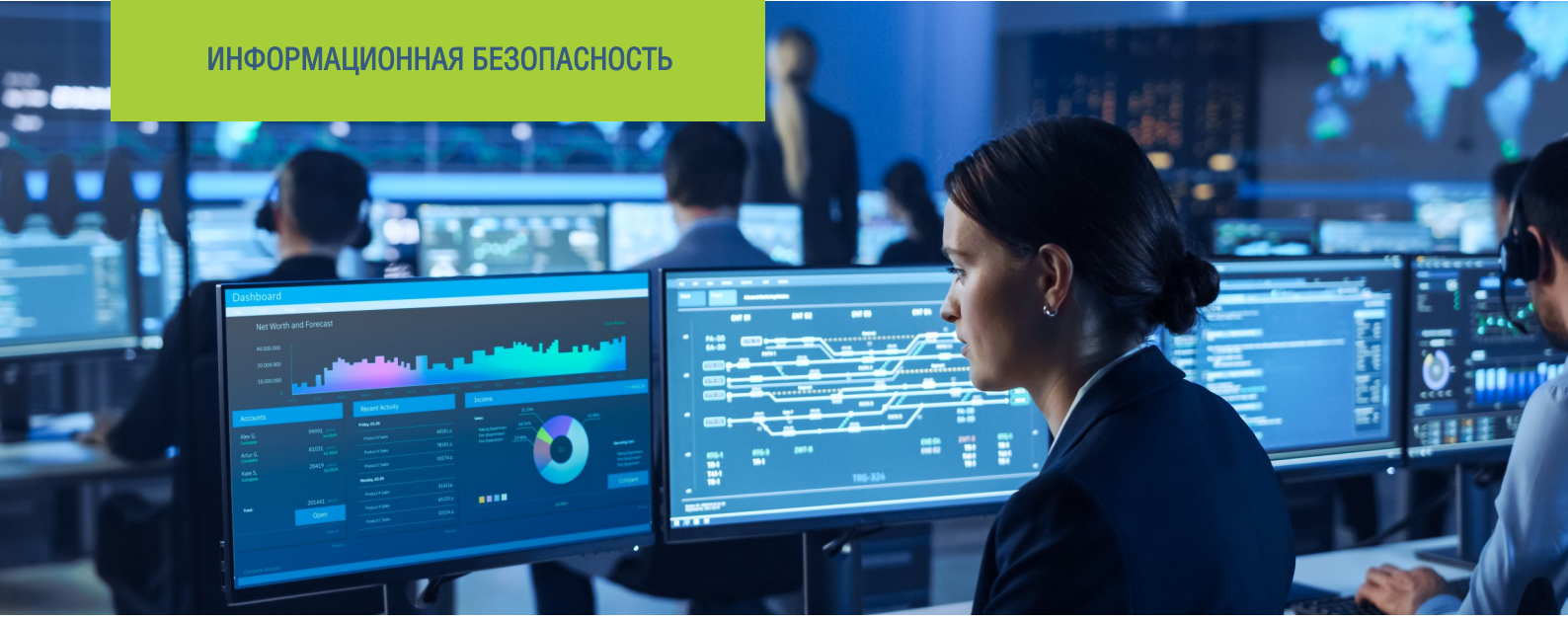


Работа R-Vision EVO через однонаправленный шлюз InfoDiode

На фоне роста числа киберугроз, требования бизнеса к защите информации меняются: на смену классическому подходу к построению центров мониторинга и реагирования на инциденты информационной безопасности, где каждый продукт выполняет отдельную конкретную функцию, пришел новый, экосистемный подход. Экосистемы позволяют организациям комплексно подойти к вопросам кибербезопасности, обеспечить решение задач на стыке технологий, а также сфокусироваться на наиболее приоритетных для компаний бизнес-процессах. Функционирование SOC требует уделять особое внимание безопасному сбору данных с критических объектов с учетом оперативности такого сбора. С одной стороны, необходимо предоставлять информацию в системы управления событиями информационной безопасности (SIEM) и центры мониторинга информационной безопасности (SOC), а с другой — обеспечить надёжную изоляцию критически значимых сегментов (АСУ ТП, ОКИИ, ОПО) от любых внешних воздействий по каналам связи.

В качестве решения могут выступать технологии однонаправленной передачи данных, основанные на принципах физической изоляции одного сетевого сегмента от другого, обеспечивающие возможность передачи данных из закрытого контура во внешние сети. Такие технологии гарантируют целостность и доступность инфраструктуры и данных в защищенном сегменте и исключают риски внешнего несанкционированного воздействия на такой сегмент.

