Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2020, № 1, с. 39-46.

Поступила: 20.05.2020
Окончательный вариант: 11.06.2020

УДК 004.032.24:004.056.2:007.2

Разработка защищённой системы контроля компьютеров, периферийного оборудования и программного обеспечения в доменной сети

Джамалетдинов Р.И.*, Иванцов А.М.

*ulsuoso@mail.ru
УлГУ, Ульяновск, Россия

Настоящая работа посвящена исследованию информационных систем по контролю ИТ-активов, учитывая функционал и защищенность данных систем. Проведен сравнительный анализ существующих информационных систем с выявлением их достоинств, разработана концептуальная модель защищенной информационной системы. Дано описание разработанного программного обеспечения, предназначенного для контроля ИТ-активов, работающего в доменной сети УлГУ.

***Ключевые слова**: защищенная система контроля компьютеров сети, инструментарий WMI, инвентаризация, сбор сведений о системе, контроль ИТ-активов*

Введение

В современном мире ни одна компания не может существовать без компьютерных технологий. При этом компьютер – это сложная система, состоящая из разнообразных устройств и элементов: блок питания, процессор, материнская плата, видеоадаптер, оперативная память, монитор, клавиатура и прочее, и за всеми этими деталями и составляющими для эффективного использования необходимо тщательно следить: проводить техническое обслуживание, инвентаризировать во избежание потерь и утечек информации.

По мере роста и развития каждая компания рано или поздно приходит к тому, что требуется навести полный порядок в ИТ (информационно-технологической) инфраструктуре предприятия, получить контроль над перемещениями техники, спланировать сервисные работы, заказы и закупки, списания и учет компьютеров [1]. Необходима возможность в любой момент времени централизованно получать полную информацию о состоянии подотчетного ИТ оборудования. Инвентаризация компьютеров становится важной

составляющей ИТ отдела. Зачастую необходима информация о том, где и когда покупалась та или иная техника, срок гарантии, не было ли несанкционированной подмены комплектующих в компьютере сотрудников и др. Использование автоматизированной системы облегчит и ускорит работу весь обслуживающий персонал ИТ-отдела и сократит потери компании за счет сокращения затрат на обслуживание компьютеров.

Для плодотворной работы персонала, контроля программных активов необходимо эффективное управление, контроль и защита программных активов в масштабе УлГУ, а также эффективное управление, контроль и защита информации о связанных активах, необходимых для управления программными активами, тщательное отслеживание программного обеспечения, установленного на рабочих местах [2]: помимо постороннего программного обеспечения, расходующего понапрасну оперативную память, могут быть занесены вирусные программы, пагубно влияющие на весь производственный процесс предприятия и несущие вредоносный характер. Для успешной автоматизации процессов УлГУ, в первую очередь, необходимо провести анализ работы предприятия с целью выявления проблемных и «узких» мест в работе компании для дальнейшего их устранения и усовершенствования.

1. Сравнительный анализ основных типовых средств контроля ИТ – активов.

Рассмотрим существующие типовые средства контроля активов информационных технологий, чтобы выявить их достоинства и недостатки. Необходимо выбрать систему, которую используем как основу защищенной системы.

Обобщенные преимущества и недостатки рассмотренных программных продуктов представлены в таблице 1.

Таблица 1. Сравнение программных продуктов

Прог.Прод. / Особен-ности	AIDA 64	HWiNFO	10-Страйк	Checkcfg	ScanMonitor
1	2	3	4	5	6
Отсутствие необходимости в установке на клиентские ПК	-	-	+	-	+
Отсутствие необходимости обновлений для снятия показаний	-	+	+	+	+
Автоматическое сканирование в сети	+	-	+	+	+
Возможность формировать отчет	+	-	+	+	-

Возможность фильтровать полученную информацию	+	-	+	+	-
Возможность читать журнал ошибок	+	-	+	-	+
Возможность отслеживать состояние системы в реальном времени	+	+	+	-	+
Цена продукта для организации	-	+	-	+	+

Из представленных выше приложений выгоднее всего отличаются программные системы 10-страйк, комплекс программ Checkcfg.

