

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Информационная безопасность

Лабораторная работа № 2

Выполнили студенты:

Маслова Ксения, Группа № Р34681

Неизвестная Екатерина, Группа № Р34701

Морозова Екатерина, Группа № Р34681

Вдовенко Мария, Группа № Р34684

Преподаватель: Оголюк Александр Александрович

г. Санкт-Петербург

2022

Лабораторная работа № 2

Разрешения NTFS

Отчет:

Иерархия каталогов:

Volume in drive E is files
Volume Serial Number is C6AD-0209

Directory of E:\For WIN\laba

10/18/2022	02:45 PM	<DIR>	.	
10/18/2022	02:45 PM	<DIR>	..	
06/05/2022	03:23 AM		511 create	
06/05/2022	05:07 PM		69 database.properties	
10/18/2022	02:45 PM		0 directory.txt	
06/04/2022	06:07 PM		72 helios.bind	
06/05/2022	04:51 PM	<DIR>	lib	
06/05/2022	05:10 PM	<DIR>	src	
		4 File(s)	652 bytes	

Directory of E:\For WIN\laba\lib

06/05/2022	04:51 PM	<DIR>	.	
06/05/2022	04:51 PM	<DIR>	..	
06/05/2022	01:50 PM		36,876	
			org.apache.servicemix.bundles.commons-codec-1.2_5.jar	
06/04/2022	05:48 PM		1,040,139 postgresql-42.3.4.jar	
		2 File(s)	1,077,015 bytes	

Directory of E:\For WIN\laba\src

06/05/2022	05:10 PM	<DIR>	.	
06/05/2022	05:10 PM	<DIR>	..	
06/05/2022	01:03 AM	<DIR>	classesandenums	
06/05/2022	01:22 AM	<DIR>	commands	
06/05/2022	05:09 PM	<DIR>	DatabaseWorkers	
06/04/2022	10:53 PM	<DIR>	exceptions	
06/05/2022	05:10 PM	<DIR>	main	
05/13/2022	11:21 PM	<DIR>	META-INF	
06/05/2022	03:23 AM	<DIR>	utility	
		0 File(s)	0 bytes	

Directory of E:\For WIN\laba\src\classesandenums

06/05/2022	01:03 AM	<DIR>	.	
06/05/2022	01:03 AM	<DIR>	..	

05/06/2022	12:20 AM	1,296	Coordinates.java
05/06/2022	12:20 AM	350	Country.java
05/06/2022	12:20 AM	346	EColor.java
05/06/2022	12:20 AM	349	HColor.java
05/06/2022	12:21 AM	1,193	Location.java
06/05/2022	01:03 AM	4,958	Person.java
06/04/2022	07:38 PM	833	User.java
	7 File(s)	9,325	bytes

Directory of E:\For WIN\laba\src\commands

06/05/2022	01:22 AM	<DIR>	.
06/05/2022	01:22 AM	<DIR>	..
03/29/2022	05:16 PM		1,086 AbstractCommand.java
06/04/2022	10:42 PM		2,098 AddCommand.java
06/04/2022	10:42 PM		2,175 AddIfMinCommand.java
06/04/2022	10:42 PM		665 ClearCommand.java
05/06/2022	12:35 AM		148 Command.java
05/06/2022	12:35 AM		1,504 ExecuteScriptCommand.java
05/06/2022	12:35 AM		327 ExitCommand.java
05/06/2022	12:35 AM		1,263 FilterStartsWithNameCommand.java
05/06/2022	12:35 AM		586 GroupCountingByIdCommand.java
05/06/2022	12:35 AM		607 HelpCommand.java
05/06/2022	12:35 AM		2,020 InfoCommand.java
05/06/2022	12:35 AM		1,255 PrintUniqueLocationCommand.java
06/04/2022	10:53 PM		2,267 RemoveByIdCommand.java
06/05/2022	01:22 AM		2,766 RemoveGreaterCommand.java
06/05/2022	01:22 AM		2,772 RemoveLowerCommand.java
06/05/2022	12:26 AM		533 ShowCommand.java
06/05/2022	12:27 AM		4,479 UpdateCommand.java
	17 File(s)		26,551 bytes

