CyberLympha®

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ АСУ ТП и SCADA

15 февраля 2022 года

Алексей Комаров
zlonov.com

218.57

ЧТО ТАКОЕ УПРАВЛЕНИЕ **УЯЗВИМОСТЯМИ В АСУ ТП?**

CyberLympha®

УЯЗВИМОСТЬ:

Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.
ГОСТ Р 56546-2015

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ:

В общем случае - это бизнес-процесс выявления, установления приоритетов, исправления или снижения негативных последствий и составления отчетов об уязвимостях программных (программно-технических) средств АСУ ТП и АСУ ТП как системы в целом (ошибки конфигураций, архитектуры).

ПРИКАЗ №239 ФСТЭК РОССИИ 1/4

CyberLympha®

- **РАЗРАБОТКА** организационных и технических мер по обеспечению безопасности значимого объекта
  - 11.1. б) анализ возможных уязвимостей значимого объекта и его программных, программно- аппаратных средств
- **ВНЕДРЕНИЕ** организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
  - 12. е) анализ уязвимостей значимого объекта и принятие мер по их устранению
- **ОБЕСПЕЧЕНИЕ** безопасности значимого объекта в ходе его эксплуатации
  - 13.2. а) анализ уязвимостей значимого объекта, возникающих в ходе его эксплуатации

https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

ПРИКАЗ №239 ФСТЭК РОССИИ 2/4

CyberLympha®

- 12.6. Анализ уязвимостей значимого объекта проводится в целях выявления недостатков (слабостей) в подсистеме безопасности значимого объекта и оценки возможности их использования для реализации угроз безопасности информации. При этом анализу подлежат **уязвимости кода**, **конфигурации** и **архитектуры** значимого объекта.

- Анализ уязвимостей проводится для всех программных и программно-аппаратных средств, **в том числе средств защиты информации**, значимого объекта.

https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

ПРИКАЗ №239 ФСТЭК РОССИИ 3/4

CyberLympha®

При проведении анализа уязвимостей применяются следующие способы их выявления:

а) анализ проектной, рабочей (эксплуатационной) **документации** и организационно-распорядительных документов по безопасности значимого объекта;

б) анализ **настроек** программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта;

в) выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, посредством **анализа состава** установленного программного обеспечения и обновлений безопасности **с применением средств контроля (анализа) защищенности и (или) иных средств защиты информации**;

г) выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, **сетевых служб**, доступных для сетевого взаимодействия, **с применением средств контроля (анализа) защищенности**;

д) **тестирование на проникновение** в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации.

https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

ПРИКАЗ №239 ФСТЭК РОССИИ 4/4

CyberLympha®

- Применение способов и средств выявления уязвимостей осуществляется субъектом КИИ с **учетом особенностей функционирования** значимого объекта.
- Допускается проведение анализа уязвимостей **на макете (в тестовой зоне)** значимого объекта или макетах отдельных сегментов значимого объекта.
- Анализ уязвимостей значимого объекта проводится до ввода его в эксплуатацию на этапах, определяемых субъектом КИИ.
- В случае выявления уязвимостей значимого объекта, которые могут быть использованы для реализации (способствовать возникновению) угроз безопасности информации, принимаются меры, направленные на их устранение или исключающие возможность использования (эксплуатации) нарушителем выявленных уязвимостей.
- По результатам анализа уязвимостей **должно быть подтверждено**, что в значимом объекте, **отсутствуют уязвимости, как минимум содержащиеся в БДУ ФСТЭК России** [...], **или выявленные уязвимости не приводят к возникновению угроз безопасности информации** в отношении значимого объекта.

https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

ОСОБЕННОСТИ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В АСУ ТП

CyberLympha®

- Промышленные системы управления часто используют устаревшее оборудование и программное обеспечение, которые больше не получают обновлений безопасности.
- Сканирование систем может создавать риски для технологических процессов.
- Установка исправлений для постоянно работающих систем невозможна.
- Анализ уязвимостей в АСУ ТП должен включать не только программные уязвимости, но и уязвимости конфигураций и архитектуры (незащищенные порты и службы, небезопасное управление учетными записями и т.д.).

ПРОГРАММА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ ВКЛЮЧАЕТ

CyberLympha®

1. Инвентаризация активов с максимальной контекстуализацией
2. Оценка активов на наличие уязвимостей
3. Приоритизация тех уязвимостей, для которых возможна эксплуатация и результат эксплуатации которых может быть наиболее негативен
4. Устранение уязвимостей с помощью исправлений программного обеспечения, изменений конфигураций или применения иных компенсирующих мер

АВТОМАТИЗИРУЙ ЭТО!

