ДИСЦИПЛИНА

Защита информации

Раздел 3. "Программно-аппаратные средства обеспечения информационной безопасности (ПАСОИБ)"

Тема 3. Защита от вредоносного программного обеспечения

Занятие 3/2. Групповое занятие

Тема:

Защита от вредоносного программного обеспечения

Учебные вопросы:

1. Классификация методов и средств обнаружения вредоносного программного обеспечения
2. Архитектура средств обнаружения вредоносного программного обеспечения

Цели занятия

- Рассмотреть классификацию механизмов защиты от ВПО, выявить их основные достоинства и недостатки
- Оценить эффективность вероятностных механизмов распознавания

Литература

Основная

1. Программно-аппаратные средства обеспечения информационной безопасности. В 2 ч. Ч. 1. Защита от разрушающих программных средств : пособие / А. Г. Мацкевич, С. В. Снигирев, Д. А. Свечников. – Орёл : Академия ФСО России, 2011. – 141 с.
2. Программно-аппаратные средства обеспечения информационной безопасности. В 2 ч. Ч. 2. Методы и средства локальной защиты ПЭВМ / А. В. Козачок [и др.]. – Орёл : Академия ФСО России, 2015. – 143 с.
3. Управление информационной безопасностью ТКС: учебно-методическое пособие/А.Н. Цибуля и др. – Орёл : Академия ФСО России, 2018. – 248 с.

Дополнительная

1. Aycock John. Computer Viruses and Malware. – Calgary: Springer, 2006. – p. 227.
2. Холмогоров, В. PRO ВИРУСЫ. 2-е издание. Научно-популярное издание / Валентин Холмогоров. – Санкт-Петербург : ООО «Страта», 2017. – 162 с. : ил.
3. Майкл Саттон, Адам Грин, Педрам Амини. Fuzzing: Исследование уязвимостей методом грубой силы. – Пер с англ. – Санкт-Петербург : Символ-Плюс, 2009. – 560 с. : ил.
4. Комплексная защита информации в корпоративных системах: уч. пособие / В.Ф. Шаньгин. – Москва : ИД «ФОРУМ»: ИНФРА-М, 2010. – 592 с. : ил. – (Высшее образование).
5. Записки исследователя компьютерных вирусов / К. Касперски. – Санкт-Петербург : Питер, 2005. – 316 с. : ил.
6. Компьютерные вирусы и антивирусы: взгляд программиста / К. Е. Климентьев. – Москва : ДМК Пресс, 2013. – 656 с. : ил.
7. Зайцев, О. В. ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. – С. Петербург : БХВ-Петербург, 2006. – 304 с. : ил.
8. ГОСТ Р 51188–98. Испытания программных средств на наличие компьютерных вирусов

Вопросы для самоконтроля

1. Классификация методов противодействия ВПО
2. Классификация технических средств защиты от ВПО
3. Перечислить нормативно-правовые акты в области защиты от ВПО на федеральном и ведомственном уровне (не менее 2-х по каждому уровню)
4. Технологии проактивной защиты
5. Дать определение «полиморфизм»
6. Перечислить методы защиты от переполнения буфера
7. Пояснить сущность защиты от ВПО на основе эмуляции кода
8. Пояснить сущность защиты от ВПО на основе изолированной программной среды (песочницы)


РСФСР
ТЫ
ПРОВЕРЯЛ СВОЙ КОМПЬЮТЕР НА ВИРУС?

ВОПРОС 1

Классификация методов и средств обнаружения вредоносного программного обеспечения

Детерминированные методы обнаружения ВПО

принятие решения о наличии/отсутствии ВПО – бинарное (двухзначное), т. е. или обнаружено или не обнаружено

Логические методы обнаружения ВПО

принятие решения о наличии/отсутствии ВПО – вероятностное (например, обнаружено ВПО с вероятностью 78 %)

Вероятность распознавания ВПО

		Вирус существует?	
		Да	Нет
Вирус обнаружен?	Да	Верно	α-ошибка (1-го рода) Ложное срабатывание (False positive)
	Нет	β-ошибка (2-го рода) Пропуск цели (False negative)	Верно

Детерминированные методы

+ надежное обнаружение известных штаммов ВПО
– сложности с обнаружением новых штаммов ВПО

Логические методы обнаружения ВПО

+ обнаружение новых штаммов ВПО
– высокие ошибки 1-го и 2-го родов при обнаружении ВПО

Классификация механизмов распознавания ВПО

Детерминированные

- сигнатурные анализаторы
- инспекторы изменений

Логические

- **Экспертные методы**
  - эвристические анализаторы
    - статические
      - структурные анализаторы
    - динамические
  - поведенческие блокираторы
    - обнаружение злоупотреблений
    - обнаружение аномалий
- **Методы машинного обучения**
  - нейросетевые анализаторы
  - гистограммный подход
  - нейронечеткие анализаторы
  - статистический анализ
  - методы на основе марковских цепей
  - методы на основе скрытых марковских моделей
  - методы на основе формулы Баейса

Сигнатурные анализаторы

Сигнатурный анализатор – это механизм распознавания вредоносных программ, основанный на выделении из анализируемого файла последовательности байт (сигнатуры) однозначно характеризующий конкретную программ с потенциально опасными последствиями (штамм разрушающего программного средства).

