG As an Output Format' is set to Disabled	CIS Microsoft Office 2016 Benchmark	-
<input type="checkbox"/>	150	Ensure 'Online Content Options' is set to Enabled (Allow Office to connect to the internet)	CIS Microsoft Office 2016 Benchmark	-
<input type="checkbox"/>	149	Ensure 'Disable Smart Document's Use of Manifests' is set to Enabled	CIS Microsoft Office 2016 Benchmark	-
<input type="checkbox"/>	148	Ensure 'Legacy Format Signatures' is set to Disabled	CIS Microsoft Office 2016 Benchmark	-
<input type="checkbox"/>	147	Ensure 'Suppress External Signature Service' is set to Enabled	CIS Microsoft Office 2016 Benchmark	-

Рисунок 5.18 – Страница рекомендаций стандарта

Title: Ensure 'Information Bar' is set to Enabled

Description: >-

This policy setting allows you to manage whether the Information Bar is displayed for Internet Explorer processes when file or code installs are restricted. By default, the Information Bar is displayed for Internet Explorer processes. The recommended state for this setting is: Enabled. (Check: groove.exe, excel.exe, mspub.exe, powerpnt.exe, pptview.exe, visio.exe, winproj.exe, outlook.exe, spDesign.exe, exprwd.exe, msaccess.exe, onent.exe, mse7.exe)

Rationale: >-

The information bar can help users to understand when potentially malicious content has been blocked, on the other hand, some users may be confused by the appearance of the bar or unsure how to respond.

Audit: >-

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_securityband\ "Office Application.exe"

Remediation: >-

To implement the recommended configuration state, set the following Group Policy setting to Enabled.

Computer Configuration\Administrative Templates\Microsoft Office 2016 (Machine)\Security Settings\IE Security\Information Bar

Рисунок 5.19 – Информация по рекомендациям в yaml формате

					БИС.502900.007 ПЗ	Лист
Изм	Лист	№ докум.	Подпись	Дата		44

Программные файлы проверок стандарта хранятся по относительному пути «scripts\cis_microsoft_office_2016». В случае, если необходимо переместить их в другое место, нужно дополнительно указать путь в панели администратора в соответствующей модели (рис. 5.20).

Home › Benchmarks › Benchmarks › CIS Microsoft Office 2016 Benchmark

Change benchmark HISTORY

Name: CIS Microsoft Office 2016 Benchmark

Work status: active ▼

Original doc: Обзор... Файл не выбран.

Comment: v1.1.0-11-30-2016

Scripts folder: scripts\cis_microsoft_office_2016

Delete
Save and add another
Save and continue editing
SAVE

Рисунок 5.20 – Вкладка редактирования описания стандарта безопасности

В панели администратора можно изменять конфигурации пользователей и восстанавливать, в случае если пользователи их случайно удалили.

Все конфигурации расположены во вкладке «Configurations». Для редактирования конфигурации нужно нажать на имя соответствующей конфигурации. После нажатия откроется соответствующее окно (рис. 5.21).

В случае сбоев и возникновения проблемных ситуаций со сканированиями, можно принять соответствующие меры через панель администратора:

- освободить очередь;
- удалить объект сканирования;
- выставить определенный статус сканирования.

Change configuration




User:	admin  
Name:	Scan Virtual Machines
Benchmarks:	<div>CIS Microsoft Office 2016 Benchmark </div> <div>Hold down "Control", or "Command" on a Mac, to select more than one.</div>
Hosts text:	192.168.1.101 192.168.1.102 192.168.1.103
Wmi login:	Администратор

Рисунок 5.21 – Вкладка редактирования конфигураций

5.6 Тестирование приложения

5.6.1 Ручное тестирование проверки стандарта с использованием виртуальных машин

Для тестов с использованием виртуальных машин больше подходит ручное тестирование, так как оно заключается в настройке и запуске виртуальных машин с определенным количеством активных пользователей.

Для ручного тестирования был подготовлен набор тестов (табл. 5.5).

Таблица 5.5 – Набор ручных тестов

Цель теста	Условие теста	Особенности
Проверка сканирования машины, настроенной в соответствии со стандартом	Все проверки завершились со статусом "Compliant"	ВМ "All Good Staand"; 1 активный пользователь
Проверка сканирования машины, настроенной не в соответствии со стандартом	Все проверки завершились со статусом "Not Compliant"	ВМ "All Bad Stand"; 1 активный пользователь

Продолжение таблицы 5.5

Цель теста	Условие теста	Особенности
Проверка сканирования ненастроенной машины,	Проверки 119, 123, 135, 138, 141, 144 завершились со статусом "Compliant", остальные - "Not compliant"	BM "Not configured Stand"; 1 активный пользователь
Проверка сканирования машины без активных пользователей	Проверки 117-153 завершились со статусом "Not applicable", остальные - "Compliant"	BM "All Good Stand"; без активных пользователей
Проверка сканирования машины с несколькими активными пользователями	В таблицах результатов проверок (117-153) должны быть настройки обоих пользователей	BM "All Bad Stand"; 2 активных пользователя
Проверка сканирования нескольких машин	Должны провериться все машины	BM "All Good Stand", "All Bad Stand", "Not configured Stand"; 1 активный пользователь
Проверка очередности выполнения сканирований	Сканирования должны дожидаться своей очереди	BM "All Good Stand", "All Bad Stand", "Not configured Stand"; В настройках выставить максимальное количество одновременных сканирований – 2

В результате ручного тестирования, ошибки в проверках стандарта обнаружены не были и все тесты прошли успешно, что говорит о корректной проверке стандарта безопасности.

