Оценка эффективности

программы повышения осведомленности в области ИБ

При проведении программы повышения осведомленности необходимо:

- **Определить направление**
  - чего мы хотим достигнуть?
- **Определить текущее состояние**
  - как обстоят дела на настоящий момент?
- **Реализовать программу**
- **Оценить эффективность**
  - что изменилось за время проведения работ?

Базируется на политиках безопасности

- Пароль должен состоять из цифр, букв…
- Запрещается использовать корпоративный пароль на внешних сайтах
- Запрещается копировать конфиденциальные документы на внешние носители информации
- Беспроводные интерфейсы должны отключаться, когда они не используются
- Запрещается запускать исполняемые файлы, полученные по электронной почте

…

Определить текущее состояние

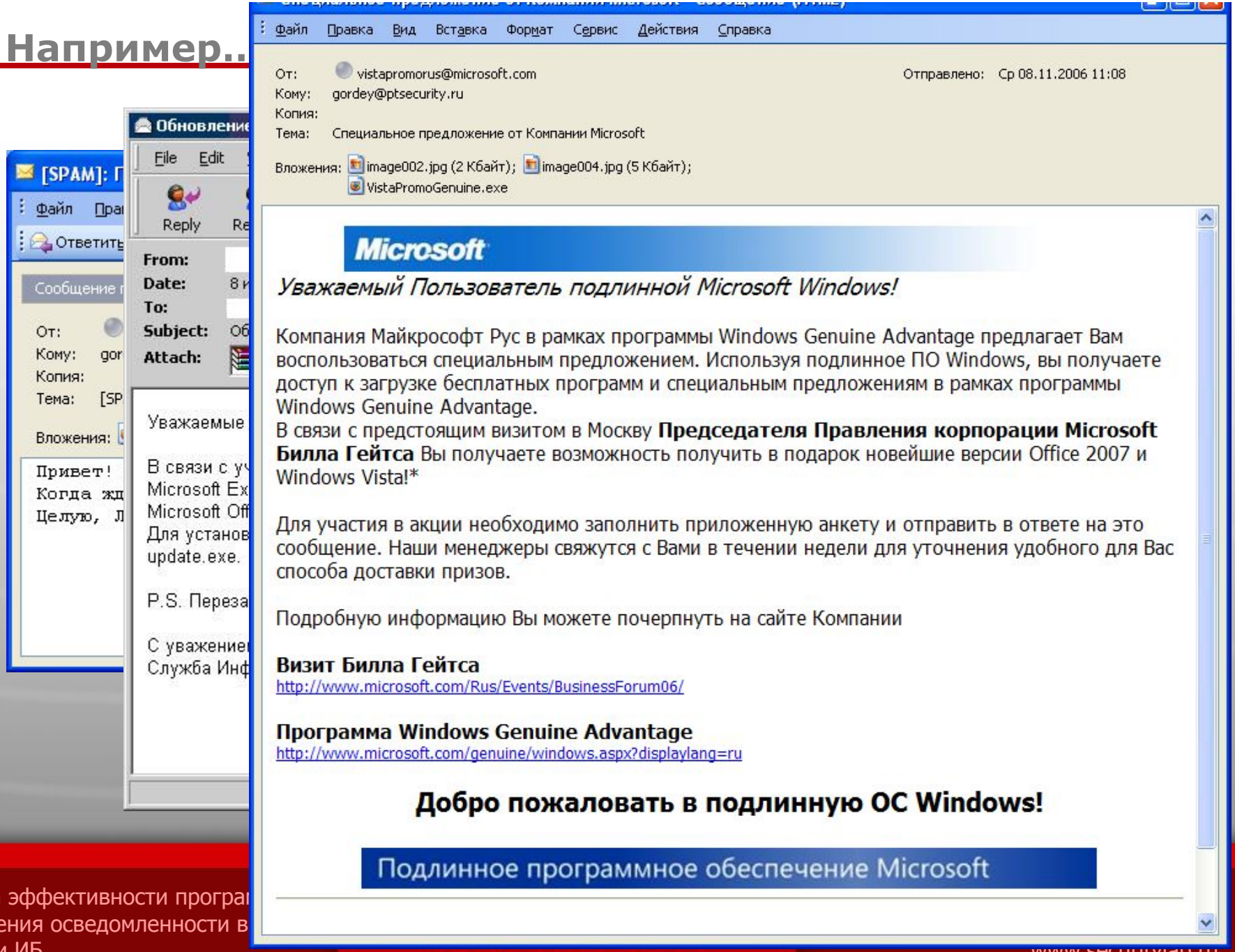
Например, программа направлена на снижение таких рисков, как:

- Распространение сетевых червей
- Заражение системы троянской программой
- Атаки типа «фишинг»
- И
- И

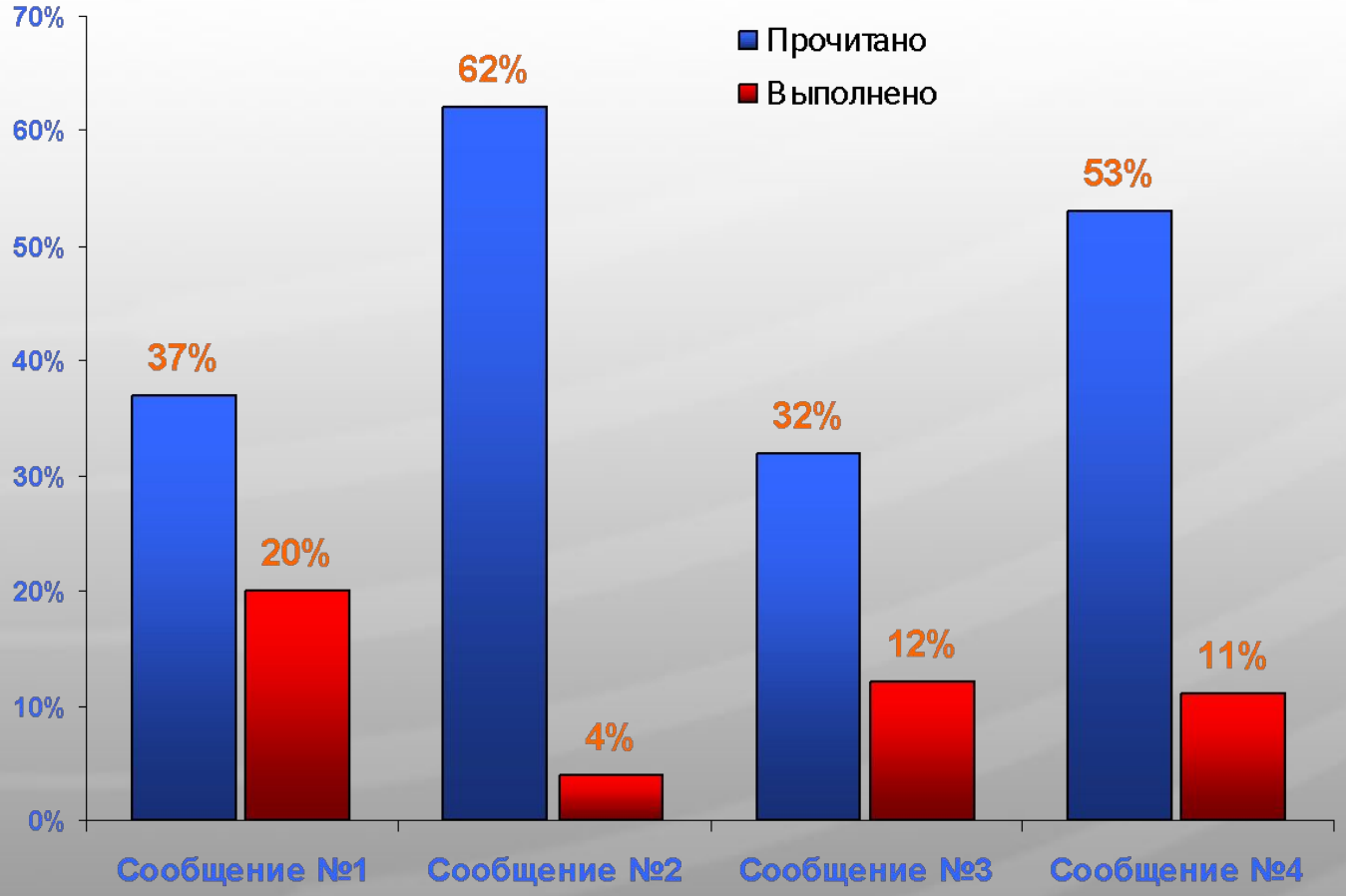
Испо
масс
хаке

Описание сообщения	Эмулируемая атака
Почтовое сообщение личного содержания, направленное третьему лицу, с приложенным исполняемым файлом.	Распространение сетевых червей Целевое заражение системы троянской программой
Сообщение от внешнего лица, пользующегося определенным авторитетом, содержащее приложенный исполняемый файл.	Распространение сетевых червей Целевое заражение системы троянской программой
Сообщение от сотрудника Заказчика, содержащее ссылку на внешний Web-сайт. Ссылка указывает на исполняемый файл.	Целевое заражение системы троянской программой
Сообщение от внешнего лица, содержащее ссылку на Web-сайт. Ссылка указывает на Web-страницу, содержащую форму ввода персональных данных.	Атаки типа «фишинг», сбор персональных данных

Например..