Типы сигнатур:

1. Сплошные

Например: **Win95/WinVir-14** = a14001e87201baa801b9ae0290e82f01e85201baa801b9ae

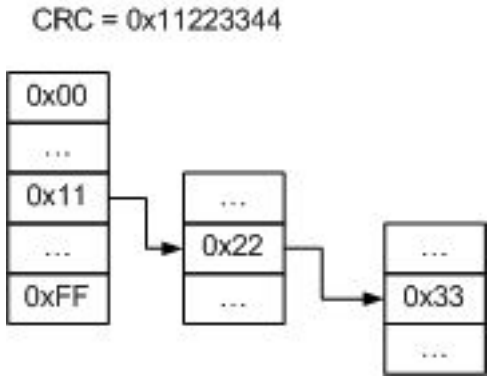
2. Разряженные (регулярные), состоящие из нескольких сплошных сигнатур, между которыми располагается любое или строго определенное количество байт, значения которых могут принимать произвольное значение
Например: **Win32/BJFnt** = EB::3A::::1EEB::CD209CEB::CD20EB::CD2060EB

3. Универсальные (редуцированные маски)

Сигнатурные анализаторы

Подходы к построению алгоритма сигнатурного распознавания вредоносных программ:

1) поиск подстроки, представляющей собой сигнатуру, в файле;
2) поиск по контрольным суммам (все сигнатуры разбиваются на блоки по 8 байт, вычисляются CRC32 этих блоков и строится дерево контрольных сумм, при этом временная сложность поиска равна 1).
3) поиск редуцированных масок



Дерево CRC (временная сложность):

$$S_t = O(1)$$

Достоинства данного подхода:

1) 100 %-е обнаружение известных антивирусному средству штаммов вредоносных программ;
2) высокая скорость анализа файлов.

Недостатки:

1) практически нулевая вероятность распознавания неизвестного вредоносного кода;
2) необходимость своевременного обновления баз данных антивирусного средства.

Редуцированные маски (универсальные сигнатуры)

Основаны на применении **универсального преобразования** данных для кода вредоносной программы, после выполнения которого будет получена сигнатура вируса

Такой подход применяется как вспомогательное средство для **противодействия полиморфным вирусам**

Использование сигнатур для детектирования полиморфных вирусов

Наиболее быстро обнаруживаются полиморфные вирусы, построенные по «классической схеме»:

- Основное тело защифровано с переменным ключом
- Фрагмент расшифровки конструируется таким образом, чтобы его алгоритм в разных экземплярах вируса сохранялся прежним, но конкретные реализации различались

Идея детектирования: **постоянная сигнатура присутствует в момент окончания расшифрования**

Обнаружение на основе: **трассировки или эмуляции кода**

Инспекторы изменений

Инспектор изменений – механизм распознавания разрушающих программных средств, позволяющий определить факт заражения файла по средствам вычисления контрольной суммы и сравнения ее с эталонной контрольной суммой файла.

Достоинства:
1) вероятность обнаружения известных, модифицированных или новых вредоносных программ стремится к 100 %;
2) высокая скорость анализа файлов.

Недостатки:
1) необходимо иметь базу данных эталонных контрольных сумм всех файлов, которую создать практически невозможно;
2) ряд типов файлов подвергаются постоянному изменению (например файлы Microsoft Office) и вычисление их контрольных сумм бессмысленно;
3) база данных инспекторов изменений огромна и составляет сотни тысяч записей (по количеству объектов в ОС).

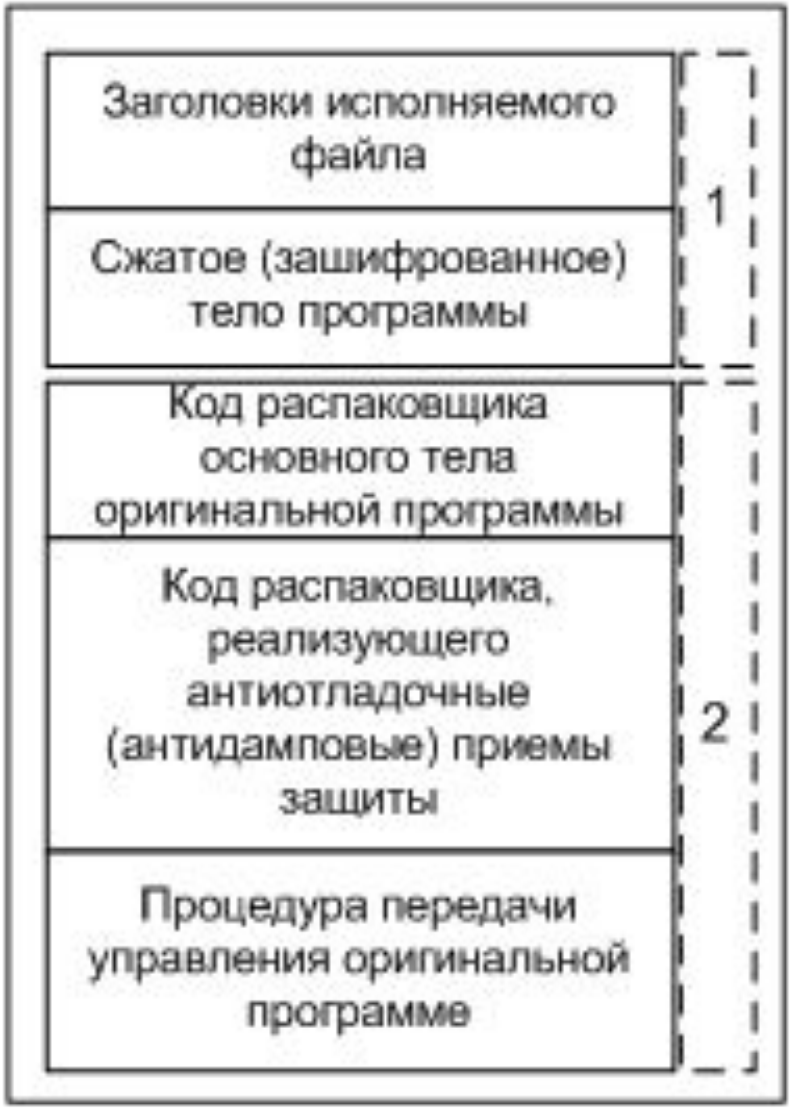
Пример, технология IChecker реализованная в AVP Касперского

