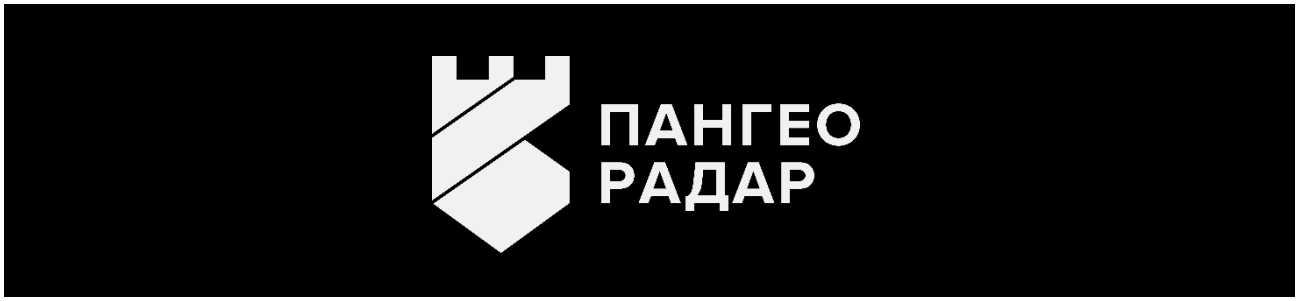

Безопасность финансовых (банковских) операций

Анализ соответствия SIEM «Платформа Радар» требованиям ГОСТ 57580.1-2017

Согласно Р ГОСТ 57580.1-2017 о безопасности финансовых операций кредитным и некредитным финансовым организациям требуется обеспечить безопасность с помощью комплекса технических и организационных мер. Для соответствия ГОСТ требуются решения по информационной безопасности различных классов.

Одним из основополагающих решений может по праву называться SIEM, так как SIEM реализует меры процесса «Управление инцидентами». В данный процесс входят 33 технические меры, однако, это не всё, что можно покрыть с помощью SIEM «Платформа Радар».

Всего с помощью SIEM «Платформа Радар» можно покрыть 119 технических мер, а также 24 меры покрыты для внутренних компонентов системы. Ниже вы можете ознакомиться с перечнем этих мер с разделением на процессы и подпроцессы.

Требования к СЗИ

Примечание:

- «**Т**» - требуется техническая мера защиты информации
- «**О**» - требуется организационная мера защиты информации
  (Способ реализации «О» может быть реализован технической мерой защиты информации)
- «**Н**» - мера является необязательной
- «*****» - система реализует данную меру для внутренних компонентов

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
Процесс 1 "Обеспечение защиты информации при управлении доступом" Подпроцесс "Управление учетными записями и правами субъектов логического доступа"				
УЗП.1 - *	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями	Т	Т	Т
УЗП.10 - *	Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа	Т	Т	Т
УЗП.11 - *	Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации	Т	Т	Т
УЗП.18 - *	Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа	О	Т	Т

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
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
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
УЗП.29	Закрепление АРМ пользователей и эксплуатационного персонала за конкретными субъектами логического доступа	Н	Н	О
Подпроцесс "Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа"				
РД.1 - *	Идентификация и однофакторная аутентификация пользователей	Т	Т	Н
РД.3 - *	Идентификация и однофакторная аутентификация эксплуатационного персонала	Т	Н	Н
РД.5 - *	Аутентификация программных сервисов, осуществляющих логический доступ с использованием технических учетных записей	Т	Т	Т
РД.8 - *	Сокрытие (неотображение) паролей при их вводе субъектами доступа	Т	Т	Т
РД.11 - *	Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин	Т	Т	Т
РД.13 - *	Обеспечение возможности выполнения субъектом логического доступа - работниками финансовой организации процедуры принудительного прерывания сессии логического доступа и (или) приостановки осуществления логического доступа (с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа)	Т	Т	Т
РД.14 - *	Автоматическое прерывание сессии логического доступа (приостановка осуществления логического доступа) по истечении установленного времени бездействия (неактивности) субъекта логического доступа, не превышающего 15 мин, с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа	Т	Т	Т
РД.15 - *	Выполнение процедуры повторной аутентификации для продолжения осуществления логического доступа после его принудительного или автоматического прерывания (приостановки осуществления логического доступа), предусмотренного мерами РД.13 и РД.14 настоящей таблицы	Т	Т	Т
РД.19 - *	Смена паролей пользователей не реже одного раза в год	Т	Т	Т
РД.20 - *	Смена паролей эксплуатационного персонала не реже одного раза в квартал Выполнение совместно с РД.19 возможно при аутентификации через AD.	Т	Т	Т

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
РД.21 - *	Использование пользователями паролей длиной не менее восьми символов	Т	Т	Т
РД.22 - *	Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов Выполнение совместно с РД.21 возможно при аутентификации через AD.	Т	Т	Т
РД.23 - *	Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры	Т	Т	Т
РД.25 - *	Обеспечение возможности самостоятельной смены субъектами логического доступа своих паролей	Т	Т	Т
РД.30 - *	Авторизация логического доступа к ресурсам доступа, в том числе АС	Т	Т	Т
РД.31 - *	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа	Т	Т	Т
РД.32 - *	Реализация ролевого метода (с определением для каждой роли прав доступа) при разграничении логического доступа в АС	Н	Н	Т
РД.33 - *	Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС	Т	Т	Т
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
РД.44	Регистрация действий пользователей и эксплуатационного персонала, предусмотренных в случае компрометации их аутентификационных данных	Н	О	О
Подпроцесс "Защита информации при осуществлении физического доступа"				
ФД.21	Регистрация событий защиты информации, связанных с входом (выходом) в помещения (из помещений), в которых расположены объекты доступа	Н	Н	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.4	Контроль фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректного размещения в сегментах вычислительных сетей финансовой организации	О	Т	Т
ИУ.5	Контроль выполнения операций по созданию, удалению и резервному копированию ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин)	Н	Т	Т
ИУ.6	Контроль фактического состава эксплуатируемых объектов доступа и их корректного размещения в сегментах вычислительных сетей финансовой организации	Н	О	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
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

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
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
ВСА.14	Регистрация фактов выявления аномальной сетевой активности в рамках контроля, предусмотренного мерами ВСА.1-ВСА.8 таблицы 16	Н	Т	Т
ЗВС.1 - *	Применение сетевых протоколов, обеспечивающих защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации при осуществлении логического доступа с использованием телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией	Т	Т	Т
ЗВС.2 - *	Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых финансовой организацией	Т	Т	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 настоящей таблицы, в соответствии с установленными правилами и протоколами сетевого взаимодействия	Н	Т	Т
ЗБС.9	Регистрация попыток подключения к беспроводным точкам доступа с незарегистрированных устройств доступа, в том числе из-за пределов финансовой организации	Н	Н	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 таблицы 20	Н	Т	Т
Процесс 3 "Контроль целостности и защищенности информационной инфраструктуры"				
ЦЗИ.1	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами контуров безопасности и иными внутренними сетями финансовой организации При импорте отчетов сканеров уязвимостей	Н	Т	Т

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЦЗИ.2	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между внутренними вычислительными сетями финансовой организации и сетью Интернет При импорте отчетов сканеров уязвимостей	О	Т	Т
ЦЗИ.3	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет При импорте отчетов сканеров уязвимостей	О	Т	Т
ЦЗИ.4	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным в вычислительных сетях финансовой организации, подключенных к сети Интернет При импорте отчетов сканеров уязвимостей	О	Т	Т
ЦЗИ.5	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный удаленный доступ При импорте отчетов сканеров уязвимостей	О	Т	Т
ЦЗИ.6	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным во внутренних вычислительных сетях финансовой организации При импорте отчетов сканеров уязвимостей	Н	Т	Т
ЦЗИ.12	Контроль размещения и своевременного обновления на серверном и сетевом оборудовании ПО средств и систем защиты информации, прикладного ПО, ПО АС, системного ПО и сигнатурных баз средств защиты информации, в том числе с целью устранения выявленных уязвимостей защиты информации При импорте отчетов сканеров уязвимостей	О	О	Т
ЦЗИ.13	Контроль размещения и своевременного обновления на АРМ пользователей и эксплуатационного персонала ПО средств и систем защиты информации, прикладного ПО, ПО АС и системного ПО, в том числе с целью устранения выявленных уязвимостей защиты информации	О	О	Т
ЦЗИ.15	Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации после выполнения обновлений ПО, предусмотренного мерой ЦЗИ.12 настоящей таблицы	О	Т	Т
ЦЗИ.20	Контроль состава разрешенного для использования ПО АРМ пользователей и эксплуатационного персонала	О	Т	Т
ЦЗИ.22	Контроль состава ПО серверного оборудования	Н	О	Т
ЦЗИ.23	Контроль состава ПО АРМ пользователей и эксплуатационного персонала, запускаемого при загрузке операционной системы	Н	Т	Т
ЦЗИ.27	Регистрация фактов выявления уязвимостей защиты информации	Н	Т	Т
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

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
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 кода	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
ПУИ.31	Регистрация результатов выполнения контентного анализа информации, предусмотренного мерами ПУИ.5, ПУИ.11, ПУИ.15, ПУИ.17 таблицы 30	Н	Т	Т
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 таблицы 33	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 таблицы 33	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

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
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
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.5	Установление и применение единых правил регистрации и классификации инцидентов защиты информации в части состава и содержания атрибутов, описывающих инцидент защиты информации, и их возможных значений	О	Т	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

Условное обозначение и номер меры	Содержание мер системы защиты информации	Уровень защиты информации		
		3	2	1
ЗСВ.37	Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации	Т	Т	Т
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
Направление 3 "Контроль процесса системы защиты информации"				
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
КЗИ.4	Периодический контроль (тестирование) полноты реализации технических мер защиты информации	О	Т	Т
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
Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений				
ЖЦ.22	Регистрация внесения изменений в АС, включая обновление прикладного ПО	Н	О	О
ЖЦ.23	Регистрация операций по изменению параметров настроек технических мер системы защиты информации АС	О	Т	Т

Как подробнее узнать о Платформе «Радар»?

Документация по продукту
docs.pangeoradar.ru

Сайт компании
pangeoradar.ru

Новостной канал в Telegram
t.me/pangeoradar

О компании

ООО "Пангео Радар" образовано в июне 2018 года для развития и продвижения на российском рынке кибербезопасности программной платформы «Radar Platform Rus» (далее - «Платформа Радар»), современного решения для автоматизации работы центров мониторинга и реагирования на события информационной безопасности (Security Operations Center, SOC).

Компания имеет лицензии ФСТЭК России на разработку и производство средств защиты информации, а также на деятельность по технической защите конфиденциальной информации (№1867 и №3566 от 11.02.2019г).,

«Платформа Радар» - новый российский продукт для построения SOC

– исходные коды и база знаний принадлежат российскому ООО «Пангео Радар», хранятся в репозитории на территории РФ, модернизируются российскими программистами;

- программное обеспечение «Radar Platform Rus» включено в единый реестр российских программ для ЭВМ и баз данных за № 4791 (Приказ Минкомсвязи России от 23.11.2018 № 651);

- Платформа Радар имеет сертификат ФСТЭК России на соответствие требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий по 4 уровню доверия, внесена в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации (№4210 от 5.02.2020).

Использование «Платформы Радар» рекомендуется при создании и модернизации SOC крупных российских предприятий и корпораций, в том числе – для замещения используемых в настоящее время программных решений иностранных правообладателей.