



MaxPatrol VM

версия 2.8

Список поддерживаемых систем

© Positive Technologies, 2025.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 10.06.2025

Содержание

1.	Об этом документе.....	4
2.	АСУ ТП	5
3.	Операционные системы.....	8
4.	Сетевое оборудование	10
5.	Системы управления базами данных	11
6.	Серверное ПО	12
7.	Системы безопасности	14
8.	Системы криптографической защиты информации	16
9.	Приложения.....	17
10.	О технической поддержке.....	23

1. Об этом документе

Документ содержит информацию об основных системах, которые Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM) может сканировать в режиме пентеста, идентификации узлов и на которых может обнаруживать уязвимости.

Документ адресован специалистам, выполняющим установку и интеграцию MaxPatrol VM в организации. Рекомендуется применять документ как источник дополнительной информации о MaxPatrol VM одновременно с другими руководствами по продукту.

Комплект документации MaxPatrol VM включает в себя следующие документы:

- Этот документ.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство оператора — содержит сценарии использования продукта для управления информационными активами организации.
- Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с MaxPatrol VM для аудита активов.
- Руководство разработчика — содержит информацию о доступных в MaxPatrol VM функциях сервиса REST API.
- Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с MaxPatrol VM.

2. АСУ ТП

В этом разделе представлена информация об автоматизированных системах управления технологическим процессом (АСУ ТП), которые поддерживает MaxPatrol VM.

Таблица 1. АСУ ТП

Название	Версия	Расчет уязвимостей	Информация о лицензиях
AVEVA (Wonderware) Application Server	3.5.0–20.0.0	+	–
AVEVA (Wonderware) Archestra	1.0.0–5.5.0	+	–
AVEVA (Wonderware) Auto- Build Core	5.5.0–20.0.0	+	–
AVEVA (Wonderware) FactorySuite Gateway	5.5.0–20.0.0	+	–
AVEVA (Wonderware) Historian	10.0.0–20.0.0	+	–
AVEVA (Wonderware) Historian Client	10.0.0–20.0.0	+	–
AVEVA (Wonderware) Historian Search	10.0.0–20.0.0	+	–
AVEVA (Wonderware) Information Model	2012–2020	+	–
AVEVA (Wonderware) Information Server	04.05.0–5.6.0	+	–
AVEVA (Wonderware) Insight	10.0.0–20.0.0	+	–

Название	Версия	Расчет уязвимостей	Информация о лицензиях
AVEVA (Wonderware) Insight Publisher	5.5.0–20.0.0	+	–
AVEVA (Wonderware) InTouch	5.5.0–20.0.0	+	–
AVEVA (Wonderware) InTouch Access Anywhere	10.0.0–20.0.0	+	–
AVEVA (Wonderware) InTouch Access Anywhere Server	10.0.0–20.0.0	+	–
AVEVA (Wonderware) InTouch OMI	5.5.0–20.0.0	+	–
AVEVA (Wonderware) License Server	3.5.0–20.0.0	+	–
AVEVA (Wonderware) Logger	5.5.0–20.0.0	+	–
AVEVA (Wonderware) System Platform	2012–2020	+	–
Siemens AG Automation License Manager	3–7	+	–
Siemens AG SIMATIC Logon	6–18	+	–
Siemens AG SIMATIC NET PC Software	6–18	+	–
Siemens AG SIMATIC PCS 7	4.0–9.1	+	–
Siemens AG SIMATIC STEP 7	4.0–5.6	+	–
Siemens AG SIMATIC WinCC	5.0–7.5	+	–

Название	Версия	Расчет уязвимостей	Информация о лицензиях
Siemens AG SIMATIC WinCC Runtime	5.0–7.5	+	–
Siemens AG TIA Portal	12–17	+	–
Yokogawa CENTUM VP	R4–R6	+	+
Yokogawa ProSafe-RS	R2–R4	+	+

3. Операционные системы

В этом разделе представлена информация об операционных системах, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста ОС и их версии могут не определиться.

Таблица 2. Операционные системы

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
«РЕД ОС»	7.1–7.3	–	+	+ только для версии 7.3
AlmaLinux	8, 9	–	+	+
ALT Linux	Simply Linux 9, 10, Альт 8 СП Рабочая станция, Альт 8 СП Сервер, Альт Образование 9, 10, Альт Рабочая станция 9, 10, Альт Рабочая станция К 9, 10, Альт Сервер 9, 10, Альт Сервер Виртуализации 9, 10	–	+	+
Astra Linux CE	Последняя версия	–	+	–
Astra Linux SE	1.5–1.7	–	+	+ только для версии 1.7
CentOS Linux	7, 8	+	+	+
Debian Linux	8–11	+	+	+
FortiOS	4–7.2	–	+	+
HP HP-UX	11.31	–	+	–
IBM AIX	7	–	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Microsoft Windows	XP SP3, Server 2003 SP2, Vista, Server 2008, 7, Server 2008 R2, 8, Server 2012, 8.1, Server 2012 R2, 10 (1507) – 10 (21H2), Server 2016, Server 2019, 11, Server 2022	+	+	+
openSUSE Leap	42.1–15.4	–	+	+
openSUSE Tumbleweed	Последняя версия	–	+	+
Oracle Enterprise Linux	6–9	–	+	+
Oracle Solaris	10.11–11.4	+	+	–
Red Hat Enterprise Linux	4–9	+	+	+
Rocky Linux	8, 9	–	+	+
SUSE Enterprise Linux	11, 12, 15	–	+	+
Ubuntu Linux	18.04–22.04 Только LTS-версии	+	+	+

4. Сетевое оборудование

В этом разделе представлена информация о сетевом оборудовании, которое поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста сетевое оборудование и его версии могут не определиться.

Таблица 3. Сетевое оборудование

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Alcatel OmniSwitch (AOS)	Все версии	–	+	–
Arista EOS	Все версии	–	+	–
Check Point GAIa	Все версии	–	+	–
Check Point SPLAT	Все версии	–	+	–
Cisco ASA	Все версии	–	+	+
Cisco ASA v	Все версии	–	+	+
Cisco FTD	6.6 и выше	–	+	–
Cisco IOS	Все версии	+	+	+
Cisco IOS XE	Все версии	–	+	+
Cisco IOS XR	Все версии	–	+	+
Cisco Nexus	Все версии	–	+	+
Cisco PIX	Все версии	–	+	+
Cisco WLC (AireOS)	Все версии	–	+	+
Eltex ESR	1.18 и выше	–	+	–
Eltex MES	Все версии	–	+	–
Fortinet FortiGate	Все версии	–	+	–
Huawei VRP	Все версии	–	+	+
Juniper Junos OS	5.0 и выше	–	+	+
Avaya (Nortel) ERS	Все версии	–	+	–
Palo Alto Networks PAN-OS	Все версии	–	+	+
QTECH QSW	7	–	+	–

5. Системы управления базами данных

В этом разделе представлена информация о системах управления базами данных, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста СУБД и их версии могут не определиться.

Таблица 4. СУБД

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
ClickHouse (Linux)	21 и более новые	–	+	+
MariaDB	Все версии	–	+	+
Microsoft Access	2000–2019	–	+	+
Microsoft SQL Server	2000–2019	+	+	+
MongoDB	Все версии	+	+	+
MySQL	Все версии	+	+	+
Oracle Database	Все версии	+	+	+
PostgreSQL	Все версии	+	+	+
Redis	1.3–7.2	–	+	+

6. Серверное ПО

В этом разделе представлена информация о серверном программном обеспечении, которое поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста ПО и его версии могут не определиться.

Таблица 5. Серверное ПО

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Acronis Cyber Protect Management Server	15	–	+	+
Apache HTTP Server	Все версии	+	+	+
Apache Tomcat (Linux)	Все версии	+	+	+
Apache Tomcat (Windows)	Все версии	+	+	+
Atlassian Jira Service Management (Linux)	3.1.10 и выше	–	+	+
Atlassian Jira Software (Linux)	7.0.0 и выше	–	+	+
Atlassian Jira Work Management (Linux)	7.0.0 и выше	–	+	+
Logstash 8	Все версии	–	+	+
MDaemon Email Server	Все версии	+	+	–
Microsoft Active Directory	Все версии	+	+	+
Microsoft DNS Server	Все версии	+	+	–
Microsoft Dynamics AX	4–2012 R3	–	+	–
Microsoft Exchange	Все версии	+	+	+
Microsoft Internet Information Services	5–10	+	+	+
Microsoft Office Online Server	2016	–	+	–
Microsoft Office Web Apps	2010–2013	–	+	–
Microsoft Project Server	2003–2019	–	+	+
Microsoft SharePoint Foundation	2010–2013	–	+	+
Microsoft SharePoint Server	2003–2019	–	+	+

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Microsoft Skype for Business Server	2015–2019	–	+	–
Microsoft System Center Operations Manager	2007–2012	–	+	–
Microsoft System Center Virtual Machine Manager	2008–2012	–	+	–
Microsoft Windows Internet Name Service Server	Все версии	+	+	+
Nginx	1.19 и более новые	+	–	+
OpenResty	Все версии	–	+	+
Positive Technologies Application Firewall	Все версии	–	+	–
Squid HTTP Proxy Server	Все версии	–	+	+
Veeam Backup & Replication Server	11	–	+	–
VMware vCenter Server	Все версии	+	+	+

7. Системы безопасности

В этом разделе представлена информация о системах безопасности, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста системы безопасности и их версии могут не определяться.

Таблица 6. Список систем безопасности

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
AVG Anti-Virus	2013	—	+	—
AVG Anti-Virus Business Edition	2013	—	+	—
AVG Anti-Virus Free	2013	—	+	—
AVG Internet Security	2013	—	+	—
AVG Internet Security Business Edition	2013	—	+	—
Dr.Web Anti-Virus	3—6	—	+	—
Dr.Web Enterprise Server	6	—	+	—
Dr.Web Security Space	3—8	—	+	—
ESET Endpoint Antivirus	3	—	+	—
ESET Endpoint Security	3—5	—	+	—
ESET NOD32 Antivirus	2—4	—	+	—
ESET Smart Security	3—4	—	+	—
ESET Mail Security	Все версии	—	+	—
ESET File Security	Все версии	—	+	—
Kaspersky Security Center	10—11, 13—14.2	—	+	—
Kaspersky Anti-Virus	Все версии	—	+	—
Kaspersky Endpoint Security	Все версии	—	+	—
McAfee AntiVirus Plus	Все версии	—	+	—
McAfee Internet Security	Все версии	—	+	—
McAfee Total Protection	Все версии	—	+	—
McAfee VirusScan Enterprise	8.8	—	+	—

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Norton 360	2004–2013	—	+	—
Norton AntiVirus	2006–2013	—	+	—
Norton Internet Security	2006–2013	—	+	—
Symantec AntiVirus Corporate Edition	9–10	—	+	—
Symantec Endpoint Protection	11–14	—	+	—
Trend Micro Antivirus	16–17	—	+	—
Trend Micro Internet Security	16	—	+	—
Trend Micro Internet Security Pro	16	—	+	—
Trend Micro OfficeScan Client	6–11	—	+	—
Trend Micro OfficeScan Server	6–11	—	+	—
Trend Micro PC-cillin Internet Security	1–15	—	+	—
Trend Micro ServerProtect	5	—	+	—

8. Системы криптографической защиты информации

В этом разделе представлена информация о системах криптографической защиты информации, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста СКЗИ и их версии могут не определиться.

Таблица 7. Список систем криптографической защиты информации

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
«КриптоПро», Administration	Все версии	–	+	–
«КриптоПро», CSP	Все версии	–	+	–
«КриптоПро», JCP	Все версии	–	+	–
«КриптоПро», JTLS	Все версии	–	+	–
«КриптоПро», TLS	Все версии	–	+	–
Gpg4win	Все версии	–	+	–
OpenSSL	Все версии	–	+	–
PGP Desktop	Все версии	–	+	–
ViPNet Client	3–4	–	+	–
ViPNet Coordinator HW	3	–	+	–

9. Приложения

В этом разделе представлена информация о приложениях, которые поддерживает MaxPatrol VM.

Внимание! При сканировании в режиме пентеста приложения и их версии могут не определиться.

Таблица 8. Список приложений

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
7-Zip	Все версии	–	+	+
«Яндекс Диск»	Все версии	–	+	–
Acronis Cyber Protect Agent	15	–	+	+
ActivePerl	Все версии	–	+	–
ActivePython	Все версии	–	+	–
ActiveTcl	Все версии	–	+	–
Adobe Acrobat	Все версии	–	+	+
Adobe Acrobat DC	Все версии	–	+	+
Adobe Acrobat Reader	Все версии	–	+	+
Adobe Acrobat Reader DC	Все версии	–	+	+
Adobe Pepper Flash for Google Chrome	11–32	–	+	–
Ammyy Admin	Все версии	–	+	–
Ansible	2.10–6	–	+	–
Ansible Core	2.10–2.13	–	+	–
AnyDesk	Все версии	+	–	–
Apache HTTP Server (Linux)	2.2–2.4	+	+	+
Apache Struts	Все версии	–	+	–
Apache Subversion	Все версии	–	+	–
Apache Tomcat (Linux)	8–10	+	+	+
Apache Tomcat (Windows)	8–10	+	+	+
Artifactory	6–7	–	+	–
Atlassian Confluence	7 и выше	–	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Bitwarden	Все версии	–	+	–
Bloodhound	Все версии	–	+	–
Cain & Abel	Все версии	–	+	–
Check Point GAI	Все версии	–	+	+
CollabNet Subversion	Все версии	–	+	–
Dashlane Desktop	Все версии	–	+	–
Delphi	Все версии	–	+	–
Deluge	Все версии	–	+	–
Dropbox	Все версии	–	+	–
Flash Player for Microsoft Internet Explorer	1–32	–	+	–
Foxit Reader	Все версии	–	+	–
GitLab	13–14	–	+	–
GitLab Community Edition (GitLab CE)	Все версии	–	+	+
GitLab Enterprise Edition (GitLab EE)	Все версии	–	+	+
GitLab Runner	Все версии	–	+	+
Go	Все версии	–	+	–
Google Chrome	Все версии	–	+	+
HAproxy	2	–	+	–
HPE Integrated Lights-Out (iLO)	2–5	+	+	+
Hyper-V	1.0–1.4	–	+	+
iCloud	Все версии	–	+	–
IrfanView	Все версии	–	+	–
iTunes	Все версии	–	+	–
Java Platform	Все версии	–	+	–
JFrog Artifactory	6–7	–	+	–
John the Ripper	Все версии	–	+	–
Kayako Classic	1.19 и выше	–	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Keeper Password Manager	Все версии	–	+	–
Kibana	8.0 и выше	–	+	+
LogMeIn Pro	Все версии	–	+	–
MaxPatrol 8	Все версии	+	+	–
Microsoft .NET Framework	1–4.8	–	+	+
Microsoft Defender	1–6	–	+	–
Microsoft Edge	Все версии	–	+	+
Microsoft Edge (Chromium)	Все версии	–	+	+
Microsoft Excel	2003–2016	–	+	+
Microsoft Excel Viewer	2000–2007 SP3	–	+	–
Microsoft Internet Explorer	Все версии	–	+	+
Microsoft Lync	2010–2013	–	+	+
Microsoft OneDrive	Все версии	–	+	–
Microsoft OneNote	2003–2016	–	+	+
Microsoft Office	2003	–	+	+
	2007	–	+	+
	2010	–	+	+
	2013	–	+	+
	2013 Click-to-Run	–	–	–
	2016	–	+	+
	2016 Click-to-Run	–	–	–
Microsoft Office Compatibility Pack	2007	–	+	–
Microsoft Office InfoPath	2003–2013	–	+	–
Microsoft Outlook	2003–2016	–	+	+
Microsoft PowerPoint	2003–2016	–	+	+
Microsoft PowerPoint Viewer	2000–2010	–	+	–
Microsoft PowerShell Core	6	–	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Microsoft Pragmatic General Multicast	5.1–6.3	–	+	–
Microsoft Project	2003–2016	–	+	+
Microsoft Publisher	2003–2016	–	+	+
Microsoft Remote Desktop Connection Client	5–10	–	+	+
Microsoft SharePoint Services	2–3	+	+	+
Microsoft Silverlight	1–5	–	+	+
Microsoft Teams	0–1	–	+	–
Microsoft Terminal Services	Все версии	–	+	–
Microsoft Visio	2003–2016	–	+	+
Microsoft Visio Viewer	2003–2013	–	+	–
Microsoft Visual Studio	2010–2019	–	+	+
Microsoft Visual Studio Code	Все версии	–	+	–
Microsoft Windows Media	6–12	–	+	+
Microsoft Windows Remote Management	Все версии	–	+	–
Microsoft Word	2003–2016	–	+	+
Microsoft Word Viewer	2000–2003	–	+	+
Microsoft XML Core Services	2–6	–	+	+
Mimikatz	Все версии	–	+	–
Mozilla Firefox	Все версии	–	+	+
Mozilla Firefox ESR	Все версии	–	+	+
mIRC	6–7	–	+	–
mRemoteNG	Все версии	–	+	–
Nessus	Все версии	–	+	–
Notepad++	Все версии	–	+	–
OpenOffice	2–4	–	+	–
OpenVPN	Все версии	+	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
Opera Web Browser	Все версии	–	+	–
Passwork	4	–	+	–
PDF-XChange Viewer	Все версии	–	+	–
PHP	Все версии	+	+	–
Pidgin	Все версии	–	+	–
Privoxy	3	–	+	–
Python	2–3	–	+	–
Radmin Server	Все версии	+	+	–
Radmin Viewer	Все версии	–	+	–
Ruby	Все версии	–	+	–
SAP GUI	4–7	–	+	–
Signal	Все версии	–	+	–
Skype for Windows	0–7	–	+	–
Slik Subversion	Все версии	–	+	–
SumatraPDF	Все версии	–	+	–
TeamCity	2018–2023	–	+	+
TeamViewer	Все версии	+	+	–
Techinline Remote Desktop	Все версии	–	+	–
Telegram Desktop	Все версии	–	+	–
Thunderbird	Все версии	–	+	+
TightVNC Server	Все версии	–	+	–
TightVNC Viewer	Все версии	–	+	–
Tor	Все версии	–	+	–
Tor Browser	Все версии	–	+	–
TortoiseSVN	Все версии	–	+	–
uTorrent	Все версии	–	+	–
Veeam Agent for Microsoft Windows	Все версии	–	+	–
Viber	Все версии	–	+	–
VirtualBox	6.1 и выше	–	+	+
VisualSVN Server	Все версии	–	+	–

Название	Версия	Пентест	Идентификация узлов	Расчет уязвимостей
VLC Media Player	Все версии	–	+	–
VMware ESXi	6–7	–	+	+
VMware Player	Все версии	–	+	–
VMware Tools	10 и выше	–	+	+
VMware vCenter	6–7	+	+	+
VMware Workstation	Все версии	–	+	–
WeChat	Все версии	–	+	–
WhatsApp	Все версии	–	+	–
Windows Media Center	5	–	+	+
WinPcap	4	–	+	–
WinRAR	Все версии	–	+	–
XenAppServer	6.5	–	+	–
XnView	Все версии	–	+	–
XSpider	4–8	+	+	–
Zabbix Agent	4–6	–	+	–
Zabbix Server	4–6	–	+	–
Zoom	Все версии	–	+	–

10. О технической поддержке

Базовая техническая поддержка доступна для всех владельцев действующих лицензий на MaxPatrol VM в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies предоставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках технической поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

Примечание. Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к portalу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг технической поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по технической поддержке продукта не включают в себя услуги по переустановке продукта, решению проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по технической поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 9. Время реакции на заявку

Уровень значимости заявки	Критерии значимости заявки	Время реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист технической поддержки сообщает вам:

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют около 3000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.