Обнаружение упакованного ВПО

Под **упакованным исполняемым файлом** понимается исполняемый файл, прошедший обработку и структурное изменение под воздействием особого вида программ (упаковщиков), для сжатия и затруднения анализа программного кода

Упаковщики

- **сжимающие**, цель которых – устранение избыточности программного кода и соответственно уменьшение размера файла (например, UPX, AsPack, NsPack)
- **протекторы**, дополнительно обладающие механизмами затруднения исследования программы на предмет ее безопасности (например, PeCompact, AsProtect, Yoda, Obsidium, Telock, Armadillo, Orient)



Типовая структура упакованного исполняемого файл

Классификация механизмов распознавания ВПО

Эвристические анализаторы

Эвристический анализатор – это механизм распознавания программ с потенциально опасными последствиями, основанный на выделении косвенных признаков, характерных для вредоносных программ, потенциально опасных последовательностей машинных команд (команд некоторого командного интерпретатора) и событий, возникающих в процессе выполнения этого кода, а также на анализе их на предмет вредоносности.

Типы эвристических анализаторов:

1. **Статические**, основанные на эвристическом анализе исследуемого файла, без его "псевдо" выполнения в безопасной среде;

2. **Динамические**, отличающиеся от статических эвристических анализаторов наличием механизма эмуляции программного кода исследуемой программы.

Примеры косвенных признаков, используемых эвристическими анализаторами

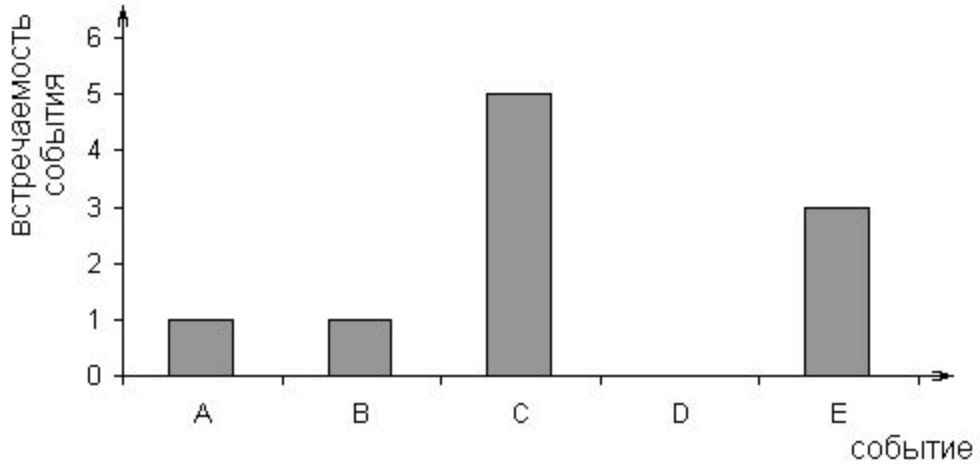
- Наличие «мусорного» (обфусцированного) кода («метаморфные» вирусы)
- Нестандартная структура исполняемого файла
  - несколько секций кода
  - наличие бита разрешения записи в секцию кода
  - «свежая» дата создания у заведомо «несвежего» файла
- Циклы расшифрования кода
- Самомодифицирующийся код («полиморфные» вирусы)
- Использование недокументированных API-вызовов
- Манипуляция векторами прерываний
- Использование нетипичных инструкций, особенно таких, которые не генерируются компиляторами
- Наличие строковых данных с неприличными или выражениями
- Различие между точкой входа исполняемого кода и фактическим размером файла.
- Различие статистики встречаемости байт или инструкций кода между незашифрованным кодом и зашифрованным

Эвристические анализаторы

Для принятия решения используется следующие подходы:

1) гистограммный метод;
2) метод, основанный на поиске эвристических масок;
3) метод, основанный на применении многослойных нейронных сетей.

