

АКЦИОНЕРНОЕ ОБЩЕСТВО «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ» (АО «ПМ»)

БАЗА ДАННЫХ СИГНАТУРНЫХ ПРАВИЛ ОБНАРУЖЕНИЯ АТАК AM RULES

Инструкция по установке баз данных сигнатур правил обнаружения атак AM Rules на примере ViPNet IDS NS 3.7

На 22 листах

Москва 2023

Аннотация

Настоящий документ является инструкцией по установке Базы данных сигнатурных правил обнаружения атак AM Rules (далее - БРП).

БРП существуют во множестве вариантов в зависимости от системы защиты информации (далее - СЗИ), для которой они предназначены. Данная инструкция описывает процесс ручной установки БРП на систему обнаружения вторжений ViPNet IDS NS 3.7. Установка на другие системы линейки ViPNet IDS NS производится в аналогичном порядке.

СОДЕРЖАНИЕ

Π	ЕРЕЧЕНЬ СОКРАЩЕНИЙ	.4
1	Общие сведения	.5
2	Инструкция по развертыванию ViPNet IDS NS 3.7 VA	.6
	2.1 Инструкция по развертыванию виртуальной машины ViPNet ID)S
	NS 3.7 VA	.6
	2.2 Инструкция по первичной аутентификации в ViPNet IDS NS 3	.7
	VA1	10
	2.3 Инструкция по установке и активации лицензии	13
3	Инструкция по установке БРП	20
4	Инструкция по установке AM Ruleset Analyzer	22

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

AO «ПМ»	Акционерное общество «Перспективный мониторинг»
БРП	База данных сигнатурных правил обнаружения атак AM Rules
СЗИ	Система защиты информации
ИБ	Информационная безопасность

1 Общие сведения

Основным направлением деятельности АО «ПМ» является оценка практической защищенности информационных систем, выявление их уязвимостей при помощи средств инструментального и ручного анализа, реагирование на инциденты безопасности, разработка Программного комплекса автоматизированного поиска, обработки и визуализации данных из открытых источников «Тардис» и Программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire».

БРП предназначена для конфигурирования СЗИ для эффективного обнаружения компьютерных атак и других событий ИБ (далее - События). БРП предоставляет инструкции (далее - Правила), на основе которых СЗИ создает внутреннюю логику обнаружения, а также конфигурационные файлы. События могут быть просмотрены в интерфейсе СЗИ, экспортированы или автоматически отправлены на внешние обработчики.

5

2 Инструкция по развертыванию ViPNet IDS NS 3.7 VA

Порядок подготовки ViPNet IDS NS VA:

 установить компьютер, предназначенный для установки платформы виртуализации;

подключить компьютер к сети переменного тока напряжением
 220 В;

 подключить выбранный сетевой интерфейс компьютера коммутационным кабелем к сетевому оборудованию сегмента локальной сети;

 установить на компьютер одну из поддерживаемых платформ виртуализации, в соответствии с документацией производителя;

– если ViPNet IDS NS VA предназначен для анализа трафика в физической сети, подключить выбранный сетевой интерфейс компьютера с установленной платформой виртуализации коммутационным кабелем к сетевому адаптеру устройства дублирования трафика;

подготовить на платформе виртуализации виртуальную машину
 ViPNet IDS NS VA (см. подраздел 2.1);

– активировать лицензию для ViPNet IDS NS VA;

– установить Базу решающих правил.

2.1 Инструкция по развертыванию виртуальной машины ViPNet IDS NS 3.7 VA

На платформах виртуализации Oracle VM VirtualBox, VMware Workstation Pro и VMware vSphere ESXi виртуальная машина ViPNet IDS NS VA импортируется из образа ПО ViPNet IDS NS в формате OVA. Описание развертывания виртуальной машины ViPNet IDS NS VA приведено на примере аппаратной платформы виртуализации VMware vSphere ESXi. Предполагается, что в сети уже развернут сервер VMware vCenter Server, а к нему настроено подключение клиента vSphere Client.

6

Для развертывания потребуется файл с образом ПО ViPNet IDS NS в формате OVA - ids-ns-va-3.7.0-[Номер сборки].оva из комплекта поставки.