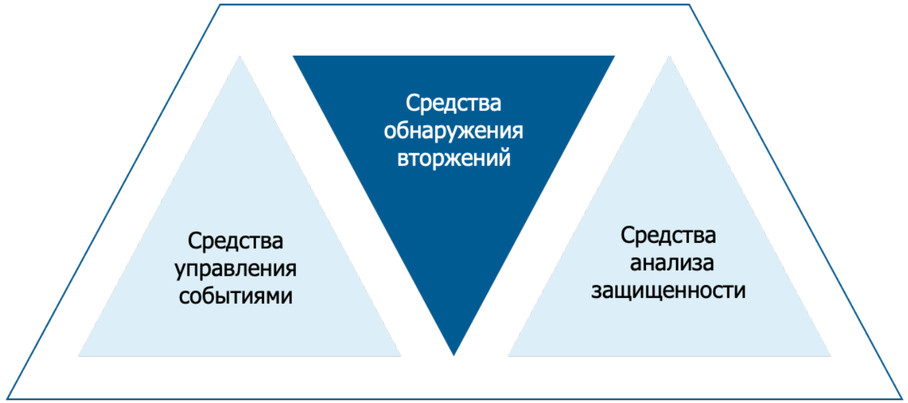
Автоматизируй всё, что делаешь,
а что не можешь автоматизировать - сделай иначе и автоматизируй.

CL DATAPK
ПРОГРАММНЫЙ КОМПЛЕКС

CyberLympha®

CyberLympha
DATAPK

Непрерывный комплексный мониторинг
и анализ состояния информационной безопасности
промышленных систем автоматизации



Классы средств защиты информации в соответствии с Приказом №235 ФСТЭК России

- Создан для АСУ ТП и учитывает все требования к средствам защиты информации
- Реализует все необходимые возможности класса промышленных СОВ
- Обладает дополнительным функционалом нескольких классов решений
- Сертифицирован ФСТЭК России
- Защищает значимые объекты КИИ в РФ
- Протестирован производителями АСУ ТП

CL DATAPK –
БОЛЬШЕ ЧЕМ ПРОМЫШЛЕННОЕ СОВ

CyberLympha®

АНАЛИЗ СЕТЕВОГО ТРАФИКА

- Пассивное получение данных посредством SPAN или зеркальных портов сетевого оборудования
- Визуализация карты сети и потоков
- Выявление и инвентаризация узлов
- Обнаружение несанкционированных подключений и потоков данных

ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ

- Обнаружение инцидентов ИБ на базе экспертных правил
- Получение событий от произвольных источников без использования агентов
- Поддержка новых источников событий без необходимости доработки продукта

УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ

- Контроль безопасных настроек
- Анализ соответствия требованиям ИБ
- Получение данных от произвольных источников без использования агентов
- Расширение списка поддерживаемых объектов без необходимости доработки продукта

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

- Анализ защищенности произвольных источников без использования агентов
- Поддержка БДУ ФСТЭК России и других сторонних баз уязвимостей
- Генерация выгружаемых отчетов

ПРОГРАММА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

CyberLympha®

ЭТАП	ТРУДНОСТИ
Инвентаризация активов	Неполная инвентаризация активов
Выявление уязвимостей	Недостаточная частота процесса выявления уязвимостей
Приоритизация уязвимостей	Выбор первоочередных, для которых возможна эксплуатация, и результат эксплуатации которых может быть наиболее негативен
Устранение уязвимостей	Согласование с поставщиком АСУ ТП Ограниченные «окна» для проведения работ

