Можно ли победить в борьбе с человеческим фактором?

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

ОКБ САПР

Роль администратора информационной безопасности

Администратор информационной безопасности (ИБ), как правило, обеспечивает безопасность информации, передаваемой и хранимой в информационных системах организаций при помощи средств вычислительной техники.

Основные должностные обязанности администратора ИБ

В обязанности администратора ИБ входит:

1) расследование фактов нарушения безопасности защищаемой информации;
2) обеспечение возможности выполнения установленной технологии хранения и переноса информации;
3) обеспечение антивирусного контроля;
4) обеспечение контроля за использованием пользователями носителей информации;

Основные должностные обязанности администратора ИБ

5) контроль за соблюдением пользователями требований инструкций по эксплуатации средств защиты информации (СЗИ);
6) контроль состава и целостности ПО, эксплуатируемого на СВТ;
7) …

Проблемы в работе администратора ИБ

Перечень основных проблем, с которыми сталкивается администратор ИБ при выполнении должностных обязанностей:

1) утечка информации вследствие использования съемных носителей информации за пределами контролируемой зоны;
2) сбор журналов с обеспечением неизменности их содержимого;
3) поступление в контролируемую зону вредоносного ПО;

Проблемы в работе администратора ИБ

4) использование средств хранения криптографических ключей только на СВТ созданной средой функционирования криптографии;
5) возможность несанкционированного изменения содержимого эталонных носителей программного обеспечения;
6) использование носителей информации за пределами контролируемой зоны;

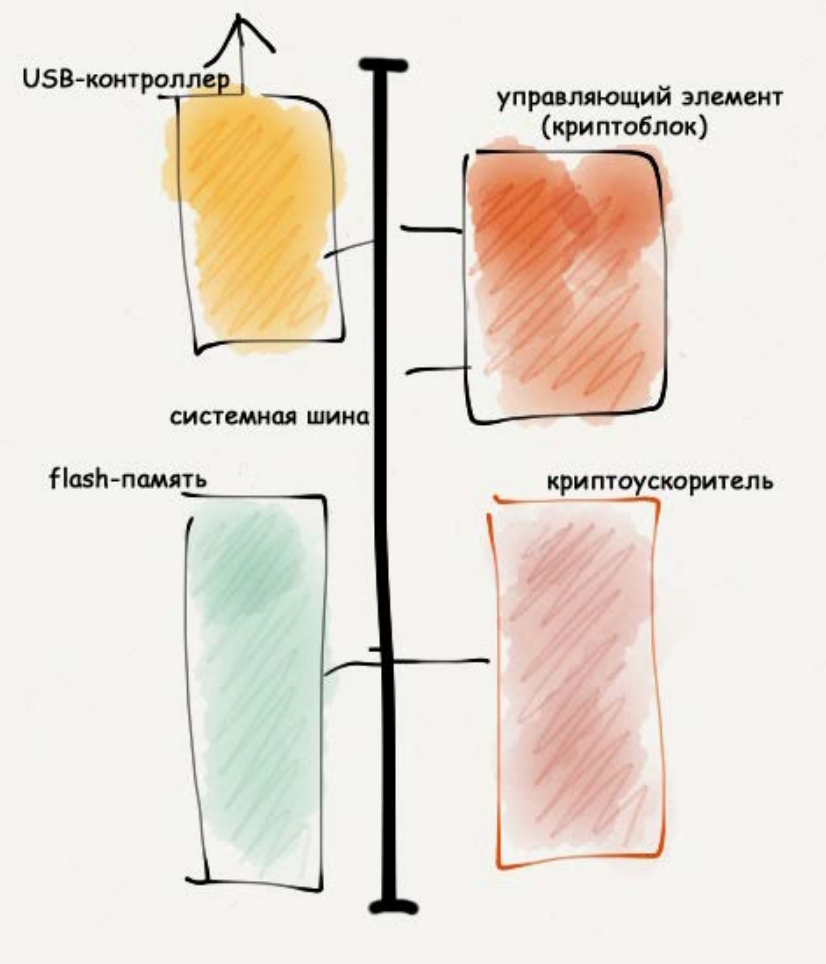
Проблемы в работе администратора ИБ

7) вынос съемных носителей за пределы контролируемой зоны;
8) несанкционированное подключение съемных носителей информации к СВТ в контролируемой зоне.

Поиск решения

Решение в задаче предотвращения проблем, возникающих в процессе работы администратора ИБ, заключается в использовании в составе информационной системы специального носителя информации (СН) с USB-интерфейсом (активного устройства с управляемым доступом к памяти) и программно-аппаратных средств защиты информации на его основе.

Структура специального носителя



Свойства специального носителя информации

- ✓ аппаратная поддержка аутентификации компьютерной системы;
- ✓ разделение секретов с компьютерной системой.

