ЧАСТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«Учебный Центр РТСофт»

ЧУ ДПО «УЦ РТСофт»

**УТВЕРЖДАЮ**

**Директор**

_____

Программа

дополнительного профессионального образования

# «Кибер-безопасность в АСУ ТП»

Москва

2017

ЧАСТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«Учебный Центр РТСофт»

ЧУ ДПО «УЦ РТСофт»

**УТВЕРЖДАЮ**

**Директор**

_____

УЧЕБНЫЙ ПЛАН

дополнительного профессионального образования

**«Кибер-безопасность в АСУ ТП»**

---

**Цель:** Целью преподавания дисциплины является формирование у обучаемых комплекса базовых знаний и практических навыков, необходимых для выполнения функциональных обязанностей в сфере разработки и сопровождения систем кибер-безопасности в АСУ ТП.

**Категория слушателей:** с высшим и средне-техническим образованием, системные интеграторы и конечные пользователи.

**Форма обучения:** очная.

**Форма контроля:** зачет по результатам практических занятий и тестирования.

**Продолжительность обучения:** 24 часа.

**Режим занятий:** 8 академических часов в день.

**Срок обучения:** по договоренности с заказчиком.

**Выдаваемый документ:** «Удостоверение о повышении квалификации»

---

| | *Наименование разделов и дисциплин* | *Всего, час* | *В том числе* | | *Форма контроля* |
|---|---|---|---|---|---|
| | | | *Лекции* | *Практические занятия* | |
| *1.* | Методика формирования доверенной программной среды в АСУ ТП и унификации защищенного взаимодействия процессов обработки данных. | 2 | 2 | | *зачет* |
| *2.* | Основные системотехнические решения и функциональные возможности ЗКП «Plato RT». Сравнительный анализ выполнения требований Пр. ФСТЭК 2014г. №31 | 2 | 2 | | *зачет* |
| *3.* | Перехват и нейтрализация угроз со стороны привилегированных, категорий пользователей (сотрудник-инсайдер, системный администратор) | 3 | 1 | 2 | *зачет* |
| *4.* | Организация (скрытой от базовой ОС) защищенной области хранения данных, порядок регистрации и автоматической обработки инцидентов безопасности | 3 | 1 | 2 | *зачет* |
| *5.* | Двухконтурная схема мониторинга и управления состоянием узлов ЛВС объекта АСУ ТП, реализация в независимом контуре («технологическом тракте») функций контроля доступности и целостности объектов защиты | 2 | 1 | 1 | *зачет* |
| *6.* | Событийно-ориентированный контроль состояния и результатов выполнения критически важных процессов АСУ ТП | 2 | 1 | 1 | *зачет* |
| *7.* | Хранение эталонных конфигураций (формуляров) и анализ текущего состояния контролируемых узлов средствами подсистемы хранения данных ЗКП «Plato RT» | 2 | | 2 | *зачет* |
| *8.* | Разделение функций по управлению функционированием АСУ ТП и управлению системой защиты с использованием АРМ ОБИ и АРМ ФК | 4 | 1 | 3 | *зачет* |
| *9.* | Реализация организационно-распорядительных функций, доверенного (защищенного) документооборота, экспресс-анализа данных в среде ЗКП «Plato RT» | 4 | 1 | 3 | *зачет* |
| | ИТОГО | 24 | 10 | 14 | |

ЧАСТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«Учебный Центр РТСофт»

ЧУ ДПО «УЦ РТСофт»

УЧЕБНАЯ ПРОГРАММА

дополнительного профессионального образования

**«Кибер-безопасность в АСУ ТП»**

---

1. **Методика формирования доверенной программной среды в АСУ ТП и унификации защищенного взаимодействия процессов обработки данных.**

   Унификация модели защиты и создание доверенной среды организации вычислительного процесса при реализации КСЗ в составе ЗКП «Plato RT» возможна только на уровне доверенных защищенных средств общесистемного программного обеспечения (ОСПО), формирующих встроенную доверенную среду исполнения прикладных задач в, общем случае, недоверенной среде общего программного обеспечения (ОПО) изделия .

   Под доверенной вычислительной средой узла ЛВС (сервер или АРМ ДЛ КСА объекта применения ЗКП «Plato RT») понимается совокупность доверенных элементов, ограниченная периметром (контуром) защиты. Различаются встраиваемые - наложенный (внешний) и внутренний периметры защиты (НПЗ и ВПЗ соответственно). В качестве базовой ОС используются ОС семейства MS Windows (для объектов, не обрабатывающих ГТ РФ).

2. **Основные системотехнические решения и функциональные возможности ЗКП «Plato RT». Сравнительный анализ выполнения требований Пр. ФСТЭК 2014г. №31.**

   Произвольное СВТ узла ЛВС в составе объекта может иметь две области функционирования прикладных процессов обработки данных: встроенную доверенную (шестигранник на варианте справа заключает ее периметр защиты) и недоверенную, которая ограничена внешним наложенным периметром защиты, применяемым ко всем процессам в составе СВТ (соответствует внешнему контуру обоих вариантов, представленных на рисунке 2.2).