ИНВЕНТАРИЗАЦИЯ АКТИВОВ В АСУ ТП

CyberLympha®

ПАССИВНЫЙ АНАЛИЗ ТРАФИКА АСУ ТП

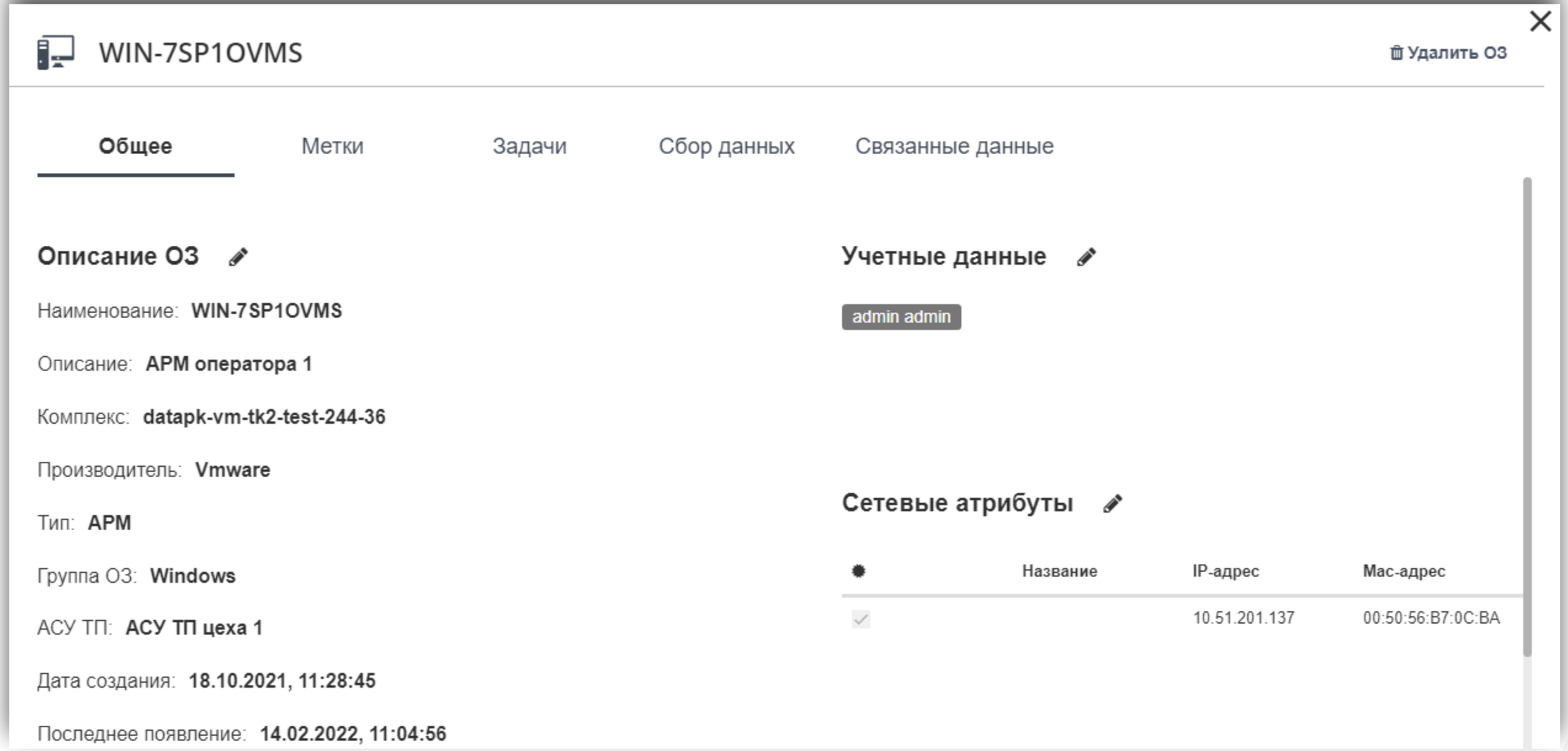
- Обнаружение сетевых узлов и ведение каталога активов
- Выявление информационных потоков и ведение их базы
- Визуализация карты активной сети
- Выявление запрещенных коммуникаций и управляющих команд (незашифрованных)
- Обнаружение вторжений (сетевых)

CL DATAPK (ДОПОЛНИТЕЛЬНО)

- Выявление «молчащих» активов
- Инвентаризация вплоть до прикладного ПО и перечня установленных обновлений
- Контроль соответствия требованиям ИБ
- Контроль неизменности конфигураций

КАРТОЧКА АКТИВА (ОБЪЕКТА ЗАЩИТЫ) - АРМ

CyberLympha®



КАРТОЧКА АКТИВА (ОБЪЕКТА ЗАЩИТЫ) - ПЛК

CyberLympha®

	Параметр	Значение
1	Собрано блоков	111/111
2	Код заказа	6ES7 315-2EH14-0AB0
3	Версия ОС	37.12.12
4	Тип модуля	CPU 315-2 PN/DP
5	Серийный номер	S C-H5D527772016
6	Наименование ПЛК	S7300/ET200M station_1
7	Наименование модуля	PLC_1
8	Состояние ПЛК	S7CpuStatusRun
9	Количество программных блоков	111
10	Позиция селектора	RUN-P
11	Параметры уровня защиты	Write Password
12	Уровень защиты ЦПУ	Read Only
13	Переключатель запуска	Unknown / N.A.
14	Уровень защиты селектора	Can Read/Write

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ В АСУ ТП

CyberLympha®

ОБЫЧНО

- Сканирование во время простоев (1 раз в год)
- Стремительное устаревание результатов сканирования искажает картину ландшафта уязвимостей
- «Щадящее» сканирование, применение стендов
- В присутствии представителей производителя АСУ ТП «на всякий случай»

CL DATAPK

- Непрерывный контроль состояния защищенности
- Актуализация информации об уязвимостях при обновлении базы сигнатур
- Безагентский опрос с правами на чтение
- Выявление ошибок в конфигурациях
- Поддержка сторонних баз (БДУ ФСТЭК)

