Міністерство освіти і науки України

Харківський національний університет ім. В. Н. Каразіна

Факультет комп’ютерних наук

Кафедра безпеки інформаційних систем і технологій

Лабораторна робота №1

*з навчальної дисципліни*

«Захист інформації в інформаційно-комунікаційних системах»

Виконав:

Студент групи КБ-41

Кравченко Є. М.

Перевірив:

Професор

Єсін В. І.

Харків – 2020 р.

**Тема:** Способы обнаружения вирусов

**Цель работы:** ознакомление с различными способами обнаружения

компьютерных вирусов и иного вредоносного программного обеспечения

действующих в операционной системе (ОС) Windows и их удаление.

**1. Выявление действия вируса в ОС Windows с помощью анализа**

**протекающих процессов.**

Определение процесса вируса в ОС Windows Действие вируса можно обнаружить путем анализа протекающих в компьютере процессов. Для его обнаружения можно воспользоваться средствами ОС, а именно программой "Task Manager" (рис. 1).

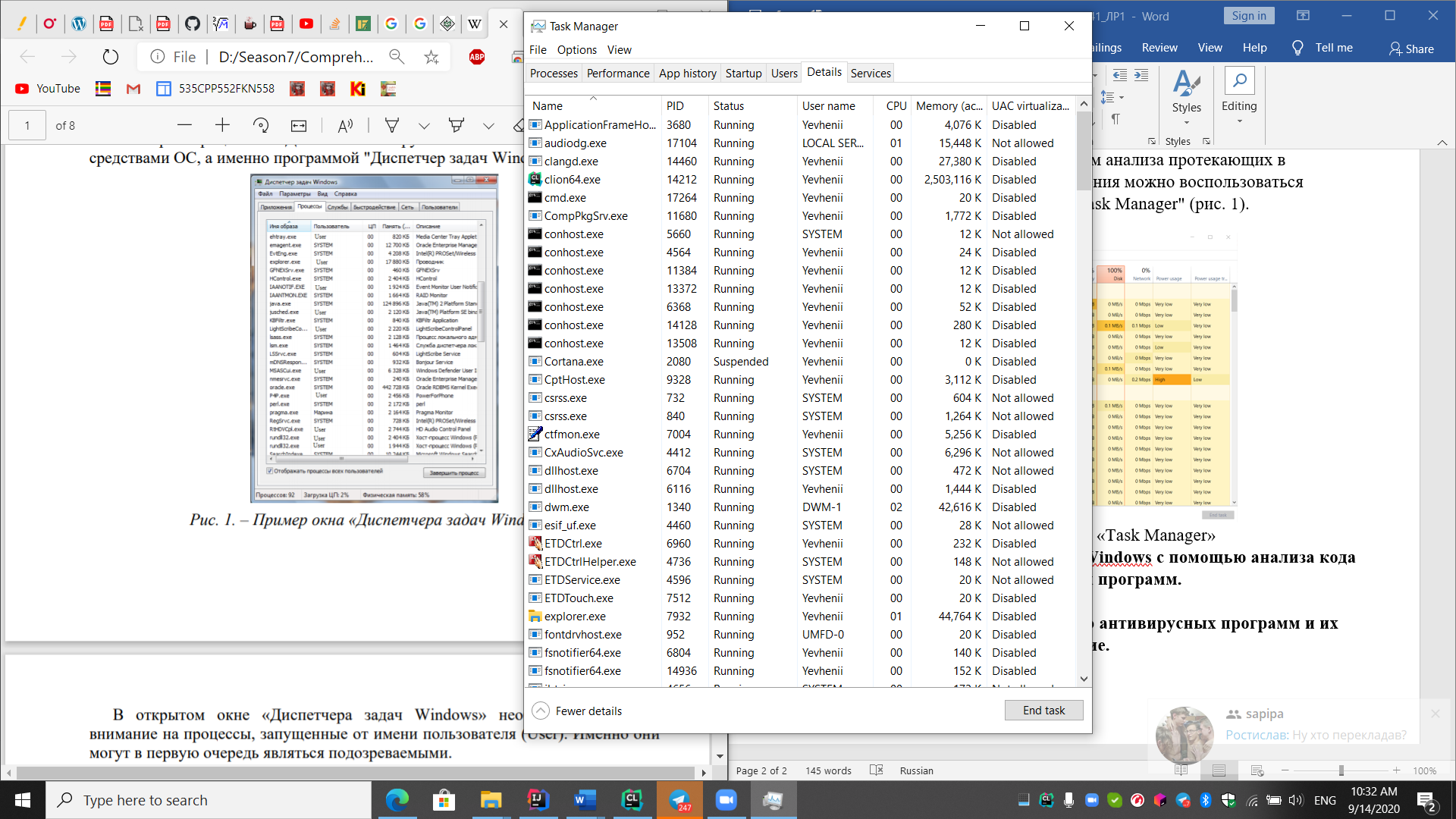


Рис. 1. – Пример окна «Task Manager»

Для выявления подозрительных действий вредоносных программ необходимо выполнить и проанализировать следующую последовательность команд:

а) отключить все программы, которые стоят в "Автозагрузке"

(sturtup)

