УДК 004.056.5:378.096

ОБСЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ КАФЕДРЫ

Стамкулова Г.К. *КГТУ им.И.Раззакова , кафедра ПОКС, город Бишкек, Кыргызстан, gulkuv@gmail.com, orcid.org/0000-0003-2782-8468*

Современная информационная система (ИС), находящаяся в производственной эксплуатации, включает в себе функции защиты, обрабатываемой в ней информации и предотвращения к ней несанкционированного доступа. Однако динамика изменения нарушений защищенности информационных систем свидетельствует о наличии ряда нерешённых задач в области защиты информации ИС, в том числе, при проектировании и эксплуатации средств защиты. На этапе проектирования системы информационной безопасности ИС необходимо определить требуемый уровень защищённости системы, а на этапе тестирования оценить параметры безопасности аудируемой системы и сопоставить их с начальным заданием по безопасности.

Ключевые слова: информационная система, ИТ-инфраструктура, стандарты, уязвимость, информационная безопасность, объект исследования, угроза, нарушитель, актив.

SECURITY SURVEY OF THE DEPARTMENT INFORMATION SYSTEM

Stamkulova G. K *KSTU named after I.Razzakov, chair POCS, Bishkek city, Kyrgyzstan,gulkuv@gmail.com*

The modern information system (IS), which is in production operation, includes the functions of security information processed in it and preventing unauthorized access to it. However,

the dynamics of changes in security breaches of information systems indicate that there are a number of unresolved problems in the field of IS information security, including when designing and operating security equipment. At the design stage of the IT security system, it is necessary to determine the required level of system security and in the testing phase, evaluate the security parameters of the system being audited and compare them with the initial security task.

Keywords: information system, IT infrastructure, standards, vulnerability, information security, object of research, threat, intruder, assets.

Введение

Использование информационных технологий является такой же необходимой потребностью для современного человека, как и пища для организма. Невозможно представить оптимальное функционирования бизнес-процессов без применения информационных систем и телекоммуникационных сетей, так как правильность принятия важных решений заключается в своевременном получении достоверной и полной информации. Информационная безопасность информационных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

Целью определения угроз безопасности информации является установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора, а в случае обработки персональных данных[5]

