23.07.2020

АМТ-ГРУП

На что обратить внимание создавая ситуационно-аналитический центр в эпоху «после пандемии»

Реалии лета 2020

Мы участвуем в конференции он-лайн

Частичные ограничения всё еще действуют 4 месяца спустя

Теперь мы знаем, что это реальность, и она может повториться

Что мы узнали?

- С какого-то момента работать в рамках большого коллектива может быть просто опасно;
- Доступ к стандартному рабочему месту может быть закрыт, даже со всеми возможными пропусками. Туда просто нельзя;
- Скорость и глубина принятия решений, контроль за их исполнением могут вырасти многократно в очень короткий период;
- Вам могут потребоваться данные о которых раньше вы просто не думали.

AMT GROUP

Какие тенденции мы видим

- Архитектура создания – САЦ это универсальный инструмент поддержки принятия решений верхнего уровня, готовый работать с необходимыми вам данными. Их спектр может быть расширен;
- Системы и процессы – нужно рационально использовать сложившуюся практику и возможность распределенного подхода к их созданию;
- Требования к интерфейсам – универсальность, возможность включения новых данных, наглядность процессов;
- Аналитика и прогнозирование – современные атрибуты ситуационного центра;
- Резервные площадки, если их нет, о них стоит задуматься;
- Информационная инфраструктура предприятия должна быть защищена, а ее мониторинг не менее важен, чем СКУД на проходной и видеонаблюдение.

AMT GROUP

Защита информационной инфраструктуры

- Почему стоит обратить внимание на защиту информационной инфраструктуры:
  - Данные ведущих игроков рынка ИБ по уязвимости корпоративных систем и АСУ ТП свидетельствуют о том, что у злоумышленника всегда есть шанс найти уязвимость;
  - Рабочие процессы должно быть защищены;
  - Вы должны понимать что происходит в вашей сети, как защищены ваши данные.
- Организация рабочего места и процессов для контроля защищенности информационной инфраструктуры предприятия – инвестиции в инфраструктуру и сохранность данных.

AMT GROUP

Ландшафт угроз информационной безопасности промышленных сетей

67%
Векторов атак с целью проникновения в сеть АСУ ТП характеризуются низким уровнем сложности

64%
Недостатки и ошибки в фильтрации и сегментации сетей АСУ ТП были внесены администраторами предприятий

61%
Выявленных уязвимостей в компонентах АСУ ТП относятся к критической и высокой степени риска

175 000
Компонентов АСУ ТП доступно онлайн в Интернет

73%
Промышленных компаний недостаточно защищены от внешних кибератак

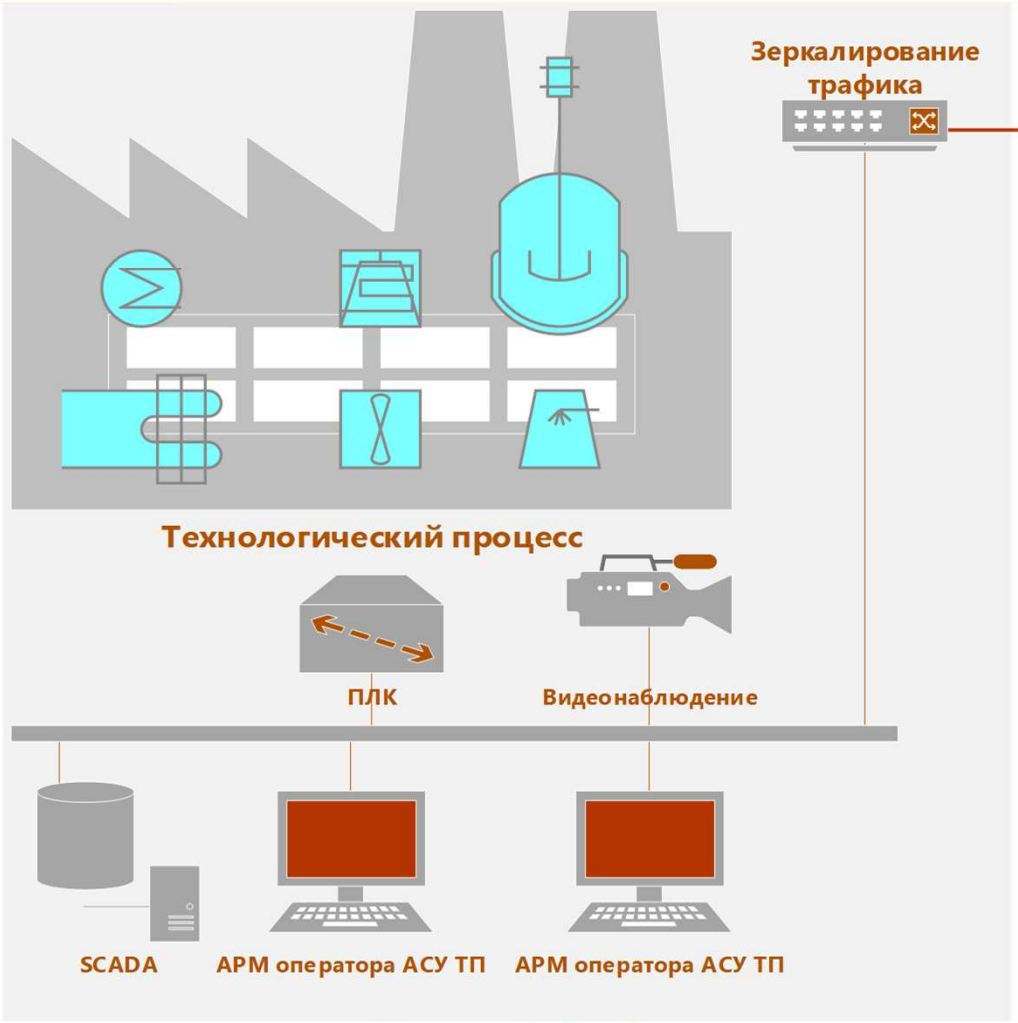
82%
Промышленных организаций не готовы противостоять внутреннему нарушителю