Directory of E:\For WIN\laba\src\DatabaseWorkers

06/05/2022	05:09 PM	<DIR>	.
06/05/2022	05:09 PM	<DIR>	..
06/05/2022	05:04 PM		2,881 AuthorizationHelper.java
06/05/2022	12:50 AM		22,316 DataBaseCollectionManager.java
06/04/2022	07:04 PM		6,441 DataBaseHandler.java
06/05/2022	12:50 AM		6,985 DataBaseUserManager.java
06/05/2022	05:09 PM		3,494 PropHelper.java
	5 File(s)		42,117 bytes

Directory of E:\For WIN\laba\src\exceptions

06/04/2022	10:53 PM	<DIR>	.
06/04/2022	10:53 PM	<DIR>	..
05/03/2022	12:00 PM		81 CantBeNumberException.java
03/25/2022	10:02 PM		86 CollectionIsEmptyException.java
06/04/2022	05:48 PM		82 DatabaseHandlingException.java

```

05/06/2022  12:31 AM                91
IncorrectInputInScriptException.java
03/23/2022  11:10 AM                83 MustBeNotEmptyException.java
03/23/2022  11:10 AM                88
NotInDeclaredLimitsException.java
03/25/2022  10:02 PM                83 PersonNotFoundException.java
03/25/2022  10:02 PM                84 ScriptRecursionException.java
06/04/2022  10:53 PM                79 UserAccessException.java
03/24/2022  12:51 PM                90
WrongAmountOfElementsException.java
                10 File(s)                847 bytes

```

Directory of E:\For WIN\laba\src\main

```

06/05/2022  05:10 PM    <DIR>        .
06/05/2022  05:10 PM    <DIR>        ..
06/05/2022  05:10 PM                1,922 Proga.java
                1 File(s)                1,922 bytes

```

Directory of E:\For WIN\laba\src\META-INF

```

05/13/2022  11:21 PM    <DIR>        .
05/13/2022  11:21 PM    <DIR>        ..
06/05/2022  05:06 PM                49 MANIFEST.MF
                1 File(s)                49 bytes

```

Directory of E:\For WIN\laba\src\utility

```

06/05/2022  03:23 AM    <DIR>        .
06/05/2022  03:23 AM    <DIR>        ..
06/05/2022  03:23 AM                8,711 CollectionManager.java
06/04/2022  10:42 PM                2,209 CommandManager.java
05/06/2022  12:35 AM                621 Console.java
05/06/2022  12:35 AM                1,380 FileReaderForScript.java
05/06/2022  12:35 AM                19,094 QuestionAboutPerson.java
                5 File(s)                32,015 bytes

```

Total Files Listed:

```

                52 File(s)                1,190,493 bytes
                29 Dir(s)  25,023,107,072 bytes free

```

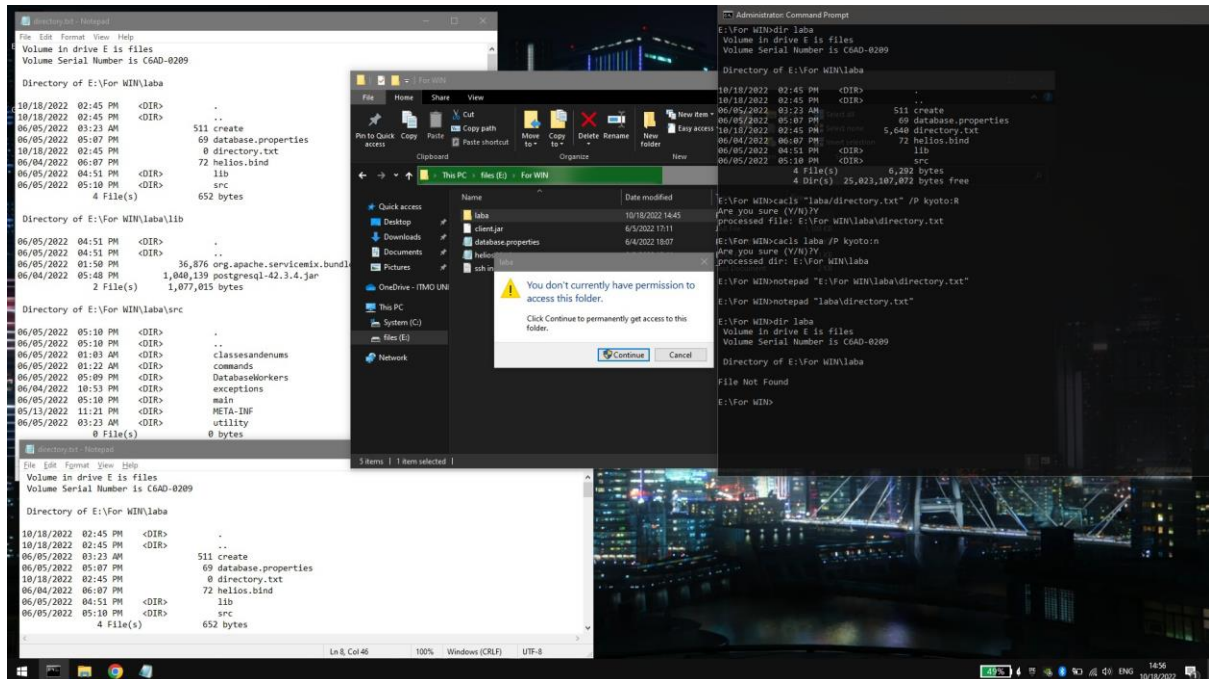
Проверка правил:

1.

Разрешения, установленные на файл, играют более важную роль при определении типа доступа пользователя, чем разрешения на папку. Если пользователю установлено разрешение No Access для папки C:\NOACCESS,

а на содержащийся в этой папке файл README.TXT -разрешение Read, он все же сможет прочитать этот файл, если при обращении к нему укажет полное имя.

Например, он сможет открыть файл в NOTEPAD командой:NOTEPAD C:\NOACCESS\README.TXT



2.

Разрешения, установленные для пользователя, складываются (аккумулируются) с разрешениями, установленными для групп, к которым он принадлежит.

Например, если на доступ к какому-либо файлу для пользователя установлено разрешение Read, а для группы Everyone - разрешение Change, пользователь сможет изменить содержимое файла или удалить его, поскольку он всегда входит в эту группу.

Из этого правила есть исключение - ситуация, при которой одним из установленных полномочий доступа является No Access; и не важно, кому именно это разрешено - пользователю или группе.

No Access всегда имеет приоритет, пользователь не сможет получить доступа к файлу или папке.

```
Administrator: Command Prompt
E:\For WIN>caccls laba\directory.txt /P kyoto:R
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\directory.txt
E:\For WIN>echo 123 > laba\directory.txt
Access is denied.
E:\For WIN>caccls laba\directory.txt /G Bce:C
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\directory.txt
E:\For WIN>echo rewriting > laba\directory.txt
E:\For WIN>more < laba\directory.txt
rewriting
E:\For WIN>caccls laba\directory.txt /P kyoto:N
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\directory.txt
E:\For WIN>echo rerewriting > laba\directory.txt
Access is denied.
E:\For WIN>more < laba\directory.txt
Access is denied.
E:\For WIN>
```

3.

Пользователи, имеющие разрешение Full Control на папку, могут удалять файлы в этой папке независимо от разрешений, установленных на файл (даже если разрешение на файл – No Access). Это следствие того, что NTFS разработана как система, удовлетворяющая стандарту POSIX. 1. Чтобы решить эту проблему (если полный набор полномочий доступа к папке действительно необходим), надо установить для папки специальный тип доступа, включающий все индивидуальные разрешения R, W, X, D, P и O. При этом пользователи получают тот же набор разрешенных действий, что и при разрешении Full Control, но теряют возможность несанкционированного удаления файлов в этой папке.

