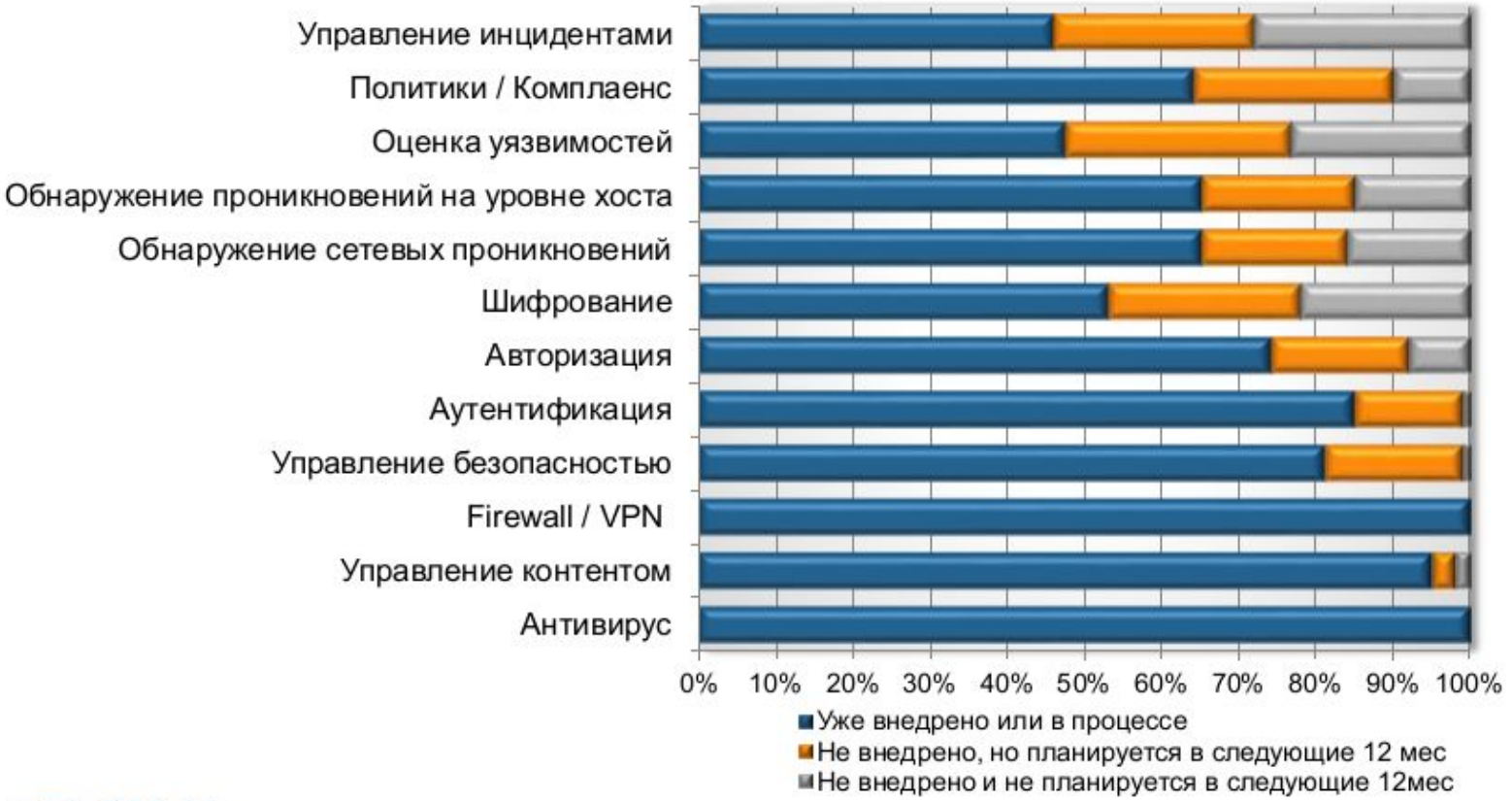
Антивирусная защита государственных информационных систем

Защита от вредоносных программ и интернет-угроз.

Истоки, принципы применения и требования.

Результаты опроса операторов информационных систем

В каком состоянии находится внедрение следующих програмных решений ИБ в вашей организации?



Источник: IDC CEMA Security Roadshow 2014 Attendee Survey

Защита от вредоносных программ и интернет-угроз в ГИС

Содержание:

- Терминология
- Правовые основания антивирусной защиты ГИС
- Эволюция вредоносных программ
- Виды вредоносных программ
- Виды интернет-угроз
- Технологии реактивной и проактивной защиты
- Эволюция антивирусных средств
- Требования к антивирусной защите

Компьютерный вирус

Компьютерный вирус

– компьютерная программа или код, отличительной особенностью которых является способность к созданию своих копий (саморепликация).

