ПАМЯТКА:

ИСПОЛЬЗОВАНИЕ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ СОБЫТИЯМИ ИБ (SIEM-СИСТЕМ) ДЛЯ ВЫПОЛНЕНИЯ НОРМАТИВНЫХ ТРЕБОВАНИЙ К ЗАЩИТЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ.



1. ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ОБЪЕКТОВ КИИ

С 2018 года действует Федеральный закон № 187-ФЗ **«О безопасности критической информационной инфраструктуры Российской Федерации»**. Согласно ст. 2 этого закона, к субъектам КИИ относятся организации, которым принадлежат информационные системы и автоматизированные системы управления в сферах:

- Оборонной, горнодобывающей, ракетно-космической, химической промышленности и металлургии;
- Топливного комплекса и энергетики, в т.ч. атомной;
- Финансового сектора;
- Транспорта;
- Здравоохранения;
- Науки;
- Связи;
- Регистрации прав и сделок с недвижимостью,

а также лица, обеспечивающие взаимодействие этих систем, например, ИТ-подрядчики организаций этих отраслей.

С 2022 года, в соответствии с Указом Президента РФ № 250 от 01.05.2022, в таких организациях создаются ИБ-подразделения, подчиненные заместителям руководителей предприятий по информационной безопасности. Эти подразделения несут функции по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Набор мероприятий в рамках этих направлений работы для объектов КИИ устанавливается Приказом ФСТЭК № 239 от 25.12.2017. К ним относятся задачи как организационного, так и технического характера, однако наиболее значительные и обязательные для субъектов КИИ всех категорий блоки мер выполняются с помощью систем мониторинга и управления событиями ИБ (SIEM).



Ниже приведен перечень мер безопасности объектов КИИ в соответствии с Приказом ФСТЭК № 239, выполнение которых осуществляется систем мониторинга и управления событиями ИБ (SIEM):

Наименование меры	Категории значимости объектов КИИ, для которых выполнение меры обязательно	Выполнение с помощью систем мониторинга и управления событиями ИБ (SIEM)
Аудит безопасности		
АУД.1 Инвентаризация информационных ресурсов	1, 2, 3	Выполняется полностью
АУД.2 Анализ уязвимостей и их устранение	1, 2, 3	Выполняется частично
АУД.3 Генерирование временных меток и (или) синхронизация системного времени	1, 2, 3	Выполняется полностью
АУД.4 Регистрация событий безопасности	1, 2, 3	Выполняется полностью
АУД.5 Контроль и анализ сетевого трафика	1	Выполняется частично
АУД.6 Защита информации о событиях безопасности	1, 2, 3	Выполняется полностью
АУД.7 Мониторинг безопасности	1, 2, 3	Выполняется полностью
АУД.8 Реагирование на сбои при регистрации событий безопасности	1, 2, 3	Выполняется полностью
АУД.9 Анализ действий отдельных пользователей	1	Выполняется полностью
АУД.10 Проведение внутренних аудитов	1, 2, 3	Выполняется полностью
Реагирование на компьютерные инциденты		
ИНЦ.1 Выявление компьютерных инцидентов	1, 2, 3	Выполняется полностью
ИНЦ.2 Информирование о компьютерных инцидентах	1, 2, 3	Выполняется полностью
ИНЦ.3 Анализ компьютерных инцидентов	1, 2, 3	Выполняется полностью
ИНЦ.4 Устранение последствий компьютерных инцидентов	1, 2, 3	Обеспечивается контроль выполнения
ИНЦ.5 Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	1, 2, 3	Обеспечивается контроль выполнения
ИНЦ.6 Хранение и защита информации о компьютерных инцидентах	1, 2, 3	Выполняется полностью
Управление доступом		
УПД.12 Управление атрибутами безопасности		Выполняется полностью
Обеспечение целостности		
ОЦЛ.4 Контроль данных, вводимых в информационную (автоматизированную) систему	1, 2	Выполняется полностью
Обеспечение доступности		
ОДТ.3 Контроль безотказного функционирования средств и систем	1, 2	Выполняется полностью
ОДТ.5 Обеспечение возможности восстановления информации	1, 2, 3	Выполняется полностью
Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)		
ЗИС.33 Исключение доступа через общие ресурсы	1	Выполняется частично

Выполнение требований к защите КИИ ФСТЭК оценивает по Методике от 11.11.2025. Показатель минимально необходимого уровня защищенности – 1 балл. Ниже приведен перечень оцениваемых параметров, выполняемых с помощью систем мониторинга и управления событиями ИБ (SIEM)*:

Показатель	Как выполняется	Оценка
Защита пользователей: реализована многофакторная аутентификация 50% и более привилегированных пользователей	Дополнительная возможность: подключение к системе мониторинга и управления событиями ИБ (SIEM) мультифактора для контроля условий входа	0,3*0,25
Защита пользователей: отсутствуют учетные записи разработчиков и сервисные учетные записи с паролями, установленными по умолчанию	Дополнительная возможность: контроль сроков, прошедших с последней смены пароля	0,2*0,25
Защита пользователей: отсутствуют активные учетные записи работников, отношения с которыми прекращены	Дополнительная возможность: контроль активных и неактивных учетных записей	0,2*0,25
Защита ИС: на доступных из Интернета устройствах и интерфейсах отсутствуют уязвимости критического уровня с датой публикации обновлений более 30 дней или для них приняты компенсирующие меры	Дополнительная возможность: подключение к SIEM сканера уязвимостей для мониторинга данных об уязвимостях и расследования инцидентов	0,25*0,35
Защита ИС: на 90% пользовательских устройств и серверов отсутствуют уязвимости критического уровня с датой публикации обновления более 90 дней или для них приняты компенсирующие меры		0,15*0,35
Защита ИС: обеспечено централизованное управление средствами антивирусной защиты на 80% пользовательских устройств, обновление баз антивирусов 1 раз в месяц	Дополнительная возможность: мониторинг работы антивирусной защиты	0,15*0,35
Мониторинг ИБ и реагирование: реализован централизованный сбор событий ИБ, оповещение о неудачных попытках входа для привилегированных учетных записей	Основная возможность: выполняется полностью	0,4*0,3
Мониторинг ИБ и реагирование: реализован централизованный сбор и анализ событий ИБ на всех устройствах, взаимодействующих с Интернетом	Основная возможность: выполняется полностью	0,35*0,3
Итого: меры, выполняемые с применением систем мониторинга и управления событиями ИБ (SIEM)		**0,5925**
Справочно: меры, выполняемые без применения технических средств		*0,175*
Справочно: меры, выполняемые с помощью других СЗИ		*0,2325*

*- выполнение требований к защите ОКИИ, согласно указанной методике, помимо оценки указанных параметров, предполагает выявление уязвимостей путем тестирования на проникновение.

2. ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Кроме обеспечения безопасности объектов КИИ, системы мониторинга и управления событиями ИБ (SIEM) позволяют выполнять требования приказа ФСТЭК № 21, который регламентирует защиту информационных систем персональных данных. Ниже приведен перечень мер безопасности, выполняемых с помощью таких систем согласно данному приказу:

Наименование меры	Категории значимости ИСПдН, для которых выполнение меры обязательно	Выполнение с помощью систем мониторинга и управления событиями ИБ (SIEM)
РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения	1-4	Выполняется полностью
РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	1-4	Выполняется полностью
РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	1-4	Выполняется полностью
РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	1, 2	Выполняется полностью
ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора	1-4	Выполняется полностью
УПД.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	1-4	Выполняется полностью
УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	1-4	Выполняется полностью
ИНЦ.2 Обнаружение, идентификация и регистрация инцидентов	1, 2	Выполняется полностью
ИНЦ.4 Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	1, 2	Выполняется полностью



3. ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ПО ИНФОРМИРОВАНИЮ УПОЛНОМОЧЕННЫХ ОРГАНОВ

Кроме указанных мер, обязанностью субъектов КИИ, согласно п.1 ч. 2, ч. 4 ст. 9 187-ФЗ, является незамедлительное уведомление уполномоченных органов о компьютерных инцидентах и атаках. В случаях нарушения сроков и порядка уведомления (утв. Приказами ФСБ № 368 от 24.07.2018 и № 77 от 13.02.2023), субъект КИИ может быть подвергнут штрафу в размере до 500 000 рублей по ст. 13.12.1 КоАП РФ. Операторы персональных данных также, согласно п. 12 ст. 19 152-ФЗ, обязаны сообщать властям об инцидентах с персональными данными.

С учетом необходимости оперативного и формализованного информирования уполномоченного органа, российские разработчики систем мониторинга и управления событиями ИБ (SIEM) включают в свои решения функцию автоматизированного составления и отправки отчета. Таким образом, заказчик получает не только средство защиты информации, но и готовый канал взаимодействия с НКЦКИ, не требующий затрат на самостоятельное формирование и отправку отчетной документации:

Наименование меры	Срок выполнения	Категории организаций, для которых выполнение меры обязательно	Норма законодательства	Выполнение с помощью систем мониторинга и управления событиями ИБ (SIEM)
Информирование уполномоченного органа о компьютерных инцидентах через систему ГосСОПКА	Для значимых ОКИИ – 3 часа с момента обнаружения инцидента; Для остальных ОКИИ – 24 часа с момента обнаружения инцидента	Субъекты КИИ, государственные органы, учреждения, унитарные предприятия, фонды, госкорпорации, организации с основным государственным участием	П. 2 ч.1, ч.4 ст. 9 ФЗ № 187-ФЗ «О безопасности КИИ РФ» Пп. «б» п. 1 ст. 1 ФЗ от 29.12.2025 № 568-ФЗ П. 3 приказа ФСБ России от 25.12.2025 № 547	Отчет для системы ГосСОПКА формируется автоматически, отправка производится нажатием кнопки
Информирование уполномоченного органа об инцидентах с персональными данными через систему ГосСОПКА	24 часа с момента обнаружения инцидента	Операторы персональных данных, подключенные к системе ГосСОПКА	П. 12 ст. 19 ФЗ № 152-ФЗ «О персональных данных»; п. 2 Приказа ФСБ России от 13.02.2023 № 77	

4. ИМПОРТОЗАМЕЩЕНИЕ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ СОБЫТИЯМИ ИБ (SIEM) И ТРЕБОВАНИЯ К ИХ ВЫБОРУ

Выбор применяемых ИБ-решений для объектов КИИ также регламентирован. Согласно ст. 28 Приказа ФСТЭК № 239, средства защиты объектов КИИ должны быть сертифицированы, а применение ИБ-решений из недружественных стран, в соответствии со ст. 6 Указа Президента № 250, запрещено с 2025 года. Современные российские решения по своим функциям не уступают, а в некоторых отношениях и превосходят такие иностранные продукты как:

- Qradar SIEM;
- Splunk;
- ArcSight SIEM;
- AlienVault OSSIM;
- FireEye XDR;
- Fortinet FortiSIEM;
- LogRhythm NextGen SIEM Platform;
- McAfee ESM.



Еще одним преимуществом российских систем мониторинга и управления событиями ИБ (SIEM), наряду с соответствием регуляторным требованиям, является их совместимость и возможность обмена данными с другими российскими программными продуктами. Ниже приведены некоторые из них.

Класс продукта	Наименование продукта	Уровень интеграции с системами мониторинга и управления событиями ИБ (SIEM)
Операционные системы	Astra Linux Special Edition	Информационный обмен, логирование данных
	ALT Linux	
	РЕД ОС	
Операционные системы рабочих мест	Astra Linux Desktop	
	Альт Рабочая станция	
Системы контроля инфраструктуры	РЕД АДМ	
	ALD Pro	
СУБД	Postgres Pro	
ПАК	UserGate	
	АПКШ «Континент» 3.9 / 4.0	
	ViPNet Coordinator VA / HW	
Группа продуктов	1С: Предприятие	
Система защиты от утечек информации (DLP)	СёрчИнформ КИБ	
Средства защиты информации	Сканер уязвимостей RedCheck	
	Kaspersky Endpoint Security	
	СКУД RusGuard	
	PT Application Firewall	
	Secret Net Studio	