ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по базовой настройке регистрации событий безопасности

2025

1. Обеспечить в инфраструктуре регистрацию следующих событий:

успешные и неуспешные попытки авторизации;

успешные и неуспешные попытки доступа;

изменения конфигурации;

запуск и завершение приложений, служб, процессов как со стороны пользователей, так и со стороны администраторов;

действия администраторов;

использование системных правил;

использование системных учетных записей;

создание и удаление системных объектов;

импорт и экспорт данных;

сетевые сбои, ошибки подключений.

2. Для каждой информационной системы состав регистрируемых событий безопасности необходиом определить с учетом положений национального стандарта Российской Федерации ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

3. Обеспечить обязательную регистрацию временных меток событий безопасности и идентификационных данных (например, IP-адрес источника, идентификатор пользователя).

4. Обеспечить хранение собранных событий безопасности не менее 3-х месяцев.

5. Обеспечить такой размер хранилищ журналов событий безопасности, который будет достаточным для их полноценного анализа.

6. Обеспечить резервное копирование журналов событий в обособленном хранилище, физически отделенном от информационной инфраструктуры.

7. Осуществить настройку операционных систем Windows и Linux по регистрации событий в соответствии с рекомендациями по их настройке (прилагаются).

8. Для операционных систем, средств защиты информации, межсетевых экранов, сертифицированных на соответствие требованиям по безопасности

ФСТЭК России, а также телекоммуникационного оборудования настройку регистрации событий безопасности необходимо осуществлять в соответствии с эксплуатационной документацией, поставляемой совместно с указанными средствами.

9. Обеспечить применение сертифицированных по требованиям безопасности информации ФСТЭК России средств мониторинга событий информационной безопасности. В случае отсутствия такой возможности, организовать постоянный мониторинг журналов событий доступными средствами (например, Zabbix).

Приложение 1

Рекомендации по настройке регистрации событий безопасности в операционных системах на базе Windows

1. Для осуществления настройки регистрации событий безопасности указанной операционной системы необходимо перейти в Панель управления/Система и безопасность/ Администрирование/ Локальная политика безопасности/ Конфигурация расширенной политики аудита (Рисунок 1).

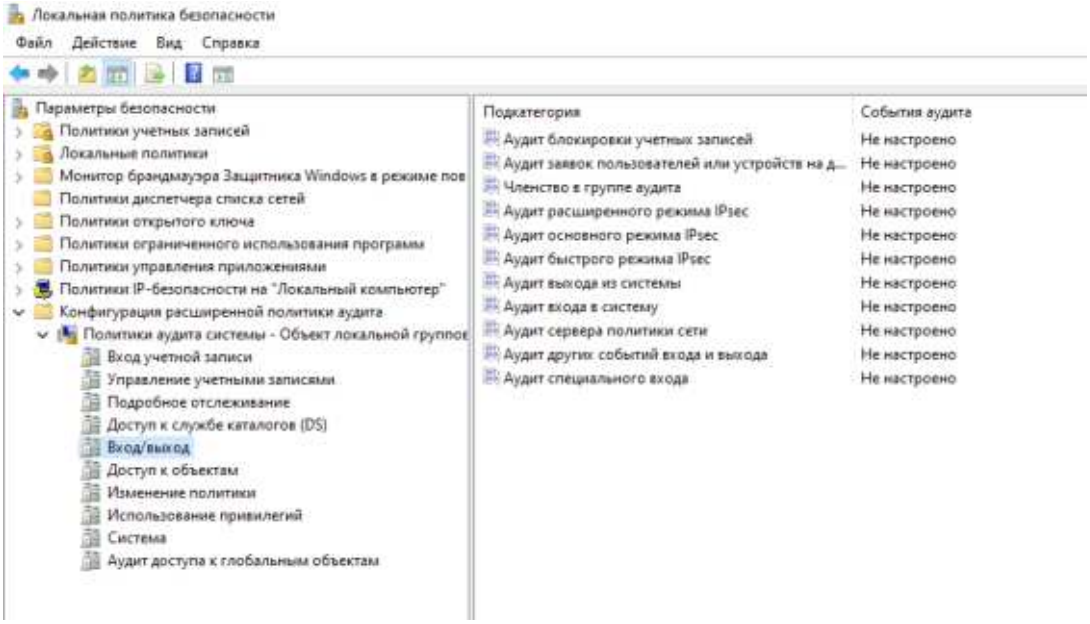

Рисунок 1 – настройка локальных политик безопасности

2. Для каждой из политик необходимо установить флаг в соответствующих полях «успех», «отказ», нажав на строку с настраиваемой политикой левой кнопкой мыши (Рисунок 2).

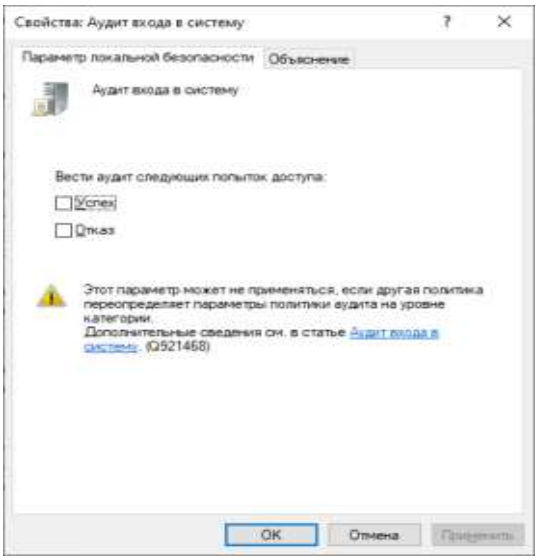

Рисунок 2 – Установка флагов на поля аудита

3. Настроить политики аудита операционной системы в соответствии с рекомендуемыми настройками, указанными в таблице 1.

Таблица 1. Рекомендуемые настройки аудита Windows

Категория	Подкатегория	Включить	Хост (контроллер домена, сервер, АРМ)	Категория (успех / отказ)
Вход учетной записи	Аудит проверки учетных данных	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит службы проверки подлинности Kerberos	+	контроллер домена	Успех и отказ
	Аудит операций с билетами службы Kerberos	+	контроллер домена	Успех и отказ
	Аудит других событий входа учетных записей	-		
Управление учетными записями	Аудит управления группами приложений	+	контроллер домена	Успех и отказ
	Аудит управления учетными записями компьютеров	+	контроллер домена	Успех
	Аудит управления группами распространения	+	контроллер домена	Успех
	Аудит других событий управления учетными записями	+	контроллер домена, сервер, АРМ	Успех
	Аудит управления группами безопасности	+	контроллер домена, сервер, АРМ	Успех
	Аудит управления учетными записями пользователей	+	контроллер домена, сервер, АРМ	Успех и отказ
Подробное отслеживание	Аудит активности DPAPI	+	контроллер домена, сервер, АРМ	Успех и отказ
	PNP-действие аудита	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит создания процессов	+	контроллер домена, сервер, АРМ	Успех
	Аудит завершения процессов	-		
	Аудит событий RPC	-		
	Проверка изменений прав маркера	-		
Доступ к службе каталогов (DS)	Аудит подробной репликации службы каталогов	+	контроллер домена	Успех и отказ
	Аудит доступа к службе каталогов	+	контроллер домена	Успех и отказ
	Аудит изменения службы каталогов	+	контроллер домена	Успех и отказ
	Аудит репликации службы каталогов	+	контроллер домена	Успех и отказ

Категория	Подкатегория	Включить	Хост (контроллер домена, сервер, АРМ)	Категория (успех / отказ)
Вход/выход	Аудит блокировки учетных записей	+	контроллер домена, сервер, АРМ	Отказ
	Аудит заявок пользователей или устройств на доступ	-		
	Членство в группе аудита	-		
	Аудит расширенного IPsec	-		
	Аудит основного IPsec	-		
	Аудит быстрого IPsec	-		
	Аудит выхода из системы	+	контроллер домена, сервер, АРМ	Успех
	Аудит входа в систему	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит сервера политики сети	-		
	Аудит событий входа и выхода	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит специального входа	+	контроллер домена, сервер, АРМ	Успех
Доступ к объектам	Аудит событий, создаваемых приложениями	-		
	Аудит служб сертификации	-		
	Аудит сведений об общем файловом ресурсе	-		
	Аудит общего файлового ресурса	-		
	Аудит файловой системы	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит подключения платформы фильтрации	-		
	Аудит отбрасывания пакетов платформой фильтрации	-		
	Аудит работы с дескрипторами	-		
	Аудит объектов ядра	-		
	Аудит других событий доступа к объектам	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит реестра	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит съемного носителя	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит диспетчера учетных записей безопасности	-		
	Аудит сверки с централизованной политикой доступа	-		
Изменение политики	Аудит изменения политики аудита	+	контроллер домена, сервер, АРМ	Успех

Категория	Подкатегория	Включить	Хост (контроллер домена, сервер, АРМ)	Категория (успех / отказ)
	Аудит изменения политики проверки подлинности	+	контроллер домена, сервер, АРМ	Успех
	Аудит изменения политики авторизации	+	контроллер домена, сервер, АРМ	Успех
	Аудит изменения политики платформы фильтрации	-		
	Аудит изменения политики на уровне правил MPSSVC	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит других событий изменения политики	-		
Использование привилегий	Аудит использования привилегий, не затрагивающих конфиденциальные данные	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит других событий использования привилегий	-		
	Аудит использования привилегий, затрагивающих конфиденциальные данные	+	контроллер домена, сервер, АРМ	Успех и отказ
Система	Аудит драйвера IPsec	-		
	Аудит других системных событий	+	контроллер домена, сервер, АРМ	Успех и отказ
	Аудит изменения состояния безопасности	+	контроллер домена, сервер, АРМ	Успех
	Аудит расширения системы безопасности	+	контроллер домена, сервер, АРМ	Успех
	Аудит целостности системы	-		
Аудит доступа к глобальным объектам	Файловая система	-		
	Реестр	-		

4. Настроить размеры журналов событий безопасности операционной системы Windows, перейдя в Панель управления/ Панель управления/Система и безопасность/ Администрирование/ Просмотр событий/ Журналы Windows / Безопасность / Свойства (Рисунок 3,4).

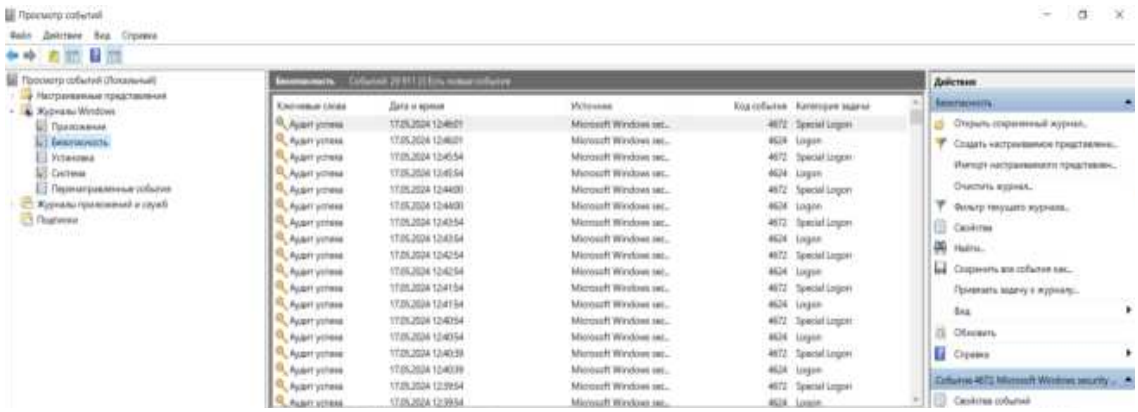

Рисунок 3 – Просмотр событий

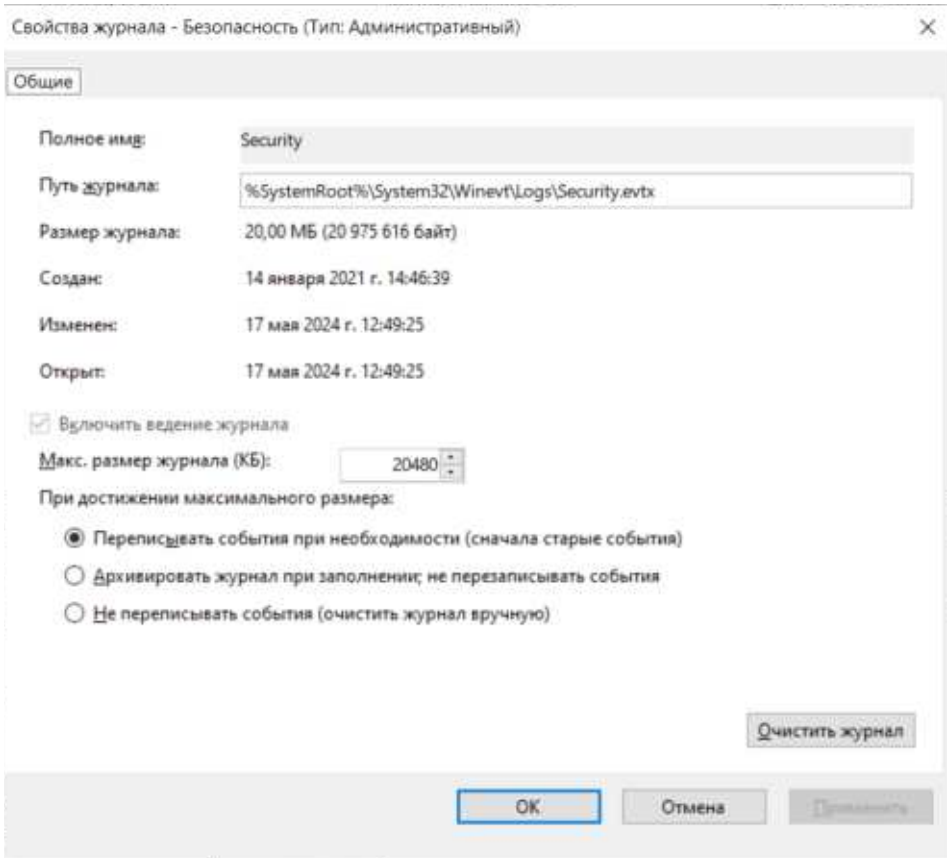

Рисунок 4 – Свойства журнала «Безопасность»

Приложение 2

Рекомендации по настройке регистрации событий безопасности в операционных системах на базе Linux

Для операционных систем на базе Linux для реализации регистрации событий безопасности рекомендуется использовать службу Auditd.

1. В случае отсутствия указанной службы на автоматизированном рабочем месте, сервере, контроллере домена, необходимо выполнить её установку на каждом объекте регистрации событий путем выполнения в терминале следующей команды:

apt-get install auditd

2. После установки необходимо запустить и включить службу путем выполнения в терминале следующих команд:

sudo systemctl start auditd

sudo systemctl enable auditd

3. Осуществить настройку службы Auditd путем редактирования параметров конфигурационного файла, который находится в директории */etc/audit/auditd.conf,* где *max_log_file* — максимальный размер журнального файла аудита в мегабайтах, *num_logs* — максимальное количество журнальных файлов аудита, *log_file* – путь к журнальному файлу аудита, *log_group* – группа, которой принадлежит журнальный файл аудита.

4. Настройку правил регистрации событий безопасности необходимо осуществлять используя утилиту auditctl. Наборы правил содержатся в файлах */etc/audit/audit.rules* и */etc/audit/rules.d/*.rules*. В таблице 1 представлены примеры правил для осуществления регистрации событий в операционных системах Linux.

Таблица 1. Примеры рекомендуемых настроек регистрации событий безопасности

Категория	**Правила**
Отслеживание изменений в директории или файле	sudo auditctl -w /var/log -p w -k var_log_changes
Аудит пользователей, групп, базы данных паролей	sudo auditctl -w /etc/group -p wa -k etcgroup
	sudo auditctl -w /etc/passwd -p wa -k etcpasswd
	sudo auditctl -w /etc/gshadow -k etcgroup
	sudo auditctl -w /etc/shadow -k etcpasswd
	sudo auditctl -w /etc/security/opasswd -k opasswd
	sudo auditctl -w /etc/adduser.conf -k adduserconf
Аудит изменений в файле Sudoers	sudo auditctl -w /etc/sudoers -p wa -k actions
Аудит паролей	sudo auditctl -w /usr/bin/passwd -p x -k passwd_modification

Категория	Правила
	sudo auditctl -w /usr/bin/gpasswd -p x -k gpasswd_modification
Аудит изменения идентификаторов групп	sudo auditctl -w /usr/sbin/groupadd -p x -k group_modification
	sudo auditctl -w /usr/sbin/groupmod -p x -k group_modification
	sudo auditctl -w /usr/sbin/addgroup -p x -k group_modification
	sudo auditctl -w /usr/sbin/useradd -p x -k user_modification
	sudo auditctl -w /usr/sbin/usermod -p x -k user_modification
	sudo auditctl -w /usr/sbin/adduser -p x -k user_modification
Аудит конфигурации и входов	sudo auditctl -w /etc/login.defs -p wa -k login
	sudo auditctl -w /etc/securetty -p wa -k login
	sudo auditctl -w /var/log/faillog -p wa -k login
	sudo auditctl -w /var/log/lastlog -p wa -k login
	sudo auditctl -w /var/log/tallylog -p wa -k login
Отслеживание запуска определенного приложения	sudo auditctl -a exit,always -F path=/usr/bin/myapp -F perm=x -k myapp_execution
Отслеживание системных вызовов	sudo auditctl -a exit,always -F arch=b64 -S execve -F uid=0 -k authentication_events
	sudo auditctl -a exit,always -F arch=b32 -S execve -F uid=0 -k authentication_events
Отслеживание сетевых подключений	sudo auditctl -a exit,always -F arch=b64 -S bind -S connect -F success=0 -k network_events
Запись в журнал аудита при подключении устройства USB	sudo auditctl -w /dev/bus/usb -p rwxa -k usb

5. Для просмотра событий безопасности необходимо использовать утилиту *aureport*. Собранная информация хранится в директории */var/log/audit/*, а файлы имеют расширение *.log*. Пример команды: *aureport option -if filename*.