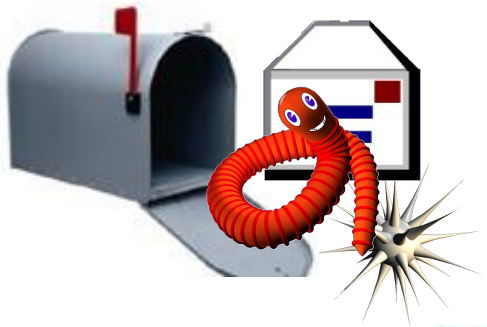
Угрозы безопасности, связанные с использованием электронной почты в организациях



Угрозы безопасности

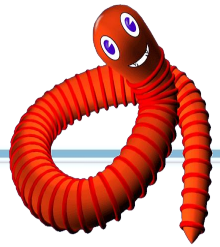
при использовании
систем электронной почты:

Угроза безопасности (субъекта информационных отношений) - потенциально возможное событие, связанное с определенными процессами или явлениями (источниками угроз), которое посредством воздействия на информацию, ее носители и процессы обработки (на компоненты АС) может привести к нанесению ущерба интересам данного субъекта.

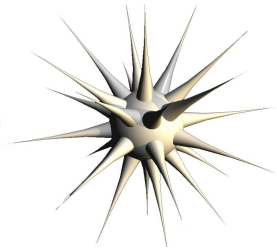
Основные угрозы безопасности

при использовании систем электронной почты:

- **Вирусы, троянские кони и ложные предупреждения о вирусах**
- **Спам (незапрашиваемая почта) и подметные (святые) письма**
- **Несанкционированный транзит почты**
- **Перехват и подделка почтовых сообщений**
- **Кража интеллектуальной собственности**
- **Снижение продуктивности работы сотрудников**
- **Ответственность за неправомерные действия сотрудников**
- **Нарушения функционирования почтовых систем**



Угрозы безопасности в СЭП



ВИРУСЫ

Вирусы - это "***саморазмножающиеся***" программы, которые при запуске стараются заразить другие программы и компьютеры. После того как программа была заражена, она сама становится "вирусоносителем", то есть вирус запускается каждый раз вместе с самой программой и продолжает заражать другие, еще не зараженные файлы.
Встречаются безвредные вирусы, которые не делают ничего кроме заражения других программ, но чаще встречаются ***вредоносные*** вирусы.

«Трояны» отличаются тем, что они обычно не заражают другие файлы, а под видом полезных маленьких программок или программ-шуток выполняют действия по ***взлому механизмов защиты***.

Угрозы безопасности в СЭП

СПАМ

СПАМ - это незапрашиваемая информация.
Это то чего Вы не хотите, но получаете.
Термин ***"спам"*** ведет свое происхождение от старого (1972) скетча английской комик-группы Monty Python Flying Circus. Посетители ресторанчика, ожидая заказ, вынуждены были слушать хор викингов, воспевающий мясные консервы (SPAM). В меню этого ресторана все блюда состояли из содержимого этих консервов.
В подавляющем большинстве случаев спам используется для рекламы.

Угрозы безопасности в СЭП

Основные цели СПАМа:

- **Реклама товара (услуги)**
- **Раскрутка сайта**
- **Платные звонки**
- **Реклама денежных пирамид**
- **Сбор информации**
- **Засылка троянов**
- **Подметные (святые) письма**

Угрозы безопасности в СЭП

Несанкционированный транзит почты

Ретрансляция (транзитная пересылка - Relay)
чужой электронной почты через ваши почтовые сервера.

Отправители спама используют ретрансляцию для рассылки с чужих серверов своих сообщений множеству адресатов, до которых они иначе не дошли бы, так как были бы отфильтрованы на основании адреса отправителя (IP-адреса и домены злостных отправителей спама содержатся в широко доступных «черных списках»).

Ретрансляция чужой почты может превратить Вашу почтовую систему в «плацдарм для рассылки» сорной почты, увеличить нагрузку на почтовые сервера и сделать компанию частично ответственной за подобную незаконную практику.

Угрозы безопасности в СЭП

Перехват и подделка почтовых сообщений

Послать электронное письмо по Интернет - это почти то же самое, что бросить открытку в обычный почтовый ящик.

Передаваемая информация может подвергнуться перлюстрации и злонамеренной модификации или фальсификации со стороны потенциальных злоумышленников.

Клиенты POP и IMAP передают ***имена и пароли*** Ваших почтовых ящиков пользователей на сервер по сети открытым текстом, что делает их легкой добычей для злоумышленников.

Без использования ***криптографических средств*** конфиденциальность, целостность, идентификацию отправителя и аутентификацию (подтверждения авторства) электронных писем обеспечить сложно.

Угрозы безопасности в СЭП

Кража интеллектуальной собственности

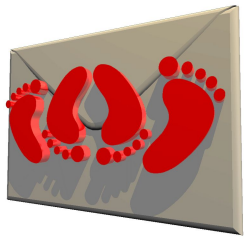
Все ли ваши сотрудники довольны работой и зарплатой?

Не переманивают ли кого-нибудь конкуренты, и не пересылает ли он будущим работодателям, в знак своей преданности, конфиденциальные материалы, среди которых:

- сведения служебного характера
- внутренние документы (тексты договоров, сведения о планируемых сделках и т.п.)
- фрагменты исходных кодов программ, которые вы создали с огромным трудом?

Угрозы безопасности в СЭП

Снижение продуктивности работы сотрудников и ответственность за их неправомерные действия



Когда они отправляют и принимают ***почту личного характера***, просматривают видео- или прослушивают аудио-файлы, которыми обмениваются со своими знакомыми (спам, анекдоты, порнография), деньги компании уходят на оплату рабочего времени сотрудников (и оплату сетевых услуг). Кроме того, это чревато перегрузкой сети из-за писем с вложениями большого объема.

Если сотрудник использует в переписке с партнерами ***ненормативную лексику***, да еще по отношению к вашим конкурентам или политическим деятелям, то кто-то потом может выдать это за официальное мнение компании.

Возможна потеря имиджа из-за случайно отправленных не по адресу писем непристойного содержания.

Угрозы безопасности в СЭП

Нарушение функционирования почтовых систем

Атаки типа ***«отказ в обслуживании»*** **(Denial of Service, DoS)** на почтовых клиентов или на почтовые серверы проводятся достаточно часто, и приводят к частичному или полному выведению почтовой системы из строя.

Практически всегда такие атаки становятся возможными ***вследствие неправильного конфигурирования серверов и клиентов электронной почты, а также окружающих компонентов сетевой инфраструктуры***.

Обеспечение безопасности СЭП

Две составляющие безопасности:

1. **Защита почтовой системы:**
   - защита сервера на уровне сети (сетевой инфраструктуры);
   - защита сервера на уровне ОС сервера;
   - защита на уровне самого почтового сервера (как приложения);
   - защита почтовых клиентов.
2. **Защита организации от угроз, связанных с информационным наполнением почтовых сообщений:**
   - антивирусное сканирование;
   - фильтрация содержимого (контента) почты:
   - защита от невостребованной (нежелательной) почты (то есть от спама).

Вопросы ?