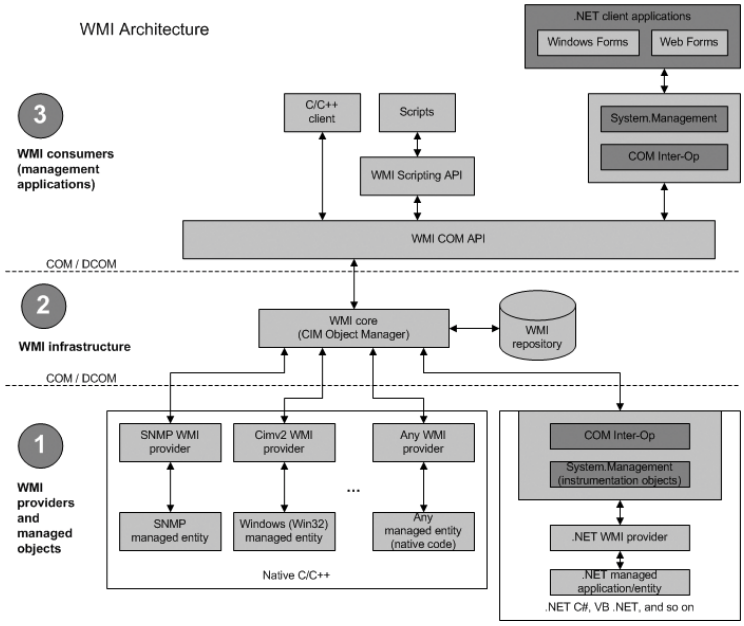

Рис. 1. Архитектура WMI

Главными достоинствами рассматриваемой реализованной автоматизированной системы по сравнению с основными программными продуктами, представленными на рынке, являются ее бесплатное внедрение на предприятии, а также отсутствие необходимости устанавливать программы-агенты на клиентские компьютеры. Для достижения таких же достоинств, необходимо использование стандартизованного механизма WMI и системы авторизации для удаленного мониторинга ПК на основе домена Microsoft Active Directory [4], что позволит построить систему, обладающую рядом преимуществ:

- Простота реализации – механизмы WMI и Microsoft AD стандартно поддерживаются Windows API и средами разработки;
- Универсальность – технологии доступны для ПК с любой ОС семейства Windows (XP, Vista, 7, 8 и 10);

- Надежность – на стороне ПК не требуется использование дополнительных программных агентов.

Для получения сведений с компьютеров в доменной сети без использования клиентского ПО будет рассматриваться технология WMI. WMI – это инструментарий управления Windows [5]. Если говорить более развернуто, то WMI – это одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows. С использованием архитектуры WMI, представленной на рис. 1, разработана концептуальная модель защищенной системы.

2. Концептуальная модель защищённой системы контроля компьютеров, периферийного оборудования и программного обеспечения в доменной сети УлГУ

Рассмотрим модель защищённой автоматизированной системы контроля компьютеров, периферийного оборудования и программного обеспечения в доменной сети. Можно предложить компоненты модели АС на первом уровне декомпозиции. С использованием концептуальной модели, изображенной на рис. 2, реализована защищенная информационная система по контролю ИТ-активов.

- Цели использования АС;
- Источники информации;
- Направление АС;
- Безопасность информации;
- Менеджмент ИТ-активов.

3. Описание реализации защищенной информационной системы по контролю ИТ-активов УлГУ

Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации [6]. Важной составляющей АС служит – безопасность. Отсутствует возможность подмены актуальности данных с запрашиваемого устройства доменной сети УлГУ, что не дает бесследно исчезать/подменять комплектующие компьютера, а, следовательно, и утечки данных. Так же по используя WMI ведется контроль лицензионного ПО и выполнение правил групповых политик безопасности.

