Санкт-Петербургский политехнический университет им. Петра Великого

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

Реферат

по дисциплине: «Защита информации»

на тему: «Три угрозы и способа защиты корпоративных

и пользовательских сетей»

Выполнил: Раскин Андрей Романович \_\_\_\_\_\_\_\_\_

Проверил: Новопашенный Андрей Гелиевич \_\_\_\_\_\_\_\_\_

Дата: «\_\_» \_\_\_\_\_\_\_\_ 2017 г.

Санкт-Петербург

2017

Оглавление

[Введение 3](#_Toc474729154)

[Корпоративные сети 4](#_Toc474729155)

[Вредоносное ПО 4](#_Toc474729156)

[Спам 4](#_Toc474729157)

[Утечка данных 5](#_Toc474729158)

[Пользовательские сети 6](#_Toc474729159)

[Фишинг 6](#_Toc474729160)

[Способы защиты 6](#_Toc474729161)

[Угрозы 6](#_Toc474729162)

# Введение

Рост популярности Интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д. Хакеры и другие злоумышленники подвергают угрозам сетевые информационные ресурсы, пытаясь получить к ним доступ с помощью специальных атак. Эти атаки становятся все более изощренными по воздействию и несложными в исполнении. Этому способствуют два основных фактора.

Во-первых, это повсеместное проникновение Интернета. К этой сети подключены миллионы компьютеров. В ближайшем будущем их число во много раз возрастет, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям также постоянно возрастает. Кроме того, широкое распространение Интернета позволяет хакерам обмениваться информацией в глобальном масштабе.

Во-вторых, это всеобщее распространение простых в использовании ОС и сред разработки. Этот фактор резко снижает требования к уровню знаний злоумышленника. Раньше от хакера требовались хорошие знания и навыки программирования, чтобы создавать и распространять вредоносные программы. Теперь, для того чтобы получить доступ к хакерскому средству, нужно просто знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышкой.

# Корпоративные сети

## Вредоносное ПО

Реализация вредоносных алгоритмов может привести как к парализации системы и ее сбоям, так и к утере, подмене или утечке информации. Все это чревато огромными имиджевыми, временными и финансовыми потерями для компании.

К таким программам относятся компьютерные вирусы, сетевые черви, программа «троянский конь».

Особенностью современных вредоносных программ является их ориентация на конкретное прикладное ПО, ставшее стандартом де-факто для большинства пользо­вателей, в первую очередь это Microsoft Internet Explorer и Microsoft Outlook. Массовое создание вирусов под продукты Microsoft объясняется не только низким уровнем безопасности и надежности программ, важную роль играет глобальное распространение этих продуктов. Авторы вредоносного программного обеспечения все активнее начинают исследовать «дыры» в популярных СУБД, связующих ПО и корпоративные бизнес-приложения, построенные на базе этих систем.

Хакеры пытаются создавать новые, изощренные виды ПО, чтобы получать доступ к ценным данным. Вирусы, черви и «троянские» программы постоянно эволюционируют, основной тенденцией их развития является полиморфизм.

Одним из главных способов защиты - **Межсетевые экраны**. Они обеспечивают разделение сетей и предотвращают нарушение пользователями установленных правил безопасности. Современные межсетевые экраны отличаются удобным управлением и большим функционалом (возможностью организации VPN, интеграции с антивирусами и др.).

## Спам

Борьба с рекламной и вредоносной рассылкой потребует около 5-ти часов в месяц, а это рабочее время, оплачиваемое работодателем. Кроме того, спам значительно увеличивает нагрузку на коммуникации, повышает трафик, снижает эффективность работы сервера.

Существуют и более опасные рассылки, которые нацелены на «заражение» компьютера или на получение доступа к конфиденциальной информации. Эти разновидности спама — особый вид интернет-мошенничества, призванный получить идентификационные данные пользователя, такие как личные и корпоративные пароли, номера кредитных карт, банковских счетов и так далее.