100%
Словарные пароли и устаревшее ПО с известными уязвимостями были выявлены в сетях каждой промышленной компании

* По данным компании Positive Technologies за 2019 год

AMT GROUP

Ситуационный центр информационной безопасности промышленных сетей



Сегмент АСУ ТП

Ситуационный центр/SOC

Основные особенности реализации SoC для АСУ ТП
Безопасный транспорт данных от промышленных сетей

- Безопасная передача данных из критически важных систем;
- Выгрузка журналов событий для последующей корреляции и обработки в системах SOC;
- Безопасная передача показаний с датчиков, видеопотока с камер наблюдения в ситуационный центр;
- Защищенная трансляция видеоконтента;
- Передача сообщений и сигналов оповещения, сигнализации

AMT GROUP

Выводы

Выводы

Создавая ситуационно-аналитический центр:

- Будьте внимательны к данным, методам работы с ними и их отображению;
- Создавая инфраструктуру учитывайте возможность распределенной работы, резервирования не только «железа», но и площадок;
- Обеспечьте защищенность информационной инфраструктуры и её мониторинг.

АО «АМТ-ГРУП»

СОЗДАНИЕ СИТУАЦИОННО-АНАЛИТИЧЕСКОГО ЦЕНТРА

Геннадий Медведев
Директор по развитию
gmedvedev@amt.ru
+7 916 672-8803

Основные параметры
«на что обратить внимание создавая САЦ в 2020 году»
к докладу на конференции ««Мониторинг и управление инцидентами: ситуационно-аналитические и диспетчерские центры»

№	Наименование
1	**Рабочие процессы (РП), данные**
1.1.	Определите РП, которые включаются в периметр работы САЦ
1.2.	Соберите всю информацию и регламенты касающиеся РП, включаемых в периметр САЦ
1.3.	Предусмотрите автоматическое и «ручное» инициирование РП
1.4.	Организуйте взаимодействие со всеми участниками РП, включая структуры внутри вашей организации и внешних контрагентов, для уточнения их ролей и регламентов взаимодействия
1.5.	Определите и согласуйте последовательность включения РП в периметр САЦ
1.6.	Будьте готовы к тому, что включение РП в периметр САЦ будет влиять на изменение РП (как этого конкретного, так и других) и это циклический процесс
1.7.	Предусмотрите возможность и алгоритмы изменения РП
1.8.	Предусмотрите возможность создания и включения в периметр новых РП
1.9.	Определите перечень данных и их источников, для использования в РП
1.10.	Предусмотрите возможность включения новых типов данных и новых источников данных для РП
2.	**Структура**
2.1.	Определите административно-штатную структуру САЦ, основанную на РП и оценке нагрузки на сотрудников
2.2.	В рамках административно-штатной структуры предусмотрите категорирование для организации территориально распределенной и удаленной работы
3.	**Интерфейс**
3.1.	Предусмотрите возможность настройки интерфейса под роли сотрудников с предоставлением им необходимой информации и прав в рамках РП
3.2.	Предусмотрите вложенность информации и возможность её пошаговой детализации
3.3.	Предусмотрите использование логических сценариев для РП и их вариативность в зависимости от хода развития событий
3.4.	Предусмотрите наглядную индикацию задач (входящих событий, поручений и др.), а также их исполнения

4.	**Резервирование**
4.1.	Предусмотрите необходимость резервирования ЦОД и коммуникаций
4.2.	Предусмотрите необходимость резервирования рабочей площадки дежурной смены САЦ, рабочей площадки штаба
4.3.	Подготовьте план действий по оперативному вводу в эксплуатацию резервного ЦОДа, резервной площадки дежурной смены, резервного штаба
4.4.	Подготовьте план действий по организации работы штаба на удаленном доступе
5.	**Мобильный штаб**
5.1.	Оцените необходимость создания мобильного штаба, примите соответствующее решение
6.	**Информационная безопасность**
6.1.	Доработайте политики информационной безопасности с учетом создания САЦ
6.2.	Защитите информационную инфраструктуру САЦ и его стыки с системами АСУ ТП от внешних воздействий
6.3.	Предусмотрите в САЦ инструменты оперативного мониторинга состояния защищенности информационной инфраструктуры
7.	**Статистика и отчетность**
7.1.	Сформулируйте основные показатели работы САЦ
7.2.	Предусмотрите инструменты статистического учета и анализа
7.3.	Сформулируйте требования и вид необходимых отчётов
7.4.	Предусмотрите инструменты для создания новых форм отчетности и аналитической обработки
8.	**Администрирование**
8.1.	Предусмотрите инструменты собственного администрирования САЦ – заведение пользователей, ролей и др.
9.	**Сервисная поддержка**
9.1.	Учтите необходимость сервисной поддержки и развития САЦ, запланируйте соответствующий бюджет на последующие годы