Проектируемая система представляется в виде множества сущностей или актеров, взаимодействующих с системой с помощью так называемых вариантов использования. При этом актером (actor), или действующим лицом, называется любая сущность, взаимодействующая с системой извне. Это может быть человек, техническое устройство, программа или любая другая система, которая может служить источником воздействия на

моделируемую систему так, как определит сам разработчик. В свою очередь, вариант использования (use case) служит для описания сервисов, которые система предоставляет актеру. Другими словами, каждый вариант использования определяет некоторый набор действий, совершаемый системой при диалоге с актером. При этом ничего не говорится о том, каким образом будет реализовано взаимодействие актеров с системой.

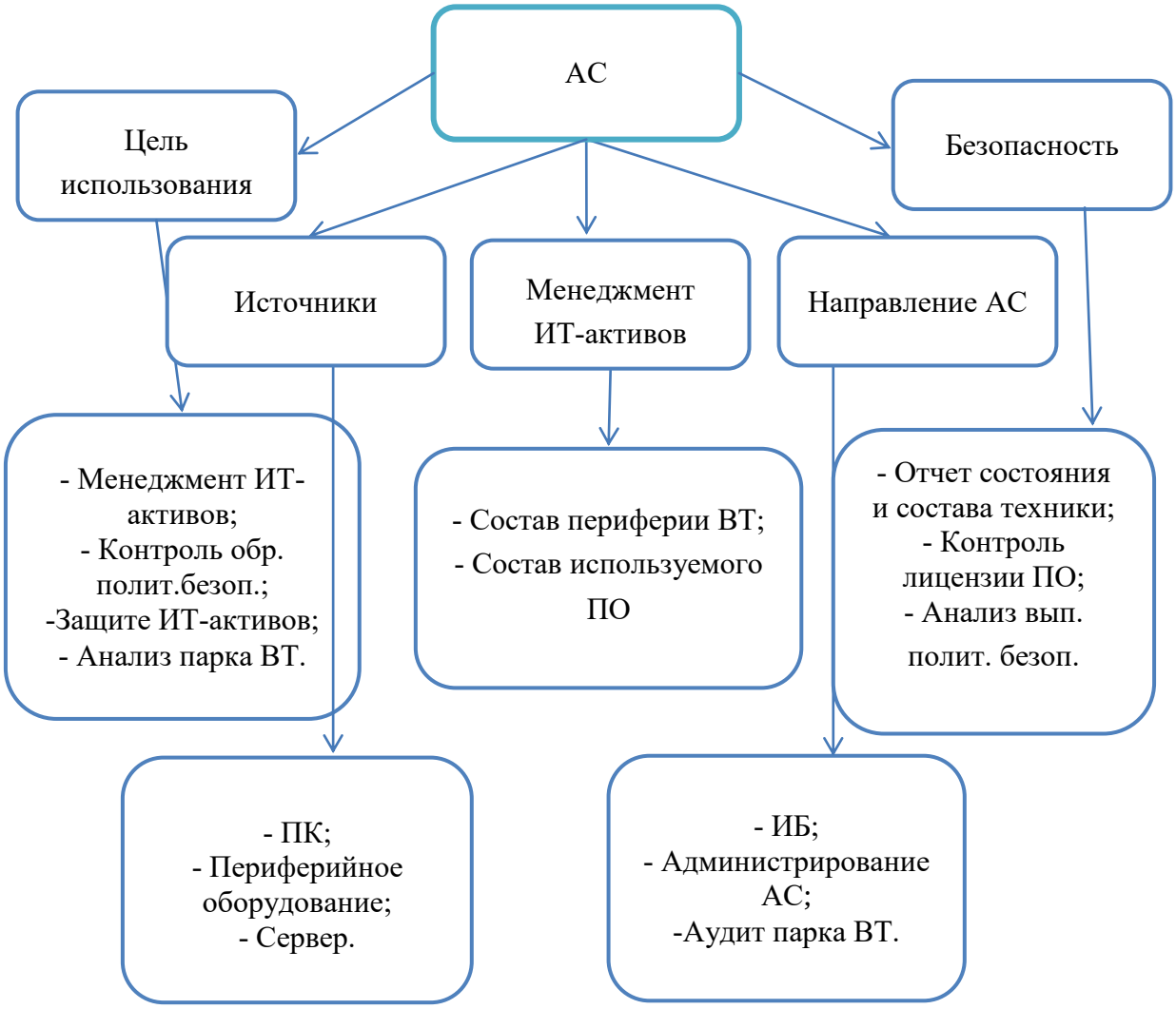

Рис.2. Концептуальная модель АС

Функциональные возможности, логику процедур и поток демонстрируется в виде диаграммы деятельности. Во многих случаях они напоминают блок-схемы, но принципиальная разница между диаграммами деятельности и нотацией блок-схем заключается в том, что первые поддерживают параллельное процессы.

Главное предназначение этой диаграммы – описать возможные последовательности состояний и переходов [7], которые в совокупности характеризуют поведение элемента модели в течение его жизненного цикла. Для описываемой системы диаграмма имеет вид, представленный на рис. 3.

