Проблемы информационной безопасности в России

Презентацию подготовила
Изьяева Снежана

К объектам, которым следует обеспечить информационную безопасность, относятся:

- Информационные ресурсы;
- Система создания, распространения и использования информационных ресурсов;
- Информационная инфраструктура общества (информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации);
- Средства массовой информации;
- Права человека и государства на получение, распространение и использование информации;
- Защита интеллектуальной собственности и конфиденциальной информации

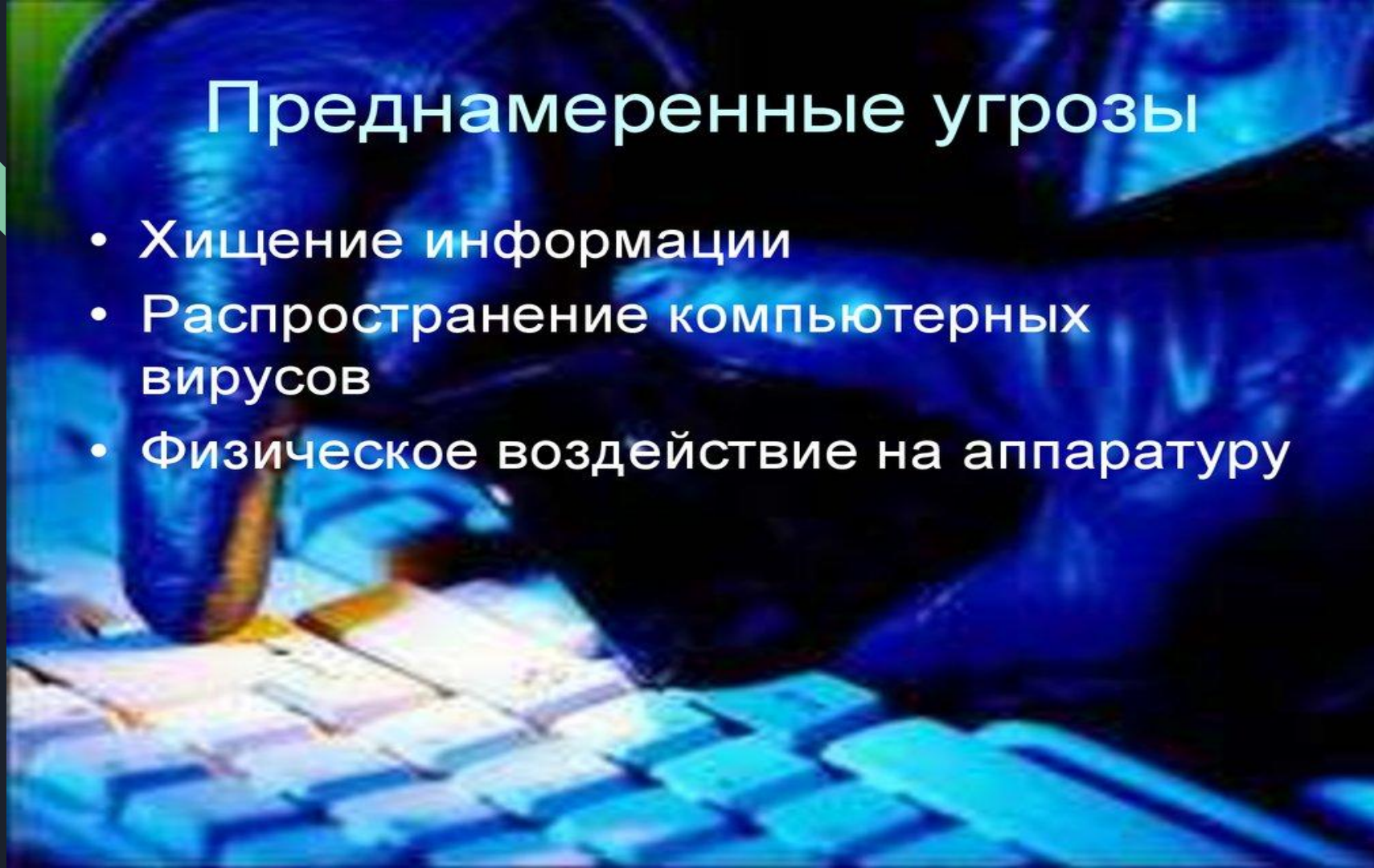
Источники основных информационных угроз для России