5.6.2 Автоматизированное тестирование модулей приложения

Тестирование модулей приложения было решено автоматизировать с помощью встроенного в Django инструмента тестирования [20]. Программные коды тестирования модуля располагаются в файлах `tests.py` в соответствующих модулях.

Тесты модуля `core` содержат проверки:

- доступности страницы авторизации;
- авторизации с корректными данными;
- отказа авторизации при вводе некорректных данных;
- отсутствие доступа к страницам у неавторизованных пользователей;
- наличия доступа к страницам у авторизованных пользователей.

Тесты модуля `tasks` содержат проверки:

- отображения таблицы конфигураций;
- отказа в добавлении конфигурации с некорректными наборами данных;
- добавления конфигурации с корректными данными;
- удаления своей конфигурации;
- отказа в доступе к конфигурации другого пользователя.

Тесты модуля `gun` содержат проверки:

- отказа в запуске сканирования, если пользователем были переданы некорректные данные;
- отказа в запуске сканирования с конфигурацией другого пользователя;
- отказа в запуске сканирования неавторизованным пользователем.

Тесты запускаются командой «`python manage.py test`» [21]. Для тестирования приложения используется тестовая база данных. Чтобы в

тестовой базе данных были необходимые данные, Django берет из соответствующих json файлов.

По результату автоматизированного тестирования (рис. 5.22) видим, что приложение прошло все тесты с положительным результатом «ок».

```
test_access_pages_with_auth (core.tests.CheckAccessPages) ... ok
test_access_pages_wo_auth (core.tests.CheckAccessPages) ... ok
test_access_signin_page (core.tests.CheckAccessPages) ... ok
test_bad_login_testuser (core.tests.CheckAccessPages) ... ok
test_good_login_testuser (core.tests.CheckAccessPages) ... ok
test_empty_parametr (run.tests.CheckRunScanningPage) ... ok
test_nonexistent_conf (run.tests.CheckRunScanningPage) ... ok
test_scan_with_foreign_conf (run.tests.CheckRunScanningPage) ... ok
test_start_scanning_by_anonim (run.tests.CheckRunScanningPage) ... ok
test_configuration_table (tasks.tests.CheckConfigurations) ... ok
test_delete_configuration_by_anonim (tasks.tests.CheckConfigurations) ... ok
test_delete_foreign_configuration (tasks.tests.CheckConfigurations) ... ok
test_delete_my_configuration (tasks.tests.CheckConfigurations) ... ok
test_empty_benchmark (tasks.tests.CheckConfigurations) ... ok
test_empty_parametr (tasks.tests.CheckConfigurations) ... ok
test_nonexistent_benchmark (tasks.tests.CheckConfigurations) ... ok
test_normal_adding_configuration (tasks.tests.CheckConfigurations) ... ok
test_not_equal_passwords (tasks.tests.CheckConfigurations) ... ok
```

```
-----
Ran 18 tests in 3.644s
```

OK

Рисунок 5.22 – Результаты автоматизированного тестирования

6 Технико-экономическое обоснование работы

6.1 Обоснование целесообразности работы

Проверка удаленной машины на безопасность офисных пакетов Microsoft Office 2016 с помощью стандарта CIS Microsoft Office может занять от 10 до 20 минут рабочего времени. Также, при монотонной проверке нескольких удаленных машин аудитором могут быть допущены ошибки, что приведет к некорректной оценке защищенности.

Приложение позволит проверять машину за 40-60 секунд. Приложению не характерна утомляемость и невнимательность, что позволит корректно оценивать защищенность проверяемых машин, тратя на это меньшее количество времени.

6.2 Организация и планирование работ

В работе участвовали:

- исполнитель (И), студент;
- руководитель (Р).

Исходя из поставленных задач были сформулированы следующие этапы работ:

- 1) составление и согласование технического задания;
- 2) обзор стандарта безопасности;
- 3) выбор технологий и средств разработки;
- 4) настройка виртуальных машин для тестирования приложения;
- 5) проектирование приложения;
- 6) написание программного кода;

					БИС.502900.007 ПЗ		
Изм.	Лист	№ докум	Подпись	Дата			
Разраб.		Койшинов Т.С.			Приложение для анализа защищенности офисных пакетов на примере Microsoft Office		
Провер.		Глухарева С.В.					
Реценз.		Мироненко Д.А.					
Н. Контр.		Якимук А.Ю.					
Утверд.		Костюченко Е.Ю.					
					Лит.	Лист	Листов
						50	8
					ТУСУР, ФБ, каф. БИС, ар. 743		

- 7) тестирование приложения;
- 8) написание пояснительной записки и защита работы.

На выполнение работы было отведено:

- для исполнителя – 22 рабочих дня (каждый день рассчитывался с учетом 8-часового рабочего дня);
- для руководителя – 24 часа для руководства и консультирования.

По выполненным задачам составлена таблица (6.1), показывающая затраты времени для выполнения работ участниками. По составленной таблице была построена диаграмма Ганта (рисунок А.1).