Порядок развертывания образа ViPNet IDS NS VA и настройки интерфейсов захвата трафика:

– запустить клиент vSphere Client и подключиться к серверу VMware vCenter Server;

в главном окне vSphere Client в меню «File» выбрать Deploy OVF
 Template и следовать указаниям мастера (Рисунок 1);

Deploy OVF Template	_		×
Source Select the source location.			
Source OVF Template Details Name and Location	Deploy from a file or URL D:\VM\IDS-NS-VA-3. 1.0-413063.ova Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.		
	≤ Back Next ≥	Ca	ncel

Рисунок 1 – Выбор файла с образом виртуальной машины

– на шаге «Source» нажать «Browse», выбрать файл формата OVA с образом виртуальной машины ViPNet IDS NS VA;

– на шаге «OVF Template Details» ознакомиться с параметрами виртуальной машины;

– на шаге «Name and Location» в поле «Name» указать имя виртуальной машины, выбрать каталог ее расположения;

– на шаге «Resource Pool» выбрать пул ресурсов, который определяет объем оперативной памяти и процессор, предоставляемый для виртуальной машины;

– на шаге «Storage» указать раздел или твердотельный накопитель из выбранного пула ресурсов, на котором будут храниться файлы виртуальной машины (Рисунок 2);

🕝 Deploy OVF Template				_		×
Disk Format In which format do you v	want to store the virtual disks?					
Source OVF Template Details	Datastore:	QCM1				
Name and Location Host / Cluster	Available space (GB):	3368,1				
Resource Pool Storage	C Thick Provision Lazy 2	Zeroed				
Disk Format	C Thick Provision Eager	Zeroed				
Network Mapping Ready to Complete	Thin Provision					
			< Back	Next >	Car	icel

Рисунок 2 – Выбор типа жесткого диска

– на шаге «Disk Format» выбрать тип жесткого диска «Thin Provision»;

– на шаге «Network Mapping» выбрать имя сети подключения с типом Bridged для управляющего сетевого интерфейса;

– на шаге «Ready to Complete» проверить настройки виртуальной машины и нажать «Finish»;

 дождаться завершения процесса развертывания виртуальной машины.

Чтобы настроить сетевой интерфейс виртуальной машины для захвата трафика из виртуальной сети: в настройках виртуальной машины для одного или нескольких (в зависимости от количества виртуальных сетей) сетевых адаптеров, назначенных в качестве интерфейсов захвата, выбрать в качестве сети подключения существующую виртуальную сеть.

Для этого:

– на панели навигации вызвать контекстное меню созданной виртуальной машины и выбрать «Edit Settings»;

8

– в окне «Virtual Machine Properties» на вкладке «Hardware» выбрать сетевой адаптер, назначенный для захвата трафика, а в списке «Network Connection» выбрать имя виртуальной сети (Рисунок 3).

IDS_TEST - Virtual Machine Prop	perties	
Hardware Options Resources		Virtual Machine Version: 8
Show All Devices	Add Remove	Device Status Connected
Hardware	Summary	Connect at power on
 Memory CPUs Video card VMCI device USB controller Hard disk 1 Network adapter 1 Network adapter 2 Network adapter 3 Network adapter 4 	2048 MB 2 Video card Restricted Present Virtual Disk VM Network VM Network VM Network VM Network 2	Adapter Type Current adapter: Flexible MAC Address 00:0c:29:c2:4d:d8 Image: Automatic Image: Manual DirectPath I/O Status: Not supported Network Connection Network label: VM Network 2 VM Network 2
Help		OK Cancel

Рисунок 3 – Подключение интерфейса захвата виртуальной машины к виртуальной сети

В свойствах виртуального коммутатора для каждой виртуальной сети, трафик которой необходимо анализировать, включить режим, позволяющий принимать все пакеты, независимо от того, кому они предназначены.

Для этого:

– перейти на вкладку «Configuration»;

– выбрать виртуальный коммутатор и нажать «Properties» (Рисунок 4);

– в окне Properties перейти на вкладку «Security» и в списке «Promiscuous Mode» выбрать «Accept» (Рисунок 5).