Гистограммный метод

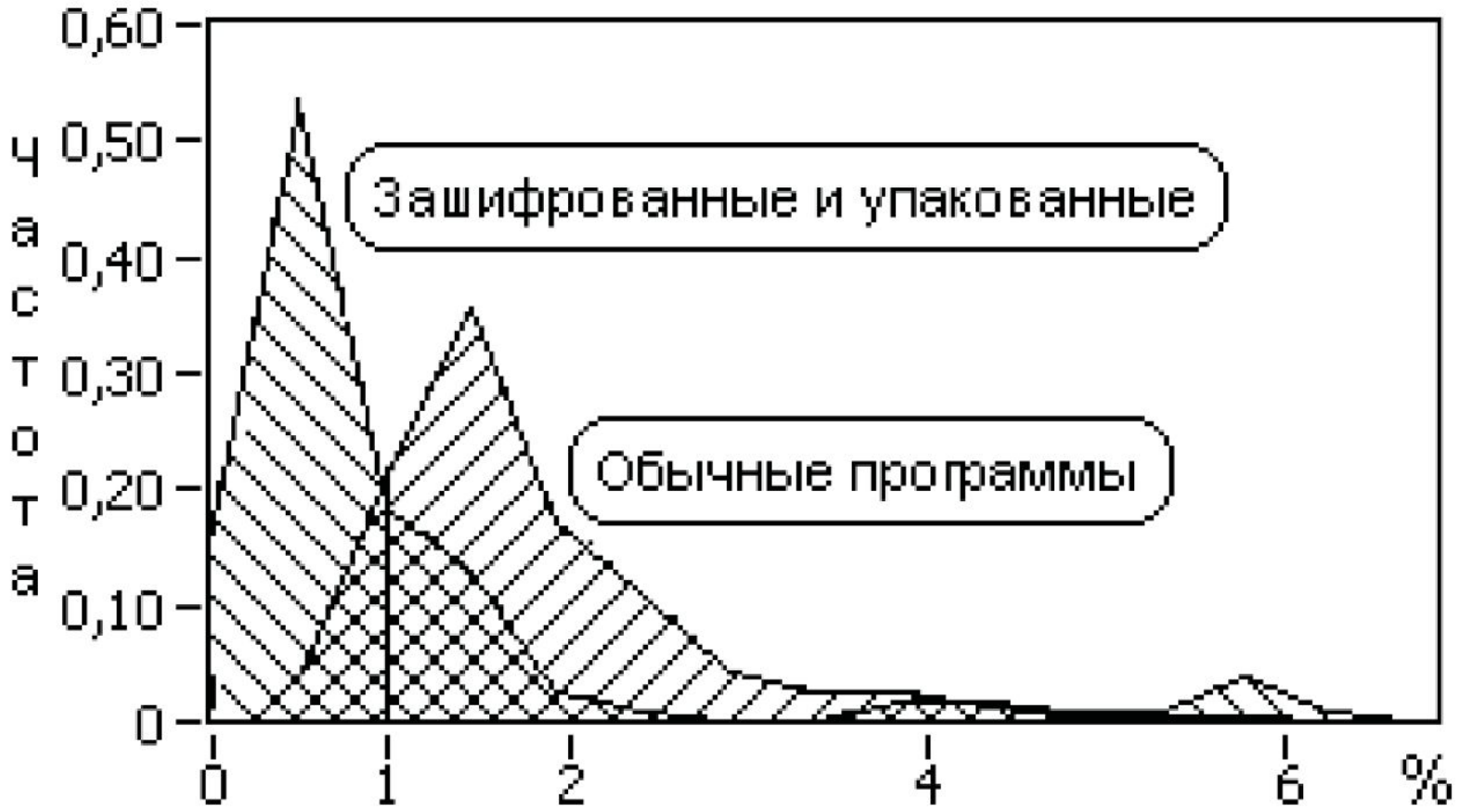


$$\begin{cases} \text{Встречаемость}(A) = 1, \\ \text{Встречаемость}(B) = 1, \\ \text{Встречаемость}(C) > 6, \\ \text{Встречаемость}(D) = 0, \\ \text{Встречаемость}(E) > 2, \end{cases}$$

Например, заражен файл файловым вирусом, если:

1) файл – исполняемый формата PE;
2) точка входа в программу в последнюю секцию;
3) количество секций в файле ≥ 5.
4) первыми инструкциями файла является последовательность

Пример: распределение доли нулевых байтов в упакованном и «обычном» коде



Эвристические анализаторы

Метод, основанный на поиске эвристических масок

Все признаки и события объединяются в цепочки (эвристические маски), подсчитывается число найденных масок и при наступлении определенного числа масок (эвристическое число) принимается решение о наличие вредоносного кода.

Необходимо наличие:

- базы данных моделей ВПО
- алгоритма анализа и принятия решения
- критерия принятия решения о наличии ВПО

Эвристические анализаторы

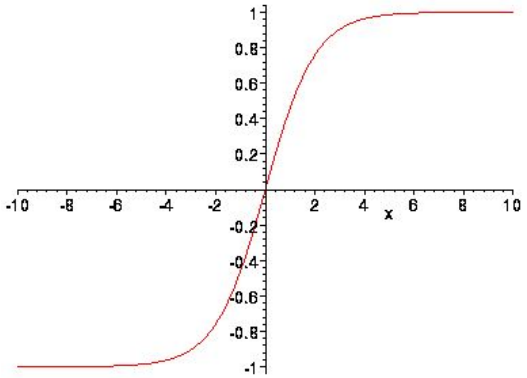
Метод, основанный на многослойных нейронных сетях

Строится многослойная нейронная сеть, на вход сети подаются все признаки и события, выходом которой является решение о наличии или отсутствии вредоносной программы (применяется топология – персептрон с сигмоидальной пороговой функцией, выходом является решение заражен / незаражен)