Вредоносная программа

Вредоносная программа – программа, используемая для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

ГОСТ Р 51275-2006

Вредоносная программа

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

ГОСТ Р 50922-2006

ГОСТ Р 53113.1-2008

Данные

Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека

ГОСТ 15971-90

Информация, представленная в формализованном виде, пригодном для передачи, интерпретации или обработки с участием человека или автоматическими средствами

ГОСТ 34.321-96

Вредоносная программа

Вредоносная (компьютерная) программа – программа, предназначенная для осуществления несанкционированного доступа к данным или средствам информационной системы или для несанкционированного воздействия на них

Правовые основания защиты от вредоносных программ и интернет-угроз

- Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и защите информации»
- Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»

Нормативные основания защиты от вредоносных программ и интернет-угроз

- «Требования о защите информации, не составляющими государственную тайну, содержащейся в государственных информационных системах»

  (утверждены приказом ФСТЭК от 11 февраля 2013 г. № 17)

- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

  (утверждены приказом ФСТЭК от 18 февраля 2013 г. № 21)

Защита от вредоносных программ и интернет-угроз

Защита информационной системы от вредоносных программ и интернет-угроз

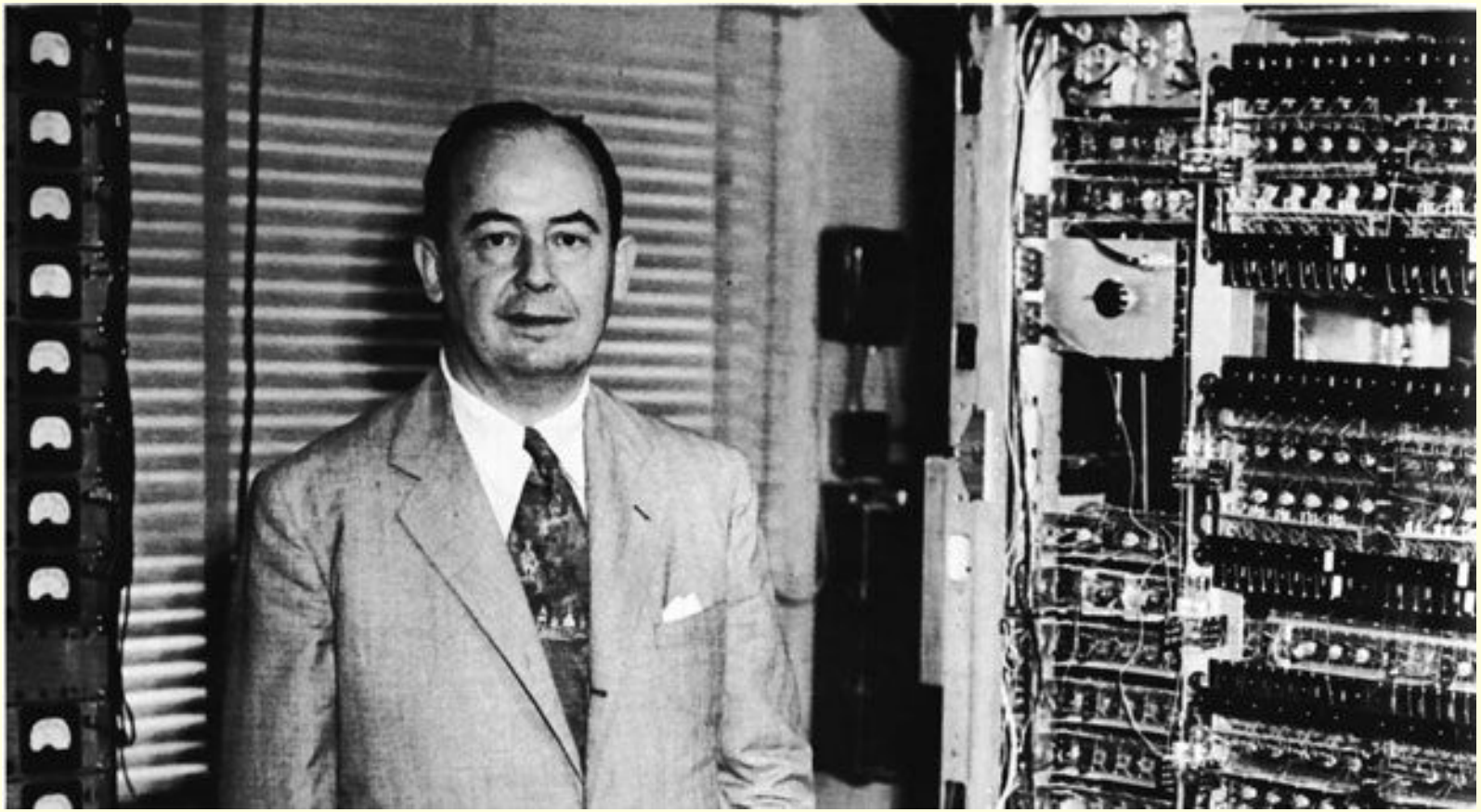
– комплекс организационных и технических (программно и аппаратно реализуемых) мероприятий по защите ресурсов автоматизированной информационной системы от воздействия вредоносных программ и интернет-угроз.