G C Home > 3 1	nventory 👂 🎁 Inventory				
IDS_TEST	Getting Started Summary Virtual View: vSphere Standard Switch Networking	, 5.5.0, 1623387 Evaluation (60 days remaining) Machines Resource Allocation Performance Configurat			
	Standard Switch: vSwitch0 Virtual Machine Port Group VM Network 2 I virtual machine(s) IDS_TEST	Physical Adapters			

Рисунок 4 – Просмотр свойств созданного виртуального коммутатора

General Security Traffic Shaping	IIC Teaming	
Policy Exceptions		
Promiscuous Mode:	Accept	•
MAC Address Changes:	Accept	▼
Forged Transmits:	Accept	▼
	OK	Cancel Help

Рисунок 5 – Включение режима Promiscuous mode

2.2 Инструкция по первичной аутентификации в ViPNet IDS NS

3.7 VA

Порядок подключения к веб-интерфейсу ViPNet IDS NS:

– запустить на терминале управления веб-браузер;

– в адресной строке веб-браузера ввести: https://[Адрес], где [Адрес]

- адрес доступа (IP-адрес или доменное имя) управляющего интерфейса ViPNet IDS NS;

пройти аутентификацию в системе обнаружения вторжений
 ViPNet IDS NS 3.7 (Рисунок 6);

◆ V/PNet IDS NS VA 875067516 - \ × +		~	-	a ×
← → C ▲ He защищено https://10.0.24.115/#monitoring		iê ☆	* 1	
		⊕ ~	0	
Amy ami Report	writel annon			
	© 2020, AO -WeiфoTeKC+			

Рисунок 6 – Аутентификация в системе

– в соответствующих полях ввести имя и пароль учетной записи. При первом подключении к веб-интерфейсу для аутентификации ввести данные встроенной учетной записи главного администратора: имя по умолчанию - admin, пароль по умолчанию - vipnet;

– нажать «Войти»;

– при первом подключении к веб-интерфейсу после успешной авторизации сменить пароль встроенной учетной записи главного администратора, заданный по умолчанию. Для этого в окне «Смена пароля» задать новый пароль самостоятельно или нажать «Сгенерировать» для выработки случайного пароля. Для подтверждения ввести новый пароль повторно и нажать Изменить (Рисунок 7).

11

Смена пароля		
Новый пароль		
	۲	Сгенерировать
 Латинские буквы Цифры Не содержит другие символы Подтверждение пароля 	 Один и тот же символ не д встречаться более трех ра Длина пароля должна быт символов 	цолжен аз подряд гь не менее 12
		۲
	Изменить	Отмена

Рисунок 7 – Смена пароля

2.3 Инструкция по установке и активации лицензии

В боковом разделе «Инфопанель» выбрать пункт «О программе» (Рисунок 8).

😻 ViPNet IDS NS VA 875067516 - И 🗙 🕂					~ - ø ×
← → С ▲ Не защищено <u>https://</u>	10.0.24.115/#monitoring				🗠 🖈 🖪 💶 👖
ViPNet IDS NS					🛍 Administrator 🗸 🌐 🖌 🕐
=	Инфопанель				
Мониторинг					
🔀 Инфопанель	Состояние сенсора	Производительность	Счётчик событий		
ГЗ События		• Загрузка ЦПУ 0%	За день За месяц	За год Всего	
Управление		 Использование ОЗУ Отери пакетов О% 	Общее количество:	20 480 574	
🔀 Сетевое окружение		 Трафик, Мбит/сек 0.000 	По уровням важности: Высокий	10 546 571	
🗙 Методы анализа			Средний Низкий	5 036 369 4 896 589	
Ф Оповещение			Информационный	1 045	
🛞 Интеграция					
Система					
🖵 Сетевые настройки				لم	
🔇 Дата и время					
💼 Учетные записи					
Э Резервное копирование					
💐 Сервисные функции					
Аудит					
🔲 Журнал аудита					
					19:49:22 25:08:2022

Рисунок 8 – Установка и активация лицензии

В открывшемся окне выбрать пункт «Установить лицензию» (Рисунок 9).