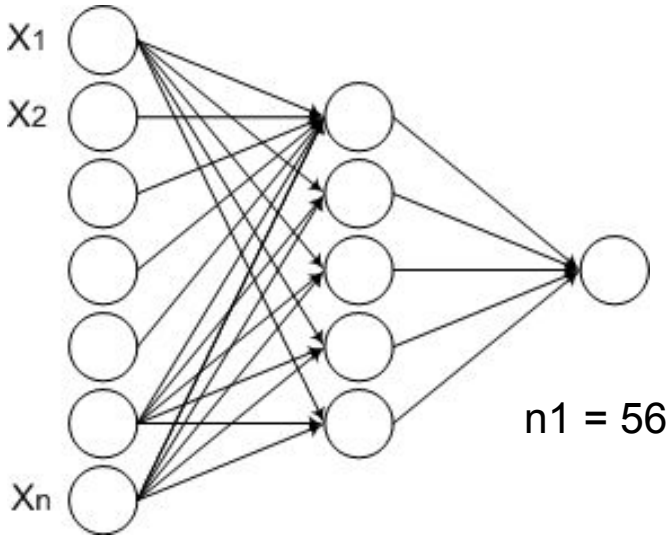
Эвристические анализаторы

Функция активации:

$$f(x) = \frac{1}{1 + e^{-\beta x}}$$



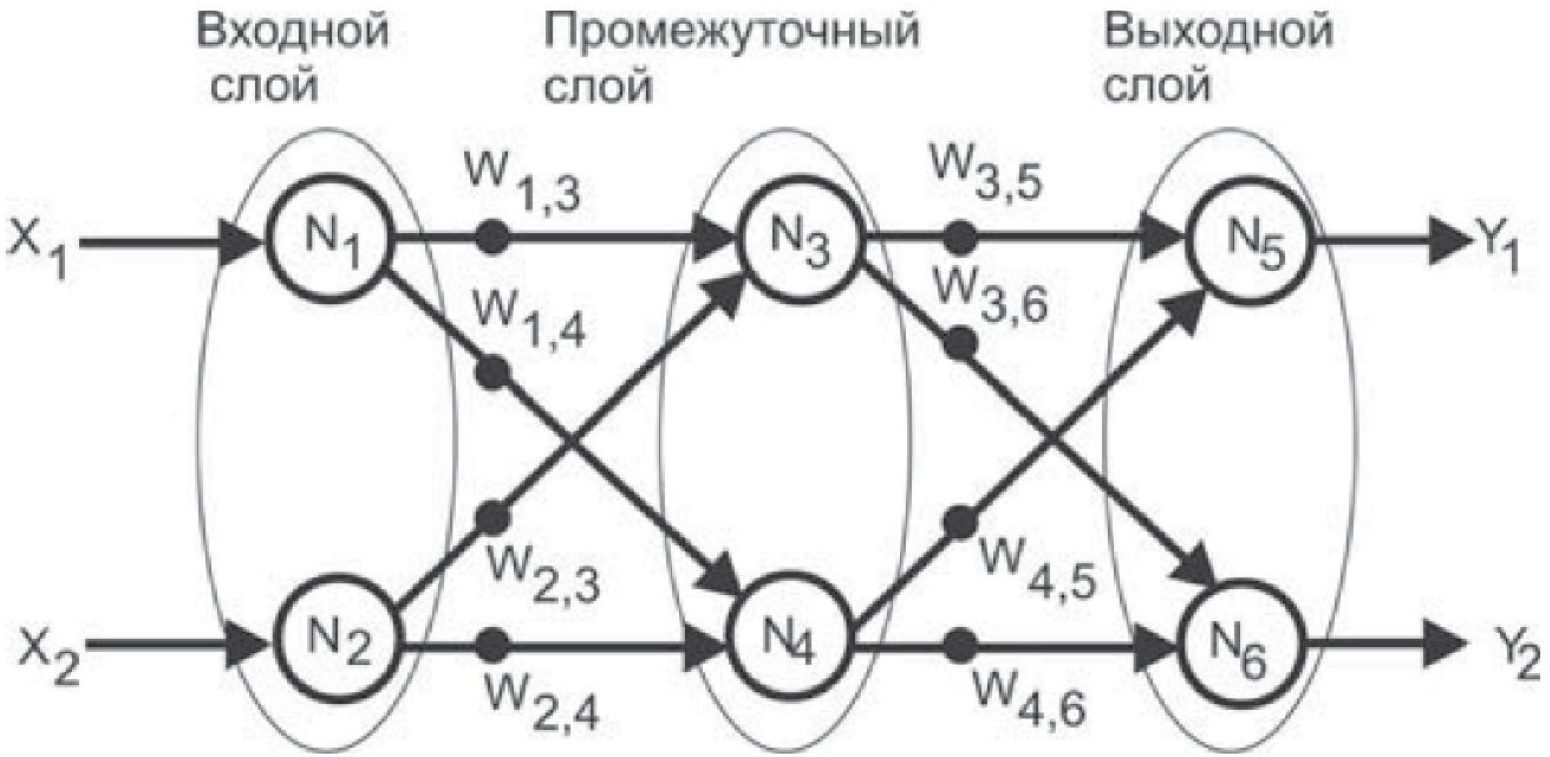
Пример нейронной сети:



n1 = 56 n2 = 17

Обучение: на основе **алгоритма обратного распространения ошибки**

Типичная структура многослойного перцептрона



Эвристические анализаторы

Достоинства эвристических анализаторов:

1. Возможность обнаружения новых или модифицированных вирусов

Недостатки:

1. Значительный уровень ложных срабатываний
2. Не высокая скорость анализа, по сравнению с сигнатурными анализаторами

Поведенческие блокираторы

Антивирусное средство отслеживает внешнее проявление активных в ОС процессов на предмет реализации потенциально опасных операций.