Таблица 6.1 – Перечень работ и оценка их трудоемкости

Этап работы	Участник	Трудоемкость	
		Нормо-часы, н-ч	Процент от общей трудоемкости
Составление и согласование технического задания	Р	3	13%
	И	8	5%
Обзор стандарта безопасности	Р	1	4%
	И	24	14%
Выбор технологий и средств разработки	Р	1	4%
	И	8	5%
Настройка виртуальных машин для тестирования приложения	Р	2	8%
	И	6	3%
Проектирование приложения	Р	3	13%
	И	20	11%
Написание программного кода	Р	8	33%
	И	50	28%
Тестирование приложения	Р	2	8%
	И	20	11%
Написание пояснительной записки и защита работы	Р	4	17%
	И	40	23%
Итого	Р	24	100%
	И	176	100%

6.3 Смета затрат

6.3.1 Затраты на оборудование

В качестве оборудования во время работы использовались:

- персональный компьютер Lenovo Thinkpad T430;
- монитор Asus;
- внешний жесткий диск Toshiba;
- компьютерная мышь.

Стоимость оборудования представлена в таблице 6.2.

Таблица 6.2 – Стоимость оборудования

Оборудование	Стоимость, руб.	Количество	Цена, руб.
Персональный компьютер	18990,00	1	18990
Монитор	6800,00	1	6800
Жесткий диск	2999,00	1	2999
Компьютерная мышь	350,00	1	350
Итого			29139

«Т.к. амортизируемым имуществом признается имущество со сроком полезного использования более 12 месяцев и первоначальной стоимостью более 100 000 рублей» [22], то амортизация не начисляется.

В итоге на оборудование было потрачено 29139 руб.

6.3.2 Расходы на оплату труда и страховые взносы

Для расчета расходов на оплату труда нужно рассчитать фонд оплаты труда (ФОТ) по формуле (6.1):

$$\text{ФОТ} = O_{\text{зп}} + D_{\text{зп}}, \quad (6.1)$$

где $O_{\text{зп}}$ – основная заработная плата, руб.

$D_{\text{зп}}$ – дополнительная заработная плата, руб.

Основная заработная плата рассчитывается по формуле (6.2):

$$O_{\text{зп}} = 3\Pi_{\text{пр}} + \text{Премия} + \text{РК}, \quad (6.2)$$

где $3\Pi_{\text{пр}}$ – прямая заработная плата, руб.

РК – районный коэффициент.

Для Томской области районный коэффициент составляет 30%, т.е. РК считаем по формуле (6.3):

$$\text{РК} = 0,3 * 3\Pi_{\text{пр}} \quad (6.3)$$

Студенты, не имеющие высшего образования, могут быть приняты на должность техника, поэтому $3\Pi_{\text{пр}}$ для исполнителя будет составлять 13800 руб./мес. (приказ ректора ТУСУР № 830 от 12.11.2018 [23]). Т.к. руководитель является доцентом, то его заработная плата будет составлять 300 руб/ч (приказ ректора ТУСУР № 323 от 28.05.2018 [23]).

Т.к. премия и дополнительная заработная плата не начислялась, то формула (6.4) примет вид:

$$\Phi OT = O_{\text{зп}} = 1,3 * 3\Pi_{\text{пр}} \quad (6.4)$$

Фонд оплаты труда для руководителя составила 9360 руб (6.5), а для исполнителя – 13979,40 руб (6.6).

$$\Phi OT_p = O_{\text{зп}(p)} = 1,3 * 7200 = 9360 \text{ (руб.)} \quad (6.5)$$

$$\Phi OT_{\text{и}} = O_{\text{зп}(\text{и})} = 1,3 * 13800 = 17940 \text{ (руб.)} \quad (6.6)$$

Согласно статье 425 НК РФ [24] страховые взносы будут состоять из:

- обязательного пенсионного страхования (22%);
- обязательного социального страхования (2,9%);
- обязательного медицинского страхования (5,1%).

Согласно Федеральному закону № 179 от 25.12.2005 также взимаются страховые тарифы на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний [25]. Для деятельности «Разработка компьютерного программного обеспечения» страховой тариф равен 0,2% [26].

Всего страховые взносы составляют 30,2 % от фонда оплаты труда.

Расходы на оплату труда и страховых взносов были подсчитаны и представлены в таблице 6.3.

Таблица 6.3 – Расходы на оплату труда

Участник	ЗПрр, руб.	РК, руб.	Озн, руб.	ФОТ, руб.	Страховые взносы, руб.	Всего
Руководитель	7200,00	2160,00	9360,00	9360,00	2826,72	12186,72
Исполнитель	13800,00	4140,00	17940,00	17940,00	5417,88	23357,88
Итого						35544,60

Всего расходы на оплату труда и страховые взносы для руководителя составляют 12186,72 руб, а для исполнителя – 23357,88 руб.

6.3.3 Затраты на основные и вспомогательные материалы

Основные и вспомогательные материалы:

- диск CD-R SmartTrack;
- конверт для диска.

Затраты на основные и вспомогательные материалы отображены в таблице 6.4.

Таблица 6.4 - Затраты на основные и вспомогательные материалы

Материал	Стоимость	Количество	Цена
CD-R диск	18	1	18
Конверт для диска	5	1	5
Итого			23

Всего затраты на материалы составляют 23 руб.

6.3.4 Затраты на электроэнергию

Затраты на электроэнергию рассчитываются по формуле 6.7:

$$C_{\text{эл}} = W_y * T_g * S_{\text{эл}} \quad (6.7)$$

где W_y – установленная мощность (кВт);

T_g – время работы оборудования (час);

$S_{эл}$ – тариф на электроэнергию (руб./кВт).

«В соответствии с приказом № 6-713 «О тарифах на электрическую энергию для населения и потребителей, приравненных к категории население, на территории Томской области на 2019 год» тариф для населения, проживающего в городских населенных пунктах в домах, оборудованных в установленном порядке стационарными электроплитами и (или) электроотопительными установками, и приравненные к ним, составляет 2,39 руб/кВтч» [27].