   Все процессы обработки данных в составе СВТ делятся на 3 класса: доверенные - функционирующие внутри периметра защиты, условно доверенные – (как правило) используются для обеспечения контролируемого экспорта данных на отчуждаемые носители, недоверенные – играют вспомогательную роль при обработке информации, не составляющей государственной тайны РФ. Отметим, что функции экспорта данных на отчуждаемые носители (в том числе на средства сетевого доступа) предоставляются только доверенным процессам.

   Доверенное программное обеспечение (ДПО) предполагает совместное выполнение нижеперечисленных условий – “обобщенных критериев доверия” (далее ОКД D[3]):

   d1 - подтвержденную независимым органом авторизацию кода и 100% правообладание им резидентами РФ (юридическими и/или физическими лицами);

   d2 - представление полного состава конструкторской и программной документации в соответствии с ГОСТ РФ;

   d3 – сопровождение жизненного цикла продукта (проектирование, разработка, сертификация, применение в составе КСА объекта) уполномоченным государственным органом (ФСТЭК РФ, МО РФ, ФСБ РФ).

   Условно-доверенное программное обеспечение (УПО) предполагает невыполнение хотя бы одного из условий определения ДПО. Недоверенным программным обеспечением (НПО) считается код, в отношении которого не выполняются все 3 вышеперечисленных требования.

   Функции хранения, обработки и передачи конфиденциальной информации, должны исполняться процессами, погруженными в доверенную среду, изоляция которой от внешних (вне периметра СВТ) и внутренних (внутри СВТ) потенциально вредоносных

воздействий должна гарантированно обеспечиваться на уровне встроенного периметра защиты.

В ЗКП «Plato RT» программными средствами реализовано 106 требований (63%) из 167, содержащихся в Приказе ФСТЭК 2014г. №31.

3. **Перехват и нейтрализация угроз со стороны привилегированных, категорий пользователей (сотрудник-инсайдер, системный администратор).**

Для локальной регистрации инцидентов безопасности и невозможности сокрытия последствий вредоносной активности со стороны внутреннего нарушителя, кроме физического разделения трактов на информационный и технологический, на всех узлах клиентской группы установлены дополнительные энергонезависимые средства хранения (жесткий диск), на которых хранится эталонная конфигурация узла и осуществляться локальная регистрация событий ИБ. Дополнительный диск должен обслуживается средствами ИКСИ+, функционирующими на уровне Ring -1, при этом доступ к нему со стороны процессов базовой ОС, исключается средствами гипервизора безопасности.

Функции по управлению безопасностью информации в объеме требований РД ФСТЭК реализуются в доверенной среде ИКСИ+ на АРМ ОБИ.

4. **Организация (скрытой от базовой ОС) защищенной области хранения данных, порядок регистрации и автоматической обработки инцидентов безопасности.**

АРМ ДЛ на уровнях гипервизора безопасности (Ring -1) и ядра базовой ОС (Ring 0). Эти компоненты создают периметры защиты – защищенные от угроз нарушения целостности и конфиденциальности области исполнения конечных приложений (комплексов задач СПО) для каждого узла гетерогенной сети. Взаимодействие между узлами осуществляется посредством транспортной магистрали (ESB-шины) передачи данных, подключение к которой возможно только доверенными средствами (API КСЗ).

Функции хранения, обработки и передачи конфиденциальной информации, а также информации, составляющей ГТ РФ, исполняется процессами, погруженными в доверенную среду, изоляция которой от внешних (вне периметра СВТ) и внутренних (внутри СВТ) потенциально вредоносных воздействий обеспечивается на уровне встраиваемого периметра защиты (ВПЗ).

Каждое СВТ в составе КСА объекта, оснащенного средствами КСЗ ЗКП «Plato RT», рассматривается как совокупность непересекающихся множеств доверенных и недоверенных программных компонентов, распределенных по иерархическим уровням вложенных слоев виртуализации, в основании которых лежит слой P0 - доступ к физическим (не виртуализируемым) аппаратным средствам и ресурсам.

Рекурсивная инициализация и функционирование контуров защиты с поддержкой вложенных слоев виртуализации процессов в составе СВТ обеспечивается доверенными средствами.

5. **Двухконтурная схема мониторинга и управления состоянием узлов ЛВС объекта АСУ ТП, реализация в независимом контуре («технологическом тракте») функций контроля доступности и целостности объектов защиты.**

Двухконтурная схема мониторинга и управления состоянием узлов ЛВС с раздельным применением технологического и информационного трактов обмена приведена ниже.

