

Компания «Код Безопасности» сообщает о выходе сертифицированной версии нового продукта — Security Studio Honeypot Manager, предназначенного для обнаружения вторжений и несанкционированного доступа к конфиденциальной информации. В настоящий момент на продукт Security Studio Honeypot Manager получен сертификат соответствия ФСТЭК России на соответствие требованиям по 4 уровню контроля отсутствия НДВ и технических условий (ТУ).

Honeypot Manager — это система защиты информации, реализующая проактивную защиту от хакерских вторжений и несанкционированных действий инсайдеров. Система имитирует работу сетевых бизнес-приложений (ERP и т.п.) на базе СУБД Oracle и регистрирует любые попытки несанкционированного доступа к ним.

Honeypot Manager позволяет усиливать защиту информационных систем организации, существенно снижая риски раскрытия данных бизнес-приложений. Кроме этого система позволяет выполнять некоторые требования, предъявляемые к системам защиты персональных данных, банковским системам и платежным системам:

- Требования ФСТЭК России к СЗИ для ПДн (Приказ № 58 и методические материалы) в части защиты персональных данных средствами имитации в системах класса К1, К2, К3 от различных угроз реализуемых с использованием протоколов межсетевого взаимодействия, а также в случае если особенности обработки персональных данных и структура ИС не позволяет сделать это другими средствами.
- Международный стандарт безопасности данных индустрии платежных карт PCI DSS.
- Стандарт Банка России СТО БР СТО БР ИББС-1.0-2008.

Honeypot Manager позволяет в режиме «реального» времени выявлять нарушителей (инсайдеров или хакеров), действующих в локальной вычислительной сети предприятия, анализировать и пресекать их действия без риска потери реальных данных. Уникальные особенности данной системы:

- Единственное средство обнаружения вторжений, основанное на имитации данных, рекомендуемое для защиты ИСПДн до класса К1 включительно;
- Может использоваться в сетях с конфиденциальной информацией (вплоть до АС 1Г) - имеет сертификат по НДВ-4 и ТУ;
- Низкий уровень ложных срабатываний – по сути это поведенческая система, регистрирующая только факты НСД;
- Не требует специально подготовленного специалиста по анализу вторжений – оповещения о событиях системы понятны обычным ИТ-администраторам;
- Достоверная имитация бизнес-приложений и их данных – для повышения качества имитации ложные данные могут создаваться на основе реальных данных заказчика;
- Может использоваться в составе систем централизованного мониторинга – такие системы входят в состав продуктов Secret Net и Security Studio.

Более подробную информацию о продукте, Вы можете найти на сайте компании «Код Безопасности».