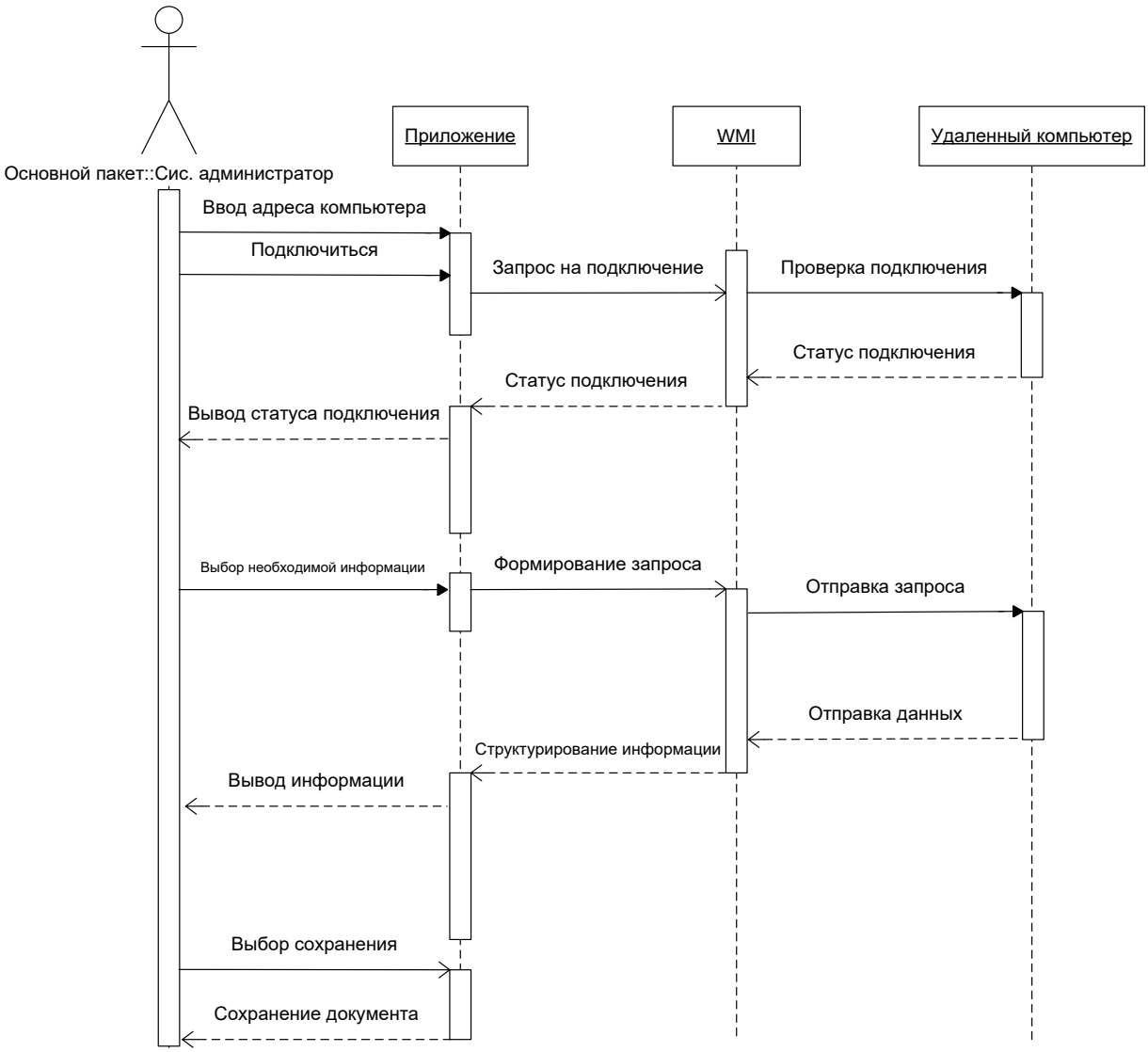

Рис. 3. Диаграмма деятельности

Диаграмма, на которой показаны взаимодействия объектов, упорядочены по времени их проявления. Основными элементами диаграммы последовательности являются обозначения объектов (прямоугольники), вертикальные линии, отображающие течение времени при деятельности объекта, и стрелки, показывающие выполнение действий объектами.

Отражая сценарии поведения в системе, эта диаграмма обеспечивает более наглядное представление порядка передачи сообщений. Графически диаграмма последовательности - разновидность таблицы, которая показывает объекты, размещенные вдоль оси X, и сообщения, упорядоченные по времени вдоль оси Y [7].

Основные функции АС представлены на рис. 4.