Аппаратная поддержка аутентификации компьютерной системы

- ✓ решение о доступе к данным принимают совместно СН и компьютерная система;
- ✓ применение технологических мер защиты от атак, связанных с несанкционированным изменением структуры аппаратного модуля;
- ✓ сложность проникновения внутрь микросхемы;
- ✓ безопасный криптографический протокол авторизации пользователя.

Разделение секретов и компьютерной системы

- ✓ взаимная аутентификация компьютерной системы и СН;
- ✓ взаимная аутентификация пользователя и СН на основании знания пароля.

Линейка специальных носителей

- ✓ защищенные носители информации «Секрет»;
- ✓ программно-аппаратный неперезаписываемый журнал («ПАЖ»);
- ✓ хранилище ключей «Идеальный токен»;
- ✓ специальный носитель «Система Ниппель»;
- ✓ специальный носитель «Секрет Администратора».

Защищенные флешки «Секрет»

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

- ✓ авторизации администратора и пользователя СН;
- ✓ настройки администратором правил доступа пользователя к информации на СН;
- ✓ взаимной аутентификации СН и компьютерной системы;
- ✓ ведения аппаратного журнала событий.

Защищенные флешки «Секрет»

позволяют обеспечить:

- ✓ перенос информации (в т.ч. ИОД) на съемных носителях исключительно в пределах контролируемой зоны;
- ✓ проведение расследования, подключался ли съемный носитель за пределами контролируемой зоны;
- ✓ предотвращение поступления в контролируемую зону вредоносного ПО на съемных носителях информации пользователей.

Защищенные флешки «Секрет»

На базе СН «Секрет» строятся продукты семейства «Секрет»: ПАК «Секрет Особого Назначения» («СОН») и ПАК «Секрет Фирмы».

«СОН» используется на отдельно взятых компьютерах, а «Секрет Фирмы» – на компьютерах локальной сети, имеющих общий управляющий элемент – Сервер Аутентификации.

По принципу, впервые реализованному в СН «Секрет», построены и другие служебные носители для различных более узких целей.

Программно-аппаратный неперезаписываемый журнал

ПАЖ используется для ведения неперезаписываемого журнала событий за счет реализации следующих 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.

Программно-аппаратный неперезаписываемый журнал

позволяет обеспечить:

- ✓ сбор журналов безопасности с СВТ для выявления фактов нарушения безопасности с обеспечением неизменности их содержимого.

«Идеальный токен»

Специальный носитель «Идеальный токен» 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.

«Система Ниппель»

СН «Система Ниппель» используется для организации однонаправленного канала передачи данных с целью защиты автоматизированных систем (АС) от нежелательного и неавторизованного раскрытия обрабатываемой, хранимой и передаваемой в АС информации конфиденциального характера.

«Система Ниппель»

позволяет:

- ✓ исключить возможность передачи данных посредством скрытых каналов;
- ✓ препятствовать нарушению работоспособности СВТ и АС;
- ✓ блокировать доступ к ресурсам СВТ;
- ✓ препятствовать нарушению целостности данных и программного обеспечения.

«Секрет Администратора»

СН «Секрет Администратора» используется для защиты эталонных образов ПО от несанкционированных модификаций и поддержания АС организации (в случае сбоев) в работоспособном состоянии.

«Секрет Администратора»

позволяет обеспечить :

- ✓ возможность восстановления функционирования компьютеров в случае возникновения нештатных ситуаций при полном или частичном выходе из строя программных составляющих СВТ;
- ✓ целостность эталонного набора программных составляющих СВТ АС.

Заключение

№	Основные должностные обязанности администратора ИБ	Проблемы, с которыми сталкивается администратор ИБ при выполнении обязанностей	Продукты, препятствующие возникновению проблем в работе администратора ИБ
1	Расследование фактов нарушения безопасности защищаемой информации.	1) сбор журналов с обеспечением неизменности их содержимого; 2) использование носителей информации за пределами контролируемой зоны;	СН «ПАЖ».
2	Обеспечение возможности выполнения установленной технологии хранения и переноса информации.	1) утечка информации вследствие использования съемных носителей информации за пределами контролируемой зоны;	СН «Система Ниппель».
3	Обеспечение антивирусного контроля.	1) поступление в контролируемую зону вредоносного ПО;	СН «Секрет Фирмы».
4	Обеспечение контроля за использованием пользователями носителей информации.	1) вынос съемных носителей за пределы контролируемой зоны; 2) несанкционированное подключение съемных носителей к СВТ в контролируемой зоне;	СН «Секрет Особого Назначения»; СН «Быстрый Секрет»; СН «Секрет Руководителя».
5	Контроль за соблюдением пользователями требований инструкций по эксплуатации средств защиты информации.	1) использование средств хранения криптографических ключей только на СВТ созданной средой функционирования криптографии;	СН «Идеальный токен».
6	Контроль состава и целостности ПО, эксплуатируемого на СВТ.	1) возможность несанкционированного изменения содержимого эталонных носителей программного обеспечения.	СН «Секрет Администратора».

Спасибо за внимание!

ОКБ САПР

www.okbsapr.ru