Классы потенциально опасных операций:

1) запуск других приложений;

2) несанкционированное обращение к сети;

3) доступ к адресному пространству других приложений;

4) изменение конфигурации и перенастройка ОС (обращение к реестру, ...)

5) аномальный файловый ввод/вывод.

Достоинства поведенческих блокираторов:

1) возможность обнаружения принципиально новых или модифицированных ВПО

2) Возможность отката потенциально опасных операций в ОС.

Недостатки:

1) вовлечение пользователя в процесс принятие решения;

2) не высокая скорость анализа, по сравнению с сигнатурными анализаторами

Частные показатели эффективности функционирования АВС

Результативность:

1) вероятность ошибки первого рода при распознавании (ложные срабатывания)

Значение $P_{ош.1} \leq 0{,}0005$;

2) вероятность ошибки второго рода при распознавании (пропуск цели)

Для логических методов значение $P_{ош.2} \leq 0{,}03$.

Оперативность:

3) время анализа объектов на предмет наличия в них потенциально опасного кода;

Ресурсоемкость:

4) объем оперативной памяти необходимой для анализа объектов

5) объем внешней памяти необходимый для хранения БД АВС

Выводы по первому учебному вопросу

1. Сигнатурный механизм распознавания ВПО является детерминированным и позволяет со 100% выявлять известные ВПО, однако не способен выявлять неизвестные
2. БД сигнатурных анализаторов необходимо поддерживать в актуальном состоянии
3. Инспекторы изменений эффективно выявляют изменения в ПО, независимо от того известным или неизвестным ВПО они были внесены, однако их применение имеет много ограничений
4. Важную роль в защите КС от ВПО играют вероятностные алгоритмы распознавания, позволяющие выявлять модифицированные штаммы
5. Несмотря на вовлечение пользователя в процесс принятия решения в проактивных анализаторах данный механизм играет исключительную роль позволяя выявлять новые вредоносные программы

ВОПРОС 2

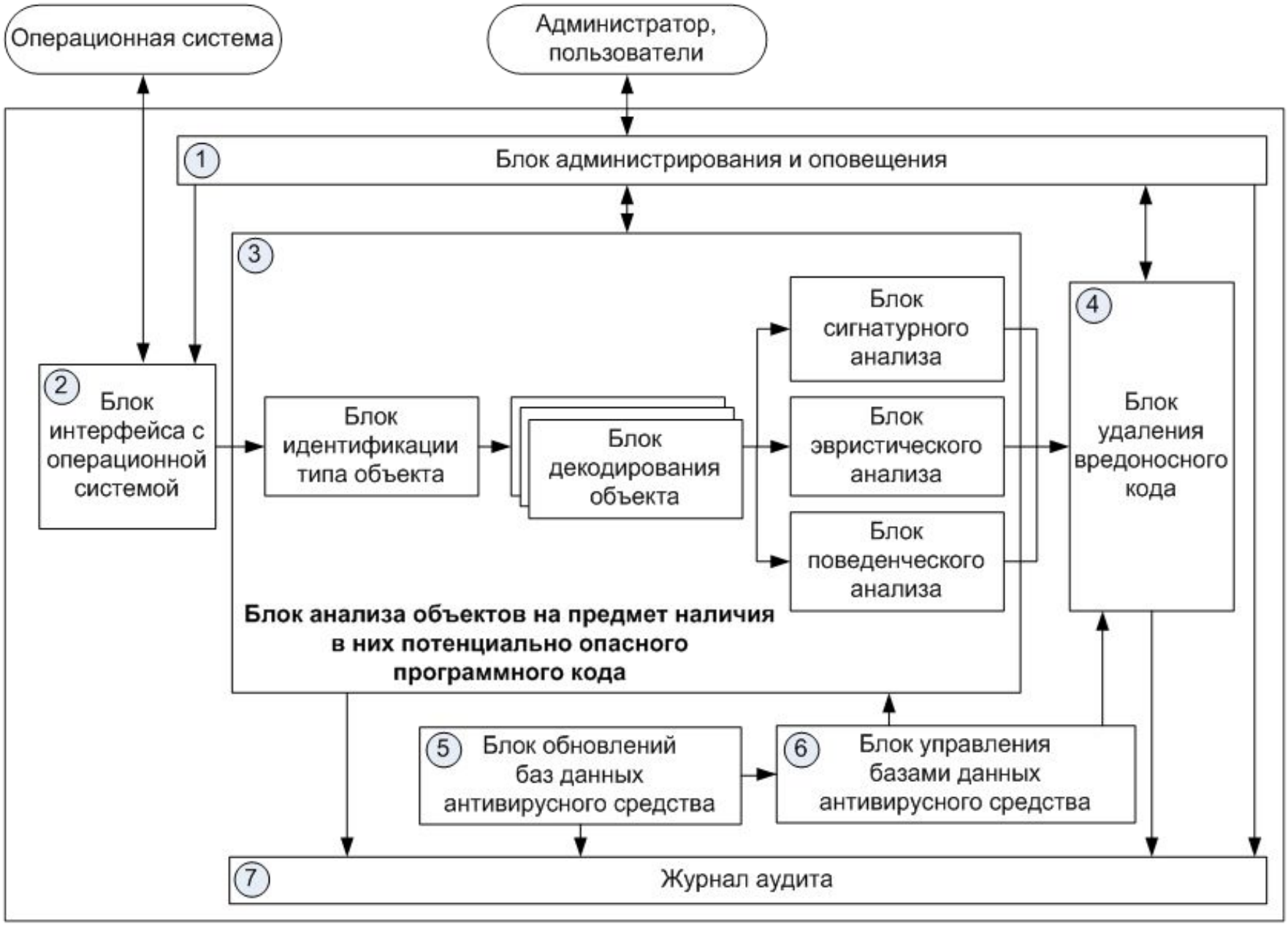
Архитектура средств антивирусной защиты

Подходы к построению антивирусных средств

1) Локальное АВС – это АВС, функционирующие на одной, выделенной ЭВМ, причем управление средством осуществляется локально