ПРИМЕР ОПИСАНИЯ УЯЗВИМОСТИ

CyberLympha®

Название	Описание	Класс	Результат	Идентификатор CVE	Базовая оценка уязвимости	Базовый вектор атаки	Меры по исправлению уязвимости
Уязвимость ASLR в .NET (MS14-046)	В Microsoft .NET Framework существует уязвимость, связанной с обходом функций безопасности. Эта уязвимость может позволить злоумышленнику обойти функцию безопасности Address Space Layout Randomization (ASLR), которая помогает защищать пользователей от широкого класса уязвимостей. Сам по себе обход этой функции безопасности не позволяет выполнить произвольный код. Однако обход функции ASLR открывает возможность выполнения произвольного кода с помощью другой уязвимости, например той, которая делает возможным удаленное выполнение кода.	VULNERABILITY	Уязвимость обнаружена	CVE-2014-4062	Средний уровень опасности (базовая оценка CVSS 2.0 составляет 4.3)	AV:N/AC:M/Au:N/C:P/I:N/A:N	Использование рекомендаций производителя: http://technet.microsoft.com/en-us/security/bulletin/ms14-046

✓ **Импорт определений OVAL запущен**
Это может занять несколько минут

ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ В АСУ ТП

CyberLympha®

ОБЫЧНО

- Тысячи критических уязвимостей (уязвимости ПО, небезопасные конфигурации, бездействующие учетных записей, слабые пароли и т.п.) при первичной оценке уязвимостей
- Уязвимости в отчёте сканера безлики - не каждая критическая уязвимость несёт одинаковую угрозу безопасности
- Оценка по CVSS не учитывает критичность актива, его окружение, наличие средств защиты и иных компенсирующих мер

CL DATAPK

- Встроенные проверки по «hardening guide» производителей
- Подсказки по выявленным уязвимостям не только в ПО, но и в конфигурациях
- Автоматизация оценки соответствия корпоративным стандартам
- Контекстное обогащение информацией об активе

ПРИМЕРЫ РЕКОМЕНДАЦИЙ ПРОИЗВОДИТЕЛЯ АСУ ТП

CyberLympha®

	Информация о рекомендации в документации Siemens «Recommended security settings for IPCs in industrial environments»	Проверяемый параметр	Значение	Соответствует ли рекомендациям Siemens
2	Раздел 4.2 документации: «Обнаружение пользовательской установки и запроса повышения прав с помощью контроля учетных записей пользователей (UAC)». Параметр: Локальная политика безопасности\Локальные политики\Параметры безопасности\Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей (рекомендуемое значение: «Автоматически отклонять запросы на повышение прав»)	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser	REG_DWORD 0x3	Не соответствует
3	Раздел 4.4 документации: «Запрет завершения работы системы без выполнения входа в систему». Параметр: Локальная политика безопасности\Локальные	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon	REG_DWORD 0x0	Соответствует

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ
В АСУ ТП

CyberLympha®

ОБЫЧНО

- Одно и то же узкое «технологическое окно» для выявления, анализа и устранения уязвимости
- Получение согласования производителя АСУ ТП на установку обновлений и принятие мер требует времени
- Проверка корректностьи устранения требует повторного сканирования, но база сигнатур сканера уже могла обновиться...

CL DATAPK

- Непрерывный мониторинг и постоянная осведомлённость позволяют подготовиться заранее
- Контекстное обогащение информации об уязвимости упрощает приоритизацию
- Информация об уязвимостях может быть предоставлена производителю АСУ ТП / сервисной организации до начала непосредственных работ

ПРИМЕР РЕЗУЛЬТАТОВ ПРОВЕРОК

CyberLympha®

	Настройка	Статус	Должно быть	Имеется
6	Размер истории паролей	Не соответствует	5	0
7	Пороговое значение блокировки (попытки)	Соответствует	0	0
8	Требовать вход в систему для изменения пароля	Соответствует	0	0
9	Принудительный выход из системы по истечении часа	Соответствует	0	0
10	Новое имя администратора	Не соответствует	"user_2"	"Administrator"
11	Новое имя гостя	Не соответствует	"user_1"	"Guest"
12	Открытый текстовый пароль	Соответствует	0	0
13	Доступ анониного пользователя к локальной политики LSA	Соответствует	0	0
14	Включить аккаунт администратора	Не соответствует	0	1

РЕЗЮМЕ

CyberLympha®

- Управление уязвимостями трудно реализуемо для АСУ ТП.
- Оценка уязвимости — это НЕ управление. Управление включает в себя принятие мер по устранению рисков с учетом окружающей среды.
- Рекомендуемый подход — автоматизация данного процесса за счёт применения набора инструментов для определения, контекстуализации и приоритизации действий.
- Такой подход обеспечивает видимость для всей инфраструктуры АСУ ТП и обеспечивает эффективное управление уязвимостями.

CyberLympha®

ВОПРОСЫ?

CyberLympha®

sale@cyberlympha.ru

CYBERLYMPHA.RU