Можно ли победить в борьбе с человеческим фактором?

О технических средствах помощи администраторам информационной безопасности в борьбе с человеческим фактором

Лыдин Сергей

ЗАО «ОКБ САПР»

Роль администратора информационной безопасности (ИБ)

Администратор ИБ, как правило, в пределах своих обязанностей обеспечивает безопасность информации ограниченного доступа (ИОД), обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (СВТ) в информационных системах (ИС) организаций

Основные должностные обязанности администратора ИБ

- Расследование фактов нарушения безопасности защищаемой информации
- Обеспечение возможности выполнения установленной технологии обработки информации
- Обеспечение антивирусного контроля
- Обеспечение контроля за использованием машинных носителей ИОД

Основные должностные обязанности администратора ИБ

- Контроль за соблюдением пользователями требований инструкций по эксплуатации средств защиты информации (СЗИ)
- Контроль состава и целостности ПО, эксплуатируемого на СВТ
- …

Постановка проблемы

Выполнение администраторами ИБ основных должностных обязанностей сопряжено с **трудностями**, которые обусловлены:

- отсутствием технических средств автоматизации деятельности администратора ИБ
- использованием пользователями мобильных и компактных средств обработки информации, «размывающими» границы контролируемой зоны организации

Расследование фактов нарушения безопасности защищаемой информации

Трудности:

- проведение расследования, подключал ли пользователь съемный носитель ИОД за пределами контролируемой зоны
- сбор журналов безопасности с автономных СВТ для проведения расследования фактов нарушения безопасности с обеспечением неизменности их содержимого

Обеспечение возможности выполнения технологии обработки информации

Трудности:

• обеспечение возможности переноса ИОД на съемных носителях исключительно в пределах контролируемой зоны

•предотвращение утечки информации посредством скрытых каналов утечки при ее передаче на автономные СВТ

Обеспечение антивирусного контроля

Трудности:

•предотвращение поступления в контролируемую зону вредоносных программных средств на съемных носителях ИОД

Обеспечение контроля за использованием машинных носителей ИОД

Трудности:

•обеспечение запрета выноса ИОД на съемных носителях за пределы контролируемой зоны

•контроль несанкционированного подключения съемных носителей ИОД к СВТ

Контроль за соблюдением пользователями требований инструкций по эксплуатации СЗИ

Трудности:

•обеспечение возможности использования средств хранения криптографических ключей исключительно на СВТ с созданной средой функционирования криптографии

Контроль состава и целостности ПО

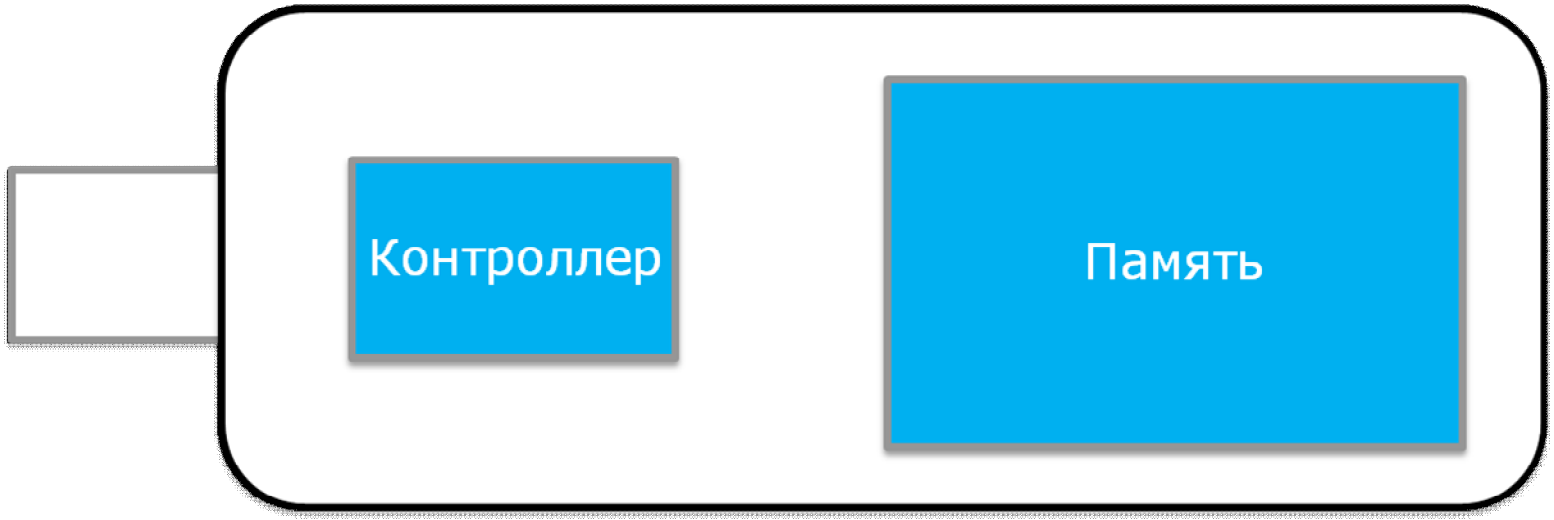
Трудности:

•предотвращение несанкционированной модификации содержимого эталонных носителей программного обеспечения

Решение

Использование в составе информационной системы специального USB-носителя информации (СН) – активного устройства с управляемым доступом к памяти – и программно-аппаратных средств защиты информации на его основе

Структура специального носителя информации



Свойства специального носителя информации

- аппаратная поддержка аутентификации компьютерной системы
- разделение секретов с компьютерной системой

Аппаратная поддержка

- решение о доступе к данным принимают совместно СН и компьютерная система
- прозрачное шифрование данных USB-носителя контроллером СН
- сложность проникновения внутрь микросхемы
- встроенные аппаратные и технологические механизмы защиты внутреннего кода
- безопасный криптографический протокол авторизации пользователя

Разделение секретов

- взаимная аутентификация компьютерной системы и СН
- взаимная аутентификация пользователя и СН на основании знания пароля (опционально)

Программно-аппаратные СЗИ на основе СН

- Линейка защищенных носителей информации пользователя «Секрет»
- Программно-аппаратный неперезаписываемый журнал («ПАЖ»)
- Хранилище ключей «Идеальный токен»
- Система однонаправленной передачи данных («СОПД»)
- «Эталонный носитель образов ПО»

Линейка «Секрет»

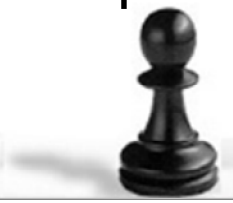
СН может использоваться только на рабочих станциях и серверах, разрешенных администратором за счет реализации механизмов:

- авторизация администратора и пользователя СН
- настройка администратором правил доступа пользователя к информации на СН
- взаимная аутентификация СН и компьютерной системы
- ведение аппаратного журнала событий

Линейка «Секрет»

Позволяет обеспечить:

- возможность переноса ИОД на съемных носителях исключительно в пределах контролируемой зоны
- проведение расследования, подключался ли съемный носитель ИОД за пределами контролируемой зоны
- предотвращение поступления в контролируемую зону вредоносного ПО на съемных носителях информации пользователей



«ПАЖ»

Специальный носитель информации используется для ведения неперезаписываемого журнала событий за счет реализации механизмов:

- предоставление возможности записи событий в журнал только на разрешенных СВТ
- предоставление возможности чтения событий из журнала только на разрешенных СВТ
- поддержка ролевой инфраструктуры
- ведение собственного журнала событий безопасности

«ПАЖ»

Позволяет обеспечить:

•сбор журналов безопасности с автономных средств вычислительной техники для проведения расследования фактов нарушения безопасности с обеспечением неизменности их содержимого

«Идеальный токен»

Специальный носитель информации используется для хранения криптографических ключей и их применения на СВТ, разрешенных администратором ИБ, за счет реализации механизмов:

авторизация администратора и пользователя СН

•настройка администратором правил доступа пользователя к информации на СН

•взаимная аутентификация СН и компьютерной системы

«Идеальный токен»

Позволяет обеспечить:

- возможность использования средств хранения криптографических ключей исключительно на СВТ с созданной средой функционирования криптографии

«СОПД»

Специальный носитель информации используется для передачи данных между защищенным и незащищенным СВТ при полном блокировании передачи в обратном направлении за счет реализации механизмов:

- при подключении к незащищенному АРМ: предоставление доступа в режиме «чтение и запись»
- при подключении к защищенному АРМ: предоставление доступа в режиме «только чтение»

«СОПД»

Позволяет обеспечить:

•предотвращение утечки информации посредством скрытых каналов утечки при ее передаче на автономные средства вычислительной техники

«Эталонный носитель»

Специальный носитель информации используется для хранения и переноса защищенных от несанкционированной модификации эталонных образов ПО за счет реализации механизмов:

- при подключении к АРМ администратора ИБ: предоставление доступа к образам ПО в режиме «чтение и запись»
- при подключении к остальным АРМ: предоставление доступа к образам ПО в режиме «только чтение»

«Эталонный носитель»

Позволяет обеспечить:

- предотвращение несанкционированной модификации содержимого эталонных носителей программного обеспечения

Спасибо за внимание!

С уважением,
Лыдин Сергей
ЗАО «ОКБ САПР»
www: www.okbsapr.ru
email: ssl@okbsapr.ru