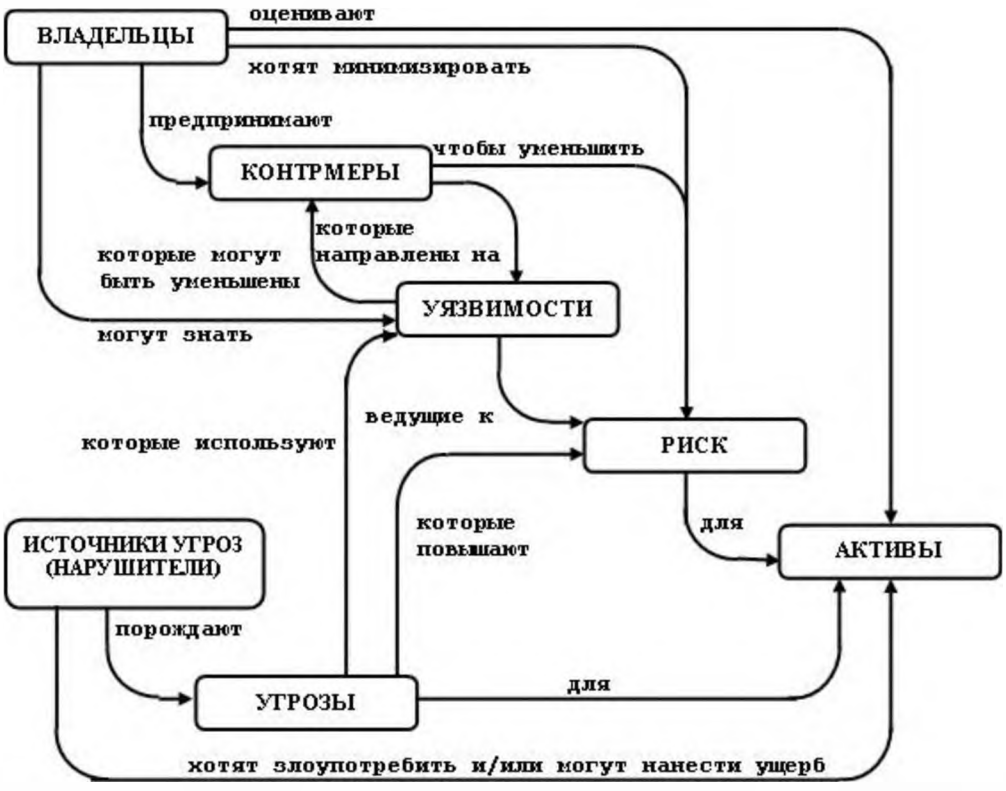


Рис. 2.1.Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2008[8]

Описание объекта обеспечения информационную безопасности

Информационная система кафедры выполняет следующие действия:

- взаимодействие между сотрудниками выпускающей кафедры путем внедрения подсистемы заданий;
- централизованную базу данных о деятельности кафедры и составление отчета на их основе;
- электронную рассылку сообщений сотрудникам, выпускникам, студентам и их родителям;
- ведение объективного рейтинга сотрудников по результатам их годовой деятельности, в целях повышения производительности работы персонала и ускорения рабочего процесса.

Для того чтобы сформулировать общие требования к функциональному поведению проектируемой системы была разработана концептуальная модель. Данная модель описывает список всех пользователей системы, а также цели, которые они преследуют при её использовании. Концептуальная модель разрабатываемой системы представлена в виде диаграммы IDEF0 AS-IS (рис. 2.2) и в виде модели вариантов использования usecase (рис. 2.3).

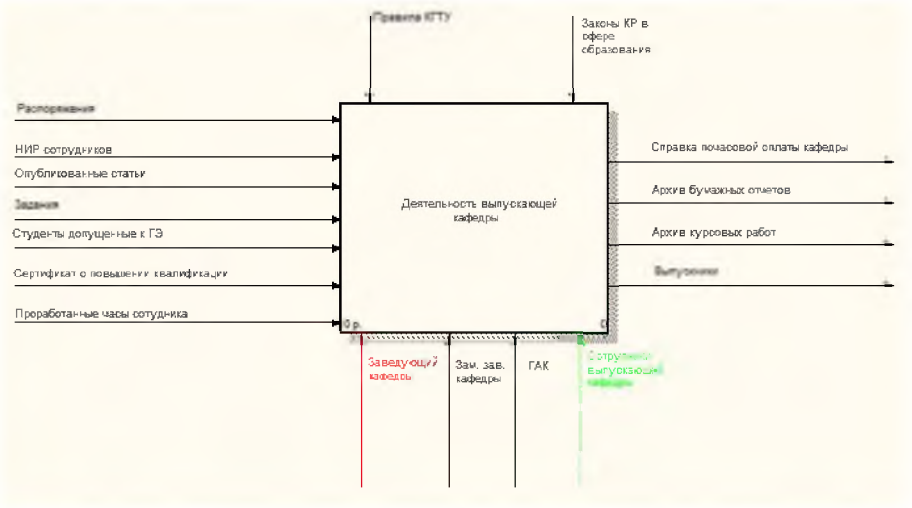


Рис. 2.2 Модель AS-IS [5] в виде контекстной диаграммы «Деятельность выпускающей кафедры»