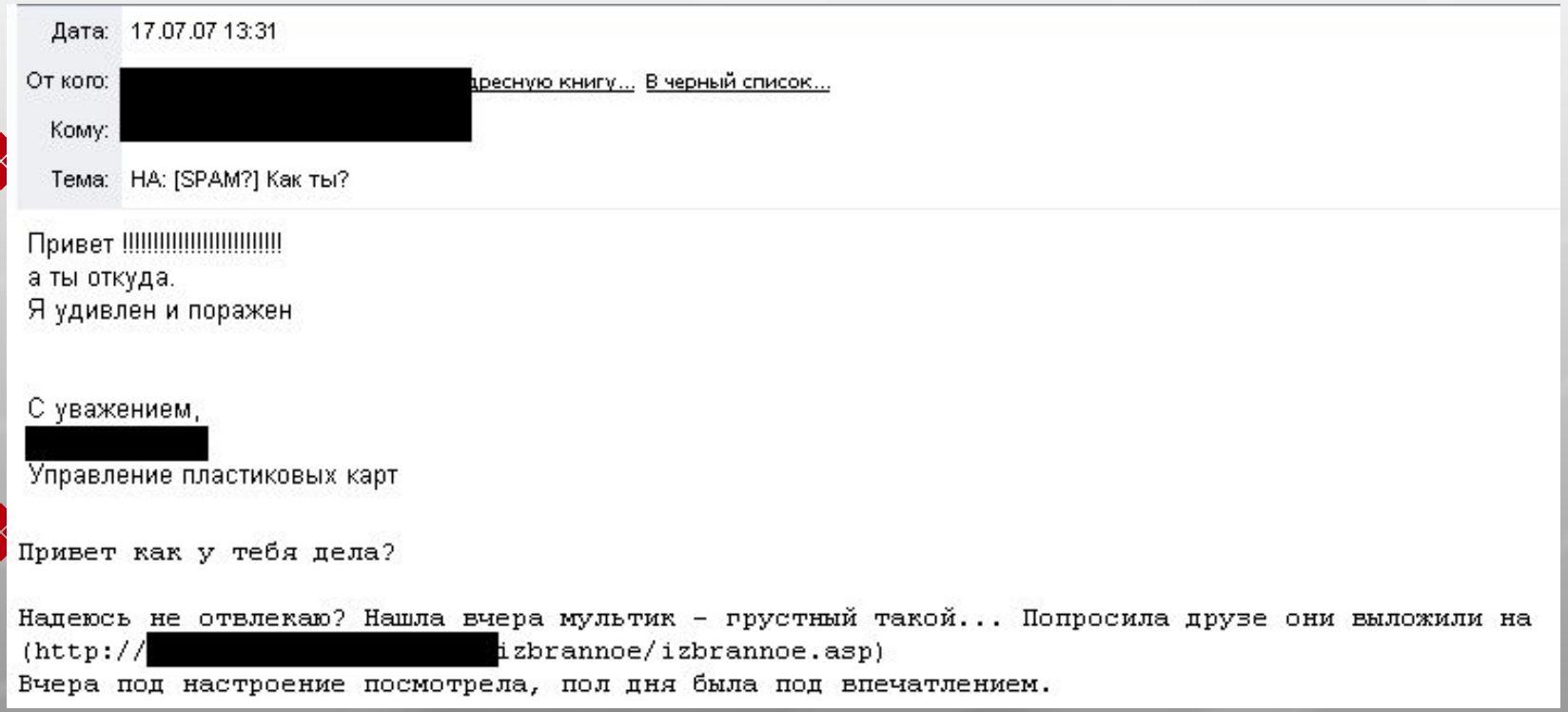

Файл Правка Вид Вставка Формат Сервис Действия Справка
От: vistapromorus@microsoft.com
Отправлено: Ср 08.11.2006 11:08
Кому: gordey@ptsecurity.ru
Копия:
Тема: Специальное предложение от Компании Microsoft
Вложения: image002.jpg (2 Кбайт); image004.jpg (5 Кбайт); VistaPromoGenuine.exe
Microsoft
Уважаемый Пользователь подлинной Microsoft Windows!
Компания Майкрософт Рус в рамках программы Windows Genuine Advantage предлагает Вам воспользоваться специальным предложением. Используя подлинное ПО Windows, вы получаете доступ к загрузке бесплатных программ и специальным предложениям в рамках программы Windows Genuine Advantage.
В связи с предстоящим визитом в Москву Председателя Правления корпорации Microsoft Билла Гейтса Вы получаете возможность получить в подарок новейшие версии Office 2007 и Windows Vista!*
Для участия в акции необходимо заполнить приложенную анкету и отправить в ответе на это сообщение. Наши менеджеры свяжутся с Вами в течении недели для уточнения удобного для Вас способа доставки призов.
Подробную информацию Вы можете почерпнуть на сайте Компании
Визит Билла Гейтса
http://www.microsoft.com/Rus/Events/BusinessForum06/
Программа Windows Genuine Advantage
http://www.microsoft.com/genuine/windows.aspx?displaylang=ru
Добро пожаловать в подлинную ОС Windows!
Подлинное программное обеспечение Microsoft
Обновление
File Edit
Reply
From:
Date:
To:
Subject:
Attach:
Уважаемые
В связи с
Microsoft Ex
Microsoft Off
Для установ
update.exe.
P.S. Переза
С уважение
Служба Инф
[SPAM]:
Файл
Ответить
От:
Кому:
Копия:
Тема:
Вложения:
Привет!
Когда жд
Целую, Л

Сводная статистика



Кто и как отреагировал на сообщение

- Вступил в переписку



Дата: 17.07.07 13:31

От кого: [redacted] адресную книгу... В черный список...

Кому: [redacted]

Тема: НА: [SPAM?] Как ты?

Привет !!!!!!!!!!!!!!!!!!!!!!!!

а ты откуда.

Я удивлен и поражен

С уважением,

[redacted]

