



## ТОП полезных Windows Event ID в расследовании инцидентов ИБ

Устаревший Event ID: версии ОС младше Windows XP и младше Windows Server 2003.

№	Event ID (Устаревший Event ID)	Краткое описание события (на русском)	Краткое описание события (на английском)
1.	1102 (517)	Журнал аудита был очищен.	The audit log was cleared
2.	4624 (528, 540)	Учетная запись успешно вошла в систему.	An account was successfully logged on.
3.	4625 (529-537, 539)	Не удалось войти в учетную запись.	An account failed to log on.
4.	4634 (538)	Учетная запись была отключена.	An account was logged off.
5.	4648 (552)	Вход был предпринят с помощью явных учетных данных.	A logon was attempted using explicit credentials.
6.	4657 (567)	Значение реестра было изменено.	A registry value was modified.
7.	4660 (564)	Объект был удален.	An object was deleted.
8.	4662 (566)	Операция была выполнена для объекта.	An operation was performed on an object.
9.	4663 (567)	Предпринята попытка доступа к объекту.	An attempt was made to access an object.
10.	4670 (N/A)	Изменены разрешения для объекта.	Permissions on an object were changed.
11.	4672 (576)	Специальные привилегии, назначенные новому входу.	Special privileges assigned to new logon.
12.	4673 (577)	Была вызвана привилегированная служба.	A privileged service was called.
13.	4688 (592)	Был создан новый процесс.	A new process has been created.
14.	4689 (593)	Процесс завершился.	A process has exited.
15.	4697 (601)	Попытка установки службы	Attempt to install a service
16.	4698 (602)	Была создана запланированная задача.	A scheduled task was created.
17.	4699 (602)	Запланированная задача была удалена.	A scheduled task was deleted.
18.	4715 (N/A)	Политика аудита (SACL) объекта была изменена.	The audit policy (SACL) on an object was changed.
19.	4719 (612)	Политика аудита системы была изменена.	System audit policy was changed.
20.	4720 (624)	Была создана учетная запись пользователя.	A user account was created.
21.	4722 (626)	Учетная запись пользователя включена.	A user account was enabled.
22.	4723 (627)	Предпринята попытка изменить пароль учетной записи.	An attempt was made to change an account's password.
23.	4724 (628)	Предпринята попытка сбросить пароль учетной записи.	An attempt was made to reset an account's password.
24.	4725 (629)	Учетная запись пользователя отключена.	A user account was disabled.
25.	4726 (630)	Удалена учетная запись пользователя.	A user account was deleted.
26.	4732 (636)	Участник был добавлен в локальную группу с поддержкой безопасности.	A member was added to a security-enabled local group.
27.	4735 (639)	Локальная группа с поддержкой безопасности была изменена.	A security-enabled local group was changed.
28.	4740 (644)	Учетная запись пользователя заблокирована.	A user account was locked out.
29.	4767 (671)	Учетная запись пользователя была разблокирована.	A user account was unlocked.
30.	4768 (672, 676)	Запрос на проверку подлинности Kerberos (TGT).	A Kerberos authentication ticket (TGT) was requested.
31.	4776 (680, 681)	Контроллер домена попытался проверить учетные данные для учетной записи.	he domain controller attempted to validate the credentials for an account.
32.	4797 (N/A)	Была сделана попытка проверить наличие пустого пароля для учетной записи.	An attempt was made to query the existence of a blank password for an account
33.	4907 (N/A)	Параметры аудита объекта были изменены.	Auditing settings on object were changed.
34.	4946 (N/A)	Изменение было внесено в список исключений брандмауэра Windows. Было добавлено правило.	A change has been made to Windows Firewall exception list. A rule was added.
35.	4947 (N/A)	Изменение было внесено в список исключений брандмауэра Windows. Правило было изменено.	A change has been made to Windows Firewall exception list. A rule was modified.
36.	5136 (566)	Объект службы каталогов был изменен.	A directory service object was modified.
37.	5140 (N/A)	Доступ к объекту общей папки сети.	A network share object was accessed.
38.	5145 (N/A)	Объект сетевого общего доступа был проверен на предмет возможности предоставления клиенту желаемого доступа.	A network share object was checked to see whether client can be granted desired access.
39.	5156 (N/A)	Платформа фильтрации Windows разрешила подключение.	The Windows Filtering Platform has allowed a connection.
40.	5157 (N/A)	Платформа фильтрации Windows заблокировала подключение.	The Windows Filtering Platform has blocked a connection.