Внешние источники

- Политика стран
- Информационная война
- Преступная деятельность
- Прочие источники

Внутренние источники

- Отставание по уровню информатизации
- Отставание по технологии
- Недостаточный уровень образования
- Прочие источники



Преднамеренные угрозы

- Хищение информации
- Распространение компьютерных вирусов
- Физическое воздействие на аппаратуру

Случайные угрозы

- Ошибки пользователя компьютера;
- Ошибки профессиональных разработчиков информационных систем: алгоритмические, программные, структурные;
- Отказ и сбои аппаратуры, в том числе помехи и искажения сигналов на линиях связи;
- Форс-мажорные обстоятельства

Политика безопасности – это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.

Методы защиты информации от преднамеренных информационных угроз

- Ограничение доступа к информации
- Шифрование информации
- Контроль доступа к аппаратуре
- Законодательные меры

Методы защиты информации от случайных информационных угроз

- Повышение надёжности работы электронных и механических узлов и элементов
- Структурная избыточность – дублирование или утроение элементов, устройств
- Функциональный контроль с диагностикой отказов

2.1. Виды источников угроз

- 2.1.1. Антропогенные источники
- 2.2.2. Техногенные источники
- 2.2.3. Стихийные бедствия

2.1.1. Атропогенные источники

- Криминальные структуры
- Потенциальные преступники и хакеры
- Недобросовестные партнеры
- Представители надзорных организаций и аварийных служб
- Представители силовых структур
- Основной персонал (пользователи, программисты, разработчики)
- Представители службы защиты информации (администраторы)
- Вспомогательный персонал (уборщики, охрана)
- Технический персонал (жизнеобеспечение, эксплуатация)

2.1.2.Техногенные источники

Внешние

- Средства связи (передачи информации)
- Сети инженерных коммуникаций (энергоснабжения, водоснабжения, отопления, вентиляции, канализации)

Внутренние

- Некачественные технические средства обработки информации
- Некачественные программные средства обработки информации
- Вспомогательные средства (охраны, сигнализации, телефонии)
- Другие технические средства, применяемые в учреждении

2.1.3. Стихийные бедствия

- Пожары,
- Землетрясения,
- Наводнения,
- Ураганы,
- Различные непредвидимые обстоятельства,
- Необъяснимые явления,
- Другие форс-мажорные обстоятельства

Политика безопасности – это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.

Методы защиты информации от преднамеренных информационных угроз

- Ограничение доступа к информации
- Шифрование информации
- Контроль доступа к аппаратуре
- Законодательные меры

Методы защиты информации от случайных информационных угроз

- Повышение надёжности работы электронных и механических узлов и элементов
- Структурная избыточность – дублирование или утроение элементов, устройств
- Функциональный контроль с диагностикой отказов

В обеспечении информационной безопасности должны быть полнее задействованы ресурсы гражданского общества. Очевидно, что государство в одиночку не способно справиться в полном объеме с задачей обеспечения информационной безопасности всех субъектов информационных отношений. Если сегодня в соответствии с законом оно полностью отвечает лишь за вопросы защиты государственной тайны, то в большинстве остальных случаев при неопределенности доли государственного участия бремя обеспечения информационной безопасности ложится на плечи граждан и общества. Это отвечает конституционному принципу самозащиты своих интересов всеми способами, не запрещенными законом. Органы государственной власти должны четко определить свои полномочия, исходя из реальных возможностей и заявленных приоритетов в обеспечении информационной безопасности.

Спасибо за внимание!