Виды спама:

1. Коммерческий спам
2. Некоммерческий спам, или анонимная массовая рассылка
   1. Политический спам.
   2. «Благотворительный» спам
   3. Мошеннический спам
   4. Цепочный спам («письма счастья»)
   5. Спам «для взрослых»
   6. Вирусный спам

Основным и самым популярным методом борьбы с нежелательной корреспонденцией является фильтрация, то есть отсеивание спама от действительно важных писем. Этот метод основан на том, что спам-письма значительно отличаются от обычных. Фильтрация разделяется на автоматическую и неавтоматическую.

*Автоматическая фильтрация спама.* Для защиты от спама используются спам-фильтры. Они могут быть установлены на пользовательских компьютерах или на серверах. Очень популярна на данный момент байесовская фильтрация спама. спам-фильтры предварительно «обучаются», то есть им отправляются уже отсортированные письма, на основе которых фильтр анализирует статистические особенности желательной корреспонденции и нежелательной. Если «обучение» происходит нормально, то фильтр помогает отсеять до 97% спама.

*Неавтоматическая фильтрация* является более трудоемкой и сложно подстраиваемой. Но в конечном счете, если грамотно подойти к вопросу, она может стать очень результативной. При неавтоматической фильтрации спам-фильтры задаются пользователем и, как правило, состоят из стоп-слов или выражений.

## Утечка данных

В последнее время все чаще фиксируются случаи промышленного шпионажа и утечки информации, от последствий которых организации терпят значительные убытки. Это связано с тем, что сегодня в любой компании активно используются различные средства коммуникации, которые одновременно являются и каналами утечки конфиденциальной информации: Интернет (электронная почта, мессенджеры), внешние устройства, повышающие мобильность бизнеса (USB-карты, PDA, съемные диски и т.д.), и принтеры.

По статистике, вероятность утечки конфиденциальной информации из-за действий сотрудника организации (инсайдера) превышает вероятность утечки в результате взлома, причем это не обязательно умышленные действия, пользователь может случайно отправить файл не тому адресату.

Деловая переписка сотрудников ведется по электронной почте, пользователи общаются посредством IM и VoIP, обмениваются файлами, ведут блоги, публикуют сообщения в соцсетях и т. д. Все эти каналы легко контролировать автоматически, мощность современных серверов и емкость носителей позволяют собирать и обрабатывать данные в реальном времени. Чтобы обнаружить и предотвратить передачу конфиденциальных данных на разных этапах (при перемещении, использовании и хранении), применяется целый класс систем защиты — DLP (Data Leak Prevention).

# Пользовательские сети

## Фишинг

Фишинг – это всё более популярный тип интернет-мошенничества, с помощью которого пытаются получить конфиденциальные данные от пользователей, чтобы затем использовать, например, для получения контроля над банковским счетом.

Почтовая рассылка, целью которой является получение от пользователя конфиденциальной информации как правило финансового характера. Такие письма составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, где пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

Самым результативным методом борьбы с мошенническими ресурсами, по мнению Group-IB, является комплекс мер, включающих проактивный мониторинг, экспертный анализ контента и реагирование по выявленным мошенническим Интернет ресурсам – с целью их оперативной нейтрализации.

## Сетевые атаки

Сетевые атаки приводят к следующимпоследствиям:

* Отказ клиентских и серверных компонентов сетей по причине перегрузки чрезмерным количеством запросов на обслуживание, т.е. запланированная или случайная DoS-атака (Denial of Service).
* Заметное замедление работы локальных и глобальных сетей по причине перегрузки каналов, работа которых блокируется чрезмерным количеством передаваемых данных, т.е. "флудинг" (от flood) каналов передачи информации.
* Заметный материальный ущерб в тех случаях, когда оплата услуг провайдера ведется по размеру передаваемого и/или принимаемого трафика.

## Вирусы и приложения типа "троянский конь"

Рабочие станции конечных пользователей очень уязвимы для вирусов и троянских коней. Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя.

Борьба с вирусами и "троянскими конями" ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и, возможно, на уровне сети. Антивирусные средства обнаруживают большинство вирусов и "троянских коней" и пресекают их распространение. Получение самой свежей информации о вирусах поможет эффективнее бороться с ними. По мере появления новых вирусов и "троянских коней" предприятие должно устанавливать новые версии антивирусных средств и приложений.