Затраты для электроэнергии на персональном компьютере составили 111.05 руб. (6.8), а для лампы накаливания – 75.72 (6.9).

$$C_{эл(пк)} = 0,264 * 176 * 2,39 = 111,05 \text{ (руб.)} \quad (6.8)$$

$$C_{эл(лампа)} = 0,18 * 176 * 2,39 = 75,72 \text{ (руб.)} \quad (6.9)$$

Данные по затратам на электроэнергию представлены в таблице 6.5.

Таблица 6.5 – Затраты на электроэнергию

Оборудование	Мощность, кВт	Время работы, час	Тариф, руб/кВт	Сумма, руб
Персональный компьютер	0,264	176	2,39	111,05
Лампа накаливания	0,18	176	2,39	75,72
Итого				186,76

Всего на электроэнергию было потрачено 187 руб.

6.3.5 Накладные расходы

В накладные расходы входят:

- пользование интернетом;
- печать пояснительной записки;
- брошюрование.

В качестве интернет-провайдера был выбран Теле2, а в качестве тарифа – «Мой онлайн+ 11_2018» [28].

Данные по накладным расходам представлены в таблице 6.6.

Таблица 6.6 – Накладные расходы

Услуга	Стоимость	Количество	Цена
Интернет	175	1	175
Печать пояснительной записки	237,1	1	237,1
Брошюрование с учетом расходных материалов	50	1	50
Итого			462,1

Накладные расходы составили 462 руб.

6.3.6 Сводная смета затрат

На основе произведенных расчетов была составлена сводная смета затрат (таблица 6.7).

Таблица 6.7 – Сводная смета затрат

Затраты	Сумма затрат
Оборудование	29139,00
Оплата труда и страховые взносы	35544,60
Основные и вспомогательные материалы	23,00
Электроэнергия	186,76
Накладные расходы	462,10
Итого	65355,46

На основе составленной сводной сметы затрат была построена круговая диаграмма (рис. 6.1). На диаграмме видно процентное соотношение затрат для каждой из статей расходов.

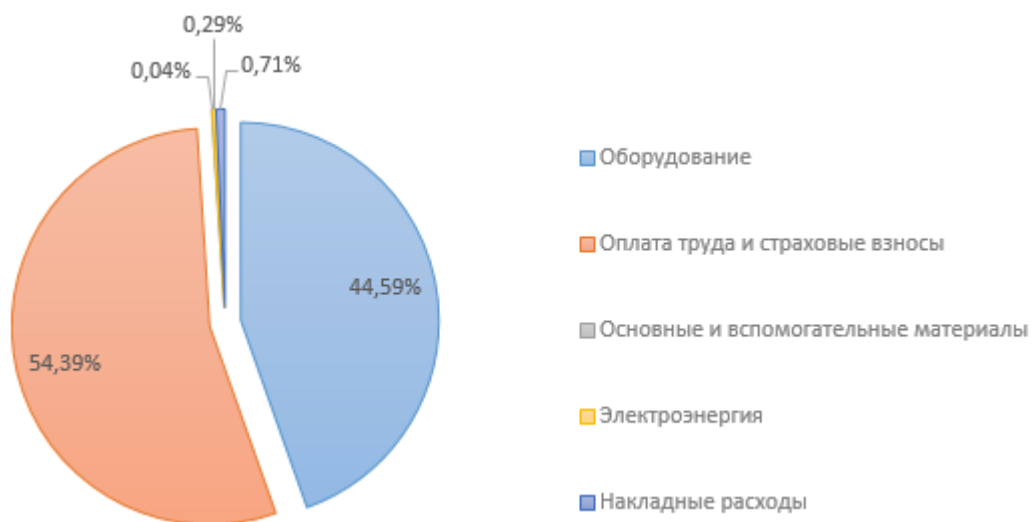


Рисунок 6.1 – Диаграмма затрат

Оплата труда и страховые взносы является самой большой статьёй расходов (54%). Второй по величине статьёй расходов является затраты на оборудование. Остальные статьи расходов не превышают 1% от общего количества затрат.

6.4 Анализ затрат на выполнение работы

В результате технико-экономического обоснования работы была обоснована целесообразность работы, были описаны участники и этапы. Была составлена смета затрат, в которой видно, что основные статьи расхода – это оборудование и оплата труда (29139 руб. и 35545 руб. соответственно).

При постоянной плановой проверке на защищенность Microsoft Office большого количества целевых машин, все затраты (61592 руб.) окупятся, т.к. приложение заменяет ручной дорогой труд на автоматизированную работу компьютера.

7 Охрана труда и безопасность жизнедеятельности

7.1 Общие положения

В статье 209 Трудового кодекса Российской Федерации охрана труда определена, как «система сохранения жизни и здоровья работников в процессе трудовой деятельности, включающая в себя правовые, социально-экономические, организационно-технические, санитарно-гигиенические, лечебно-профилактические, реабилитационные и иные мероприятия» [29]. Данная система мер имеет значительный охват как факторов воздействия на работников, так и мероприятий, для обеспечения безопасных условий труда. Данный раздел в своей основе затрагивает вопросы охраны труда и безопасности жизнедеятельности исполнителя на стадии разработки и отладки продукта, производимых с применением персонального компьютера. Вопросы, поднимаемые в разделе, будут актуальны также и в процессе использования результатов данной работы.