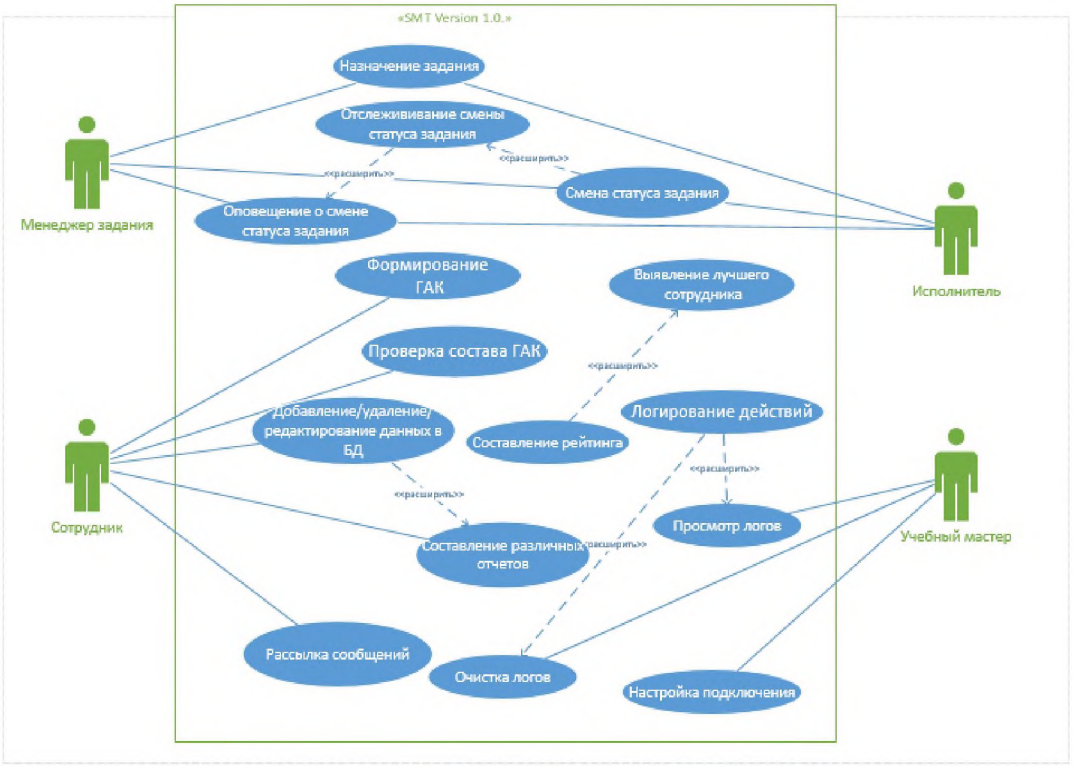


Рис. 2.3 Общая схема модели вариантов использования [5] автоматизированной системы управления деятельностью выпускающей кафедры ПОКС КГТУ им. И. Раззакова SMT Version 1.0.

Модель потоков данных начинается с построения контекстной диаграммы, представленной в рис. 2.3. Она включает в себя три внешние сущности: «Получатели рассылки сообщения», «Менеджер задания» и «Сотрудники»