2) Распределенное АВС – это АВС, построенное по технологии "агент–менеджер" и включающее в себя единый центр администрирования (менеджер АВС) и одного или нескольких агентов, расположенных на отдельных ЭВМ вычислительной сети

Архитектура локальных АВС



Этапы анализа объектов на предмет их заражения

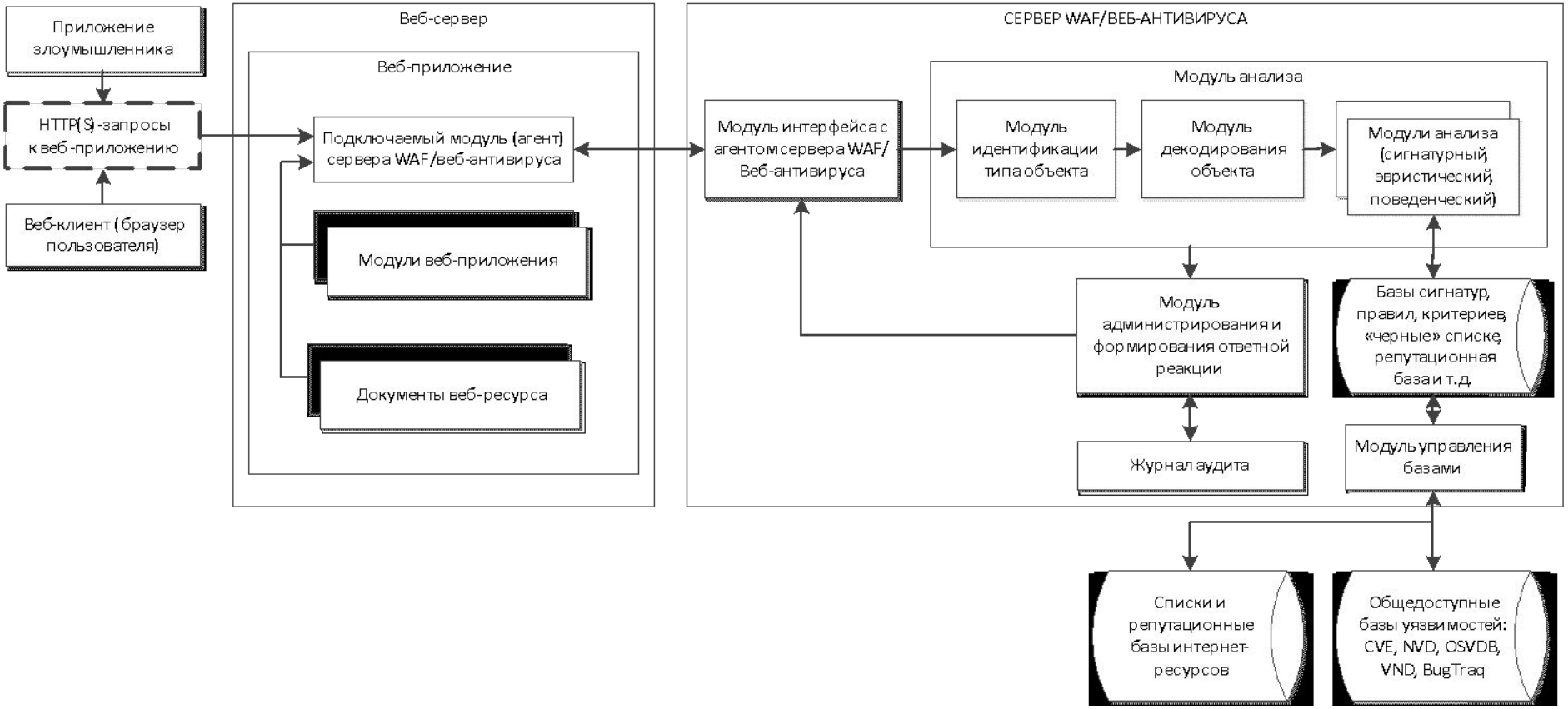
1. На вход блока идентификации типа объекта поступает некоторый объект, подлежащий отнесению его к некоторому классу

2. В зависимости от типа объекта антивирусное средство производит его декодирование в вид, приемлемый для дальнейшего анализа

3. Декодированный объект поступает в блоки анализа объекта на предмет наличия в нем вредоносного кода. Анализ заключается в выделении наиболее значимых признаков, характеризующих данный объект, и сравнении полученных признаков с эталонными значениями

Архитектура распределенных АВС

Пример архитектуры системы защиты на основе веб-антивирусов и технологий Web Application Firewall (WAF)



Требования к антивирусным средствам (ФСТЭК)