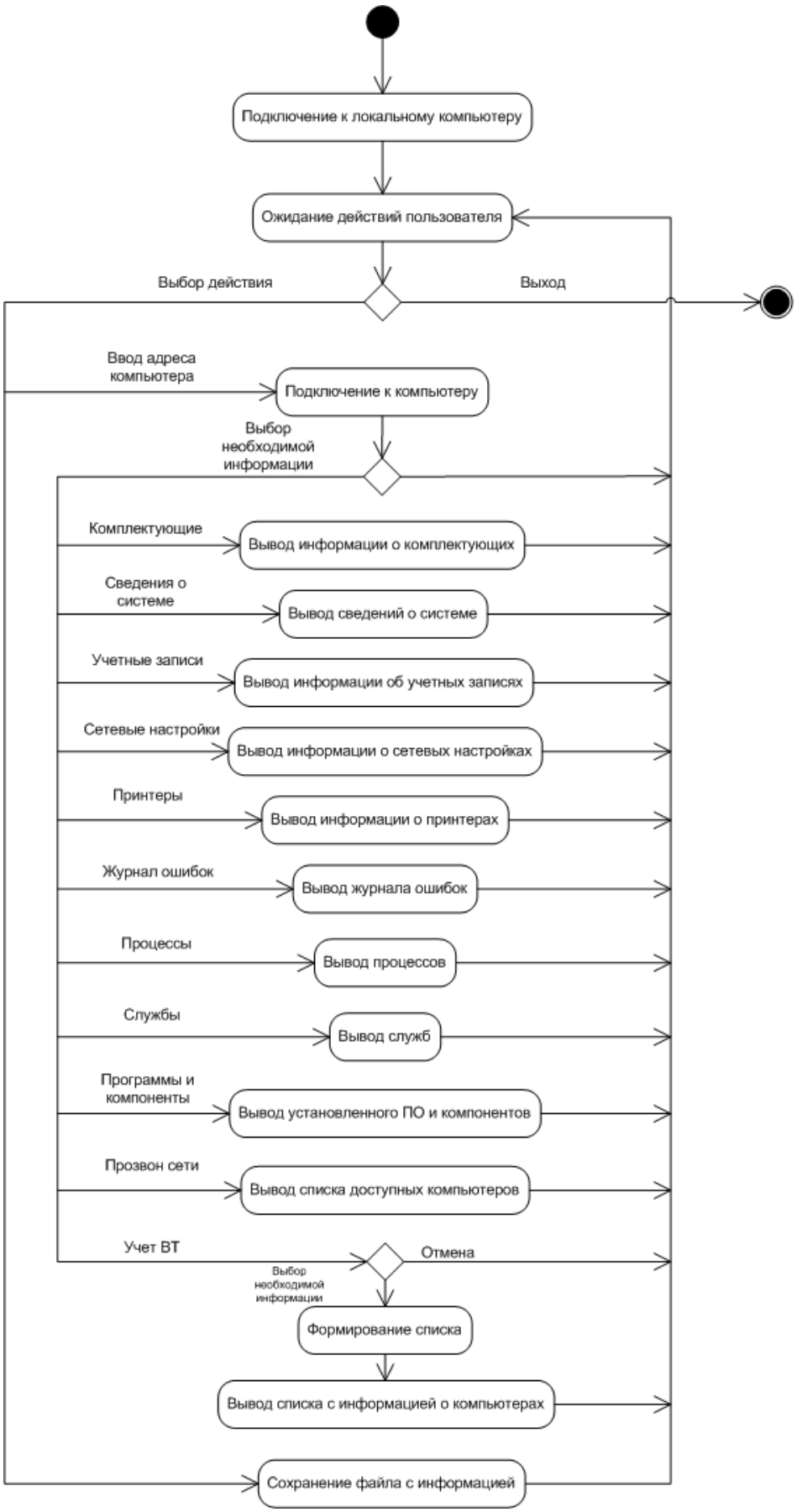

Рис.4. Функции АС

Заключение

Итогом анализа работы по разработки защищенной АС контроля ИТ-активов в доменной сети УлГУ, с использованием WMI стал программный продукт «PCScanInf.exe», собирающий информацию обо всех устройствах доменной сети без использования клиентского ПО.

Для достижения цели были выполнены задачи:

1. Рассмотрены назначения и функции АС;
2. Проведен сравнительный анализ существующих АС контроля ИТ - активов;
3. Описана концептуальная модель АС;
4. Описаны реализация функциональные возможности АС

Данная система дает возможность просматривать информацию о составе ПО и лицензий, комплектующих ПК, соблюдение правил выполнения политик безопасности, сбор сведений используемых служб и приложений на рабочем месте.

В дальнейшем продукт будет дорабатываться добавлением в него БД поддерживающий шифрование и архивирование. Использование WMI технологии не требует разбиения продукта на серверную и клиентскую часть, так как все необходимые приложения запущены в операционной системе по правилам групповой политики безопасности. Данная система внедрена и используется в отделе технического обслуживания информационных технологий УлГУ.

