

Оценка эффективности программы повышения осведомленности в области ИБ



POSITIVE / TECHNOLOGIES®

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

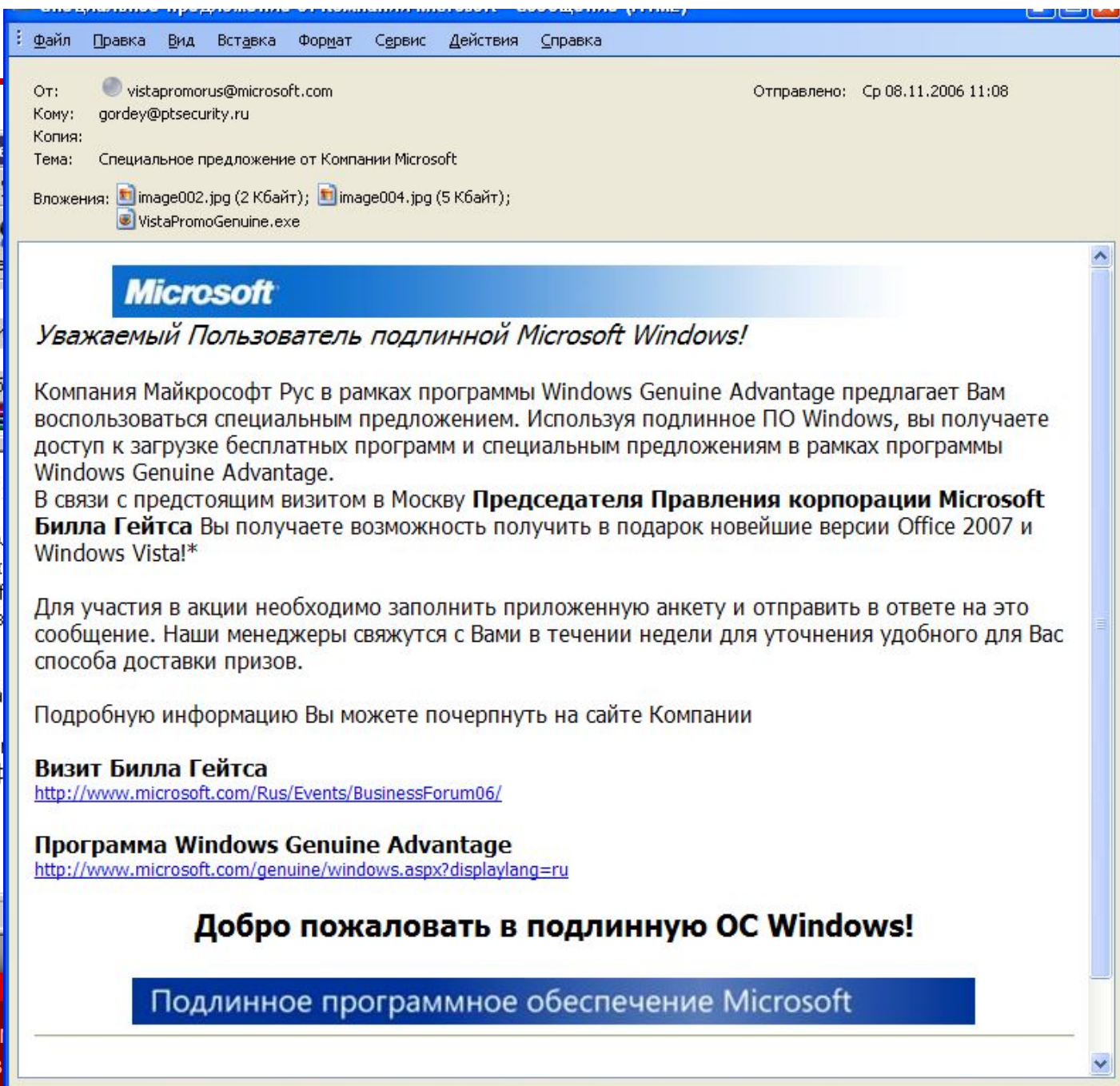
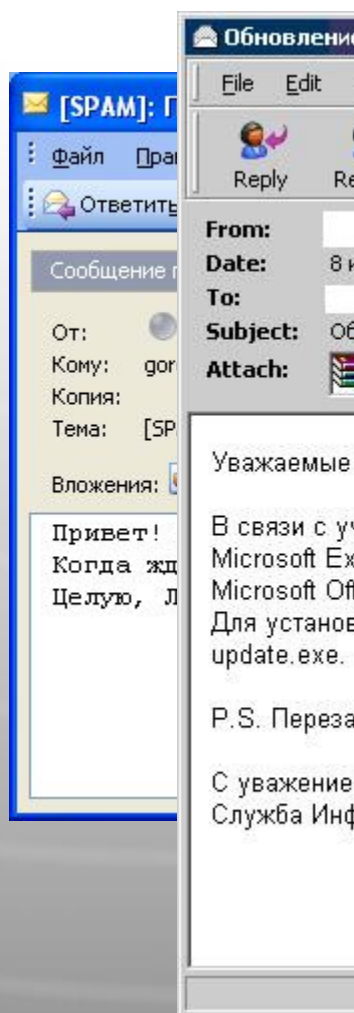
Например, программа направлена на снижение таких рисков, как:

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

Использование массовых хакерских инструментов

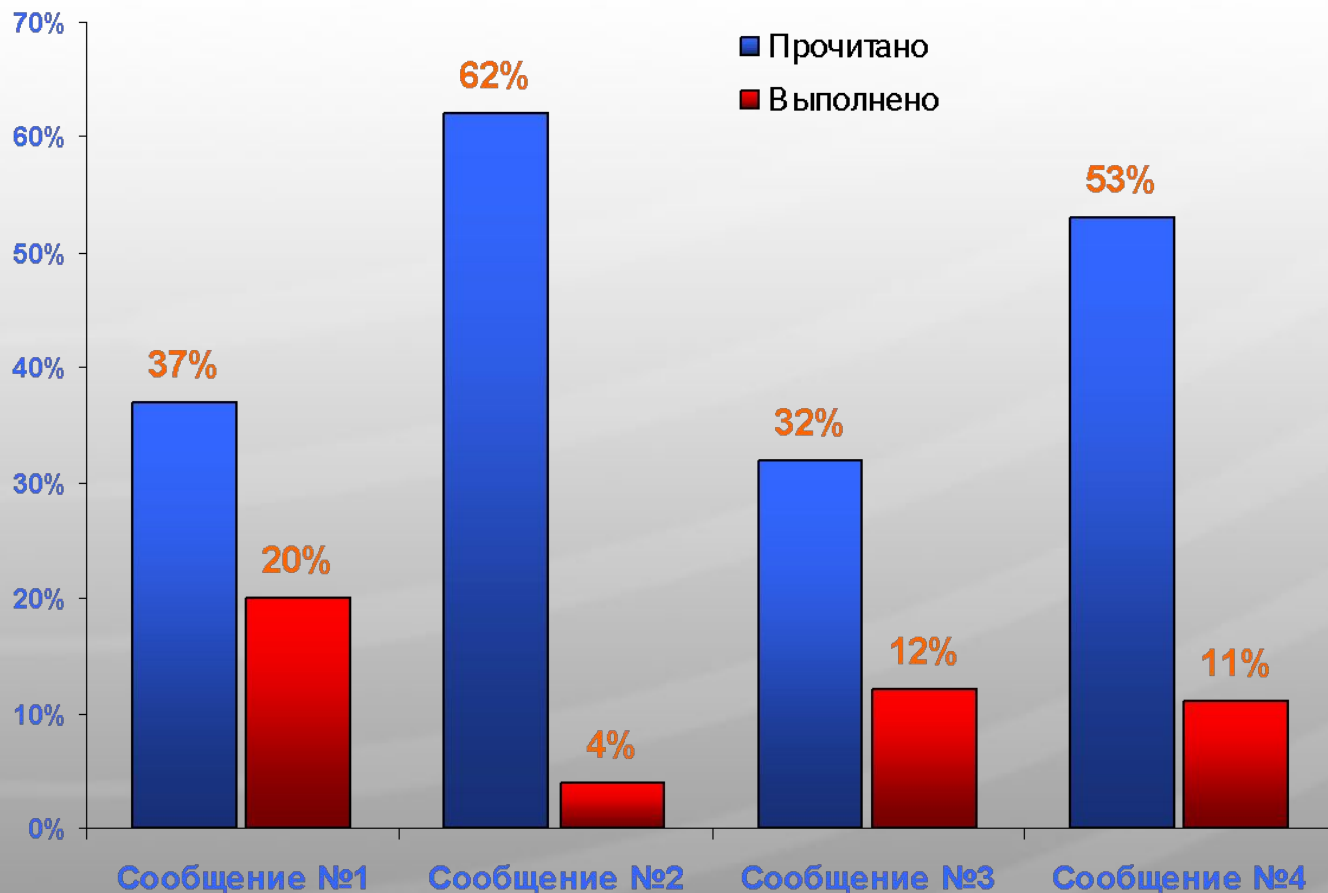
И	Описание сообщения	Эмулируемая атака
❖ И	Почтовое сообщение личного содержания, направленное третьему лицу, с приложенным исполняемым файлом.	Распространение сетевых червей Целевое заражение системы троянской программой
❖ И	Сообщение от внешнего лица, пользующегося определенным авторитетом, содержащее 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...