Антивирусная защита

Антивирусная защита

– комплекс организационных и технических (программно и аппаратно реализуемых) мероприятий по защите ресурсов автоматизированной информационной системы от воздействия вредоносных программ.

Истоки



Джон фон Нейманн

Вредоносные программы

- **BIOS-киты** (BIOS-kits)
- **Клавиатурные перехватчики** (Keyloggers)
- **Люки** (Backdoors)
- **Логические бомбы** (Logic bombs), в т.ч. **бомбы с часовым механизмом** (Time bombs)
- **Бэкдоры** (Backdoors**)**
- **Зомби** (Zombies)
- **Буткиты** (Boot viruses)
- **Руткиты** (Rootkits)
- **Троянские кони** (Троянцы) (Trojan Horses)
- **Программы-блокеры**

Интернет-угрозы

- **Подбор пароля** (Brute force attacks).
- **Перегрузка системы** (DoS-attacks)
- **Пассивное прослушивание сети** (Sniffing)
- **Перенаправление на ложный адрес** (Pharming)
- **Имитация соединения** (Spoofing), в т.ч. **DNS-заражение** (DNS poisoning)
- **«Выуживание» пароля и логина** (Phishing), в т.ч с использованием телефона (Vishing)
- **Искажение веб-страниц** (Defacement)
- **Хищение информации, используемой в системе интернет-банкинга**

Истоки

Дмитрий Лодзинский

Истоки

Евгений Касперский

Проактивные технологии защиты

- **Эвристический анализ**
- **Анализ поведения**
- **Виртуализация**
  - **эмуляция кода**
  - **ограничение привилегий выполнения (песочница)**
  - **виртуализация рабочего окружения**

Истоки

Игорь Данилов

Цель защиты от вредоносных программ

Минимизация ущерба от воздействия вредоносных программ

Задачи защиты от вредоносных программ

- Сохранение целостности данных
- Обеспечение доступности данных
- Исключение утечки сведений ограниченного доступа
- Эффективное использование вычислительных ресурсов

Принципы применения средств защиты от вредоносных программ

- Безопасность

  Должно исключаться наличие недокументированных возможностей антивирусного продукта, позволяющих (или предназначенных) выполнять деструктивные действия на средствах пользователя.

Принципы применения средств защиты от вредоносных программ

- Безопасность
- Правомочность

Для обеспечения антивирусной защиты данных допускается применение только лицензированных или свободно распространяемых программных антивирусных средств.

Принципы применения средств защиты от вредоносных программ

- Безопасность
- Правомочность
- Эффективность

Антивирусная защита информации должна давать положительный результат (по крайней мере обоснованную уверенность в нем), соизмеримый с затратами ресурсов на её реализацию.

Требования к качествам защиты от вредоносных программ

- Надёжность

– устойчивость к попыткам преодоления. Компоненты системы антивирусной защиты должны быть устойчивы к попыткам деструктивного воздействия на неё.

Требования к качествам защиты от вредоносных программ

- Надёжность
- Непрерывность

– постоянность обеспечения защитных процессов во времени и в пространстве.

Требования к качествам защиты от вредоносных программ

- Надёжность
- Непрерывность
- Своевременность (оперативность)

– обнаружение вредоносных программ в реальном времени, до их активизации или на самых ранних этапах активности

Требования к качествам защиты от вредоносных программ

- Надёжность
- Непрерывность
- Своевременность (оперативность)
- Достаточность

– обеспечение необходимого и достаточного уровня безопасности данных

Требования к качествам защиты от вредоносных программ

- Надёжность
- Непрерывность
- Своевременность (оперативность)
- Достаточность
- Адаптивность (гибкость)

– приспособляемость защиты к новым условиям без внесения кардинальных изменений

Требования к функциональности антивирусной защиты стр.1

Антивирусная защита должна обеспечивать:

- устойчивое и бесконфликтное функционирование;
- удобство инсталляции и настройки антивирусного программного обеспечения;
- высокую степень надёжности обнаружения вредоносных программ;
- проверку записываемых и читаемых файлов в режиме реального времени;
- сканирование памяти и содержимого дисков по расписанию;
- выборочное сканирование файлов и областей диска;
- проверку архивов;
- проверку трафика передаваемого по различным протоколам;

Требования к функциональности антивирусной защиты стр.2

Антивирусная защита должна обеспечивать:

- распознавать ситуации, характерные для действий вредоносных программ;
- выявление потенциально опасных кодов;
- автоматическое обновление вирусных баз данных;
- возможность удалённой установки и администрирование антивирусных программ с консоли системного администратора;
- проверку подключённых к ЛВС компьютеров, инициируемую администратором;
- возможность оповещения администратора о критических событиях, связанных с атаками;
- протоколирование событий, касающихся антивирусной защиты;
- выявление уязвимости программного обеспечения информационной системы;
- блокирование доступа к нежелательным интернет-ресурсам

Уважаемые коллеги!
Не пренебрегайте правилами и мерами обеспечения безопасности данных АИС!

Ступаков В.А.
заместитель начальника отдела
информационной безопасности