Список литературы

1. ГОСТ Р АСО/МЭК 19770-1-2014. Информационные технологии (ИТ). Менеджмент программных активов. Часть 1. Процессы и оценка соответствия по уровням. Введ. 2015-03-01.
2. ГОСТ Р 58591-2019. Интеллектуальная собственность. Бухгалтерский учет и нематериальные активы. Введ. 2019-12-01.
3. Максимов, Н.В. *Современные информационные технологии: Учебное пособие*. Форум, 2013. 512 с.
4. *Вызов WMI для получения физического серийного номера* [Электронный ресурс] https://qastack.ru/ (дата обращения 19.05.2020).
5. *Обзор средств работы с WMI для администратора.* [Электронный ресурс]. Режим доступа:http://it2web.ru/index.php/wmi/183-obzor-sredstv-raboty-s-wmi-dlya-administratora (дата обращения 19.05.2020).
6. Приказ ФСТЭК России от 11 февраля 2013 г. N 17. *Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.*
7. Андерсон К. *Сценарии* WMI *для начинающих* [Электронный ресурс]. Режим доступа*:* https://www.osp.ru/winitpro/2001/05/174893/ (дата обращения 19.05.2020).
8. Исаев, Г.Н. *Информационные технологии: Учебное пособие*: 2013. 464 с.