ПРЕДЪЯВИТЕ ДОКУМЕНТЫ, ИЛИ К ВОПРОСУ О КОНТРОЛЕ ИЗМЕНЕНИЙ НА РАБОЧИХ МЕСТАХ ПОЛЬЗОВАТЕЛЕЙ

Мозолина Н.В., МФТИ (НИУ)

Изменения на рабочих местах пользователей

Санкционированные или нет?

Изменения на рабочих местах пользователей

Санкционированные или нет?

Возможные последствия изменений:

- Нерациональное использование рабочего времени
- Промышленный шпионаж
- Угрозы безопасности
- Нарушение работоспособности системы

ПМ «Паспорт ПО» и контроль конфигураций

ПМ «Паспорт ПО»

- разработан для анализа программной среды компьютеров под управлением ОС Windows
- мониторинг состояния рабочих мест пользователя

SecCM

- концепция повышения защищённости информационной системы за счёт управления её конфигурациями
- Управление конфигурациями, ориентированного на безопасность (Security-Focused Configuration Management of Information Systems, SecCM)

Ключевые этапы деятельности SecCM

- планирование SecCM (разработка политик применения средства SecCM),
- внедрение SecCM (определение базовых конфигураций и их утверждение),
- контроль изменений конфигурации (использование некоторой панели управления конфигурации для рассмотрения и утверждения изменений в ИС)
- мониторинг уже утверждённых конфигураций.

Основные элементы «Паспорт ПО»

- серверный компонент (Сервер) с базой данных;
- компонент управления (АРМ управления);
- клиентский компонент (Клиент), устанавливаемый на подконтрольные объекты (ПКО), – рабочие места (СВТ), конфигурацию которых контролирует программный модуль;
- сервис обмена сообщениями RabbitMQ, обеспечивающий взаимодействие по сети между всеми элементами

Основные этапы работы ПМ «Паспорт ПО»

планирование SecCM внедрение SecCM	регистрация учетных записей, формирование ролей и назначение их учётным записям; формирование списка ПКО с разбиением на подразделения; формирование общей базы шаблонов; назначение шаблонов подконтрольным объектам; проведение опроса на ПКО и формирование его паспорта ПО;
контроль изменений конфигурации	сканирование ПКО по заданному расписанию или по запросу; автоматическое сравнением Сервером полученных данные о текущем состоянии ПКО с эталонным и информирует управляющий персонал о выявленных нарушениях обновление паспорта ПО или же принятие мер по устранению несоответствий
мониторинг	информация обо всех действиях по формированию как проектов паспортов ПО, так и самих паспортов ПО сохраняется в журнале событий ПМ «Паспорт ПО

Соответствие между основными процессами и объектами

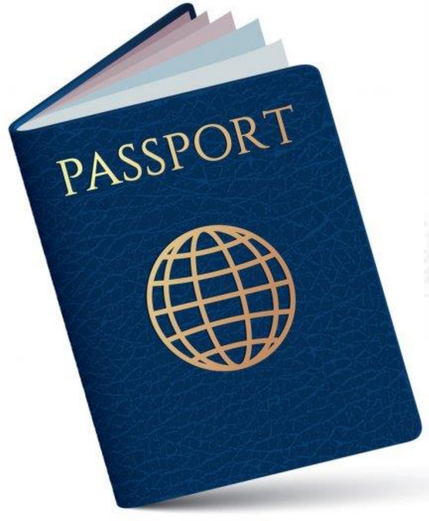
NIST.SP.800-128	ПМ «Паспорт ПО»
Управление конфигурацией, Configuration Management (CM) – набор действий, направленных на создание и поддержание целостности продуктов и систем посредством контроля процессов создания, изменения и мониторинга конфигураций этих продуктов и систем.	Набор действия по формированию базы шаблонов (типовых конфигураций СВТ), назначению их рабочим местам пользователей, формированию паспортов ПО, проведения сканирования рабочих мест и сравнения текущей конфигурации СВТ (проекта паспорта) с эталонной (паспорт ПО).
Элемент конфигурации, Configuration Item (CI) – идентифицируемая часть системы (например, аппаратное обеспечение, программное обеспечение, встроенное ПО, документация или их комбинация), которая является дискретной целью процесса управления конфигурацией.	Подконтрольный объект (ПКО) – СВТ с установленным на него Клиентом ПМ «Паспорт ПО», однозначно идентифицируется именем ПКО. Обеспечение контроля целостности конфигурации ПКО является целью применения ПМ «Паспорт ПО».

Соответствие между основными процессами и объектами

Базовая конфигурация, Baseline Configuration – набор спецификаций для системы или элемента конфигураций в системе, который был рассмотрен и согласован в определенный момент времени и который может быть изменен только через процедуры контроля изменений.	Паспорт ПО – заверенный проект паспорта ПО, содержащий информацию о конфигурации СВТ. Процесс заверения проекта заключается в его подписи пользователем ПМ «Паспорт ПО». Формирование нового паспорта ПО для СВТ возможно лишь в результате формирования нового проекта паспорта ПО, его сопоставления с действующим паспортом, а также подписи данного проекта.
План управления конфигурацией, Configuration Management Plan (CM Plan) – полное описание ролей, обязанностей, политики и процедуры, применяемых при управлении конфигурацией продуктов и системы.	ПМ «Паспорт ПО» является инструментом контроля целостности состояния программной среды, регламент же его применения для мониторинга конфигураций рабочих мест пользователей информационной системы может быть рассмотрен как план управления конфигурацией.

Заключение

Программный модуль «Паспорт ПО» позволяет решить задачу контроля изменений конфигурации рабочих мест пользователей, реализуя принципы управления конфигурациями, ориентированного на безопасность



СПАСИБО ЗА ВНИМАНИЕ!