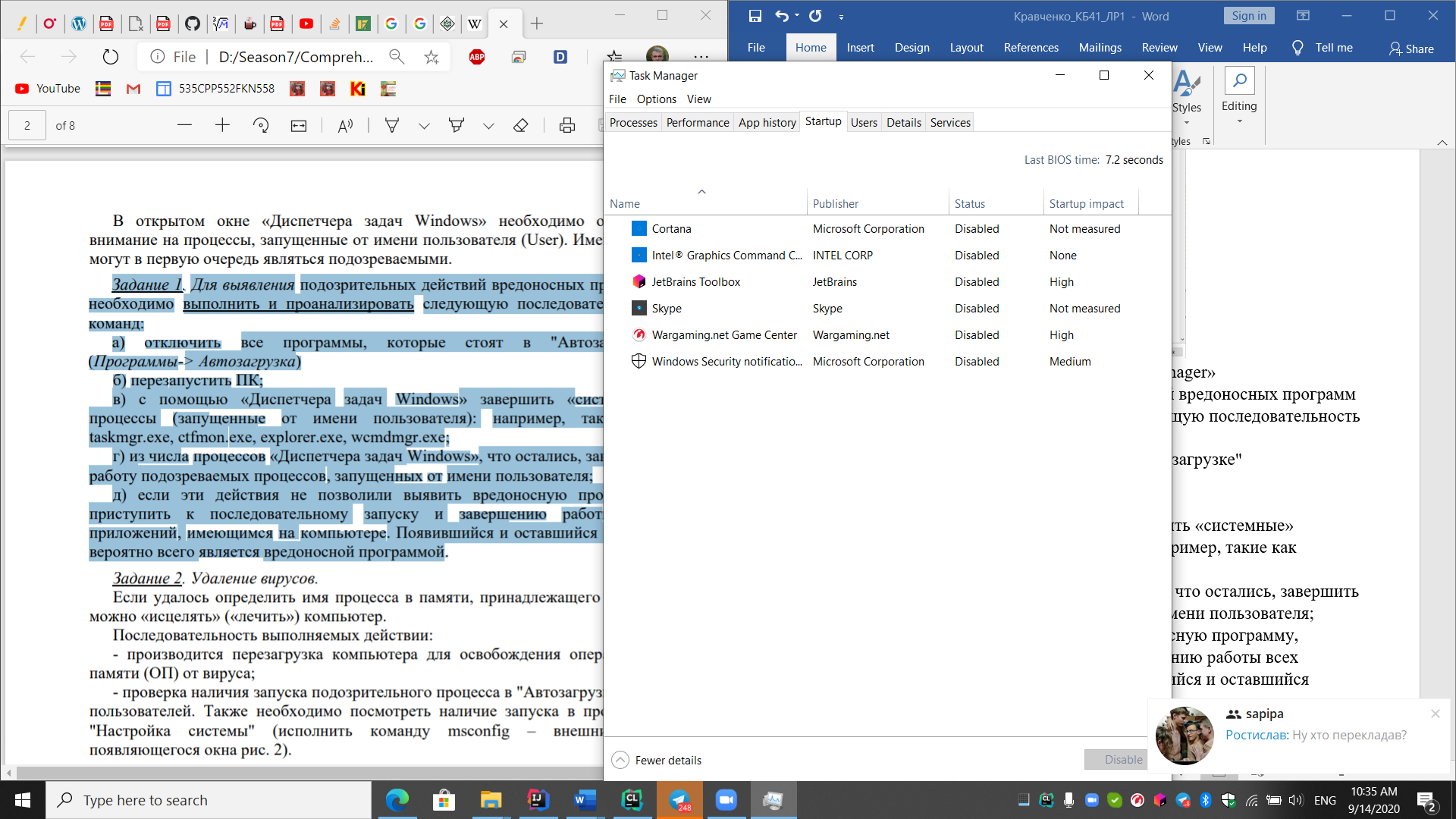


Рис. 2. – Пример отключенных приложений в меню автозагрузки

б) перезапустить ПК;

в) с помощью «Task Manager» завершить «системные» процессы (запущенные от имени пользователя): например, такие как taskmgr.exe, ctfmon.exe, explorer.exe, wcmdmgr.exe;

г) из числа процессов «Диспетчера задач Windows», что остались, завершить работу подозреваемых процессов, запущенных от имени пользователя;) если эти действия не позволили выявить вредоносную программу,приступить к последовательному запуску и завершению работы всехприложений, имеющимся на компьютере. Появившийся и оставшийся процессвероятно всего является вредоносной программой.

Если удалось определить имя процесса в памяти, принадлежащего вирусу, можно «исцелять» («лечить») компьютер. Последовательность выполняемых действии:

- производится перезагрузка компьютера для освобождения оперативной памяти (ОП) от вируса;

- проверка наличия запуска подозрительного процесса в "Автозагрузке" всех пользователей. Также необходимо посмотреть наличие запуска в программе "Настройка системы" (исполнить команду msconfig – внешний вид появляющегося окна рис. 2).