7.2 Эргономика рабочего помещения и рабочего места

Помещение, в котором проходила работа, представляет из себя комнату с площадью 20 м². Рабочее место освещает пластиковое трехстворчатое окно и лампа, расположенная посередине комнаты.

Рабочее место состоит из письменного стола, офисного кресла и компьютерной техники. Рядом со столом расположен сетевой фильтр.

Нормативный акт, регламентирующий порядок исполнения работ на персональных ЭВМ является документ «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы.

					БИС.502900.007 ПЗ		
Изм.	Лист	№ докум	Подпись	Дата			
Разраб.		Койшинов Т.С.			Приложение для анализа защищенности офисных пакетов на примере Microsoft Office		
Провер.		Давыдова Е.М.					
Реценз.		Мироненко Д.А.					
Н. Контр.		Якимук А.Ю.					
Утверд.		Костюченко Е.Ю.					
					Лит.	Лист	Листов
						58	8
					ТУСУР, ФБ, каф. БИС, ар. 743		

Санитарно-эпидемиологические правила и нормативы СанПиН 2.2.2/2.4.1340-03» [30]. Из документа взяты следующие актуальные пункты:

- освещение;
- микроклимат;
- уровень шума;
- воздействие электромагнитных полей;
- визуальные параметры видеодисплейных терминалов.

7.2.1 Освещение

Согласно Нормам и правилам СНиП 23-05-95 «Естественное и искусственное освещение» [31], освещенность рабочего места должна варьироваться в пределах от 300 до 500 люкс. Расчет освещенности производится согласно формуле (7.1):

$$E = \frac{I}{r^2} * \cos \varphi, \quad (7.1)$$

где I – сила света, кд;

r – расстояние до источника света, м;

φ – угол падения лучей света относительно нормали к поверхности.

Сила света рассчитывается по формуле (7.2):

$$I = \frac{\Phi}{4\pi}, \quad (7.2)$$

где Φ – световой поток, лм.

Рабочее место освещено лампой накаливания 150Вт. Световой поток для нее составляет 1800 лм [32].

Расчет силы света по формуле (7.3) дал следующее значение:

$$I = \frac{1800}{4\pi} = 143,24 \text{ кд} \quad (7.3)$$

Расстояние от источника света 0,6 м, угол падения лучей – 30°. Расчет формулой (7.4) дает следующий результат:

					БИС.502900.007 ПЗ	Лист
Изм	Лист	№ докум.	Подпись	Дата		59

$$E = \frac{143,24}{0,6^2} * \cos 30^\circ = 344,59 \text{ лк} \quad (7.4)$$

Данное значение освещенности рабочего места лежит в допустимых границах.

7.2.2 Микроклимат

Микроклимат рабочего помещения включает в себя следующие факторы воздействия на человека: температура воздуха, относительная влажность и скорость движения воздуха. При нарушении оптимальных показателей в помещении негативно сказывается на самочувствии человека и как результат ухудшает его работоспособность.

СанПиН 2.2.4.548-96 «Гигиенические требования к микроклимату производственных помещений» [33] устанавливает следующие оптимальные величины показателей микроклимата на рабочих местах для теплого и холодного периода года (таблица 7.1):

Таблица 7.1 – Оптимальные величины показателей микроклимата

Период года	Категория работ по уровню энергозатрат, Вт	Т. воздуха, °С	Т. поверхностей, °С	Отн. влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Ia (до 139)	22-24	21-25	60-40	0,1
	Iб (140-174)	21-23	20-24	60-40	0,1
	IIa (175-232)	19-21	18-22	60-40	0,2
	IIб (233-290)	17-19	16-20	60-40	0,2
	III (более 290)	16-18	15-19	60-40	0,3
Теплый	Ia (до 139)	23-25	22-26	60-40	0,1
	Iб (140-174)	22-24	21-25	60-40	0,1
	IIa (175-232)	20-22	19-23	60-40	0,2
	IIб (233-290)	19-21	18-22	60-40	0,2
	III (более 290)	18-20	17-21	60-40	0,3

Были взяты допустимые нормы для холодного периода года с незначительным физическим напряжением (Ia). В результате проведенных измерений данных микроклимата была составлена сравнительная таблица 7.2:

Таблица 7.2 – Сравнительная таблица

	Т. воздуха, °С	Отн. влажность воздуха, %	Скорость движения воздуха, м/с
Нормы для категории Ia	22-24	60-40	< 0,1
Показатели	22	47	< 0,1

Проведенное сравнение показателей температуры воздуха и относительной влажности воздуха в рабочем помещении подтвердило безопасность проводимых работ.

7.2.3 Уровень шума

«Экология» звука имеет одно из важных значений для благоприятной рабочей деятельности. Так превышение норм уровня звукового шума имеет неблагоприятные физические (ухудшение слуха) и психические (раздражительность) последствия. Предельно допустимые уровни шума определены санитарными нормами СН 2.2.4/2.1.8.562-96 «Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки» [34].

Для вида трудовой деятельности «программирование» и рабочего места «программистов вычислительных машин» предельно допустимые уровни звукового давления, уровни звука и эквивалентные уровни звука в данном документе определены в следующих значениях (таблицы 7.3-7.4):

Таблица 7.4 - Уровни звука и эквивалентные уровни звука

Вид деятельности	Уровни звука и эквивалентные уровни звука (в дБА)
Программирование	50

Таблица 7.3 - Предельно допустимые уровни звукового давления

Вид деятельности	Уровни звукового давления, дБ, в октавных полосах со среднегеометрическими частотами, Гц						
	31.5	63	125	250	500	1000	2000
Программирование	86	71	61	54	49	45	40

Источником шума в рабочем помещении является персональный компьютер Lenovo Thinkpad t430, а именно кулер системы вентиляции. Измерение величины уровня шума показало 26,0 дБ (рисунок 7.1), что более чем удовлетворяет требованиям.