Построенная на принципах физической изоляции, линейка продуктов InfoDiode позволяет эффективно решать задачи безопасной передачи данных в SOC из защищаемого сегмента.

Программный комплекс R-Vision EVO позволяет создавать центры SOC, в состав которых входит центр контроля информационной безопасности (ЦКИБ). Данный центр создает единую точку консолидации информации о состоянии ИБ в организации, а также является платформой для совместной работы ИБ-подразделений, координации деятельности сотрудников, распределения задач и учета выполненных мероприятий по управлению ИБ.

Были проведены всесторонние тесты программного обеспечения R-Vision ЦКИБ при совместном использовании с моделями комплексов **InfoDiode** между компонентом сбора событий в закрытом сегменте и компонентом реагирования на инциденты безопасности R-Vision ЦКИБ в открытом сегменте. Результаты комплексного тестирования подтвердили успешное и эффективное совместное использование продуктов в указанном сценарии для обеспечения высочайшего уровня защиты критических сетевых сегментов.

119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.infodiode.ru

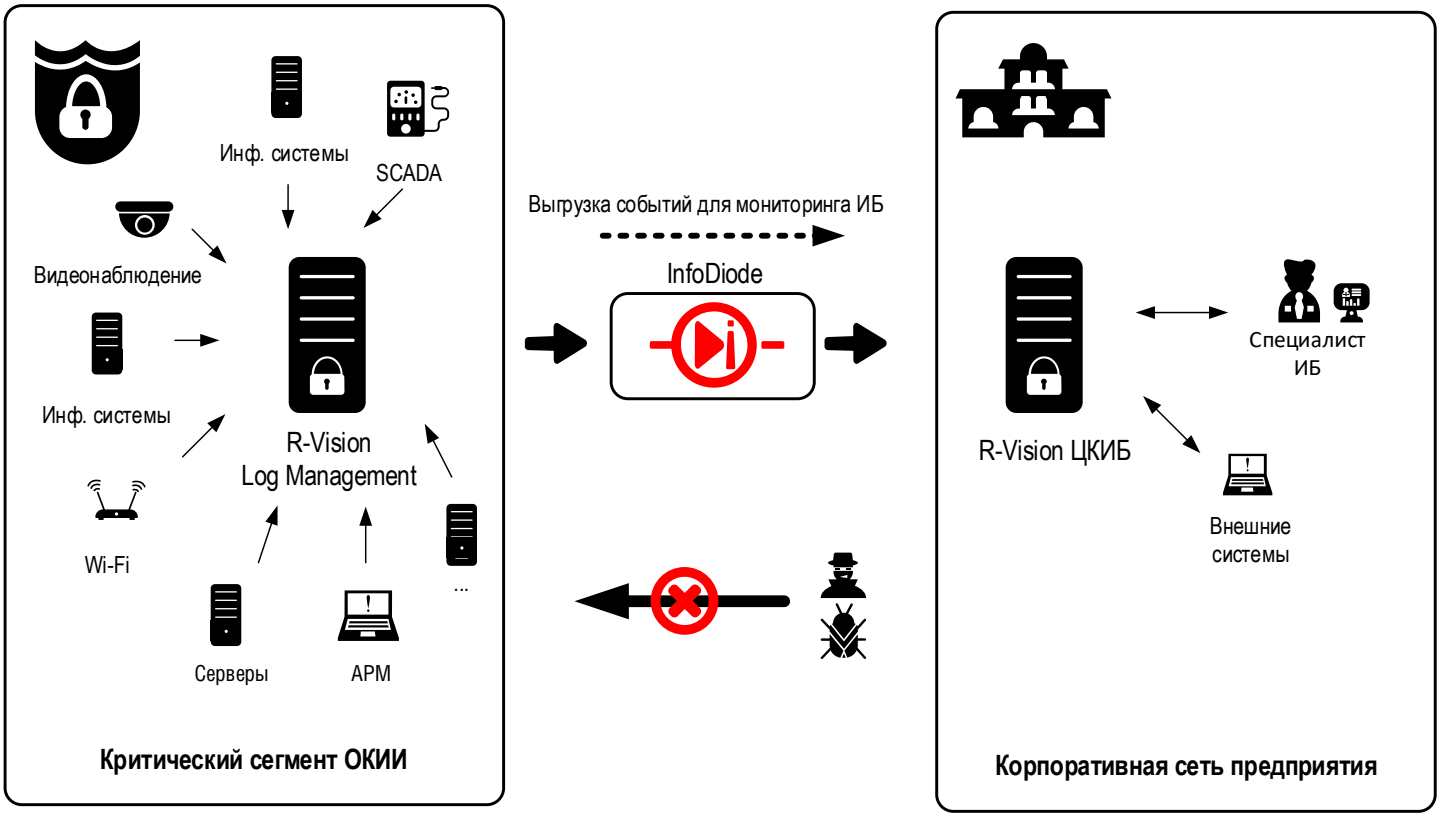
Сценарий работы R-Vision ЦКИБ через однонаправленный канал передачи данных