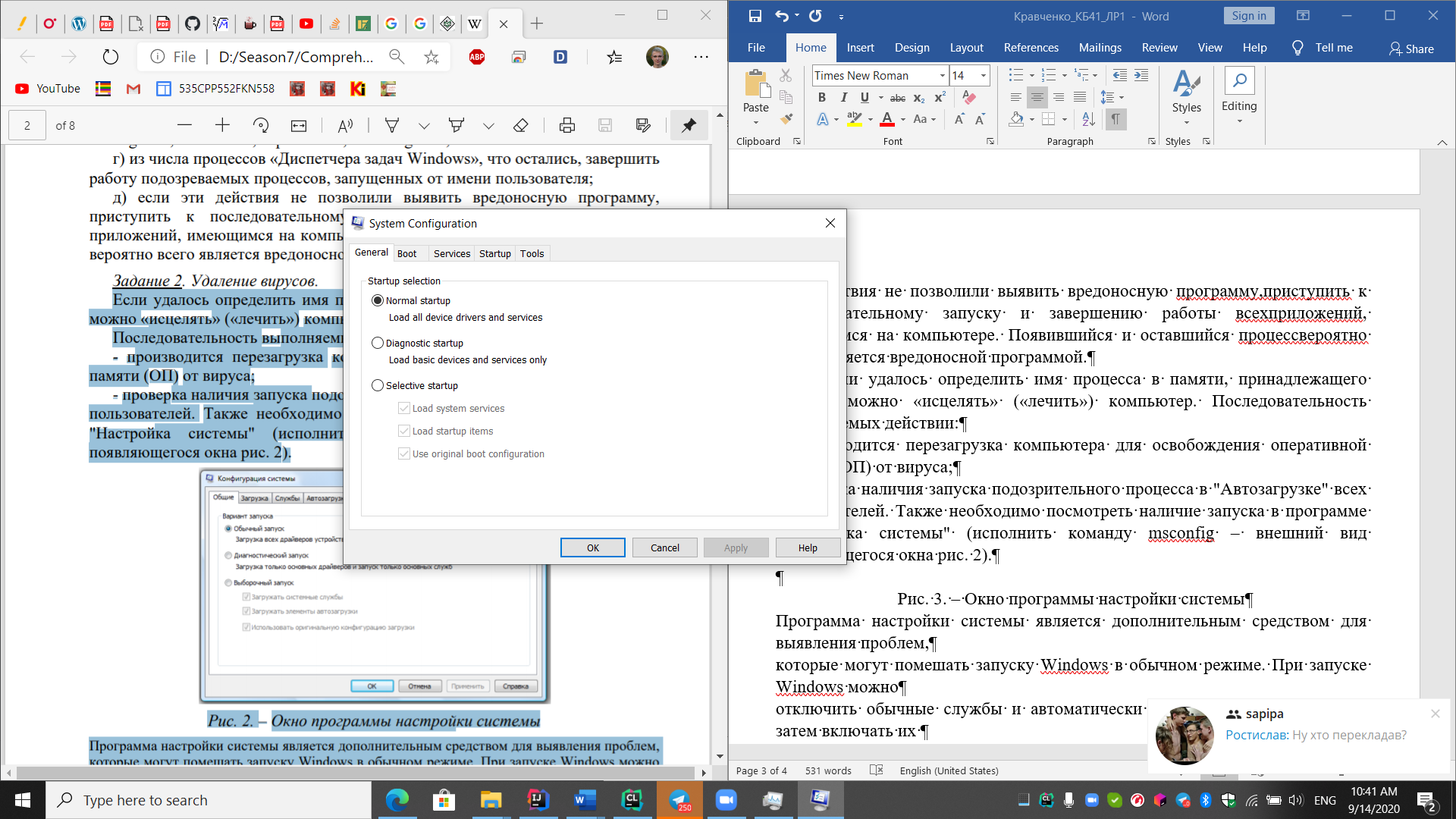


Рис. 3. – Окно программы настройки системы

Программа настройки системы является дополнительным средством для выявления проблем, которые могут помешать запуску Windows в обычном режиме. При запуске Windows можно отключить обычные службы и автоматически загружаемые программы, а затем включать их по одной. Если проблема не возникает, когда служба отключена, но появляется после ее

включения, значить эта служба может быть источником проблемы.

Программа настройки системы предназначена для поиска и изолирования неполадок, и не предусмотрена для управления загрузкой.

- производится поиск всех "измененных" EXE-файлов за последний месяц или лучше за два месяца с помощью программы поиска. Все найденное можно скопировать в один каталог.