Приказ ФСТЭК России от 20 марта 2012 г. № 28

Класс защиты / Тип средства антивирусной защиты	6	5	4	3	2	1
тип «А»	ИТ.САВЗ.А6.ПЗ	ИТ.САВЗ.А5.ПЗ	ИТ.САВЗ.А4.ПЗ	ИТ.САВЗ.А3.ПЗ	ИТ.САВЗ.А2.ПЗ	ИТ.САВЗ.А1.ПЗ
тип «Б»	ИТ.САВЗ.Б6.ПЗ	ИТ.САВЗ.Б5.ПЗ	ИТ.САВЗ.Б4.ПЗ	ИТ.САВЗ.Б3.ПЗ	ИТ.САВЗ.Б2.ПЗ	ИТ.САВЗ.Б1.ПЗ
тип «В»	ИТ.САВЗ.В6.ПЗ	ИТ.САВЗ.В5.ПЗ	ИТ.САВЗ.В4.ПЗ	ИТ.САВЗ.В3.ПЗ	ИТ.САВЗ.В2.ПЗ	ИТ.САВЗ.В1.ПЗ
тип «Г»	ИТ.САВЗ.Г6.ПЗ	ИТ.САВЗ.Г5.ПЗ	ИТ.САВЗ.Г4.ПЗ	ИТ.САВЗ.Г3.ПЗ	ИТ.САВЗ.Г2.ПЗ	ИТ.САВЗ.Г1.ПЗ

тип «А» –предназначены для централизованного администрирования средствами антивирусной защиты.

тип «Б» – предназначены для применения на серверах информационных систем

тип «В» –предназначены для применения на АРМ информационных систем

тип «Г» – предназначенныедля применения на автономных АРМ

Частные показатели эффективности функционирования АВС

1. Вероятность ошибки первого рода при распознавании (α-ошибки) (ложные срабатывания);
2. Вероятность ошибки второго рода при распознавании (β-ошибки) (пропуск цели).
3. Время анализа объектов на предмет наличия в них потенциально опасного кода.
4. Объем оперативной памяти необходимой для анализа объектов.
5. Объем внешней памяти необходимый для хранения БД АВС.

Приказ директора ФСБ России:
«Выписка из требований к антивирусным средствам»

		Вирус существует?	
		Да	Нет
Вирус обнаружен?	Да	Верно	α-ошибка (1-го рода) Ложное срабатывание (False positive)
	Нет	β-ошибка (2-го рода) Пропуск цели (False negative)	Верно

Российский рынок антивирусного программного обеспечения

Антивирусные программы	Обнаружение	Динамика	Веб-защита	Самозащита	Ложные	Оценка
Qihoo 360 Internet Security 2014	98.1%	100%	100%	50%	3	9.2
BullGuard Internet Security 2014	97.0%	75%	100%	100%	0	9.2
Kaspersky Internet Security 2014	92.4%	87.5%	86.7%	100%	0	9.1
G Data InternetSecurity 2014	98.0%	87.5%	100%	50%	1	9.0
Emsisoft Internet Security Pack 8	97.3%	100%	73.3%	50%	0	8.9
F-Secure Internet Security 2014	97.1%	87.5%	93.3%	50%	0	8.9
Bitdefender Antivirus Free Edition	96.7%	75%	100%	50%	0	8.7
McAfee Internet Security 2014	98.2%	75%	73.3%	100%	2	8.5
Norton Internet Security 2014	96.2%	62.5%	73.3%	100%	1	8.2
Bitdefender Internet Security 2014	96.6%	75%	100%	0%	0	8.2
avast! Internet Security 2014	91.9%	50%	80%	100%	0	7.9
TrustPort Internet Security 2014	98.1%	87.5%	60%	0%	0	7.8
Ad-Aware PRO Security 11	96.1%	62.5%	93.3%	0%	0	7.6
Avira Internet Security Suite 2014	96.1%	75%	46.7%	50%	1	7.5
Comodo Internet Security Premium 6.3	90.8%	100%	20%	50%	4	7.3
ESET NOD32 Smart Security 7	95.2%	37.5%	86.7%	50%	0	7.2
Avira Free Antivirus 2014	96.1%	75%	26.7%	50%	0	7.2
Ashampoo Anti-Virus 2014	97.2%	62.5%	66.7%	0%	1	7.1
Trend Micro Titanium Internet Security	92.6%	50%	100%	0%	2	7.1

Др. произв 1%

1%

Выводы по второму учебному вопросу

1) Центральным элементом любого АВС является блок анализа объектов на предмет наличия в них потенциально опасного кода, данный блок и в большей степени определяет эффективность АВС

2) Распределенные АВС позволяют производить централизованное управление всеми АВС вычислительной системы

Выводы по занятию

1. Антивирусные средства являются одним из основным способом противодействия ВПО, однако эффективность их не 100% и об этом необходимо помнить.

2. При организации защиты от ВПО в подразделениях необходимо применять *различные* методы в том числе АВС, межсетевые экраны (системы обнаружения атак) в сочетании с грамотной политикой безопасности.

ВОПРОСЫ ПО ЗАНЯТИЮ?

ЗАДАНИЕ НА САМОСТОЯТЕЛЬНУЮ ПОДГОТОВКУ

1. Доработать конспект занятия
2. Изучить рекомендованную литературу

Тема 3. Защита от вредоносного программного обеспечения

Занятие 3/2. Групповое занятие

Тема:

Защита от вредоносного программного обеспечения

Учебные вопросы:

1. Классификация методов и средств обнаружения вредоносного программного обеспечения
2. Архитектура средств обнаружения вредоносного программного обеспечения