Для АСУ ТП и ОКИИ часто применяется не только логическая, но и физическая изоляция сетей как метод защиты от внешних воздействий. При этом сохраняются требования оперативного сбора событий безопасности для централизованного мониторинга и выявления инцидентов информационной безопасности. Совместное использование решений InfoDiode и R-Vision ЦКИБ позволяет реализовать централизованный сбор событий из технологических сетевых сегментов, гарантируя изоляцию таких сегментов.

Экосистема R-Vision EVO представляет собой большое количество встроенных интеграционных механизмов, конфигураций и экспертизы, с которыми задачи по построению и развитию центра мониторинга и реагирования на инциденты ИБ становятся значительно проще и прозрачнее. Так, R-Vision ЦКИБ автоматизирует процесс управления инцидентами ИБ, агрегирует данные по инцидентам, автоматически запускает сценарии реагирования, а также управляет другими системами через механизм оркестрации.

InfoDiode является системой однонаправленной передачи данных, обеспечивающей высочайший уровень изоляции критичных информационных систем. При этом сохраняется нужный уровень их функциональности для взаимодействия со смежными информационными системами для мониторинга и передачи логов в SOC.

В закрытом сегменте располагается компонент сбора событий R-Vision, который агрегирует и передаёт события через однонаправленный шлюз InfoDiode в компонент реагирования на инциденты безопасности R-Vision ЦКИБ в открытом сегменте. В описываемом сценарии могут применяться различные продукты InfoDiode: АК InfoDiode, АПК InfoDiode PRO.



119121, Россия, Москва, Ружейный переулок, 6с1.

Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.infodiode.ru

ЗАЯВЛЕНИЕ О СОВМЕСТИМОСТИ

Между программным обеспечением

R-Vision ЦКИБ,

правообладателем которого является

ООО «Р-ВИЖН»

(Россия, 109544, г. Москва, бульвар Энтузиастов, д.2,

БЦ Голден Гейт, 23 этаж)

в дальнейшем именуемыми «**R-Vision ЦКИБ**» и «**Р-ВИЖН**»

соответственно

и

Комплексом

«AMT InfoDiode» однонаправленной передачи данных

продукция компании

АО «АМТ-ГРУП»

Россия, 115162, г. Москва, ул. Шаболовка, д. 31, корп. Б, под. 3

в дальнейшем именуемыми «**InfoDiode**» и «**АМТ-ГРУП**»

соответственно

Комплекс **InfoDiode** является системой однонаправленной передачи данных, обеспечивающий высочайший уровень изоляции критичных информационных систем, сохраняя при этом нужный уровень их функциональности для взаимодействия со смежными информационными системами.

R-Vision ЦКИБ автоматизирует процесс управления инцидентами ИБ, агрегирует данные по инцидентам, автоматически запускает сценарии реагирования, а также управляет другими системами через механизм оркестрации.

АМТ-ГРУП и **Р-ВИЖН** настоящим подтверждают следующее заявление относительно использования указанных продуктов в рамках одной системы, их совместимости и вклада в выполнение требований кибербезопасности:

АМТ-ГРУП и **Р-ВИЖН** провели всесторонние тесты программного обеспечения **R-Vision ЦКИБ** при совместном использовании с моделями комплексов **InfoDiode** в сетях передачи данных с разграничением доступа на базе **InfoDiode**, используемого в следующем сценарии:

- Между компонентом сбора событий в закрытом сегменте и компонентом реагирования на инциденты безопасности **R-Vision ЦКИБ** в открытом сегменте.

В результате тестирования было установлено, что продукты, с учётом их индивидуальных системных требований, могут использоваться совместно в указанном сценарии. Тесты подтвердили полную совместимость продуктов в заявленном сценарии использования.

АО «АМТ-ГРУП»

24 мая 2024 года

Технический директор

Подпись _____ (Б.В. Молчанов)

ООО «Р-ВИЖН»

24 мая 2024 года

Генеральный директор

Подпись _____ (В.В. Богдашов)