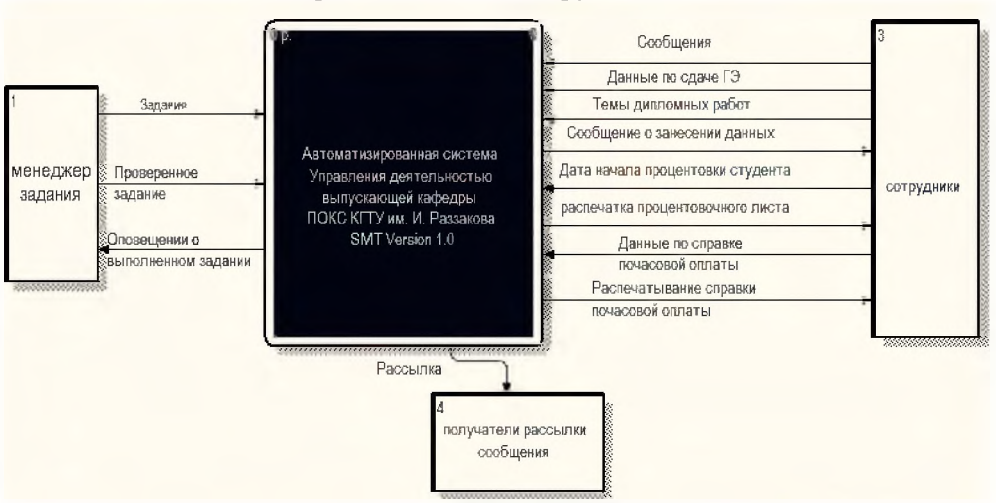
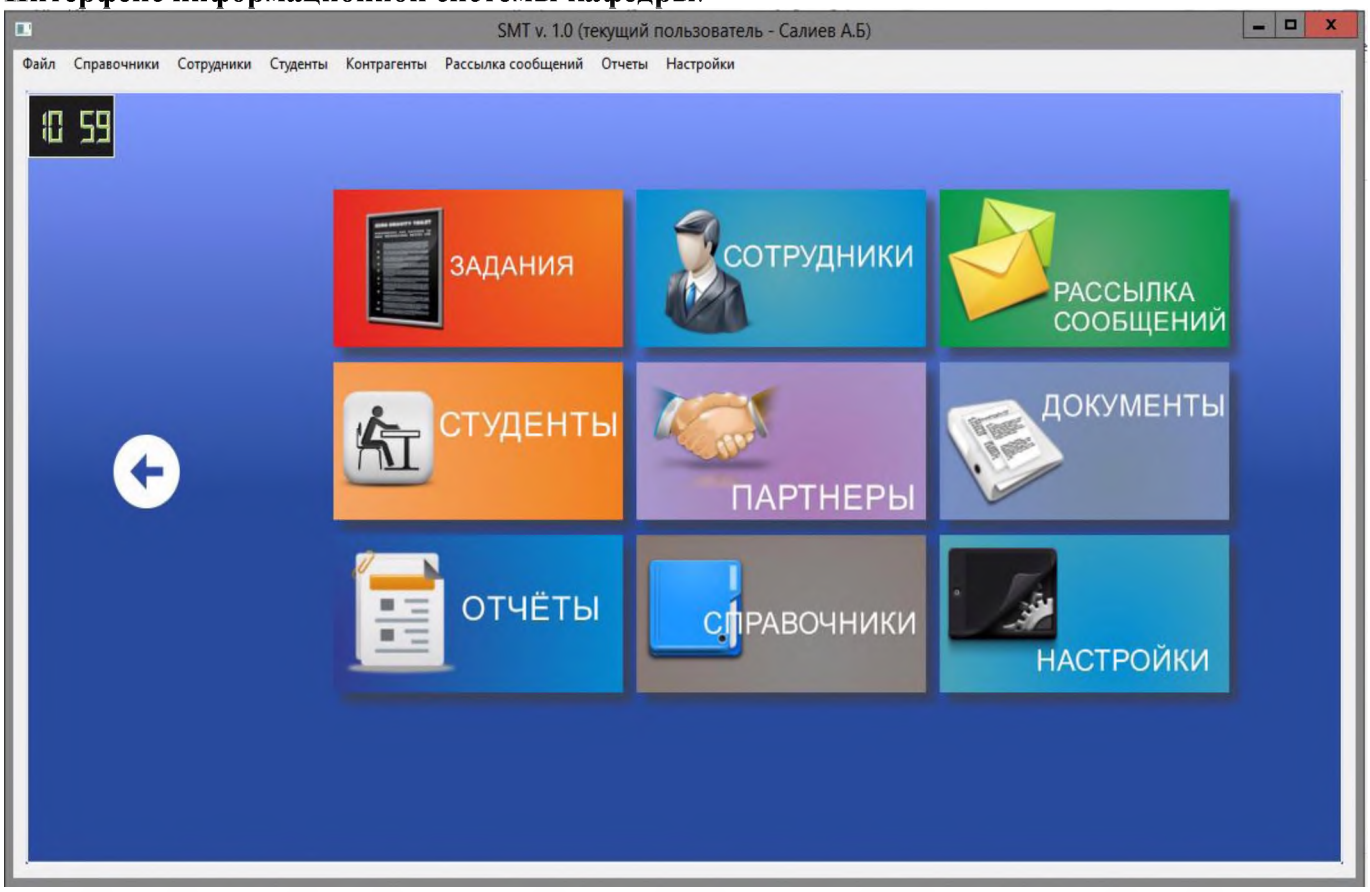


Рис. 2.4 Модель AS-TO-BE в виде диаграммы потоков данных автоматизированной системы управления деятельностью выпускающей кафедры ПОКС КГТУ им. И. Раззакова SMT Version 1.0.

Интерфейс информационной системы кафедры.



В информационную систему кафедры входят: технические средства, программные обеспечения и информационные ресурсы.