Administrator: Command Prompt

```
E:\For WIN>cacls "E:\For WIN\laba\directory.txt" /P kyoto:N
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\directory.txt
```

```
E:\For WIN>cacls "E:\For WIN\laba\directory.txt" /P Bce:N
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\directory.txt
```

```
E:\For WIN>cacls "laba" /P kyoto:F
Are you sure (Y/N)?Y
processed dir: E:\For WIN\laba
```

```
E:\For WIN>dir laba
Volume in drive E is files
Volume Serial Number is C6AD-0209
```

Directory of E:\For WIN\laba

```
10/18/2022 02:45 PM <DIR> .
10/18/2022 02:45 PM <DIR> ..
06/05/2022 03:23 AM 511 create
06/05/2022 05:07 PM 69 database.properties
10/18/2022 09:09 PM 14 directory.txt
06/04/2022 06:07 PM 72 helios.bind
06/05/2022 04:51 PM <DIR> lib
06/05/2022 05:10 PM <DIR> src
4 File(s) 666 bytes
4 Dir(s) 25,023,107,072 bytes free
```

```
E:\For WIN>del laba\directory.txt
Invalid switch - "directory.txt".
```

```
E:\For WIN>del laba\directory.txt
```

```
E:\For WIN>dir laba
Volume in drive E is files
Volume Serial Number is C6AD-0209
```

Directory of E:\For WIN\laba

```
10/18/2022 09:16 PM <DIR> .
10/18/2022 09:16 PM <DIR> ..
06/05/2022 03:23 AM 511 create
06/05/2022 05:07 PM 69 database.properties
06/04/2022 06:07 PM 72 helios.bind
06/05/2022 04:51 PM <DIR> lib
06/05/2022 05:10 PM <DIR> src
3 File(s) 652 bytes
4 Dir(s) 25,023,111,168 bytes free
```

```
E:\For WIN>
```

```

C:\ Select Administrator: Command Prompt

E:\For WIN>caccls laba /P kyoto:N
Are you sure (Y/N)?Y
processed dir: E:\For WIN\laba

E:\For WIN>dir laba
Volume in drive E is files
Volume Serial Number is C6AD-0209

Directory of E:\For WIN\laba

File Not Found

E:\For WIN>caccls laba /G kyoto:R
Are you sure (Y/N)?Y
processed dir: E:\For WIN\laba

E:\For WIN>caccls laba /G kyoto:W
Are you sure (Y/N)?Y
processed dir: E:\For WIN\laba

E:\For WIN>caccls laba /G kyoto:C
Are you sure (Y/N)?Y
processed dir: E:\For WIN\laba

E:\For WIN>dir laba
Volume in drive E is files
Volume Serial Number is C6AD-0209

Directory of E:\For WIN\laba

10/18/2022  09:16 PM    <DIR>      .
10/18/2022  09:16 PM    <DIR>      ..
06/05/2022  03:23 AM             511 create
06/05/2022  05:07 PM             69 database.properties
06/04/2022  06:07 PM             72 helios.bind
06/05/2022  04:51 PM    <DIR>      lib
06/05/2022  05:10 PM    <DIR>      src
               3 File(s)             652 bytes
               4 Dir(s)  25,023,111,168 bytes free

E:\For WIN>del laba/create
Invalid switch - "create".

E:\For WIN>del laba\create
E:\For WIN>laba\create
Access is denied.

E:\For WIN>
```

4.

Пользователь, создающий папку или файл на разделах с NTFS, становится владельцем созданного объекта. Кроме того, владельцем папки или файла может стать любой пользователь, обладающий стандартным разрешением Full Control или специальным разрешением Take Ownership.