Рисунок 7.1 – Измерение уровня шума

7.2.4 Воздействие электромагнитных полей

В помещении при выполнении работы фактором электромагнитных полей (ЭМП) за исключением низковольтного адаптера питания для мобильного телефона и самого телефона рассматривается персональный компьютер – ноутбук фирмы Lenovo Thinkpad t430. Прочие, кроме

компьютера, бытовые устройства и устройства связи либо отсутствуют, либо находятся в отключенном состоянии, поэтому определенной статистики в рассматриваемом вопросе оказать не могут.

Персональный компьютер рассматривается, как источник широкого спектра ЭМП различной интенсивности, в том числе:

- переменные низкочастотные ЭМП;
- электромагнитное излучение низкого (от 5 Гц до 2 кГц) радиочастотного диапазона;
- электромагнитное излучение высокого (от 2 кГц до 400 кГц) радиочастотного диапазона;
- электростатическое поле.

Согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» [30] временные допустимые уровни электромагнитного поля, создаваемых персональным компьютером, представлены в таблице (7.5):

Таблица 7.5 - Гигиенические требования к персональным ЭВМ

Наименование параметров		Временной допустимый уровень (ДПУ)
Напряженность электростатического поля	в диапазоне частот 5 Гц - 2 кГц	25 В/м
	в диапазоне частот 2 кГц - 400 кГц	2,5 В/м
Плотность магнитного потока	в диапазоне частот 5 Гц - 2 кГц	250 нТл
	в диапазоне частот 2 кГц - 400 кГц	25 нТл
Напряженность электростатического поля		15 В/м

Низкочастотные поля в частотном диапазоне до 2 кГц, могут создаваться блоками сетевого питания в трансформаторном исполнении. Высокочастотные поля в частотном диапазоне 2 – 400 кГц, создаются импульсными блоками питания.

В качестве источника электростатического поля обычно рассматриваются экраны мониторов с электронно-лучевой трубкой (ЭЛТ),

несущей высокий электростатический потенциал (ускоряющее напряжение ЭЛТ). Первичным решением этой проблемы было оборудование мониторов, произведенных после 1998 г., эффективной системой защиты от электростатического поля. После отказа от мониторов с ЭЛТ и особенно массовым использованием портативных ПЭВМ («ноутбуков») параметр электростатического напряжения уменьшился на порядки.

Также общий тренд в уменьшении мощности потребления отдельных элементов (экран, материнская плата, процессор, узлы связи) портативных ПЭВМ позволил значительно уменьшить так же и мощность импульсных блоков питания и тем самым снизить степень высокочастотного электромагнитного излучения.

7.2.5 Визуальные параметры видеодисплейных терминалов

Визуальные параметры регламентируются пунктами СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» [30] и отображены в таблице 7.6.

Таблица 7.6 – Гигиенические требования к персональным ЭВМ

Параметры	Допустимые значения
Яркость белого поля	Не менее 35 кд/кв. м
Неравномерность яркости рабочего поля	Не более +/- 20%
Контрастность (для монохромного режима)	Не менее 3:1
Временная нестабильность изображения (мелькания)	Не должна фиксироваться
Пространственная нестабильность изображения (дрожание)	Не более $2 \times 10(-4L)$, где L - проектное расстояние наблюдения, мм

Все визуальные параметры удовлетворяют требованиям.

7.3 Общие требования по электробезопасности и пожаробезопасности

ГОСТ 12.1.019-2017 «Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты» регламентирует требования к электробезопасности [35]. Основным поражающим фактором является электрический ток, протекающий через человека. Установлены пороговые значения тока, определяющие степень поражения:

- пороговый ощутимый ток: 0.5-1.5 мА;
- пороговый не отпускающий ток: 10-20 мА;
- пороговый фибрилляционный ток: 50-80 мА;
- смертельно опасный ток: 100мА и более.

Правила пожарной безопасности регулируются государственным стандартом ГОСТ Р 12.0.001-2013 [36].

Опасными факторами, воздействующими на людей и материальные ценности, являются:

- пламя и искры;
- повышенная температура окружающей среды;
- токсичные продукты горения и термического разложения;
- дым;
- пониженная концентрация кислорода.

8 Заключение

Для анализа защищенности был выбран стандарт безопасности CIS Microsoft Office 2016 и описана структура этого стандарта. На основе рекомендаций стандарта по настройке групповых политик и проверке настроек через системный реестр Windows была составлена таблица соответствий, которая использовалась для составления конфигурационного файла проверок стандарта.

Для разработки приложения были выбраны:

- система контроля версий;
- язык программирования и веб-фреймворк;
- интегрированная среда разработки;
- средства виртуализации.

Для тестирования приложения были созданы и настроены три виртуальные машины, которые содержат в себе определенные настройки групповых политик.

Была спроектирована инфологическая модель данных и структура приложения.

Для проверки соответствия настроек групповых политик были разработаны скрипты проверки, которые запускаются приложением и на основе результата проверок оценивается защищенность Microsoft Office.

Был описан пользовательский интерфейс, проведено ручное и автоматизированное тестирование приложения.

Задачи были выполнены, цель достигнута.

