АГАТ
системы управления

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «АГАТ- системы управления» - управляющая компания холдинга «Геоинформационные системы управления»

220600, г.Минск,
пр.Независимости,117
Тел.: (+375-17) 267-44-55
Факс: (+375-17) 267-25-05

http://www.agat.by
E-mail: agat@agat..by

АГАТ
системы управления

Актуальные проблемы обеспечения кибербезопасности

Авторы доклада:
Бобов М.Н., Горячко Д.Г.,
Спесивцев В.В.
Тел.: (+375-17) 287 -13- 57

АГАТ
системы управления

Основные определения

Кибербезопасность – способность инфокоммуникационной среды противостоять преднамеренно организованной совокупности действий с участием программно технических средств (ПТС), направленной на нанесение экономического, технического или информационного ущерба.

Инфокоммуникационная среда – совокупность телекоммуникационных сетей с обеспечивающей их функционирование технологической инфраструктурой, компьютерного оборудования с установленным программным обеспечением, используемая в человеческой деятельности (личности, организации, государства).

Кибератака – предумышленно организованная совокупность действий с участием программно технических средств (ПТС), направленная на нанесение экономического, технического или информационного ущерба. Например, получение секретных сведений по различным аспектам.

Киберзащищенность – свойство объекта инфокоммуникационной среды, характеризующее его возможности предотвращать образование ущерба от кибератак или ограничивать его величину допустимыми нормами.

АГАТ
системы управления

Главная цель кибератак

Проникновение в защищаемую инфокоммуникационную среду и установление над ней контроля

Проникновение - преодоление средств защиты периметра, используя слабости и уязвимости функционирующего программного обеспечения.

Установление контроля – получение несанкционированного доступа к узлам инфокоммуникационной среды и обрабатываемой в ней информации.

АГАТ
системы управления

Известные инструменты кибератак:

Фишинг, Троян, DDoS-атака, Ботнет, Backdoor, Черви, Классические файловые вирусы, Вирус-вымогатель (шифровальщик), Вредоностная программа (зловред), Руткит, Фрод, Флуд

Инфраструктура «Киберпреступление как услуга»

- **Cybercrime as a Service (CaaS):**
  - Ransomware as a Service (RaaS);
  - Malware as a Service (MaaS);
  - Fishware as a Service (FaaS);
  - ……

АГАТ
системы управления

СОВРЕМЕННЫЕ
легальные каналы проникновения

Сервисы:

- распространение программного обеспечения
- обновление программного обеспечения

Технологии:

- аппаратная виртуализация

АГАТ
системы управления

СПОСОБЫ распространения ПО

Software as a Service:

- облачные вычисления
- грид-вычисления

Поставщик разрабатывает веб-приложение и самостоятельно управляет им, предоставляя заказчикам доступ к программному обеспечению через интернет.

АГАТ
системы управления

ОБНОВЛЕНИЕ ПО

Цель:

- исправление имеющихся ошибок в программе;
- устранение обнаруженных уязвимостей или дыр безопасности;
- расширение функциональных возможностей программы.

Своевременное обновление ПО:

- такой же массовый и приоритетный сервис, как и распространение
- требует использования инструментов централизованного и удаленного управления и контроля.

АГАТ
системы управления

АКТУАЛЬНАЯ ПРОБЛЕМА

Поставляемое и обновляемое ПО может содержать **программные закладки**

скрытно внесенные в программное обеспечение функциональные объекты, которые при определенных условиях способны обеспечить несанкционированное программное воздействие

АГАТ
системы управления

Программная закладка

Опасность:

- принимает активные меры по маскировке своего присутствия в системе

- реализует практически неограниченный доступ к системным ресурсам

- трудно обнаруживается стандартными средствами администрирования

АГАТ
системы управления

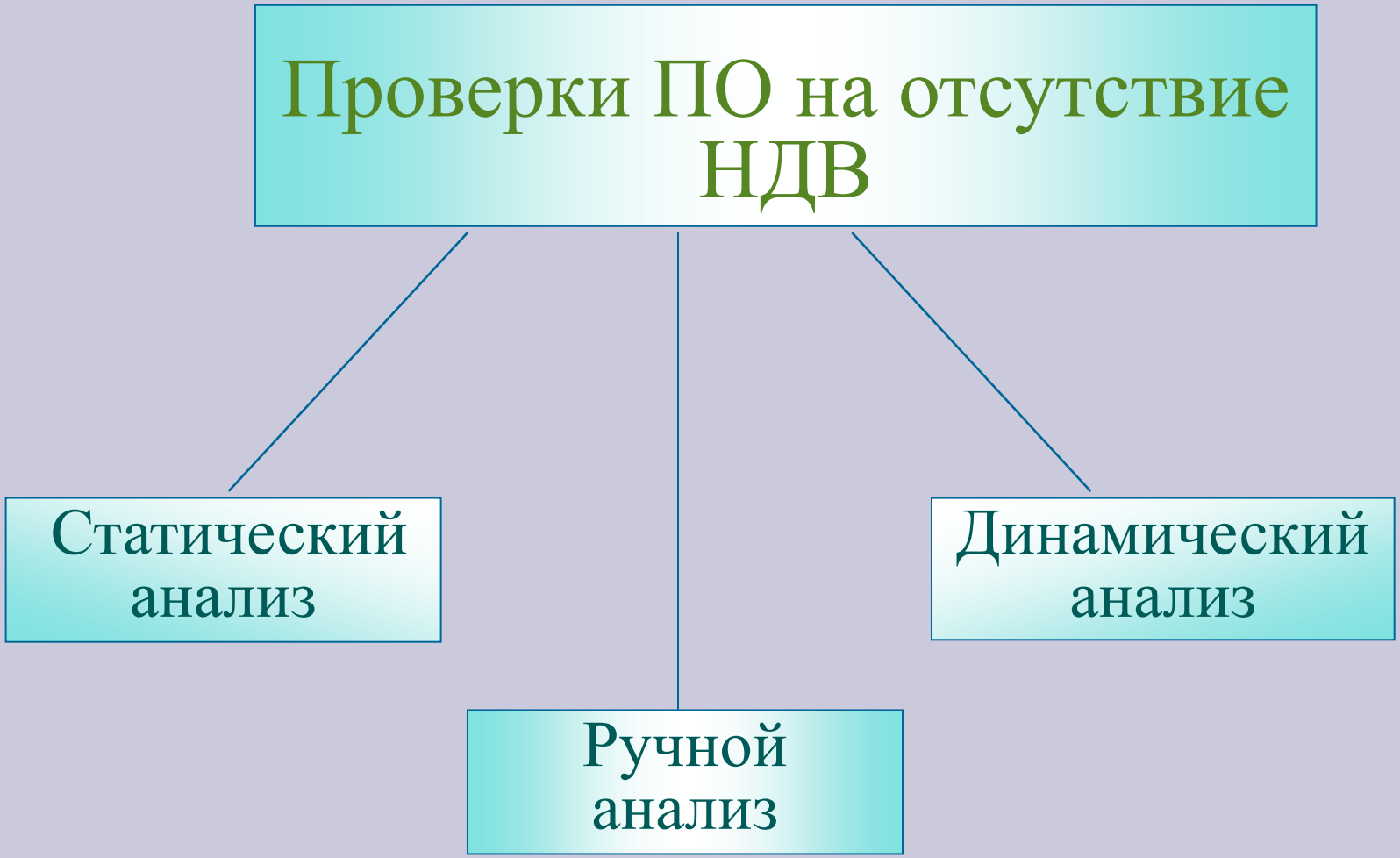
МЕРЫ противодействия программным закладкам

- проведение проверок ПО на наличие НДВ;

- использование «песочниц».

АГАТ
системы управления

Противодействие программным закладкам



АГАТ
системы управления

Противодействие программным закладкам

ОСОБЕННОСТИ
проведения проверок ПО на отсутствие НДВ

- Наличие исходного кода проверяемого ПО и его детального описания
- Необходимость изучения проверяемого ПО для подготовки соответствующих методик
- Использование сложных инструментальных средств проверки

АГАТ
системы управления

Противодействие программным закладкам

Песочница — специально выделенная среда для безопасного исполнения компьютерных программ

ВОЗМОЖНОСТИ

- анализ программ, файлов в виртуальной среде, идентичной используемой у пользователя (версия ОС, версии прикладного ПО и т. д.) в автоматическом режиме
- не требует специальных знаний в части анализа кода от администратора системы
- обнаруживает следы целевой атаки и блокирует её на стадии доставки зловредного кода пользователю.
- позволяет обнаружить вредоносный код «нулевого дня»

АГАТ
системы управления

Противодействие программным закладкам

ОСОБЕННОСТИ использования песочниц

- Проблематична реализация на уровне рабочих станций в связи со значительными затратами вычислительных ресурсов
- Большая нагрузка на систему из-за необходимости обеспечения повышенной безопасности исполнения проверяемого кода
- Реализация проверок ПО в режиме «off-line»
- Использование специализированных программно-аппаратные комплексов, работающих на уровне сети

АГАТ
системы управления

Аппаратная виртуализация

N п/п	Процессоры / Характеристики	Intel Core	Intel Pentium	Intel Celeron	Intel Xeon	Intel Atom Processor C	Intel Atom Processor E	Intel Atom Processor X,Z	AMD Atlon, Phenon
1	Технология виртуализации Intel (VT-x)	+	+	+	+	+	+	+	
2	Технология виртуал… для на… ввода/…								
3	Новые… AES								
4	Secure…								
5	Технол… Truste…								
6	Intel S… Extens…								
7	Технол…								

Техно… **Intel Virtualization для направленного ввода/вывода**

Технология Intel Virtualization Technology для направленного ввода/вывода дополняет поддержку виртуализации в процессорах на базе архитектуры IA-32 (VT-x) и в процессорах Itanium® (VT-i) функциями виртуализации устройств ввода/вывода. Технология Intel® Virtualization для направленного ввода/вывода помогает пользователям увеличить безопасность и надежность систем, а также повысить производительность устройств ввода/вывода в виртуальных средах.

АГАТ
системы управления

АКТУАЛЬНАЯ ПРОБЛЕМА

Потенциально все ЭВМ на основе процессоров с аппаратной виртуализацией подвержены угрозам нарушения информационной безопасности, поскольку становится возможной реализация **тотального контроля компьютера.**

кто первый захватил оборудование виртуализации, тот в состоянии создать для всех последующих желающих с ней поработать соответствующую программно-аппаратную среду.

АГАТ
системы управления

ТЕХНОЛОГИЯ тотального контроля компьютера

Основана на использовании двух компонент: **Гипердрайвера и Агента.**

Гипердрайвер – программа резидентно находящаяся в оперативной памяти и использующая аппаратную виртуализацию центрального процессора для создания виртуальной среды, с помощью которой осуществляется управление и контроль аппаратным и программным обеспечением компьютера.

Агент – программа управления гипердрайвером и получение информации от него.

АГАТ
системы управления

ТЕХНОЛОГИЯ
тотального контроля компьютера

АГАТ
системы управления

ТЕХНОЛОГИЯ тотального контроля компьютера

Что делать ?