Оценка эффективности программ повышения осведомленности в области ИБ

Сводная статистика



Кто и как отреагировал на сообщение

❖ Вступил в переписку

Дата: 17.07.07 13:31

От кого: [REDACTED] [дресную книгу...](#) [В черный список...](#)

Кому: [REDACTED]

Тема: НА: [SPAM?] Как ты?

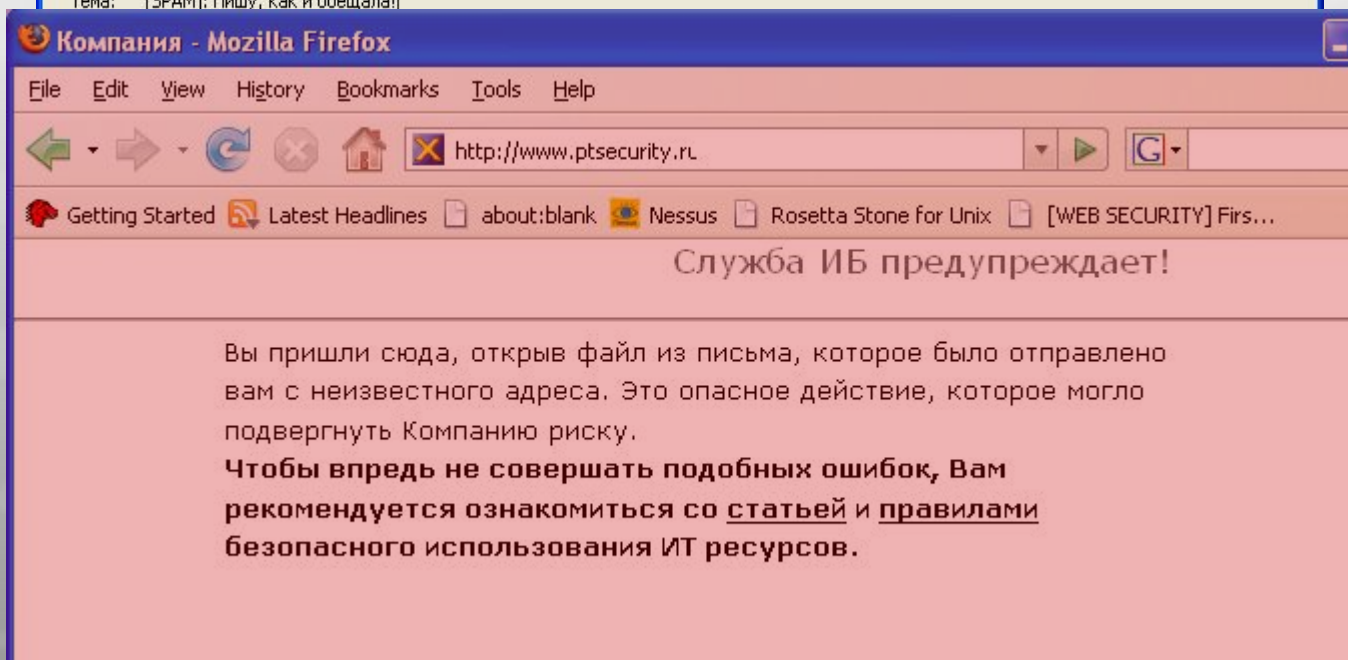
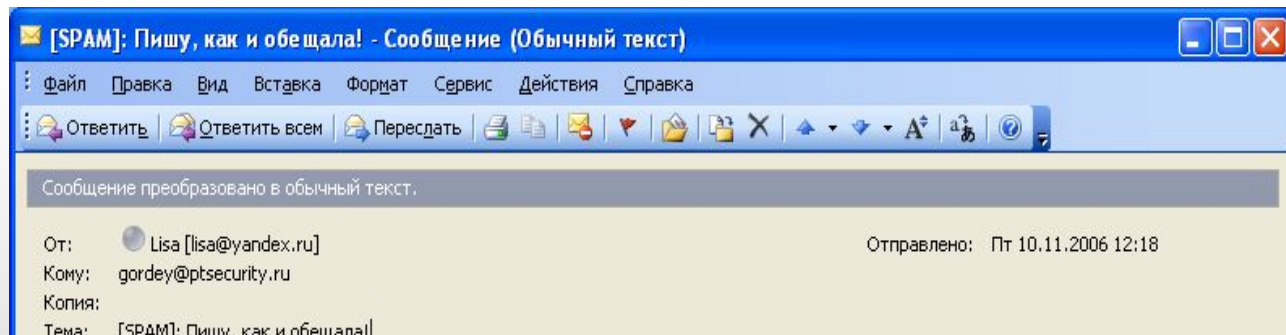
Привет !!!!!!!!!!!!!!!!!!!!!!!
а ты откуда.
Я удивлен и поражен

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](http://[REDACTED]izbrannoe/izbrannoe.asp))
Вчера под настроение посмотрела, пол дня была под впечатлением.

Совмещение «оценки» с «повышением»



- ❖ 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...*

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