Владелец всегда имеет возможность прочитать информацию о разрешениях на доступ к папке или файлу и изменить их, даже если ему ничего не разрешено или установлено разрешение No Access.

```
Select Administrator: Command Prompt
E:\For WIN\laba>mkdir newdir1
E:\For WIN\laba>mkdir newdir2
E:\For WIN\laba>type nul > file1
E:\For WIN\laba>type nul > file2
E:\For WIN\laba>takeown /f newdir1
SUCCESS: The file (or folder): "E:\For WIN\laba\newdir1" now owned by user "HOME-PC\kyoto".
E:\For WIN\laba>takeown /f file1
SUCCESS: The file (or folder): "E:\For WIN\laba\file1" now owned by user "HOME-PC\kyoto".
E:\For WIN\laba>cacls newdir1 /P kyoto:N
Are you sure (Y/N)?Y
processed dir: E:\For WIN\laba\newdir1
E:\For WIN\laba>cacls file1 /P kyoto:N
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\file1
E:\For WIN\laba>cacls newdir2 /P Администраторы:N
Are you sure (Y/N)?Y
processed dir: E:\For WIN\laba\newdir2
E:\For WIN\laba>cacls file2 /P Администраторы:N
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\file2
E:\For WIN\laba>dir /q /ad
Volume in drive E is files
Volume Serial Number is C6AD-0209

Directory of E:\For WIN\laba

10/18/2022  11:43 PM    <DIR>          BUILTIN\Администраторы .
10/18/2022  11:43 PM    <DIR>          BUILTIN\Администраторы ..
06/05/2022  04:51 PM    <DIR>          BUILTIN\Администраторы lib
10/18/2022  11:43 PM    <DIR>          HOME-PC\kyoto      newdir1
10/18/2022  11:43 PM    <DIR>          BUILTIN\Администраторы newdir2
06/05/2022  05:10 PM    <DIR>          BUILTIN\Администраторы src
               0 File(s)                0 bytes
               6 Dir(s)  25,023,111,168 bytes free
```

```
Select Administrator: Command Prompt

E:\For WIN\laba>caccls newdir1
E:\For WIN\laba\newdir1 HOME-PC\kyoto:(OI)(CI)N

E:\For WIN\laba>caccls newdir2
E:\For WIN\laba\newdir2 BUILTIN\Администраторы:(OI)(CI)N

E:\For WIN\laba>caccls file1
E:\For WIN\laba\file1 HOME-PC\kyoto:N

E:\For WIN\laba>caccls file2
E:\For WIN\laba\file2 BUILTIN\Администраторы:N

E:\For WIN\laba>caccls file1 /P kyoto:F
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\file1

E:\For WIN\laba>caccls file2 /P Администраторы:F
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\file2
```

Кроме того, владельцем папки или файла может стать любой пользователь, обладающий стандартным разрешением Full Control или специальным разрешением Take Ownership

```
Administrator: Command Prompt

E:\For WIN\laba>icaccls file1 /SETOWNER infobez
processed file: file1
Successfully processed 1 files; Failed processing 0 files

E:\For WIN\laba>dir /q file1
Volume in drive E is files
Volume Serial Number is C6AD-0209

Directory of E:\For WIN\laba

10/18/2022  11:43 PM                0 HOME-PC\infobez      file1
               1 File(s)                  0 bytes
               0 Dir(s) 24,754,675,712 bytes free

E:\For WIN\laba>caccls file1 /P infobez:N
Are you sure (Y/N)?Y
processed file: E:\For WIN\laba\file1

E:\For WIN\laba>
```

```
Выбрать Командная строка
E:\For WIN>dir /q laba\file1
Том в устройстве E имеет метку files
Серийный номер тома: C6AD-0209

Содержимое папки E:\For WIN\laba

18.10.2022  23:43                0 HOME-PC\infobez      file1
              1 файлов                0 байт
              0 папок  24 754 675 712 байт свободно

E:\For WIN>caccls laba\file1
E:\For WIN\laba\file1 HOME-PC\infobez:N

E:\For WIN>caccls laba\file1 /P infobez:F
Вы уверены? [Y(да)/N(нет)]Y
обработан файл: E:\For WIN\laba\file1

E:\For WIN>caccls laba\file1
E:\For WIN\laba\file1 HOME-PC\infobez:F

E:\For WIN>
```

Доп задание:

CACLS.EXE

Заменить разрешения для всех файлов *.exe (должны присутств. в иерархии созданных каталогов) со stud (Full Access) на Администратор (Full Access).

[Не добавит права для польз. Администратор, а заменить права stud на права Администратор, после операции в списке доступа stud быть не должно.]

Проверить возможность доступа к файлам *.exe

```
Select Administrator: Command Prompt

E:\Downloads\Stray>caccls Stray.exe
E:\Downloads\Stray\Stray.exe HOME-PC\kyoto:F

E:\Downloads\Stray>caccls Stray.exe /E /R kyoto
processed file: E:\Downloads\Stray\Stray.exe

E:\Downloads\Stray>caccls Stray.exe /G Администраторы:F
Are you sure (Y/N)?Y
processed file: E:\Downloads\Stray\Stray.exe

E:\Downloads\Stray>caccls Stray.exe
E:\Downloads\Stray\Stray.exe BUILTIN\Администраторы:F

E:\Downloads\Stray>Stray.exe

E:\Downloads\Stray>
```