Информационная система является локальной информационной системой с подключением к внешним к внешним ИС, в том числе к сетям общего пользования. Технические средства, а именно оборудования сервера информационной системы расположены в помещении, находящемуся в пределах контролируемой зоны, службами ИБ. Информационные активы хранятся на рабочих станциях сотрудников (АРМ) и на сервере системы. На каждой АРМ установлен клиент информационной системы, посредством которой будет производится взаимодействие сотрудников.

В рабочем процессе данной системы участвуют два типа субъекта: пользователь и администратор. Пользователями данной системы являются любой сотрудник организации, зарегистрированный в системе, вне зависимости от ранга и должности сотрудника. Администратор занимается обслуживанием и настройкой информационной системы. Задачи системы:

- Формирование справочников для хранения входных и результирующих сведений
- Учет посещаемости и успеваемости студентов
- Учет спортивных достижений студентов
- Учет результатов олимпиад
- Учет проведения научных конференций и семинаров
- Планирование учебного процесса
- Мониторинг и выдача поручений
- Учет приказов и поручений
- Учет защиты выпускных работ
- Учет прохождения учебных, производственных и предквалификационных

практик

- Формирование и учет состава ГАК
- Учет проведения научно-исследовательских работ

Классификация активов объекта

Активы данного объекта делятся на 2 типа: информационные активы и среды обработки информационных активов. К информационным активам данного объекта относятся «Персональные данные» и информация относящейся к «Открытой информации», «Служебной информации». Активы 3-х типов представлены в таблице 1 в соответствии уровням иерархии информационной инфраструктуры.

Таблица 1. Среда обработки актива по уровням иерархии информационной инфраструктуры

Уровни иерархии информационной инфраструктуры	Типы объектов среды обработки ИА
Физический уровень	АРМ
	Серверная станция
Сетевой уровень	Маршрутизатор
Уровень сетевых приложений и сервисов	TCP/IP
	FTP/UDP
Уровень операционных систем	Системное ПО
	Файлы «Персональными данными»
Уровень приложений и сервисов	Клиентское приложение

Таблица 2. Уязвимости активов

Процесс, реализуемый на объекте	Информационный актив (ИА)		Актив, относящийся к объекту среды обработки ИА	
	Тип актива	Приоритеты политики ИБ	Тип актива	Уязвимости
Регистрация нового пользователя	Персональные данные	К, Ц, Д	АРМ	Отсутствие контроля физического доступа, логического доступа
			Серверная станция	
			Клиентское приложение	Уязвимости кода; Отсутствие руководств пользователя
Авторизация пользователя	Персональные данные	К, Ц, Д	АРМ	Отсутствие контроля физического доступа
			Серверная станция	
Авторизация пользователя	Открытая информация	Ц, Д	АРМ	Отсутствие контроля физического доступа
			Серверная станция	Отсутствие контроля физического доступа
			Клиентское приложение	Уязвимости архитектуры; Отсутствие руководств пользователя

Проведение по всем формам обучения лекций лабораторных практических семинарских и других видов учебных занятий предусмотренных учебными планами	Открытая информация	Ц, Д	АРМ	Отсутствие контроля физического доступа
			Серверная станция	
			Маршрутизатор	Уязвимости конфигурации
			TCP\IP	Уязвимости протокола
			Клиентское приложение	Уязвимости язык программирования Отсутствие руководств пользователя

ОПИСАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Таблица 3. Модель угроз ИБ

Угроза ИБ	Источник угрозы ИБ	Актив				Метод реализации угрозы ИБ на среду обработки ИА	Последствия реализации угрозы	Объекты, исп. для реализации угроз
		ИА	Приоритеты политики ИБ	Среда обработки ИА	Уязвимость среды обработки ИА			
У-1. Хищение носителей информации	Н-1	Персональные данные, Информация ограниченного доступа	К, Ц, Д	АРМ	Отсутствие контроля физического доступа	Изменение конфигурации, настроек устройства	Нарушение К, Ц, Д.	Внедрение ложного объекта сети
				Серверная станция				Специальное разработанное ПО
	Н-2	Информация ограниченного доступа	Ц, Д, К	АРМ	Отсутствие контроля физического доступа	Неконтролируемая модификация информационного актива	Нарушение Ц, Д, К	С применением программных средств ОС
				Серверная станция				Внедрение ложного объекта сети
У-2. НСД к информационным ресурсам	Н-2	Открытая информация	Ц, Д	АРМ	Отсутствие контроля физического доступа	Несанкционированный физический доступ	Нарушение Ц, Д	технологические выходы из программ
				Серверная станция				аппаратные закладки
				Клиентское приложение	Уязвимости ПО	Использование специального ПО		технологические выходы из программ