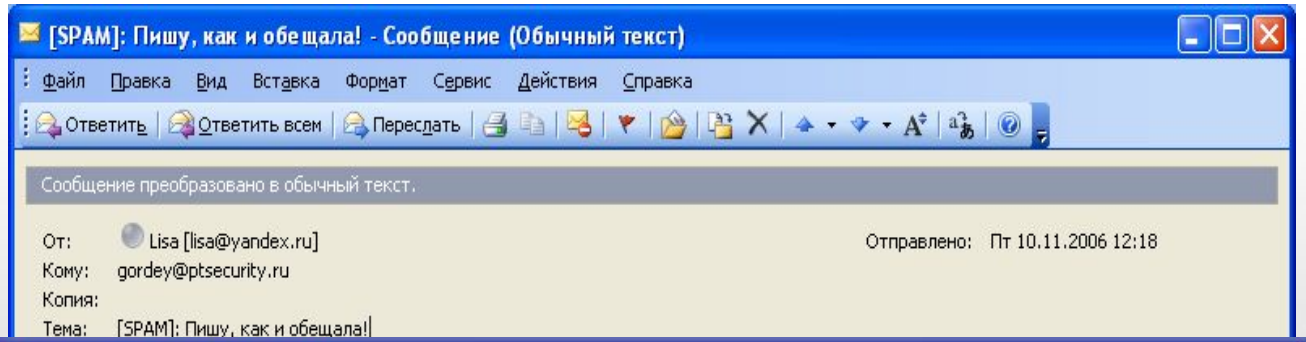
Управление пластиковых карт

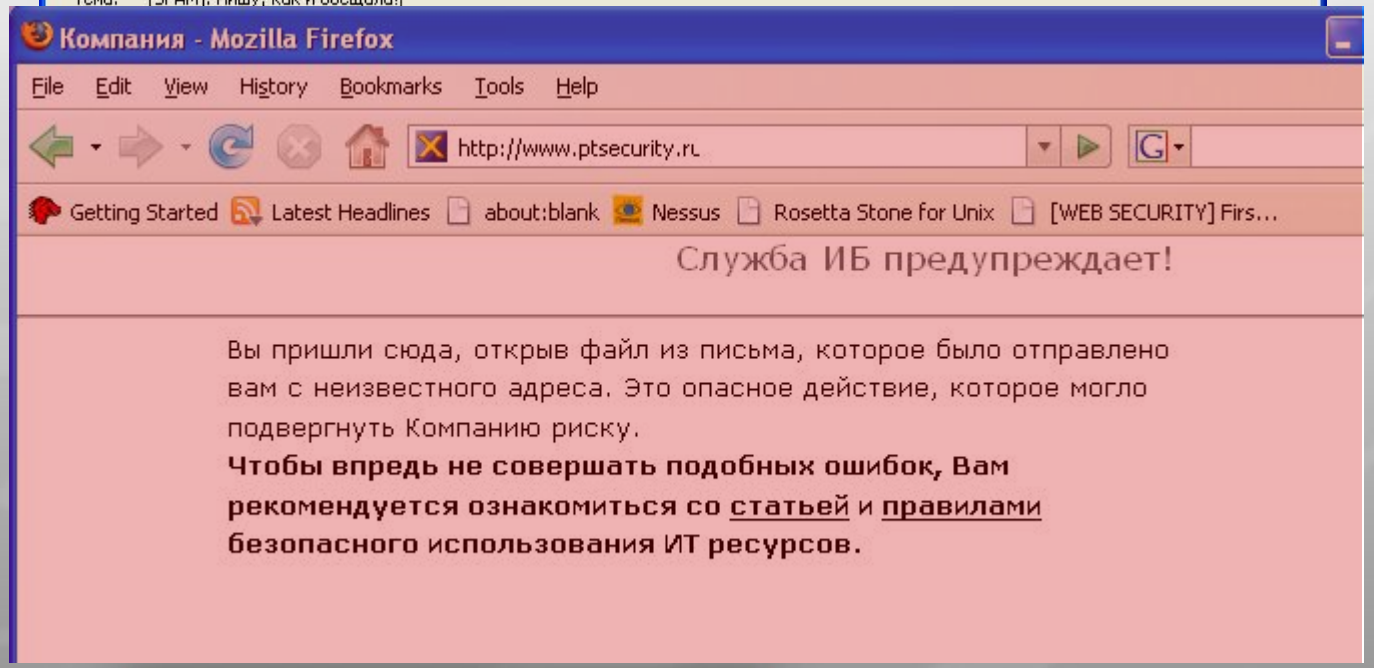
Привет как у тебя дела?

Надеюсь не отвлекаю? Нашла вчера мультик - грустный такой... Попросила друзе они выложили на (http://[redacted]izbrannoe/izbrannoe.asp)

Вчера под настроение посмотрела, пол дня была под впечатлением.

Совмещение «оценки» с «повышением»





Резюме

- **Планируя программу повышения осведомленности необходимо учитывать работы по оценке эффективности**
- **Для каждого из направлений Программы вырабатываются свои критерии и методы оценки эффективности**
  - Например, проведение серии согласованных атак, и отслеживание реакции пользователей на них
- **Появляется возможность использовать простые количественные критерии эффективности (BSC/KPI)**
- **Результаты оценки эффективности может использоваться как действенный механизм повышения осведомленности**
  - *А безопасники у нас суровые. Вон, Петр Иванович в прошлом месяце какое-то не то письмо открыл, так его фотку на доске позора, как пособника шпионов повесили. Так что ты того, аккуратней…*

Вопросы

Positive Technologies
+7 495 744 01 44
pt@ptsecurity.ru