Список использованных источников

- 1 KLA11396Multiple vulnerabilities in Microsoft Office [Электронный ресурс]. – Режим доступа: <https://vulners.com/kaspersky/KLA11396> (дата обращения: 15.01.19)
- 2 CIS. About us [Электронный ресурс]. – Режим доступа: <https://www.cisecurity.org/about-us/> (дата обращения: 15.01.19)
- 3 CIS Benchmarks [Электронный ресурс]. – Режим доступа: <https://www.cisecurity.org/cis-benchmarks/> (дата обращения: 15.01.19)
- 4 CIS Microsoft Office Benchmarks [Электронный ресурс]. – Режим доступа: https://www.cisecurity.org/benchmark/microsoft_office/ (дата обращения: 15.01.19)
- 5 CIS Benchmark Landing Page [Электронный ресурс]. – Режим доступа: <https://learn.cisecurity.org/benchmarks> (дата обращения: 15.01.19)
- 6 Что такое системный реестр Windows [Электронный ресурс]. – Режим доступа: <https://alpinefile.ru/windows-registry.html> (дата обращения: 15.01.19)
- 7 Администрирование с помощью WMI [Электронный ресурс]. – Режим доступа: <http://www.sysengineering.ru/administration/administration-usingwmi/> (дата обращения 15.01.19)
- 8 Ветки реестра Windows [Электронный ресурс]. – Режим доступа: <http://vindavoz.ru/poleznoe/251-chto-takoe-reestr.html> (дата обращения 15.01.19)
- 9 SID (Security Identifier) [Электронный ресурс]. – Режим доступа: [https://ru.bmstu.wiki/SID_\(Security_Identifier\)](https://ru.bmstu.wiki/SID_(Security_Identifier)) (дата обращения 15.01.19)
- 10 Getting Started - About Version Control [Электронный ресурс]. – Режим доступа: <https://git-scm.com/book/en/v2/Getting-Started-About-Version-Control> (дата обращения 15.01.19)
- 11 Getting Started - A Short History of Git [Электронный ресурс]. – Режим доступа: <https://git-scm.com/book/en/v2/Getting-Started-A-Short-History-of-Git> (дата обращения 15.01.19)

12 Язык программирования Python [Электронный ресурс]. – Режим доступа: <https://web-creator.ru/articles/python> (дата обращения 15.01.19)

13 Методика MTV (или MVC) [Электронный ресурс]. – Режим доступа: <https://djbook.ru/ch05s02.html> (дата обращения 15.01.19)

14 Лучшие IDE и редакторы кода для Python [Электронный ресурс]. – Режим доступа: <https://tproger.ru/translations/python-ide/> (дата обращения 15.01.19)

15 Welcome to VirtualBox.org! [Электронный ресурс]. – Режим доступа: <https://www.virtualbox.org/> (дата обращения 15.01.19)

16 Системные требования для ОС Windows 7 [Электронный ресурс]. – Режим доступа: <https://support.microsoft.com/ru-ru/help/10737/windows-7-system-requirements> (дата обращения 15.01.19)

17 Настройка сетевого моста в VirtualBox [Электронный ресурс]. – Режим доступа: <http://it-mate.ru/stati/oracle-vm-virtualbox/6-nastrojka-setevogo-mosta-v-virtualbox.html> (дата обращения 15.01.19)

18 Setting up a Remote WMI Connection [Электронный ресурс]. – Режим доступа: <https://docs.microsoft.com/en-us/windows/desktop/wmisdk/connecting-to-wmi-remotely-starting-with-vista> (дата обращения 15.01.19)

19 Administrative Template files (ADMX/ADML) and Office Customization Tool for Office 365 ProPlus, Office 2019, and Office 2016 [Электронный ресурс]. – Режим доступа: <https://www.microsoft.com/en-us/download/details.aspx?id=49030> (дата обращения 15.01.19)

20 Testing in Django [Электронный ресурс]. – Режим доступа: <https://docs.djangoproject.com/en/2.1/topics/testing/> (дата обращения 15.01.19)

21 Writing and running tests [Электронный ресурс]. – Режим доступа: <https://docs.djangoproject.com/en/2.1/topics/testing/overview/> (дата обращения 15.01.19)

22 НК РФ Статья 256. Амортизируемое имущество [Электронный ресурс]. – Режим доступа:

					БИС.502900.007 ПЗ	Лист
Изм	Лист	№ докум.	Подпись	Дата		68

http://www.consultant.ru/document/cons_doc_LAW_28165/df53ee1751d3e93dbf8c0d34076675da18a2fd06/ (дата обращения: 21.01.19)

23 Нормативные документы ТУСУР [Электронный ресурс]. – Режим доступа: <https://regulations.tusur.ru/> (дата обращения: 22.01.19)

24 НК РФ Статья 425. Тарифы страховых взносов [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28165/a3f603ffd57b1431ed51e1693ba710093347235d/ (дата обращения: 21.01.19)

25 Федеральный закон от 22.12.2005 N 179-ФЗ (с изм. от 25.12.2018) «О страховых тарифах на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний на 2006 год» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_57243/3d0cac60971a511280cbba229d9b6329c07731f7/ (дата обращения: 22.01.2019)

26 Приказ Минтруда России от 30.12.2016 N 851н «Об утверждении Классификации видов экономической деятельности по классам профессионального риска» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_211247/be36cee5708544a08141c875687f98b2247feda5/ (дата обращения: 22.01.2019)