У-3. Несанкционированное сканирование сети	Н-2	Открытая информация	Ц, Д	АРМ	Отсутствие контроля физического доступа	Несанкционированный физический доступ	Нарушение Ц, Д	Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа
				Серверная станция				Отказ в обслуживании
				Маршрутизатор	Уязвимости ПО	Использование специального ПО		Сканирование сети
				TCP/IP	Уязвимости протокола			Анализ сетевого трафика
				Клиентское приложение	Отсутствие необходимых средств защиты			технологические выходы из программ
У-4. Подмена доверенного объекта сети	Н-2	Открытая информация	Ц, Д	АРМ	Отсутствие контроля физического доступа	Несанкционированный физический доступ; Несанкционированный логический доступ;	Нарушение Ц, Д	Специальное разработанное ПО
				Серверная станция				вести сеанс работы с объектом сети от имени доверенного субъекта

				Маршрутизатор	Уязвимости ПО	Использование специального ПО		Анализ сетевого трафика
				FTP\UDP	Уязвимости протокола			Анализ сетевого трафика
				Клиентское приложение	Отсутствие необходимых средств защиты			Вредоносные программы
У-5. Внедрение вредоносной программы	Н-2	Открытая информация	Ц, Д	АРМ	Отсутствие контроля физического доступа	Несанкционированный физический доступ; Несанкционированный логический доступ;	Нарушение Ц, Д	
				Серверная станция				вести сеанс работы с объектом сети от имени доверенного субъекта
				Системное ПО	Уязвимости ПО	Заражение программы (троян)		Вредоносные программы
				Файлы с «Персональными данными» и «Служебная тайна»	Отсутствие программ ЗИ	Заражение программы		Вредоносные программы
У-6. Присвоение чужого идентификатора и пароля	Н-1	Персональные данные	К, Ц, Д	АРМ	Отсутствие контроля физического доступа	Несанкционированный физический доступ; Несанкционированный логический доступ;	Нарушение К, Ц, Д.	вести сеанс работы с объектом сети от имени доверенного субъекта

				Серверная станция				вести сеанс работы с объектом сети от имени доверенного субъекта
				Клиентское приложение	Уязвимости ПО	Вскрытие или перехватывание пароли		Угроза выявления пароля
У-7. Отказ в обслуживании	Н-2	Открытая информация	Ц, Д	Серверная станция	Отсутствие контроля логического доступа	Перегрузка ресурсов; Несанкционированный логический доступ	Нарушение Ц, Д	вести сеанс работы с объектом сети от имени доверенного субъекта
				Маршрутизатор	Уязвимости ПО	Перегрузка ресурсов		Неавторизованное использование оборудования
				FTP\UDP	Уязвимости протокола	Использование специального ПО		Анализ сетевого трафика
				TCP\IP				Анализ сетевого трафика

УДК: 004.42:539.38

ТОПТОЛГОН КҮЧТӨР ТАРАБЫНАН КЫСЫЛГАН ТИЛКЕДЕГИ СЕРПИЛГИЧ ДЕФОРМАЦИЯЛАРДЫ EXCEL ЧӨЙРӨСҮНДӨ САНДЫК ЭСЕПТӨӨ ЖӨНҮНДӨ

Стамкулова Г.К. *КГТУ им.И.Раззакова, кафедра ПОКС, город Бишкек, Кыргызстан, gulkuv@gmail.com) orcid.org/0000-0003-2782-8468*

Серпилгич деформацияны Excel чөйрөсүндөгү дискреттик моделди [1,3] колдонуу менен сандык эсептөөнүн маселелери каралат. Топтолгон күчтөр тарабынан кысылган аяккы тилкедеги жылышуулардын жана чоюучу деформациялардын өзгөрүүлөрүнүн мыйзам ченемдүүлүктөрү аныкталды.

Маанилүү сөздөр: Серпилгич деформация, сандык эсептөө, күч, атом, модель.