ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСУ ТП В ЭЛЕКТРО ЭНЕРГЕТИКЕ

Объекты исследования:
информационные измерительные системы в составе АСУ ТП электроэнергетического объекта (ТИ и ТС, АИИС КУЭ, АСТУЭ, СОТИ АССО)

Модули мониторинга:
сервисный календарь, модуль оценки собираемости и отправки данных в ИИС, программы мониторинга сетевой активности, запущенных процессов и служб

Применяемые технологии:
ансамблевые методы машинного обучения, нейронные сети, нечеткая логика

МИРОНЕНКО ЯРОСЛАВ ВЛАДИМИРОВИЧ
АО «РЭС Групп», г. Владимир

ОСНОВНЫЕ НАПРАВЛЕНИЯ АУДИТА ИБ

Перехват данных

Попытка получения информации из систем третьими лицами

В практике подобные случаи отсутствовали

Диверсия

Изменение функционирования системы таким образом, чтобы нанести материальный или репутационный урон владельцу

Проникновение в АВС

Попытки (осознанные и неосознанные) выхода в АВС предприятия с использованием оборудования технологической сети

В практике случаи осознанного проникновения в АВС отсутствовали

Нецелевое использование GSM-связи

Опрос чужого оборудования по каналам GSM-связи с использованием звонящего модема рассматриваемой системы

Нецелевое использование GPU и CPU

Нецелевое использование оборудования системы для личного обогащения (например, для майнинга криптовалюты на сервере системы)

Неконтролируемый доступ неквалифицированных лиц

Получение доступа к управлению системой лицами, которые не имеют достаточной квалификации и могут своими действиями нанести урон владельцу системы

РЕАЛИЗАЦИЯ АЛГОРИТМА РАБОТЫ ПРОГРАММНОГО КОМПЛЕКСА

ХОРОШИЙ УЧЕНИК	ПЛОХОЙ УЧЕНИК
Функционирование системы	
Использование сервисных модулей для оценки: собираемости данных в системе, отправке регулярных отчетов пользователям, выполнения регламентных работ в системе (техническое обслуживание, испытания), модернизации системы	
Процессы и службы	
Определение перечня процессов и технологических служб, характерных как для нормального функционирования системы, так и для случаев восстановления работы системы	*Мониторинг всех запуска всех процессов и служб, не характерных для данной системы и отсутствующих в перечне*
Список подключений	
Определение списка пользователей, допущенных к работе с системой, в том числе с использованием удаленного доступа	*Мониторинг всех подключений к системе, определение подключений со стороны пользователей, отсутствующих в списке*
Трафик каналов связи	
Определения перечня процессов и технологических служб, характерных как для нормального функционирования системы, так и для случаев восстановления работы системы	*Мониторинг всех запуска всех процессов и служб, не характерных для данной системы и отсутствующих в перечне*

РЕЗУЛЬТАТЫ МОНИТОРИНГА

Случаев перехвата управления информационными системами

не зафиксировано

1 случай

обнаружения запущенного процесса майнинга криптовалюты на сервере ИИС

Подозрительная активность в системе

Не характерные для ИИС процессы и действия пользователей

1 случай

использования GSM-канала для опроса измерителей в другой ИИС предприятия

Случаев подключения непосредственно к сетевому оборудованию

не зафиксировано

Некорректная работа каналов связи

Использование каналов связи для подключения к оборудованию вне контура ИИС

2 случая

входа в систему без технологической необходимости

Случаев использования технологической сети для доступа в АВС

не зафиксировано

Подозрительный доступ к системе извне

Доступ к системе с использованием технологий удаленного доступа

СПАСИБО ЗА ВНИМАНИЕ!

Мироненко Ярослав Владимирович
АО «РЭС Групп»

+7 904 030 89 20
yaroslav.mironenko@inbox.ru