✤ ViPNet IDS NS VA 875067516 - 1 × +						~	- o ×
← → С 🔺 Не защищено Мёрк//	10.0.24.115/#monitoring					匠 🏠	* 🛛 🕕 🗉
ViPNet IDS NS						🙆 Administrator 🛩	0 * @
=	Инфопанель						
манизорние							
ВВ Инфолленти	Состояние сенсора	VIPNet IDS NS	×	событий			
P3 Codernes		Версия	_				
Yeghinosom		© 2020, АО «ИНФОТЕКС»			20 480 574		
Сетавое окружания		По всем возникающим вопросам обращайтесь в компанию ИнфоТеКС.					
😪 Merrapa asameta		Be6-cairt: www.infotecs.ru E-mail: soft@infotecs.ru					
да окелецияние		Телефон для регионов России: В 800 250-0-260	1				
(b) spearstanting		Телефон для Москвы: +7 495 737-61-92					
Cilcium		ИНФОРМАЦИЯ О ЛИЦЕНЗИИ					
P Сетения настройки		Лицензия не установлена					
🔇 Дата и преми		Лицензия не активирована					
😂 Учетные записи							
(3) Резераное копирование							
🖏 Сервисные функция							
hear.							
n							
C without states							
		Установить лиц	цензию				
	1					< 10.5	0/16 25.08/2022

Рисунок 9 – Установка и активация лицензии

В диалоговом окне «Загрузка файла» нажать на иконку папки, чтобы выбрать файл лицензии (Рисунок 10).

* V/PNet IDS NS VA 875057516 - F × +					~	- a ×
← → С ▲ Не защищено https://	10.0.24.115/#monitoring				B \$	* 🗆 🛈 :
VIPNet IDS NS					Administrator 🛩	⊕ • Ø
	Инфопанель					
Monsrephie						
ЕЭ Мефоланиза	Состояние сенсора	Производительность		Счётчик событий		
Coduction	 Reprint Galasi mpanian or 25.08.2022 Airmenio 31080 npabio isa 31115 					
🔛 Отчаты	 Malware detection annovaer Bepose Obser Malware detection 5493 or 03.08.2022 	• Использование 03У				
Vopbilineee	 Отключен анализ IP-панотов, зацифрованнок с пожланию ПО VIPNet 	 Потери пакетов Трафик, Мбит/сек 	0% 92.979			
😥 Сатевое окрумение	 Включен заристический внализ 	100%	A	Средний		
🙊 Методы вналива	Загруз	ка файла		Х плониелії		
ј Правила внализа						
45 Quonemission	Выберит	е файл с лицензией в формате ITCSLIC или	TOZ.			
 Musubation 	The gas	via e populare roz gorikno navenaroch co s	JUSS NUTION .	~		
Састима	Empobu	те фанл		8		
🖵 сетевые настройки						
🕚 дата и время			Sarpyaims C	Этмена		
🙆 Учитные записи						
О Реперанов коптрования						
😵 соринских функции						
Augur:						
C Hypnan aygarra						
					10.5	1.1.6. 25.06.2022

Рисунок 10 – Установка и активация лицензии

Далее с помощью диалогового окна операционной системы загрузить файл лицензии (Рисунок 11).

	· · · · · · · · ·	IDD (D.) 7 LESE		~		CKI LESL
рядочить 🔻	Новая папка					EE 👻 🛄
л Имя	/	N	Дата изменения	Тип	Размер	
	ense_2694808-1-1-IDSNS_2	0.04.2022_2694827-1.itcslic	02.06.2023 13:08	Файл "ITCSLIC"	2 КБ	
Э						
• ~						

Рисунок 11 – Выбор файла лицензии

После чего в боковом разделе «Инфопанель» в блоке «Состояние сенсора» нажать «Активировать» (Рисунок 12).

		Сенсор остановлен. Лиценаия не активирована		
😵 ViPNet IDS NS				🛍 Administrator 🗸 🌐 🖌 🕐
	Инфопанель			
🛃 Инфопанель	Состояние сенсора	Производительность	Счётчик событий	
🛱 События	• Лицензия не активирована Активировать	• Загрузка ЦПУ 10% • Использование 03У 18%	За день За месяц За год Всего	
Управление	• Остановлен сервис сенсора	• Потери пакетов 0%	Общее количество: 0	
🔀 Сетевое окружение	• Самотестирование завершено с Показать	 Трафик, Мбит/сек 0.000 	По уровням важности: Высокий 0	
🕀 Методы анализа	ошибкой.	100%	Средний 0	
🗭 Оповещение	 Отключен анализ IP-пакетов, зашифрованных с помощью ПО ViPNet 		Низкий U Информационный 0	
🛞 Интеграция	• Включен эвристический анализ			
Система		10 MBert/c		
🖵 Сетевые настройки				
🔇 Дата и время				
💼 Учетные записи				
Резервное копирование				
🖏 Сервисные функции				
Аудит				
🚺 Журнал аудита				

Рисунок 12 – Окно инфопанели с кнопкой «Активировать»

После нажатия кнопки «Активировать» пользователю будет предложено

ознакомиться и принять лицензионное соглашение (Рисунок 13).

/iPNet IDS NS
ИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ НА ИСПОЛЬЗОВАНИЕ ViPNet IDS NS
еред началом установки, копирования либо иного использования ViPNet IDS NS нимательно ознакомьтесь с условиями использования, содержащимися в настоящем оглашении.
становка, запуск или иное начало использования ViPNet IDS NS означает адлежащее заключение настоящего Соглашения и ваше полное согласие со всеми го условиями. Если вы не согласны безоговорочно принять условия настоящего оглашения, вы не имеете права устанавливать, настраивать и использовать рограмму.
астоящее соглашение заключается между Вами, Конечным пользователем, и АО 1нфоТеКС" (127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, эмната 29) и содержит информацию об авторском праве и объёме еисключительных прав использования ViPNet IDS NS.
спользование ViPNet IDS NS означает Ваше полное и безоговорочное принятие астоящего соглашения и готовность нести ответственность в случае его нарушения в рответствии с нормами законодательства РФ.
случае несогласия с изложенными ниже условиями, соглашение считается езаключенным, и Вы не вправе использовать ViPNet IDS NS.
1. Определение понятий
Программа для ЭВМ (программное обеспечение, ПО) – представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других технических устройств в целях получения определенного результата, а также эксплуатационная документация, предоставляемая в печатном и в электронном виде.
 Я прочитал и полностью принимаю лицензионное соглашение Принять Отклонить

Рисунок 13- Лицензионное соглашение с конечным пользователем

В случае, если ViPNet IDS NS развёрнут без доступа в Интернет, а у терминала управления доступ в Интернет настроен, активация возможна по электронной почте. Для этого необходимо выбрать «Запросить активацию по e-mail» в окне активации лицензии (Рисунок 14).

Чтобы получить доступ к функционалу ViPNet IDS NS, необходимо активировать лицензию. Активация подтверждает подлинность продукта ViPNet IDS NS на компьютере и тот факт, что он не установлен на большем числе компьютеров по сравнению с тем, которое разрешено условиями лицензионного соглашения. Активируйте лицензию через Интернет, если компьютер имеет доступ к сети. Если доступ в Интернет ограничен, вы можете воспользоваться возможностью активации лицензии по E-mail. В ответном письме вы получите код активации, который нужно ввести в поле ниже. Активировать через Интернет Запросить активацию по E-mail Сформировать текст запроса Ключ продукта 8XQ8-8GMN-WWG9-XG68 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активировать лицензию Активировать лицензию Закрыть Мактивации Активации	ия лицензии ViPNet IDS NS			
Чтобы получить доступ к функционалу ViPNet IDS NS, необходимо активировать лицензию. Активация подтверждает подлинность продукта ViPNet IDS NS на компьютере и тот факт, что он не установлен на большем числе компьютеров по сравнению с тем, которое разрешено условиями лицензионного соглашения. Активируйте лицензию через Интернет, если компьютер имеет доступ к сети. Если доступ в Интернет ограничен, вы можете воспользоваться возможностью активации лицензии по E-mail. В ответном письме вы получите код активации, который нужно ввести в поле ниже. Активировать через Интернет Запросить активацию по E-mail Сформировать текст запроса Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Закрыть	gusevatelcandr@infateca-		guaevalessendriĝinfolaca-nt 2023 06 28 17 33	
активиции под ворждает подлитносто продлита чи чество чо по компьютерси и тот факт, что от не установлен на большем числе компьютеров по сравнению с тем, которое разрешено условиями лицензионного соглашения. Активируйте лицензию через Интернет, если компьютер имеет доступ к сети. Если доступ в Интернет ограничен, вы можете воспользоваться возможностью активации лицензии по E-mail. В ответном письме вы получите код активации, который нужно ввести в поле ниже. Активировать через Интернет Запросить активацию по E-mail Сформировать текст запроса Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активации	улучить доступ к функционалу ViF ия полтверждает поллинность пр	Net IDS NS, необходимо ан иликта ViPNet IDS NS на ко	тивировать лицензию. мпьютере и тот факт, ито он не установлен на	
Активируйте лицензию через Интернет, если компьютер имеет доступ к сети. Если доступ в Интернет ограничен, вы можете воспользоваться возможностью активации лицензии по E-mail. В ответном письме вы получите код активации, который нужно ввести в поле ниже. Активировать через Интернет Запросить активацию по E-mail Сформировать текст запроса Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активировать лицензию	числе компьютеров по сравнени	ю с тем, которое разреше	ю условиями лицензионного соглашения.	
Активируите лицензию через интернет, если компьютер имеет доступ к сети. Если доступ в Интернет ограничен, вы можете воспользоваться возможностью активации лицензии по E-mail. В ответном письме вы получите код активации, который нужно ввести в поле ниже. Активировать через Интернет Запросить активацию по E-mail Сформировать текст запроса Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активировать лицензию	×	MSK-M0553		
ответном письме вы получите код активации, который нужно ввести в поле ниже. Активировать через Интернет Запросить активацию по E-mail Сформировать текст запроса Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активировать лицензию Активировать лицензию	ите лицензию через интернет, ес туп в Интернет ограничен, вы мо:	и компьютер имеет дост ете воспользоваться воз	уп к сети. можностью активации лицензии по F-mail. В	
Активировать через Интернет Запросить активацию по E-mail Сформировать текст запроса Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активировать лицензию Закрыть Закрыть	и письме вы получите код актива	ии, который нужно ввест	и в поле ниже.	
Активировать через Интернет Запросить активацию по E-mail Сформировать текст запроса Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активировать лицензию Закрыть Закрыть				
Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активировать лицензию	оовать через Интернет Запро	ить активацию по E-mail	Сформировать текст запроса	
Ключ продукта 8XQ8-8GMN-WWG9-XG68 Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Код активации Активировать лицензию Закрыть Закрыть	gusev.ateksandr@infotecs-		puer valeksend r Christersent	
Код компьютера 4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL Активировать лицензию Закрыть	одукта 8XQ8	3GMN-WWG9-XG68		
Код активации Активировать лицензию Закрыть	њютера 4H34	W4-5B5384K-53SZVNM-7Y	ZQN5X-5GS42PL	
Закрыть		INFOTECS-NI NGC MOSES		
Закрыть	Бации		Активировать лицензию	
Закрыть				
)bITb			
	OTECSANT			

Рисунок 14 – Запросить активацию по E-mail

Далее автоматически откроется выбранное в ОС приложение для работы с электронной почтой (Рисунок 15).

	От 👻		
	Кому	offlinereg2; WORLD of	f-line Registration
оправите	Копия	INFOTECS-MT	
	СК		
	Тема	Регистрация ViPNet	
активации е		мо опправить по адр	ecy <u>reg@infotecs.biz</u> .
Не изменяй	те это письм	мо опправить по адр о.	ecy <u>reg@infotecs.biz</u> .
Не изменяй Локализаци	те это письм я: RUS	мо отправить по адр о.	ecy <u>reg@infotecs.biz</u> .
Не изменяй Локализаци Пользовате	ато необходи іте это письмі ия: RUS ль:	мо отправить по адр о.	ecy <u>reg@infotecs.biz</u> .
Не изменяй Локализаци Пользовате. Организаци	ате это письм ия: RUS ль: ия:	мо отправить по адр о.	ecy <u>reg@infotecs.biz</u> .
Не изменяй Локализаци Пользовате. Организаци Продукт: Vil	iте это письм iя: RUS ль: iя: PNet IDS NS	мо отправить по адр о.	ecy <u>reg@infotecs.biz</u> .
Не изменяй Локализаци Пользовате. Организаци Продукт: Vil Версия: 1	ire это письм iя: RUS ль: iя: PNet IDS NS	мо отправить по адр о.	ecy <u>reg@infotecs.biz</u> .
Не изменяй Локализаци Пользовате Организаци Продукт: Vil Версия: 1 Серийный н	ite это письм iя: RUS ль: iя: PNet IDS NS iomep: 8XQ8-	мо отправить по адр o. -WWG9-XG68	ecy <u>reg@infotecs.biz</u> .
Не изменяй Покализаци Пользовате Организаци Продукт: Vil Версия: 1 Серийный н Код компьк	ire это письми iя: RUS ль: iя: PNet IDS NS iomep: 8XQ8- prepa: 4H342	мо отправить по адр о. -WWG9-XG68 W4-5B5384K-	-7YZQN5X-5GS42PL

Рисунок 15 – Окно шаблона сообщения Microsoft Outlook

Код активации из ответного сообщения необходимо ввести в поле «код активации» и нажать «Активировать лицензию».

В случае наличия доступа к Интернету необходимо выбрать «Активировать через Интернет» (Рисунок 16).

ктивация лицензии ViPNet	IDS NS	
Чтобы получить доступ к функцис Активация подтверждает подлин большем числе компьютеров по (оналу ViPNet IDS NS, необходимо активировать лицензию. ность продукта ViPNet IDS NS на компьютере и тот факт, что он не установлен на сравнению с тем, которое разрешено условиями лицензионного соглашения.	
Активируйте лицензию через Инт	гернет, если компьютер имеет доступ к сети.	
Если доступ в Интернет ограниче ответном письме вы получите ко	н, вы можете воспользоваться возможностью активации лицензии по E-mail. В д активации, который нужно ввести в поле ниже.	
Активировать через Интернет	Запросить активацию по E-mail Сформировать текст запроса	
Ключ продукта	8XQ8-8GMN-WWG9-XG68	
Код компьютера	4H342W4-5B5384K-53SZVNM-7YZQN5X-5GS42PL	
Код активации	Активировать лицензию	

Рисунок 16 – Активация через Интернет

В случае успешной активации лицензии – это будет отражено в разделе «О программе» (Рисунок 17)



Версия 3.7.0-582985 Аппаратная платформа: ViPNet IDS NS VA Имя сенсора: ViPNet IDS NS VA 251530290 © 2020, AO «ИнфоТеКС»

По всем возникающим вопросам обращайтесь в компанию ИнфоТеКС:

Веб-сайт: www.infotecs.ru E-mail: soft@infotecs.ru Телефон для регионов России: 8 800 250-0-260

Телефон для Москвы: +7 495 737-61-92

ИНФОРМАЦИЯ О ЛИЦЕНЗИИ

Идентификатор лицензии	3203978/1/1-IDSNS
Срок действия лицензии	до 20.04.2024
Подписка на обновление правил обнаружения	до 20.04.2024
Подписка на обновление базы Malware detection	до 20.04.2024

> ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

Рисунок 17 – Информация о продукте с активированной лицензией

3 Инструкция по установке БРП

В боковом списке перейти в раздел «Правила анализа», далее в меню «Настройка» выбрать пункт «Обновить базу правил» (Рисунок 18).