27 Приказ № 6-702 от 27.12.2018 «О тарифах на электрическую энергию для населения и потребителей, приравненных к категории население, на территории Томской области на 2019 год» [Электронный ресурс]. – Режим доступа: https://www.ensb.tomsk.ru/upload/Prikaz_DTR_27.12.2018_%E2%84%96_6-702_tarif_naselenie_na_2019.pdf (дата обращения: 21.01.19)

28 Тариф «Мой онлайн» [Электронный ресурс]. – Режим доступа: <https://tomsk.tele2.ru/tariff/my-online> (дата обращения: 21.01.2019)

29 ТК РФ Статья 209. Основные понятия [Электронный ресурс]. – Режим доступа:

					БИС.502900.007 ПЗ	Лист
Изм	Лист	№ докум.	Подпись	Дата		69

http://www.consultant.ru/document/cons_doc_LAW_34683/78f36e7afa535cf23e1e865a0f38cd3d230eecf0/ (дата обращения: 20.01.19)

30 О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03 [Электронный ресурс]. – Режим доступа: <http://base.garant.ru/4179328/> (дата обращения: 20.01.19)

31 Строительные нормы и правила СНиП 23-05-95 «Естественное и искусственное освещение» [Электронный ресурс]. – Режим доступа: <http://base.garant.ru/2306278/> (дата обращения: 20.01.19)

32 Световой поток типичных источников света и световая отдача [Электронный ресурс]. – Режим доступа: <http://tehtab.ru/guide/guidephysics/lightandcolor/lightflowefficiency/> (дата обращения: 20.01.2019)

33 Санитарные правила и нормы СанПиН 2.2.4.548-96 «Гигиенические требования к микроклимату производственных помещений» [Электронный ресурс]. – Режим доступа: <http://base.garant.ru/4173106/> (дата обращения: 20.01.2019)

34 Санитарные нормы СН 2.2.4/2.1.8.562-96 «Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки» [Электронный ресурс]. – Режим доступа: <http://base.garant.ru/4174553/> (дата обращения: 20.01.2019)

35 ГОСТ Р 12.1.019-2017 «Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты» [Электронный ресурс]. – Режим доступа: <http://base.garant.ru/55171892/> (дата обращения: 20.01.2019)

36 ГОСТ Р 12.0.001-2013 Система стандартов безопасности труда [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/1200105195> (дата обращения: 20.01.2019)

					БИС.502900.007 ПЗ	Лист
						70
Изм	Лист	№ докум.	Подпись	Дата		

Приложение А
(справочное)
Диаграмма Ганта

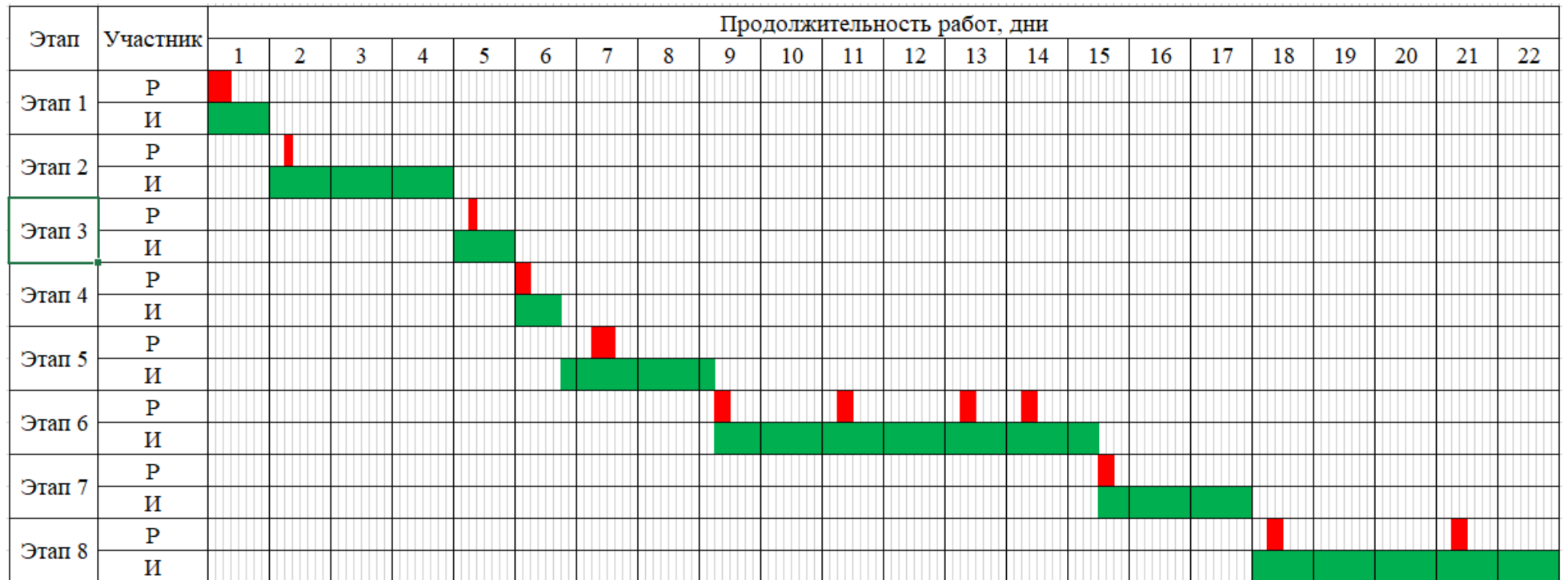


Рисунок А.1 – Диаграмма Ганта