ПАНГЕО РАДАР

БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

Анализ соответствия SIEM «Платформа Радар» требованиям приказа ФСТЭК №21 от 18 февраля 2013

Согласно приказу ФСТЭК РФ от 18 февраля 2013 №21 (об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных) операторам ПДн требуется обеспечить безопасность с помощью комплекса технических и организационных мер. Для соответствия приказу требуются решения по информационной безопасности различных классов.

Одним из основополагающих решений может по праву называться SIEM, так как SIEM реализует меры из разделов «Регистрация событий безопасности (РСБ)» и «Выявление инцидентов и реагирование на них (ИНЦ)». Данные разделы содержат 13 мер, однако, это не всё, что можно покрыть с помощью SIEM «Платформа Радар».

Всего с помощью SIEM «Платформа Радар» можно покрыть 19 мер, а также 20 мер покрыты для внутренних компонентов системы. Ниже вы можете ознакомиться с перечнем этих мер с разделением на разделы.

Построение системы защиты персональных данных следует начать именно с системы класса SIEM по многим причинам:

- SIEM не требует изменения инфраструктуры. Многие решения по информационной безопасности требуют установки ПО на рабочие станции или изменение сетевой инфраструктуры при внедрении. SIEM же устанавливается «рядом», не влияет на уже существующие процессы, что делает его внедрение безболезненным для администраторов и рядовых сотрудников. Это позволяет в кротчайшие сроки закрыть широкий список технических мер для соответствия приказу ФСТЭК от 18 февраля 2013 №21;
- SIEM является единым центром мониторинга информационной безопасности. Именно SIEM позволяет централизованно мониторить журналы со всех систем информационной безопасности, уменьшая нагрузку на отдел информационной безопасности. Администраторам не придётся использовать множество различных СЗИ, достаточно использовать лишь интерфейс SIEM. Это позволит освободить ресурсы отдела ИБ для внедрений других технических средств;
- Выявление инцидентов ИБ. Любое СЗИ в отдельности не даёт возможности выявить сложные и целенаправленные атаки. SIEM учитывает журналы сразу всех источников при детектировании инцидентов. Это позволяет снизить нагрузку на отдел ИБ;

- Комплексный мониторинг. SIEM анализирует события не только СЗИ, а также и события ИТ систем. SIEM позволит выявлять инциденты даже при отсутствии внедренных СЗИ, используя только события с сетевого оборудования, операционных систем, журналов приложений, баз данных и пр. Внедрение SIEM позволит выявлять и обрабатывать инциденты информационной безопасности на ранних этапах построения системы безопасности при обработке ПДн.
- Лёгкое расширение. Внедрение SIEM является более выгодным в начале построения системы безопасности. При раннем внедрении SIEM нагрузка по подключению СЗИ в качестве источников событий и разработки дополнительных правил корреляции равномерно распределится на весь срок внедрения всех СЗИ. Если же SIEM будет внедряться одним из последних, то данный объем работ придётся выполнять в рамках внедрения SIEM системы, что скажется или на сроках внедрения, или на качестве настройки;
- Построение процесса реагирования на инциденты. SIEM позволяет вести работу по найденным аномалиям. Операторы системы смогут отслеживать текущий статус инцидентов, вести историю работы с инцидентами. Также Платформа «Радар» позволяет отправлять найденные инциденты в НКЦКИ и ФинЦЕРТ;

Описанные причины делают внедрение SIEM системы приоритетной задачей в рамках построения системы безопасности персональных данных.

Требования к СЗИ

Примечание:

- «**+**» - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных
- Меры по обеспечению безопасности персональных данных, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.
- «✓» - система покрывает данную меру
- «**В**» - система покрывает данную меру для внутренних компонентов

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных				Соответствие Платформы Радар
		4	3	2	1	
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)						
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+	В
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+	В
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+	В
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+	В
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+	В

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных				Соответствие Платформы Радар
		4	3	2	1	
II. Управление доступом субъектов доступа к объектам доступа (УПД)						
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+	В
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+	В
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+	В
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+	В
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+	В
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+	В
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+	В
III. Ограничение программной среды (ОПС)						
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения					В
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+	В
IV. Защита машинных носителей персональных данных (ЗНИ)						
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных					✓
ЗНИ.7	Контроль подключения машинных носителей персональных данных					✓
V. Регистрация событий безопасности (РСБ)						
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+	✓
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+	✓
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+	✓
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти					✓
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+	✓
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе					✓
РСБ.7	Защита информации о событиях безопасности	+	+	+	+	✓
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)						
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+	✓
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+	✓

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных				Соответствие Платформы Радар
		4	3	2	1	
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)						
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+	✓
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему					В
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему					В
X. Обеспечение доступности персональных данных (ОДТ)						
ОДТ.1	Использование отказоустойчивых технических средств					В
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+	В
XI. Защита среды виртуализации (ЗСВ)						
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+	✓
XIV. Выявление инцидентов и реагирование на них (ИНЦ)						
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+	✓
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+	✓
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+	✓
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+	✓
ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+	✓
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+	✓
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)						
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+	В
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+	В

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.