Безопасность значимых объектов критической информационной инфраструктуры

В соответствии с № 187-ФЗ

О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Согласно 187-ФЗ «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» предприятиям требуется соблюдать ряд требований, в том числе по взаимодействию с ГосСОПКА, а также обеспечивать безопасность с помощью комплекса технических и организационных мер. Для соответствия требованиям необходимо внедрение решений по информационной безопасности различных классов.

Одним из основополагающих решений может по праву называться SIEM, так как SIEM реализует меры категории «Реагирование на инциденты информационной безопасности (ИНЦ)». В данный процесс входят 6 мер защиты, однако, это не всё, что можно покрыть с помощью Платформы Радар.

В регулировании безопасности критической информационной инфраструктуры участвуют:

- **Федеральный закон от 26 июля 2017 г. № 187-ФЗ** "О безопасности критической информационной инфраструктуры Российской Федерации"
- **Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235** "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования"
- **Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239** “Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации”

Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 (п.18) добавляет требование по сертификации используемых СЗИ. Платформа Радар имеет сертификат ФСТЭК по 4 уровню доверия № 4210 от 05.02.2020 (переоформлен 15.03.2022). Также Платформа Радар имеет встроенный модуль для взаимодействия с ГосСОПКА. Модуль входит в базовый пакет поставки и не требует дополнительного лицензирования.

Всего с помощью Платформы Радар можно покрыть 18 мер обеспечения безопасности, а также 19 мер обеспечения безопасности покрыты для внутренних компонентов системы. Ниже вы можете ознакомиться с перечнем этих мер:

Анализ соответствия Платформы «Радар» требованиям приказа ФСТЭК от 25 декабря 2017 г. № 239

Примечание:

- «**+**» - мера является обязательной
- «**-**» - меры применяются при адаптации и дополнении базового набора мер, а также при разработке компенсирующих мер в значимом объекте критической информационной инфраструктуры соответствующей категории значимости.
- «**В**» - система реализует данную меру для внутренних компонентов

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Соответствие Платформа Радар
		3	2	1	
I. Идентификация и аутентификация (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+	В
ИАФ.4	Управление средствами аутентификации	+	+	+	В
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+	В
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+	В
II. Управление доступом (УПД)					
УПД.1	Управление учетными записями пользователей	+	+	+	В
УПД.2	Реализация модели управления доступом	+	+	+	В
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+	В
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+	В
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+	В
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	+	+	В
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	-	-	+	В
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения	-	+	+	В
IV. Защита машинных носителей информации (ЗНИ)					
ЗНИ.7	Контроль подключения съемных машинных носителей информации	+	+	+	+
V. Аудит безопасности (АУД)					
АУД.1	Инвентаризация информационных ресурсов	+	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+	+
АУД.6	Защита информации о событиях безопасности	+	+	+	+
АУД.7	Мониторинг безопасности	+	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+	+
АУД.9	Анализ действий отдельных пользователей	-	-	+	+
АУД.10	Проведение внутренних аудитов	+	+	+	+
IX. Обеспечение доступности (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств	-	+	+	В
ОДТ.2	Резервирование средств и систем	-	+	+	В
ОДТ.3	Контроль безотказного функционирования средств и систем	-	+	+	В
ОДТ.7	Кластеризация информационной (автоматизированной) системы	-	-	-	В
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+	+	+	В
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)					
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+	В
ЗИС.19	Защита информации при ее передаче по каналам связи	+	+	+	В
XII. Реагирование на компьютерные инциденты (ИНЦ)					
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+	+

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Соответствие Платформа Радар
		3	2	1	
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+	+
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+	+
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+	+
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+	+	+	+
XIII. Управление конфигурацией (УКФ)					
УКФ.4	Контроль действий по внесению изменений	-	-	-	+
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)					
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+	+	+	+
XVI. Обеспечение действий в нештатных ситуациях (ДНС)					
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	-	-	-	+

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.