6. **Событийно-ориентированный контроль состояния и результатов выполнения критически важных процессов АСУ ТП.**

Реакция КСЗ на нарушения целостности ПО (в процессе загрузки и динамически в процессе работы), а также события (инциденты ИБ) выполняется в автоматическом режиме с использованием словаря сценариев и, собственно, самих файлов (документов) - сцнариев, содержащих описание последовательности необходимых действий по восстановлению целостности и блокировке процессов (задач) на заданном узле. Сценарии разрабатываются с использованием среды программирования Python. Управление выполнением сценариев осуществляется встроенными в ЗКП «Plato RT» общесистемными средствами ИКСИ.

7. **Хранение эталонных конфигураций (формуляров) и анализ текущего состояния контролируемых узлов средствами подсистемы хранения данных ЗКП «Plato RT».**

Подсистема хранения данных строится на основе доверенных компонентов многомерной темпоральной СУБД (СУБДмт) «SLON» из состава ИКСИ, дополненных средствами бескомпроматного хранения в среде специализированной файловой системы,

функционирующей на уровне Ring -1 под управлением гипервизора безопасности HYPERON (ИКСИ+). Доступ к функциям (сервисам) хранения СУБДмт «SLON» обеспечивается посредством темпорального расширения встроенного SQL-интерфейса для всех приложений, функционирующих под управлением ИКСИ. Доступ к файловой системе гипервизора безопасности HYPERON обеспечен только процессам КСЗ ЗКП «Plato RT», при этом удаленный доступ предоставляется исключительно средствами АРМ ОБИ.

Темпоральные возможности СУБДмт «SLON» используются для хранения заданных конфигураций объекта и управления версионностью ПО ЗКП «Plato RT» средствами АРМ ФК.

**8. Разделение функций по управлению функционированием АСУ ТП и управлению системой защиты с использованием АРМ ОБИ и АРМ ФК.**

Регистрация событий, связанных с нарушением целостности и доступности всех узлов производится по технологическому тракту на АРМ ОБИ и АРМ ФК.

Функциональный контроль реализуется только на АРМ ФК, при этом управление безопасностью информации в объеме требований РД ФСТЭК реализуется в доверенной среде ИКСИ+ только средствами АРМ ОБИ.

Журнал регистрации событий системы защиты, в частности, состоит из следующих полей:

- «Дата-время» (в данном поле хранятся даты и время запросов);
- «Код операции» (в данном поле хранятся коды операций запросов);
- «Код результата» (в данном поле хранятся коды результатов выполнения запросов);
- «ЛМ отправителя» (в данном поле хранятся имена ЛМ – отправителей запросов);
- «ВУ отправителя» (в данном поле хранятся номера ВУ – отправителей запросов);
- «ЛМ получателя» (в данном поле хранятся имена ЛМ – получателей запросов);
- «ВУ получателя» (в данном поле хранятся номера ВУ – получателей запросов);
- «Идентификатор» (в данном поле хранятся идентификаторы пользователей, выполнявших запрос. Данное поле может быть пустым, если запрос выполнялся до прописки пользователя);
- «Ранг» (в данном поле хранятся ранги полномочий пользователей, выполнявших запрос.

Ведение данного журнала обеспечивается на АРМ ОБИ средствами ИКСИ+, кроме того, на всех узлах клиентской группы производится независимая локальная регистрация инцидентов ИБ на уровне Ring -1 средствами гипервизора безопасности.

**9. Реализация организационно-распорядительных функций, доверенного (защищенного) документооборота, экспресс-анализа данных в среде ЗКП «Plato RT».**

Данные функции реализуются с использованием встроенных в ИКСИ доверенных компонентов:

Платформа автоматизации процессов документооборота

Предназначена для построения многоуровневых защищенных ECM-систем предприятий и организаций. Использует встроенную интеграционную шину CAPI для подключения внешних систем документооборота и поддержки нескольких параллельных контуров прохождения информации - *служебного* (деловая переписка), *организационно-распорядительного* (управление инфраструктурой) и *личного* (неформальное взаимодействие абонентов с гарантией конфиденциальности)

Интерактивный экспресс-анализатор данных

Обеспечивает быструю (в online-режиме) автоматическую или ручную настройку на источники данных и проведение по заданному шаблону или непосредственно пользователем анализа множества объектов (т.н. “фоновой группы”), обладающих набором однотипных свойств, значения которых могут быть представлены в количественном или качественном выражении. Формируемая системой интегральная оценка отражает ранг (место) каждого объекта в группе с точки зрения целевой функции (задачи), определяемой конечным пользователем-аналитиком

Графическая визуализация позволяет отображать информацию в удобном для восприятия виде с использованием графических объектов, гистограмм, таблиц и шаблонов анализа количественных и качественных показателей (индикаторов), характеризующих предметную область, обеспечивает экспорт выходных данных - текстовых файлов, таблиц, диаграмм и др. в офисные приложения.