

ПРОЕКТ

ПО

Информационная безопасность

Выполнила: **Иголина Марина**

Александровна «Тазинская основная
общеобразовательная школа» Большеберезниковского
муниципального района РМ

Цель проекта:

**Познакомиться с основами
информационной безопасности,
определить основные направления
развития этой области знаний,
сформировать элементы
«информационной культуры».**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ -

**защищенность информации и поддерживающей ее
инфраструктуры от любых случайных или
злонамеренных воздействий, результатом которых
может явиться нанесение ущерба самой
информации, ее владельцам или поддерживающей
инфраструктуре**

ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ -

**минимизация ущерба, прогнозирование и
предотвращение злонамеренных
воздействий**

Что угрожает информационной безопасности

1. Действия, осуществляемые авторизованными пользователями

- целенаправленная кража или уничтожение данных на рабочей станции или сервере;
- повреждение данных пользователем в результате неосторожных действий.



Что угрожает информационной безопасности

2. "Электронные" методы воздействия, осуществляемые хакерами

- несанкционированное проникновение в компьютерные сети;
- DOS-атаки.

Хакеры - люди, занимающиеся компьютерными преступлениями как профессионально (в том числе в рамках конкурентной борьбы), так и просто из любопытства



Атака типа DOS (сокр. от Denial of Service - "отказ в обслуживании") - это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечет за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации и т. п.

Что угрожает информационной безопасности

3. Компьютерные вирусы

Отдельная категория электронных методов воздействия - компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, Интернет и электронную почту. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компании.

Что угрожает информационной безопасности

4. Спам

Спам (англ. *spam*) — рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, не выразившим желания их получать. Легальность массовой рассылки некоторых видов сообщений, для которых не требуется согласие получателей, может быть закреплена в законодательстве страны. Например, это может касаться сообщений о надвигающихся стихийных бедствиях, массовой мобилизации граждан и т. п. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем. Незапрошенные сообщения в системах мгновенного обмена сообщениями (например, ICQ) носят название SPIM (англ. *Spam over IM*).

Что угрожает информационной безопасности

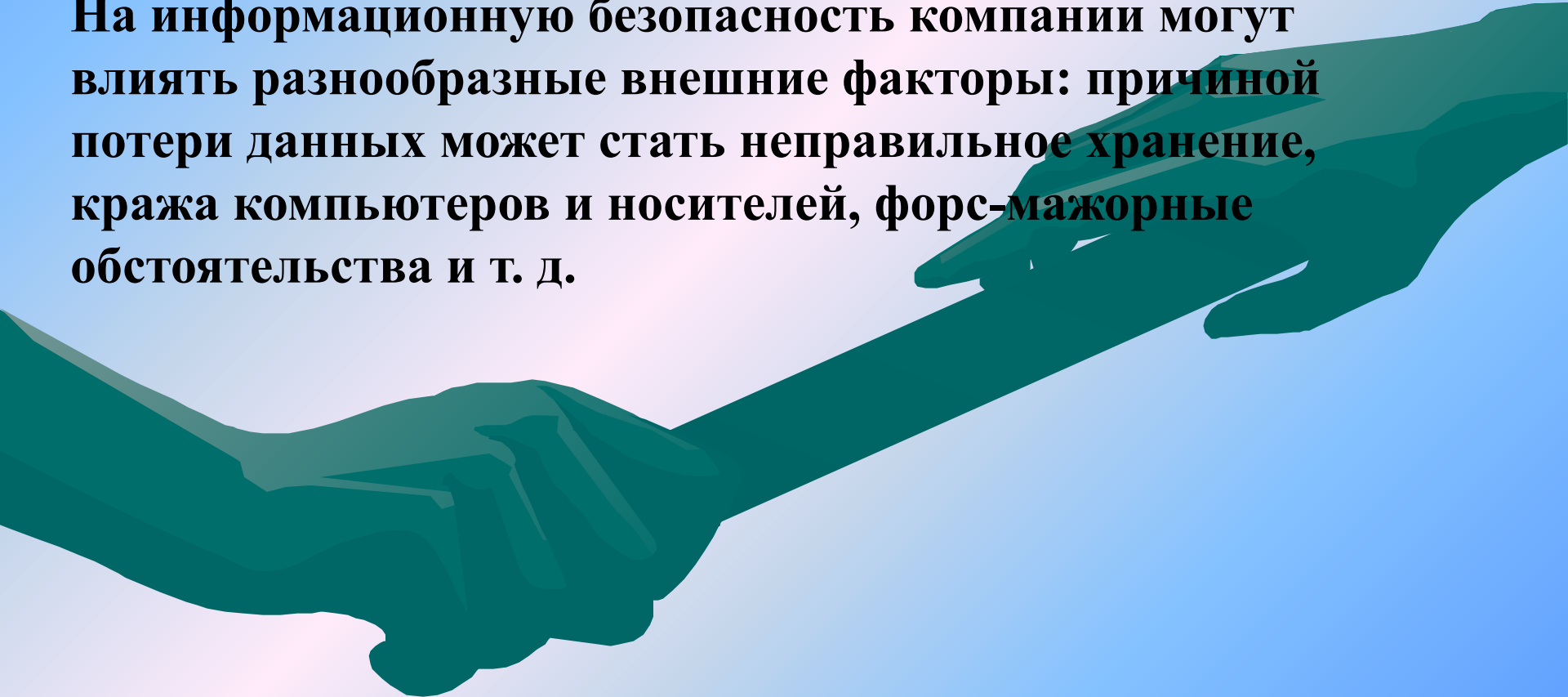
4. Спам

- электронная почта в последнее время стала главным каналом распространения вредоносных программ;
- спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает у сотрудников чувство психологического дискомфорта;
- как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых спамерами (зачастую подобного рода события потерпевшие стараются не разглашать);
- вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям; опасность потери корреспонденции особенно возрастает при использовании черных списков RBL и других "грубых" методов фильтрации спама.

Что угрожает информационной безопасности

5. "Естественные" угрозы

На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т. д.



Методы обеспечения информационной безопасности:

