НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«КУРЧАТОВСКИЙ ИНСТИТУТ»
Институт физики высоких энергий имени А.А. Логунова
Национального исследовательского центра
«Курчатовский институт»

Препринт 2020–1

Е.И. Галкин

Оптимизация системы распределённой антивирусной защиты организации для ОС Windows на примере ИФВЭ

Протвино 2020

УДК 539.1.074.3 М-24

Аннотация

Галкин Е.И. Оптимизация системы распределённой антивирусной защиты организации для ОС Windows на примере ИФВЭ: Препринт НИЦ «Курчатовский институт» – ИФВЭ 2020–1. – Протвино, 2020. – 17 с., 2 табл., библиогр.: 18.

Работа посвящена актуальной задаче организации защиты компьютеров, работающих под управлением ОС Windows, объединённых в локальные сети организаций или предприятий. Приводится обоснование и описываются преимущества использования с этой целью комплекса программ “Лаборатории Касперского”. Рассматриваются особенности реализации и оптимизации системы распределённой антивирусной защиты компьютеров в локальной сети НИЦ «Курчатовский институт» – ИФВЭ.

Abstract

Galkin E.I. Optimization of distributed anti-virus protection system for Windows by example IHEP: NRC «Kurchatov Institute» – IHEP Preprint 2020–1. – Protvino, 2020. – p. 17, tables 2, refs.: 18.

The work is devoted to the actual task of organizing the protection of computers running Windows, united in local networks of organizations or enterprises. The article provides a justification and describes the advantages of using the Kaspersky Lab software for this purpose. The paper considers the features of implementation and optimization of the distributed anti-virus protection system for computers in the local area network of NRC «Kurchatov Institute» – IHEP.

Введение

В любой организации, в которой используется интернет, существует проблема обеспечения кибербезопасности. С каждым годом растёт статистика попыток заражения программного обеспечения (ПО) вредоносными программами. Наиболее распространёнными в России в 2019 году были шпионские троянские программы, шифровальщики и рекламное ПО [1]. Компьютерам организаций угрожают сетевые и хакерские атаки, фишинговые письма, разнообразные трояны и вирусы, использующие уязвимости в системном и прикладном ПО и веб-уязвимости, а также черви, боты, руткиты и т.п.

Поскольку компьютеры под управлением различных версий Windows вот уже много лет удерживают уверенное лидерство среди пользователей во всём мире (75-90% всех ПК) [2], именно ОС Windows является главной мишенью для создателей вредоносного ПО. В России доля Windows на рынке персональных компьютеров ещё выше, чем в остальном мире. Следовательно, защита Windows-систем от вредоносного ПО приобретает особую актуальность.

Угрозы часто возникают из-за ошибок операционных систем, которые после их обнаружения становятся уязвимостями. Таким образом, своевременное обновление компонент ОС с уязвимостями становится одной из важных задач комплексной защиты. В Windows такие обновления обычно называются обновлениями безопасности. То же самое относится и к популярному ПО других производителей, ошибки в котором приводят к уязвимостям [3].

Для организации надёжной системы распределённой антивирусной защиты Windows-устройств организации требуется специализированное программное обеспечение. Конечные пользователи, которые, как правило, не являются специалистами

по защите данных, должны быть максимально освобождены от задач по организации и текущему обслуживанию антивирусного ПО. Желательно, чтобы контроль за своевременным обновлением антивирусных баз данных, периодической проверкой данных и программ, нахождение и устранение уязвимостей в ПО, защита от сетевых атак и прочие подобные задачи выполнялись централизованно с минимальным участием конечных пользователей. В то же время у пользователя должна быть возможность самостоятельно выполнять полную или выборочную проверку данных на своём устройстве в любое время, получать сообщения и отчёты об обнаруженных вирусах, уязвимостях и прочих угрозах, менять некоторые настройки антивирусной программы.

Перечисленным выше требованиям полностью удовлетворяет комплекс программ “Лаборатории Касперского” [4]. Он состоит из серверов администрирования Kaspersky Security Center (KSC) [5], клиентских антивирусных программ Kaspersky Endpoint Security (KES) [6] и Агентов администрирования для связи клиентов с соответствующими им серверами. Сервера могут объединяться в иерархическую структуру разной топологии в соответствии с организационной и территориальной структурой организации или предприятия. Управление конечными устройствами осуществляется на серверах администрирования путем создания, настройки и запуска на них групповых политик и задач.

Особенности и преимущества использования антивирусных программ “Лаборатории Касперского”

Комплекс программ “Лаборатории Касперского” является одним из немногих отечественных программных продуктов, который широко известен во всём мире. Среди официальных поставщиков антивирусного ПО для Windows (всего их менее 40 на конец 2019 г.) [7] упоминаются также российские Dr.Web и NANO Security. Kaspersky Lab вошла в тройку лучших поставщиков по данным отчётов Gartner [8] и AV-Test [9] по критическим возможностям для защиты конечных устройств в бизнесе за 2018 и 2019 годы. В РФ комплекс антивирусных программ “Лаборатории Касперского” однозначно является самым популярным антивирусным продуктом [10, 11, 12]. Среди мировых

производителей антивирусного ПО можно отметить и других, наряду с Kaspersky Lab, стабильных лидеров разных рейтингов – это компании BitDefender и Symantec, немного уступают им McAfee, ESET, Microsoft и Avast.

ПО Kaspersky Lab умеет делать всё, что нужно для защиты современных компьютеров от всех типов угроз: блокирует подозрительные сайты, проверяет все файлы, следит за здоровьем системы в режиме реального времени, предоставляет возможности для поиска и устранения уязвимостей и многое другое. Программы “Лаборатории Касперского” могут работать практически на всех используемых сегодня системах Windows (от XP, Vista и выше) и Windows Server (от 2003 и выше). Их также можно установить на другие платформы и на мобильные устройства (почти все Linux-системы, Android, iOS MDM, macOS и др.), поддерживаются различные платформы виртуализации. Далеко не все антивирусы могут похвастаться таким широким охватом. Из перечисленных выше производителей антивирусного ПО таким же охватом обладают лишь Symantec и ESET.

Несомненным преимуществом Kaspersky Lab также является мощная база технической поддержки, позволяющая найти ответы практически на все вопросы по вирусам и защите информации (причём на русском языке).

Немаловажным фактором при выборе антивирусных программ помимо функционального преимущества является также доступная цена защиты в расчёте на одно защищаемое устройство. Стоимость первоначальной покупки антивирусного ПО лидирующих в этой области компаний (Kaspersky Lab, Symantec и ESET) примерно сопоставима. Немного дешевле обойдётся покупка ПО ещё одного лидера в этой области – BitDefender. Но, в отличие от конкурентов, Kaspersky Lab предлагает льготную программу продления установленных лицензий на следующие годы. Например, для НИЦ “Курчатовский институт” – Институт физики высоких энергий (далее просто ИФВЭ) продление лицензий обходится почти в полтора раза дешевле полной стоимости продукта. Антивирус Microsoft является предустановленным в последних версиях Windows и, следовательно, полностью бесплатным, но в ранних версиях Windows он либо отсутствует, либо уже не поддерживается. К тому же этот антивирус обладает ограниченным функционалом по сравнению с конкурентами.

Локальная вычислительная сеть ИФВЭ имеет разветвлённую иерархическую структуру. Сотни компьютеров под управлением ОС Linux и Windows располагаются в десятках разных зданий, расположенных на большой территории. Все здания связаны каналами связи (в основном высокоскоростными) с Информационно-Вычислительным Центром (ИВЦ). Организационная структура института не всегда совпадает с территориальной, рабочие места некоторых подразделений могут находиться в нескольких зданиях, иногда находящихся далеко друг от друга. Сегменты локальной сети располагаются по географическому принципу: в каждом здании или в группе рядом стоящих зданий – свой сегмент. В некоторых крупных зданиях может размещаться несколько сегментов локальной сети.

По характеру работы также имеются свои особенности: одна дневная смена для большинства рабочих мест, круглосуточная работа на некоторых рабочих местах, во время периодических сеансов на ускорителе некоторые подразделения переходят на круглосуточный режим работы, наличие постоянно включенных компьютеров и серверов, наличие на компьютерах чувствительной информации. Все перечисленные особенности говорят о том, что защиту клиентских компьютеров необходимо делегировать специалистам по информационным технологиям из специализированного подразделения – Отдела Математики и Вычислительной Техники (ОМВТ).

Среди линейки программ “Лаборатории Касперского” для антивирусной защиты организаций и предприятий предназначена программа Kaspersky Security Center, устанавливаемая на серверах администрирования. Она используется для централизованного решения основных задач по управлению и обслуживанию системы защиты вычислительной сети организации. При помощи KSC можно [5]:

- формировать иерархию серверов администрирования для управления сетью собственной организации, а также сетями удалённых офисов и подразделений;

- формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым;

- управлять системой антивирусной безопасности, построенной на основе программ “Лаборатории Касперского”;

- выполнять удалённую установку программ “Лаборатории Касперского” и других производителей программного обеспечения;

- удалённо управлять программами, установленными на клиентских устройствах (делать обновления, искать и закрывать уязвимости и т.д.), с помощью единой консоли;

- централизованно распространять лицензионные ключи программ “Лаборатории Касперского” на все клиентские устройства;

- получать статистику и отчёты о работе программ и устройств;

- получать уведомления о критических событиях в работе программ;

- централизованно работать с файлами, помещёнными программами защиты на карантин или в резервное хранилище.

Следует упомянуть, что клиентскими устройствами могут быть персональные компьютеры и серверы с установленными на них ОС Windows, Windows Server, Linux, Mac OS, а также различные мобильные устройства. На клиентских устройствах устанавливается программа Kaspersky Endpoint Security, а также Агент администрирования для связи с сервером KSC. KES обеспечивает комплексную защиту компьютера от различного вида угроз, сетевых и мошеннических атак. С помощью KES можно [6]:

- проверять по требованию или по расписанию компьютер на присутствие вирусов и других программ, представляющих угрозу;

- контролировать все попытки запуска программ;

- обновлять антивирусные базы и модули программ;

- устанавливать гибкие ограничения доступа к веб-ресурсам для разных групп пользователей;

- блокировать запуск исполняемого файла, если попытка запустить его из уязвимой программы не была инициирована пользователем (защита от эксплойтов);

- защищать персональные данные пользователя и ресурсы операционной системы от нежелательных вторжений;

- выполнять откат действий, произведённых вредоносными программами в операционной системе;

- при каждом обращении к файлу проверять его на присутствие вирусов и других программ, представляющих угрозу;

- проверять трафик, поступающий на компьютер по протоколам HTTP и FTP, устанавливать принадлежность ссылок к вредоносным или фишинговым веб-адресам;

- проверять сообщения электронной почты на наличие в них вирусов и других программ, представляющих угрозу;

- обнаруживать и блокировать попытки сетевых и хакерских атак;

- предотвращать подключение к компьютеру заражённых USB-устройств, имитирующих клавиатуру (защита от атак BadUSB);

- шифровать файлы и папки, а также жёсткие и съёмные диски;

- формировать различные отчёты о работе программ;

- блокировать и отправлять заражённые и подозрительные файлы на карантин;

- уведомлять пользователя о важных событиях в системе защиты компьютера;

- повышать эффективность защиты компьютера за счет оперативного получения информации о репутации файлов, веб-ресурсов и ПО, полученной от пользователей во всем мире (Kaspersky Security Network).

Управлять настройками параметров KES можно с консоли сервера администрирования KSC с помощью механизма групповых политик, либо разрешать настраивать параметры всем или избранным пользователям клиентских устройств. Но в последнем случае пользователи должны обладать достаточной квалификацией и знаниями по работе с ПО “Лаборатории Касперского”. Правильнее, наверное, чтобы настройкой большинства параметров KES занимался опытный администратор сервера.

Варианты развёртывания системы защиты предприятий и организаций с использованием Kaspersky Security Center

Сервер администрирования KSC может иметь несколько подчинённых серверов администрирования на разных уровнях иерархии. Уровень вложенности подчинённых серверов не ограничен. При этом в состав групп администрирования главного сервера будут входить клиентские устройства всех подчиненных серверов. Таким образом, независимые участки компьютерной сети могут управляться различными серверами администрирования, которые, в свою очередь, управляются главным сервером. Частным случаем подчиненных серверов администрирования являются виртуальные серверы администрирования.

Иерархию серверов администрирования можно использовать для следующих целей [5, 13, 14]:

- ограничение нагрузки на сервер администрирования (по сравнению с одним установленным в сети сервером);

- сокращение трафика внутри сети и упрощение работы с удалёнными офисами (нет необходимости устанавливать соединение между главным сервером KSC и всеми устройствами сети, которые могут находиться, например, в других регионах; достаточно установить в каждом участке сети подчинённый сервер, распределить устройства в группах администрирования подчинённых серверов и обеспечить им соединение с главным сервером по быстрым каналам связи);

- разделение ответственности между администраторами антивирусной безопасности, при этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации;

- использование KSC сервис-провайдерами (для управления сразу несколькими организациями, для которых можно создать виртуальные сервера администрирования).

Выбор структуры защиты организации определяют следующие факторы [5]:

- топология сети организации;

- организационная структура;

- общее количество устройств;

- число сотрудников, отвечающих за защиту сети, и распределение обязанностей между ними;

- аппаратные ресурсы, которые могут быть выделены для установки компонентов управления защитой;

- пропускная способность каналов связи, которые могут быть выделены для работы компонентов защиты в сети организации;

- допустимое время выполнения важных административных операций в сети организации (к таким операциям относятся, например, распространение обновлений антивирусных баз и изменение политик для клиентских устройств).

При выборе структуры защиты рекомендуется сначала определить имеющиеся сетевые и аппаратные ресурсы, которые могут использоваться для работы централизованной системы защиты.

После анализа сетевой и аппаратной инфраструктуры нужно ответить на следующие вопросы:

- возможно ли обслуживание всех клиентов одним сервером администрирования или требуется иерархия серверов?

- какая аппаратная конфигурация серверов администрирования требуется для обслуживания всех клиентов за приемлемое время?

- требуется ли использование агентов обновлений для снижения нагрузки на каналы связи?

После ответа на перечисленные вопросы можно составить набор допустимых структур защиты организации. В сети организации можно использовать одну из следующих типовых структур защиты:

- один сервер администрирования (все клиентские устройства подключены к одному серверу, роль агента обновлений выполняет сервер администрирования);

- один сервер администрирования с агентами обновлений (все клиентские устройства подключены к одному серверу, в сети выделены клиентские устройства, выполняющие роль агентов обновлений);

- иерархия серверов администрирования (для каждого большого сегмента сети выделен отдельный сервер, включённый в общую иерархию серверов администрирования, роль агента обновлений выполняет главный сервер);

- иерархия серверов администрирования с агентами обновлений (для каждого сегмента сети выделен отдельный сервер, включённый в общую иерархию серверов администрирования).

Наиболее важным преимуществом использования серверов администрирования Kaspersky Security Center является существенное сокращение внешнего трафика. Всё программное обеспечение в среде Windows для эффективной и безопасной работы регулярно требует установки новых обновлений и версий. Объём таких обновлений постоянно увеличивается. Без сервера KSC сотни компьютеров самостоятельно скачивают все необходимые обновления из внешней сети (причём очень часто одни и те же, что приводит к многократному дублированию внешнего трафика). KSC позволяет централизованно скачивать из внешней сети в своё серверное хранилище все обновления,

которые могут потребоваться клиентским устройствам, а потом по локальной сети раздавать их клиентам. В сотни раз сокращается внешний трафик.

Помимо этого, пользователи освобождаются от необходимости самостоятельно следить за своевременностью обновления разных программ. Чем дольше не обновляется какая-либо программа, тем больше вероятность, что в ней отыщется какая-нибудь уязвимость. Сервер KSC сам находит и по возможности устраняет уязвимости в ПО, поддерживая актуальность программ. Для закрытия остальных уязвимостей и обновления стороннего ПО KSC предоставляет мощный инструментарий. Порой скачивание объёмных обновлений из внешней сети заметно замедляет работу компьютера и занимает много времени. Скачивание тех же обновлений с сервера KSC по локальной быстродействующей сети происходит быстро и незаметно для пользователя.

Оптимизация системы защиты абонентов Windows в сети ИФВЭ

В табл. 1 приведены сведения об аппаратных и системных характеристиках антивирусных серверов ИФВЭ на конец 2018 г., а также минимальные требования, предъявляемые к серверам администрирования Kaspersky Security Center 10/11 [15].

Таблица 1. Аппаратные и системные характеристики антивирусных серверов ИФВЭ на конец 2018 г. и минимальные требования к ним

Сервер	**ОП**, Гб	**Ядер ЦП**	**СУБД**	**Диск**, Гб	**Свободно**, Гб
Сервер 1	**3**	4	**MS SQL Server 2005**	100	30
Сервер 2	**2**	2	MS SQL Server 2014	100	35
Сервер 3	**3**	4	MS SQL Server 2014	100	45
Сервер 4	**3**	4	**MS SQL Server 2005**	120	55
Мин. требования	**4**	1	**MS SQL Server 2008**		10/100*

*** -** требования к свободной памяти на диске с KSC: без функциональности “Системное администрирование” / с данной функциональностью.

Жирным шрифтом выделены пункты, не соответствующие минимальным требованиям. Из табл. 1 видно, что не выполнялись минимальные требования к оперативной памяти (ОП) для всех серверов. Также следовало обновить версию системы управления базами данных (СУБД) на двух серверах.

По поводу дисковой памяти следует сделать следующее замечание. В ИФВЭ не используется функциональность “Системное администрирование”, которая оплачивается отдельно (примерно на 45% дороже) [16]. В KSC 10/11 есть возможность использования сервера администрирования в качестве WSUS-сервера. WSUS (Windows Server Update Services) – это локальный сервер обновлений Windows, который синхронизируется с сайтом обновлений Microsoft, скачивая обновления, которые могут быть распространены внутри корпоративной локальной сети. Это позволяет значительно сэкономить внешний трафик компании или организации. В случае использования такой возможности требования к дисковой памяти возрастают. Вероятно, такая возможность была бы полезна в ИФВЭ.

Невыполнение минимальных требований “Лаборатории Касперского” приводило к очень медленной работе серверов (особенно Сервера 2), сбоям в работе консоли KSC (в среднем несколько раз в неделю), периодическим ошибкам в работе с базами данных, которые приводили к сбоям системы резервного копирования и к временной приостановке обновлений антивирусных баз данных у клиентов. Загруженность ОП и процессоров близка к предельной, что отчётливо было видно в системе мониторинга по многочисленным ежедневным предупреждениям и периодическим критическим событиям (чаще всего – по загрузке ОП, реже – по загрузке процессоров). И это с учётом того, что пороговые значения для них были установлены выше стандартных значений.

Далёкой от оптимальной следует признать конфигурацию серверов администрирования KSC: 4 независимых сервера, к тому же физически расположенных в одном месте. Такой вариант даже не упоминается среди возможных конфигураций, предлагаемых “Лабораторией Касперского” [13, 14]. Ближе всего к нему вариант с несколькими независимыми серверами в отдельных филиалах или отделениях организации (например, расположенных в разных городах), где внутри филиалов используются быстродействующие локальные сети, а между филиалами отсутствует быстродействующая связь. Однако топология сети ИФВЭ не удовлетворяет этим требованиям.

Остальные варианты предполагают либо иерархию серверов “главный – подчинённые”, либо единственный сервер с несколькими узлами в качестве агентов обновления или же без них.

В компьютерной сети ИФВЭ антивирусные программы Касперского установлены на менее чем 300 компьютерах. Они все объединены локальными быстродействующими сетями. С таким количеством клиентских устройств вполне может справиться один сервер администрирования. Но для повышения надёжности целесообразно добавить к нему один подчинённый сервер. Также второй сервер может оказаться полезным для испытания различных новинок и проведения экспериментов.

Таким образом, для оптимизации системы защиты абонентов Windows в сети ИФВЭ было предложено сделать следующие изменения:

1) сократить количество серверов с четырёх до двух с одновременным увеличением ОП и ядер процессоров этих серверов, чтобы с запасом выполнялись минимальные требования “Лаборатории Касперского”;

2) один сервер назначить главным (Сервер 1), второй – подчинённым (Сервер 2), всех клиентов Серверов 3 и 4 переключить на Сервер 1;

3) обновить СУБД до MS SQL Server 2014 (возможно, с единственной серверной частью на главном сервере);

4) увеличить дисковую память главного сервера минимум до 500 Гб и попробовать назначить его WSUS-сервером;

5) внутри серверов сделать двухуровневую иерархию групп “здание – подразделение”.

Все предложенные изменения были выполнены в течение 2019 г. Также было обновлено серверное ПО с KSC 10 до KSC 11. В табл. 2 отражено состояние серверов администрирования на конец 2019 года.

Сервер 2 соответствует организационной структуре института и управляет достаточно большим количеством компьютеров на удалённой от ИВЦ компактной территории, там есть свой администратор.

Таблица 2. Аппаратные и системные характеристики антивирусных серверов ИФВЭ на конец 2019 г. и минимальные требования к ним

Сервер	**ОП**, Гб	**Ядер ЦП**	**СУБД**	**Диски**, Гб	**Свободно**, Гб
Сервер 1	12	6	MS SQL Server 2014	100+250	40+200
Сервер 2	6	4	MS SQL Server 2014	100	30
Мин. требования	4	1	MS SQL Server 2008		10/100*

***** - требования к свободной памяти на диске с KSC: без функциональности “Системное администрирование” / с данной функциональностью.

Можно отметить, что сбои в работе консоли KSC практически прекратились. Ошибки в работе с базами данных стали единичными. За последние 3 месяца 2019 г. был только один сбой системы резервного копирования KSC (на подчинённом Сервере 2). На порядок реже стали возникать ситуации временной приостановки обновлений антивирусных баз данных на отдельных клиентских устройствах. Нормализовалась загрузка ОП и процессоров серверов. Отсутствие каких-либо предупреждений в системе мониторинга в течение нескольких дней стало нормой.

Эксперимент с назначением главного сервера администрирования WSUS-сервером не увенчался успехом сразу по нескольким причинам. Во-первых, объём обновлений Windows в последние годы резко вырос. Гигабайт обновлений в месяц – это уже почти норма, а иногда бывает значительно больше. В документации [17] говорится, что на WSUS-сервере обычно должно храниться от 200000 до 300000 актуальных обновлений. Даже если принять, что средний размер одного обновления будет 10 Мб, в сумме для такого сервера потребуется диск не менее 3 Тб. Можно снизить его объём, отключив определённые классы обновлений (например, самые объёмные – для драйверов устройств) или, например, до минимума сократив время хранения обновлений, но это уже будет неполноценный WSUS-сервер. Во-вторых, WSUS-сервер можно назначить без функциональности “Системное администрирование”, но создать и выполнить задачу синхронизации с Серверами обновлений Microsoft при этом нельзя. А без синхронизации WSUS-сервер опять же получается не совсем полноценным. В-третьих, какая-то часть обновлений Windows (в основном небольшие обновления

безопасности) и без WSUS-сервера может устанавливаться через KSC (с помощью задачи закрытия уязвимостей). К тому же не составляет труда при необходимости вручную создать инсталляционный пакет и задачу для установки почти любого обновления. Также следует учесть, что подавляющее большинство компьютеров в институте приобреталось централизованно, т.е. имеется несколько больших партий компьютеров одинаковой сборки с одинаковым ПО. Многие обновления зависят от версий Windows и от производителей комплектующих компьютеров, которых сейчас очень много. Получается, что в ИФВЭ огромная часть обновлений на WSUS-сервере будет не востребованной. Следовательно, скачивание и обслуживание таких обновлений на сервере в рамках локальной сети института можно признать нецелесообразным.

Наиболее заметным результатом оптимизации стало ускорение работы ПО “Лаборатории Касперского” как на серверах, так и на клиентских устройствах. Время выполнения некоторых операций в консоли сервера администрирования (особенно связанных с записью или изменением данных в СУБД) сократилось на несколько порядков. Также были оптимизированы настройки групповых политик в соответствии с последними рекомендациями “Лаборатории Касперского” [5]. В результате на клиентских устройствах практически прекратились случаи, когда активность антивирусной программы не давала пользователям выполнять свои задания. К примеру, если полтора года назад на компьютере впервые устанавливался KES, то сразу после установки и перезагрузки выполнялась полная проверка дисков и некоторые другие задачи (в частности, сбор данных о компьютере и их отправка на сервер), которые могли на час-два просто заблокировать компьютер, то теперь через пять минут после перезагрузки уже вполне можно работать, хотя поначалу может быть небольшое подтормаживание.

Таким образом, любой пользователь сети ИФВЭ, работающий под управлением ОС Windows, может подключиться к серверам администрирования [18] и получить следующие преимущества:

- оперативное ежедневное обновление антивирусных баз данных и программ;
- еженедельную проверку всех данных и программ;
- нахождение и устранение уязвимостей в системном и прикладном ПО;
- защиту от сетевых и хакерских атак с временной блокировкой IP-адресов злоумышленников;

- оптимальные настройки KES с помощью групповых политик;

- получение отчётов и сообщений о важных событиях защиты компьютера;

- автоматическую активацию и продление лицензионных ключей и др.

В то же время у пользователей есть возможность в любое время выполнить полную или выборочную проверку данных с полной настройкой параметров такой проверки; получать сообщения и отчёты об обнаруженных вирусах, уязвимостях и прочих угрозах; временно отключить антивирус Касперского; установить режим фоновой проверки; включить проверку съёмных накопителей; понизить приоритет антивирусных процессов, чтобы уступать ресурсы другим программам; назначать доверенные программы и исключения из проверки. В случае недоступности сервера администрирования антивирусные базы будут обновляться через интернет с серверов “Лаборатории Касперского”.

Замечания и выводы по использованию антивирусных программ

Наряду с наличием большого количества преимуществ у ПО “Лаборатории Касперского”, хотелось бы также отметить, с какими проблемами обычно сталкиваются при использовании этого ПО в организациях.

Техподдержка “Лаборатории Касперского” иногда бывает медлительна. Одну, казалось бы, небольшую проблему они решали целых 8 месяцев! Большинство других проблем решалось, конечно, быстрее – обычно менее месяца, иногда за несколько дней. Как правило, техподдержка рассматривает проблемы по существу только после установки последних версий программ и утилит с установленными последними патчами, даже если они ещё не являются стабильными, т.е. не до конца протестированными. После установки таких обновлений изначальная проблема часто сразу оказывается решённой, но могут обнаружиться новые неприятности в неожиданных местах. Какой-то цугцванг получается: либо живи с нерешённой старой проблемой, либо её можно решить, но с риском получить новую проблему, а может быть и не одну.

А является ли принцип бета-тестирования, практически ставший стандартом при разработке любого ПО, правильным во всех областях? Особенно когда дело касается космоса, транспорта, атомной энергетики, банковской и военной сферы? Ведь ошибка в

таком приложении может привести к трагическим последствиям. Поэтому программы, используемые в этих областях, должны быть сверхнадёжными, защищёнными и ни при каких условиях не должны вести себя непредсказуемо. Антивирусное ПО должно помогать в решении проблемы защиты информации, а не являться источником новых проблем. Антивирусное ПО должно отвечать самым строгим критериям надёжности, ведь главная его задача – защита компьютеров. Причём компьютеры могут стоять в крупных банках, на атомных электростанциях или на объектах ядерной физики, где любые ошибки могут очень дорого стоить.

К сожалению, можно также отметить, что порой после обновлений программ “Лаборатории Касперского” проявлялись старые ошибки, что очень нервирует пользователей. Также нередко возникают проблемы с удалением и переустановкой ПО. Удаление Kaspersky Endpoint Security средствами Windows или с помощью задачи деинсталляции в KSC не всегда удаляет антивирус полностью, что приводит к невозможности новой установки KES. Приходится использовать специальную утилиту kavremover. А однажды был случай, когда и эта утилита не смогла удалить KES, и тогда пришлось переустанавливать Windows. Казалось бы, если какая-либо программа начала сбоить, то самым надёжным способом является удалить её и установить заново. Некоторые даже Windows время от времени переустанавливают. Для решения многих проблем переустановка оказывается самым быстрым и надёжным методом, но не для ПО “Лаборатории Касперского”.

Некоторые пользователи в последнее время отказываются от антивируса Касперского и переходят на Защитник Windows (Windows Defender) компании Microsoft или на другое антивирусное ПО. И их можно понять. Порой программы “Лаборатории Касперского” являются источником разных проблем (временная перегруженность процессора; многократные перезагрузки компьютера в случае неудачной установки обновления; непредсказуемые последствия при неожиданных выключениях ПК, если в это время шло обновление антивирусного ПО и т.п.), хотя в последнее время здесь наблюдается заметный прогресс, и программы “Лаборатории Касперского” работают всё надёжнее и быстрее. В то же время Защитник Windows в последних тестах показывает неплохие результаты [9]. Он является предустановленным в Windows и поэтому имеет неплохие перспективы. Это предельно простая и надёжная программа. Работает и

обновляется почти незаметно для пользователя. В прежние годы было много жалоб на то, что Защитник Windows пропускает много вирусов и троянов, что порой даже приводило к крушению системы. Но в последнее время отзывы уже скорее положительные.

Заключение

При организации распределённой системы антивирусной защиты в организациях и на предприятиях следует учитывать следующие моменты.

- Большое количество распределённых компьютеров (порой с повышенными требованиями безопасности) требует наличия централизованной системы защиты организации.
- Линейка программ “Лаборатории Касперского” отвечает всем самым строгим требованиям, предъявляемым к системам распределённой антивирусной защиты организации.
- При правильной настройке и эксплуатации серверов KSC обеспечивается надёжная защита всех подключенных устройств от вирусов, троянских программ, сетевых атак и прочих вредоносных действий, причём даже для систем с закончившимся сроком поддержки (к примеру, Windows XP).

Разработана, настроена и реализована система распределённой антивирусной защиты устройств на базе ОС Windows в ИФВЭ с использованием программ “Лаборатории Касперского”. Иерархическая система серверов с подключенными к ним клиентскими компьютерами учитывает особенности и удовлетворяет требованиям сети НИЦ “Курчатовский институт” – ИФВЭ, распределяет задачи защиты компьютеров по подразделениям и зданиям организации. Реализация и долговременная профессиональная поддержка этих задач необходима для выполнения основной задачи ИФВЭ – выполнения научных исследований, поскольку значительно экономит время сотрудников Института для выполнения своих непосредственных обязанностей.

Список литературы

[1] Актуальные киберугрозы: III квартал 2019 года. Positive Technologies, 2019.
https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q3/
[2] Desktop Operating System Market Share Worldwide. Statcounter, 2019.
https://gs.statcounter.com/os-market-share/desktop/worldwide

[3] Kaspersky threats. Уязвимости, угрозы. АО «Лаборатория Касперского», 2019. https://threats.kaspersky.com/ru/vulnerability/
[4] База знаний по продуктам для бизнеса. АО «Лаборатория Касперского», 2019. https://support.kaspersky.ru/corporate
[5] Справка Kaspersky Security Center 11. АО «Лаборатория Касперского», 2019. https://help.kaspersky.com/KSC/11/ru-RU/5022.htm
[6] KES для Windows. Организация защиты компьютера. АО «Лаборатория Касперского», 2019. https://help.kaspersky.com/KESWin/11/ru-RU/127971.htm
[7] Поставщики антивирусного программного обеспечения для Windows. Microsoft, 2019. https://support.microsoft.com/ru-ru/help/18900/consumer-antivirus-software-providers-for-windows
[8] Gartner Reviews Critical Capabilities of 21 EPP Solutions. АО «Лаборатория Касперского», 2018. https://www.kaspersky.com/critical-capabilities-for-epp-gartner
[9] The best Windows antivirus software for business users. AV-TEST, 2019. https://www.av-test.org/en/antivirus/business-windows-client/
[10] Антивирусы для Windows. Роскачество, 2018. https://rskrf.ru/ratings/tekhnologii/programmnoe-obespechenie/antivirusy-dlya-windows/#details
[11] Александр Рэйн. Выбираем самый надежный антивирус: 5 лучших программ для защиты компьютера. CNews, 2019. https://zoom.cnews.ru/publication/item/62402
[12] Евгения Баленко, Мария Коломыченко. «Роскачество» назвало лучшие антивирусы. АО «РОСБИЗНЕСКОНСАЛТИНГ», 2019. https://www.rbc.ru/technology_and_media/31/05/2019/5cefc6e59a7947349fb2efaf
[13] Как развернуть Kaspersky Security Center 10 в сети поставщика услуг. АО «Лаборатория Касперского», 2019. https://support.kaspersky.ru/14043
[14] Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования. АО «Лаборатория Касперского», 2018. https://support.kaspersky.ru/10495
[15] KSC 11. Аппаратные и программные требования. АО «Лаборатория Касперского», 2019. https://help.kaspersky.com/KSC/11/ru-RU/96255.htm
[16] Kaspersky Endpoint Security для бизнеса стандартный. АО «Лаборатория Касперского», 2019. https://www.kaspersky.ru/small-to-medium-business-security/endpoint-select
[17] KSC 11. Синхронизация обновлений Windows Update с Сервером администрирования. https://help.kaspersky.com/KSC/11/ru-RU/61470.htm
[18] Антивирус Касперского. Обзор. ИФВЭ, 2019. https://redmine.ihep.su/projects/kaspersky

Рукопись поступила 23 декабря 2019 г.

Е.И. Галкин

Оптимизация системы распределённой антивирусной защиты организации для ОС Windows на примере ИФВЭ.

Препринт отпечатан с оригинала-макета, подготовленного автором.

Подписано к печати 30.01.2020. Формат 60 × 84/16. Цифровая печать.
Печ.л. 1,25. Уч.– изд.л. 1,8. Тираж 80. Заказ 5. Индекс 3649.

НИЦ «Курчатовский институт» – ИФВЭ
142281, Московская область, г. Протвино, пл. Науки, 1
www.ihep.ru; библиотека http://web.ihep.su/library/pubs/all-w.htm

Индекс 3649

П Р Е П Р И Н Т 2020-1,
НИЦ «Курчатовский институт» – ИФВЭ, 2020