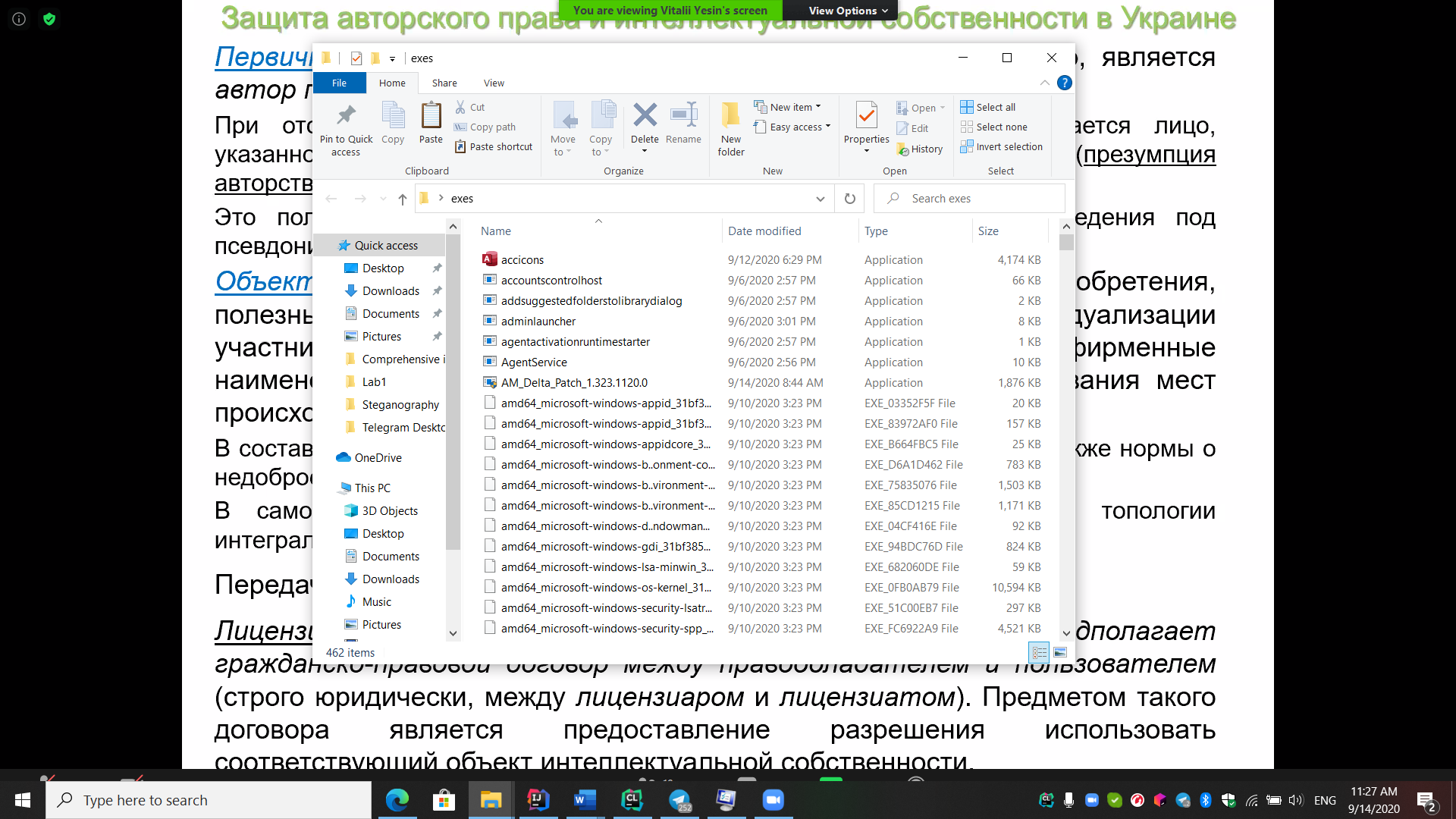


Рис. 4. – Каталог всех измененных приложений

Дальше проверить программы на наличие в них вируса поможет файловый менеджер (FAR, Total Commander и т.д.). В коде программы ведется поиск строки

*This program cannot be run in DOS mode или*

*This program must be run under Win32.*

При поиске строки в найденных файлах дубликатов не обнаружено.

Необходимо отметить, что одна из этих строк обязательно присутствует в начале кода программы. Задача заключается в том, чтобы найти еще одну такую строку. Если строка найдена – значит, в этот файл внедрился вирус. Дальше нужно проверить все найденные файлы подобным способом. После того как было выявлено, какой из файлов заражен, они заменяются незараженными – выполняется процедура простого копирования файлов, если таковые имеются. Для этого, возможно, понадобится другой компьютер без вируса. Если такого компьютера нет, придется удалить зараженные файлы и переустановить те приложения (по необходимости и ОС), из которых их

удалили. Не стоит делать деинсталляцию программ, возможно запустить вирус!

**2. Выявление действия вируса в ОС Windows с помощью анализа кода**

**подозрительных программ.**

**3. Обнаружение вирусов с помощью антивирусных программ и их удаление.**