{KOMRAD} Enterprise SIEM

Эшелон комплексная безопасность

Соответствие KOMRAD Enterprise SIEM 4 требованиям ГОСТ Р 57580.1-2017

- Безопасность финансовых (банковских) операций
- Защита информации финансовых организаций
- Базовый состав организационных и технических мер

KOMRAD Enterprise SIEM 4 дает полную видимость IT-инфраструктуры и выявляет инциденты информационной безопасности.

Для соответствия **ГОСТ Р 57580.1-2017** о безопасности финансовых операций кредитным и некредитным финансовым организациям необходимы SIEM-системы, поскольку они позволяют реализовать меры процесса «Управления инцидентами защиты информации». В этот процесс входят 32 технические меры по мониторингу и анализу событий защиты информации, обнаружению инцидентов и реагированию на них.

KOMRAD Enterprise SIEM 4 позволяет покрыть ещё 65 технических мер ГОСТа. Итого с помощью продукта заказчики могут реализовать 97 мер. В этом документе представлены требования, которые вы сможете покрыть с KOMRAD Enterprise SIEM 4.

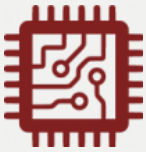
Требования к системе защиты информации

Способы реализации мер защиты информации:

- «О» – реализация путем применения организационной меры защиты информации;
- «Т» – реализация путем применения технической меры защиты информации;
- «Н» – реализация является необязательной.

По желанию финансовой организации, способ «О» может быть реализован с помощью технической меры защиты информации.

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
ПРОЦЕСС 1 «Обеспечение защиты информации при управлении доступом»				
ПОДПРОЦЕСС «Управление учетными записями и правами субъектов логического доступа»				
УЗП.22	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего привилегированными правами логического доступа, позволяющими осуществить деструктивное воздействие, приводящие к нарушению выполнения бизнес-процессов или технологических процессов финансовой организации.	Н	Т	Т
УЗП.23	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для финансовой организации, клиентов и контрагентов.	Т	Т	Т
УЗП.24	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению логическим доступом.	Т	Т	Т
УЗП.25	Регистрация событий защиты информации, связанных с действиями по управлению учетными записями и правами субъектов логического доступа	Т	Т	Т
УЗП.26	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению техническими мерами, реализующими многофакторную аутентификацию.	Н	Т	Т



Низкие требования к аппаратному обеспечению

Визуальный конструктор правил

ГОССОПКА
Обнаружение. Предупреждение. Ликвидация.

Встроенная возможность интеграции с системой ГосСОПКА

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
УЗП.27	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по изменению параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации.	Н	Т	Т
УЗП.28	Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами.	Т	Т	Т
ПОДПРОЦЕСС «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»				
РД.39	Регистрация выполнения субъектами логического доступа ряда неуспешных последовательных попыток аутентификации.	Н	Т	Т
РД.40	Регистрация осуществления субъектами логического доступа идентификации и аутентификации.	Т	Т	Т
РД.41	Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС.	Т	Т	Т
РД.42	Регистрация запуска программных сервисов, осуществляющих логический доступ.	Н	Т	Т
РД.43	Регистрация изменений аутентификационных данных, используемых для осуществления логического доступа.	Н	Т	Т
ПОДПРОЦЕСС «Идентификация и учет ресурсов и объектов доступа»				
ИУ.1	Учет созданных, используемых и (или) эксплуатируемых ресурсов доступа.	О	Т	Т
ИУ.2	Учет используемых и (или) эксплуатируемых объектов доступа.	О	О	Т
ИУ.3	Учет эксплуатируемых общедоступных объектов доступа (в том числе банкоматов, платежных терминалов).	О	О	Т
ИУ.5	Контроль выполнения операций по созданию, удалению и резервному копированию ресурсов доступа (баз дан-ных, сетевых файловых ресурсов, виртуальных машин).	Н	Т	Т
ИУ.7	Регистрация событий защиты информации, связанных с созданием, копированием, в том числе резервным, и (или) удалением ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин).	Н	Т	Т
ИУ.8	Регистрация событий защиты информации, связанных с подключением (регистрацией) объектов доступа в вычислительных сетях финансовой организации.	Н	Н	Т

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
ПРОЦЕСС 2 «Обеспечение защиты вычислительных сетей»				
ПОДПРОЦЕСС «Сегментация и межсетевое экранирование вычислительных сетей»				
СМЭ.21	Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей финансовой организации.	Т	Т	Т
ПОДПРОЦЕСС «Выявление вторжений и сетевых атак»				
ВСА.1	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между сегментами контуров безопасности и иными внутренними вычислительными сетями финансовой организации.	Н	Н	Т
ВСА.2	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между вычислительными сетями финансовой организации и сетью Интернет.	Н	Т	Т
ВСА.3	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным информационным взаимодействием между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет.	Н	Н	Т
ВСА.4	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным логическим доступом к ресурсам доступа, размещенным в вычислительных сетях финансовой организации, подключенных к сети Интернет.	Н	Т	Т
ВСА.5	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным удаленным доступом.	Н	Т	Т
ВСА.6	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным логическим доступом к ресурсам доступа, размещенным во внутренних вычислительных сетях финансовой организации.	Н	Н	Т
ВСА.7	Контроль отсутствия (выявление) аномальной сетевой активности, связанной с возможным несанкционированным доступом к аутентификационным данным легальных субъектов доступа.	Н	Н	Т
ПОДПРОЦЕСС «Защита беспроводных сетей»				
ЗБС.7	Реализация и контроль информационного взаимодействия внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3, в соответствии с установленными правилами и протоколами сетевого взаимодействия.	Н	Т	Т
ЗБС.10	Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3.	Н	Т	Т

{KOMRAD} Enterprise SIEM

Эшелон комплексная безопасность

Виды лицензий:

Base:

- Развертывание на одном узле
- Коллектор на выбор
- Ограничение 500 EPS
- Год технической поддержки «Стандарт»
- Возможность покупки дополнительных коллекторов
- Возможность расширения до All-in-one

All-in-one:

- Развертывание на одном узле
- Доступны все типы коллекторов
- Неограниченное количество EPS с источников
- Год технической поддержки уровня «Стандарт»
- Сертификат на авторизованное обучение одного специалиста
- Возможность повысить уровень лицензии до Enterprise

Enterprise:

- Развертывание на нескольких узлах
- Доступны все типы коллекторов
- Неограниченное количество EPS с источников
- Год технической поддержки уровня «Стандарт»
- Сертификат на авторизованное обучение двух специалистов

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
ПРОЦЕСС 3 «Контроль целостности и защищенности информационной инфраструктуры»				
ЦЗИ.28	Регистрация установки, обновления и (или) удаления ПО АС, ПО средств и систем защиты информации, системного ПО на серверном и сетевом оборудовании.	Н	Т	Т
ЦЗИ.29	Регистрация установки, обновления и (или) удаления прикладного ПО, ПО АС, ПО средств и систем защиты информации, системного ПО на АРМ пользователей и эксплуатационного персонала.	Н	Т	Т
ЦЗИ.30	Регистрация запуска программных сервисов.	Н	Н	Т
ЦЗИ.31	Регистрация результатов выполнения операций по контролю состава ПО серверного оборудования, АРМ пользователей и эксплуатационного персонала.	Н	Н	Т
ЦЗИ.32	Регистрация результатов выполнения операций по контролю состава ПО АРМ пользователей и эксплуатационного персонала.	Н	Т	Т
ЦЗИ.33	Регистрация результатов выполнения операций по контролю состава ПО, запускаемого при загрузке операционной системы АРМ пользователей и эксплуатационного персонала.	Н	Т	Т
ПРОЦЕСС 4 «Защита от вредоносного кода»				
ЗВК.11	Контроль отключения и своевременного обновления средств защиты от вредоносного кода.	Т	Т	Т
ЗВК.22	Регистрация операций по проведению проверок на отсутствие вредоносного кода.	Т	Т	Т
ЗВК.23	Регистрация фактов выявления вредоносного кода.	Т	Т	Т
ЗВК.24	Регистрация неконтролируемого использования технологии мобильного кода*.	Т	Т	Т
ЗВК.25	Регистрация сбоев в функционировании средств защиты от вредоносного кода.	Т	Т	Т
ЗВК.26	Регистрация сбоев в выполнении контроля (проверок) на отсутствие вредоносного код.	Т	Т	Т
ЗВК.27	Регистрация отключения средств защиты от вредоносного кода.	Т	Т	Т
ЗВК.28	Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода.	Т	Т	Т
ПРОЦЕСС 5 «Предотвращение утечек информации»				
ПУИ.28	Регистрация использования разблокированных портов ввода-вывода информации СВТ.	Н	Т	Т
ПУИ.29	Регистрация операций, связанных с осуществлением доступа работниками финансовой организации к ресурсам сети Интернет.	Н	Т	Т
ПУИ.30	Регистрация фактов вывода информации на печать.	Н	Т	Т

Для реализации процесса 6 необходима SIEM-система

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
ПРОЦЕСС 6 «Управление инцидентами защиты информации»				
ПОДПРОЦЕСС «Мониторинг и анализ событий защиты информации»				
МАС.1	Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации.	Т	Т	Т
МАС.2	Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевым оборудованием, в том числе активным сетевым оборудованием, маршрутизаторами, коммутаторами.	Н	Т	Т
МАС.3	Организация мониторинга данных регистрации о событиях защиты информации, формируемых сетевыми приложениями и сервисами.	Н	Т	Т
МАС.4	Организация мониторинга данных регистрации о событиях защиты информации, формируемых системным ПО, операционными системами, СУБД.	Н	Т	Т
МАС.5	Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями.	Т	Т	Т
МАС.6	Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов.	Т	Т	Т
МАС.7	Организация мониторинга данных регистрации о событиях защиты информации, формируемых средствами (системами) контроля и управления доступом.	Н	Н	Т
МАС.8	Централизованный сбор данных регистрации о событиях защиты информации, формируемых объектами информатизации, определенных мерами МАС.1-МАС.7.	Н	Т	Т
МАС.9	Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации.	Т	Т	Т
МАС.10	Контроль формирования данных регистрации о событиях защиты информации объектов информатизации, определенных мерами МАС.1- МАС.7.	О	Т	Т
МАС.11	Реализация защиты данных регистрации о событиях защиты информации от раскрытия и модификации, двухсторонней аутентификации при передаче данных регистрации с использованием сети Интернет.	Н	Т	Т
МАС.12	Обеспечение гарантированной доставки данных регистрации о событиях защиты информации при их централизованном сборе.	Н	Т	Т
МАС.13	Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации	Т	Т	Т
МАС.14	Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечение целостности и доступности хранимых данных регистрации.	Т	Т	Т
МАС.15	Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет.	Т	Т	Н
МАС.16	Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение пяти лет.	Н	Н	Т
МАС.17	Обеспечение возможности выполнения операции нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации.	Н	Т	Т
МАС.18	Обеспечение возможности выявления и анализа событий защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД*.	Т	Т	Т

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
МАС.19	Обеспечение возможности определения состава действий и (или) операций конкретного субъекта доступа.	Т	Т	Т
МАС.20	Обеспечение возможности определения состава действий и (или) операций субъектов доступа при осуществлении логического доступа к конкретному ресурсу доступа.	Т	Т	Т
МАС.21	Регистрация нарушений и сбоев в формировании и сборе данных о событиях защиты информации.	Н	Т	Т
МАС.22	Регистрация доступа к хранимым данным о событиях защиты информации.	Т	Т	Т
МАС.23	Регистрация операций, связанных с изменением правил нормализации (приведения к единому формату), фильтрации, агрегации и классификации данных регистрации о событиях защиты информации.	Н	Т	Т
ПОДПРОЦЕСС «Обнаружение инцидентов защиты информации и реагирование на них»				
РИ.1	Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации.	О	Т	Т
РИ.2	Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов финансовой организации.	О	Т	Т
РИ.3	Классификация инцидентов защиты информации с учетом степени их влияния (критичности) на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов финансовой организации.	О	О	Т
РИ.10	Своевременное (оперативное) оповещение членов ГРИЗИ о выявленных инцидентах защиты информации.	Н	Т	Т
РИ.15	Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации.	Т	Т	Т
РИ.16	Разграничение доступа членов ГРИЗИ к информации об инцидентах защиты информации в соответствии с определенным распределением ролей, связанных с реагированием на инциденты защиты информации.	Н	Т	Т
РИ.17	Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет.	Т	Т	Н
РИ.18	Обеспечение возможности доступа к информации об инцидентах защиты информации в течение пяти лет.	Н	Н	Т
РИ.19	Регистрация доступа к информации об инцидентах защиты информации.	Т	Т	Т
ПРОЦЕСС 7 «Защита среды виртуализации»				
ЗСВ.32	Регистрация операций, связанных с запуском (остановкой) виртуальных машин.	Т	Т	Т
ЗСВ.33	Регистрация операций, связанных с изменением параметров настроек виртуальных сетевых сегментов, реализованных средствами гипервизора.	Н	Т	Т
ЗСВ.34	Регистрация операций, связанных с созданием и удалением виртуальных машин.	Т	Т	Т
ЗСВ.35	Регистрация операций, связанных с созданием, изменением, копированием, удалением базовых образов виртуальных машин.	Т	Т	Т
ЗСВ.36	Регистрация операций, связанных с копированием текущих образов виртуальных машин.	Т	Т	Т
ЗСВ.37	Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации.	Т	Т	Т

{KOMRAD} Enterprise SIEM

KOMRAD Enterprise SIEM включен в реестр рекомендованного отечественного программного обеспечения

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
ЗСВ.38	Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации.	Т	Т	Т
ЗСВ.39	Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации.	Т	Т	Т
ЗСВ.40	Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам.	Т	Т	Т
ЗСВ.41	Регистрация операций, связанных с запуском (остановкой) ПО серверных компонент виртуализации.	Н	Н	Т
ЗСВ.42	Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации.	Т	Т	Т
ЗСВ.43	Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин.	Т	Т	Т

Требования к организации и управлению защитой информации

Направление 2 «Реализация процесса системы защиты информации»

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
РЗИ.11	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 4 класса.	Н	Н	Т
РЗИ.12	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 5 класса.	Н	Т	Н
РЗИ.13	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса.	Т	Н	Н

Направление 3 «Контроль процесса системы защиты информации»

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
КЗИ.2	Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий: • контроль фактического размещения технических мер защиты информации в информационной инфраструктуре финансовой организации; • контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации.	О	О	Т

Условное обозначение и номер меры	Содержание мер системы	Уровень защиты информации		
		3	2	1
КЗИ.9	Регистрация операций по установке и (или) обновлению ПО технических средств защиты информации.	Н	Т	Т
КЗИ.10	Регистрация операций по обновлению сигнатурных баз технических средств защиты информации (в случае их использования).	Н	Т	Т
КЗИ.11	Регистрация операций по изменению параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации.	Н	Т	Т
КЗИ.12	Регистрация сбоев (отказов) технических мер защиты информации.	Н	Т	Т

{KOMRAD}
Enterprise SIEM

Эшелон
комплексная безопасность

Присоединяйтесь к сообществу KOMRAD Enterprise SIEM 4 в Telegram

Наши эксперты, партнеры и заказчики ответят на вопросы, посоветуют полезные ссылки и будут держать в курсе новостей продукта: t.me/komrad4

Подробную информацию о продукте, а также демоверсию решения вы можете получить, отправив запрос на getkomrad@npo-echelon.ru

Эшелон
комплексная безопасность

npo-echelon.ru

sales@npo-echelon.ru

Тел: +7 (495) 223-23-92
Факс: +7 (499) 113-45-09

107023, г. Москва,
ул. Электрозаводская, д. 24
(вход со стороны 2-го
Электрозаводского
переулка)

АО «НПО «Эшелон» представляет полный спектр услуг в области информационной безопасности.
Компании-разработчики программного обеспечения являются заказчиками услуг нашей компании по проведению сертификационных испытаний или экспертизы материалов сертификационных испытаний программного обеспечения по требованиям безопасности информации.

Коммерческим и государственным организациям среднего и крупного масштаба наши эксперты помогают выстроить комплексную систему защиты информации, соответствующую современным нормативным требованиям и актуальным угрозам информационной безопасности.

Компаниям, специализирующимся в области оказания услуг по защите информации, АО «НПО «Эшелон» помогает выполнить требования, предъявляемые к соискателям лицензий ФСТЭК России, ФСБ России, Минобороны России.

Деятельность компании осуществляется на основании более 30 лицензий и аттестатов аккредитации ФСТЭК России, ФСБ России и Минобороны России и др. АО «НПО «Эшелон» аккредитовано в качестве испытательной лаборатории ФСБ России, ФСТЭК России, Министерства обороны Российской Федерации, Органа по сертификации ФСТЭК России, Органа по аттестации ФСТЭК России, Аттестационного центра Минобороны России.
Система менеджмента качества компании сертифицирована на соответствие требованиям ISO 9001, ГОСТ ИСО 9001-2008, ГОСТ РВ 15.002-2003 и стандартов СРПП ВТ.