😵 VIPNet IDS NS VA 875067516 - 🗆 🗙 🕂			~	- o	×
← → С ▲ Не защищено https://1	0.0.24.115/#rules		ピ ☆	* • •	0 :
📀 ViPNet IDS NS			🖆 Administrator 🗸	🌐 ~	0
=	Правила анализа		Cówana faranana		÷
Мониторинг ВЭ Инфоланоль		Название	оновно озу правил он рузно понозователоска Удалить все правила анали	е правила » за	из файла
ра сооблина Потчеты	□ > Группа:DELETED (0 (10 правил, активировано 10 правил)				
5	Группа: activex () (184 правила, активировано 184 правила)				
Управление	Группа: attack_response () (584 правила, активировано 582 правила)				_
🔀 Сетевое окружение	Группа: current_events () (4817 правил, активировано 4262 правила)				_
😔 Методы анализа	Группа: decoder () (142 правила, активировано 142 правила)				_
↑↑ Правила анализа	🗋 > Группа: dns 🕚 (9397 правил, активировано 1410 правил)				_
🔁 Оповещение	Группа: dos (86 правил, активировано 84 правила)				_
🛞 Интеграция	Группа: drop (6 правил, активировано 6 правил)				
	Группа: exploit (5347 правил, активировано 5257 правил)				_
Система	🗋 > Группа: ftp 🕘 (123 правила, активировано 123 правила)				_
🖵 Сетевые настройки	Группа: info (1545 правил, активировано 1539 правил)				_
🔇 Дата и время	Группа: malware () (2743 правила, активировано 2733 правила)				
💼 Учетные записи	Группа: netbios () (230 правил, активировано 230 правил)				_
О Резервное копирование	Группа: p2p () (90 правил, активировано 88 правил)				
Сервисные функции	Группа: policy (1012 правил, активировано 1006 правил)				
	Группа: preprocessor (294 правила, активировано 264 правила)				
Аудит	Группа: scada () (18 правил, активировано 18 правил)				
🚺 Журнал аудита	Группа: scan () (321 правило, активировано 321 правило)				
	🗋 > Группа: sensitive-data 🕕 (5 правил, активировано 0 правил)				
	Группа: shellcode () (50 правил, активировано 50 правил)				
	Группа: smtp (23 правила, активировано 23 правила)				
	Группа: snmp (13 правил, активировано 13 правил)				
			20:	14:36 21.07	.2022

Рисунок 18 – Обновление баз правил

В диалоговом окне «Загрузка файла» нажать на иконку папки, чтобы выбрать файл обновления БРП (Рисунок 19).

🐡 ViPNet IDS NS			lé	🛾 Administrator ~ 🌐 ~ 🕐
=	Правила анализа			
Мониторинг Ед Инфоланель	с Группир			
F3 Codemen	🔲 🗸 🧭 Правило 🖳			
🕅 Отчеты	> Группа:DELETED (10 правил, акти	вировано 10 правил)		
_	Группа: activex () (184 правила, активир	овано 184 правила)		
Управление	Группа: attack_response () (584 правила	активировано 582 правила)		
🕅 Сетевое окружение	📄 > Группа: current_events 🛞 (4817 правил, а	ктивировано 4262 правила)	_	
🕀 Методы анализа	🔲 > Группа: decoder 🛞 (142 правила, активи	Загрузка файла 🗙 🗙		
* γ * Правила анализа	🔲 > Группа: dns 🕕 (9397 правил, активирова			
🕼 Оповещение	> Группа: dos () (86 правил, активировани	Выберите файл с базой правил в формате TGZ.		
- (C) Muternause	🔲 > Группа: drop 🛞 (6 правил, активировано	Имя файла должно содержать слово "rules".		
Sik muter burden	🔲 > Группа: exploit 🛞 (5347 правил, активир	Выберите файл 🕒		
Система	🔲 > Группа: ftp 📵 (123 правила, активирова			
🖵 Сетевые настройки	Группа: info (1545 правил, активиров.			
Дата и время	🔲 > Группа: malware 🕘 (2743 правила, акти	Загрузить Отмена		
БР Учетные записи	Группа: netbios (230 правил, активира	вано изи правилу		
	🔲 > Группа: p2p 📵 (90 правил, активировани	88 правил)		
	Группа: policy (1012 правил, активирс	вано 1006 правил)		
Сервисные функции	Группа: preprocessor () (294 правила, ак	тивировано 264 правила)		
Аудият	🔲 > Группа: scada 🕘 (18 правил, активирова	но 18 правил)		
🔲 Журнал аудита	🗋 > Группа: scan 📵 (321 правило, активиров	ано 321 правило)		
	🔲 > Группа: sensitive-data 🌒 (5 правил, акти	зировано 0 правил)		
	> Группа: shellcode 🚯 (50 правил, активир	овано 50 правил)		
	> Группа: smtp () (23 правила, активирова	но 23 правила)		
	Группа: snmp () (13 правил, активирова	но 13 правил)		
				20:35:04 21.07.2022

Рисунок 19 – Обновление баз правил

С помощью диалогового окна операционной системы (на примере представлено окно Microsoft Windows 10) загрузить файл (Рисунок 20).



Рисунок 20 – Обновление баз правил

4 Инструкция по установке AM Ruleset Analyzer

AM Ruleset Analyzer не требует установки (является портативным ПО).