The background features a vibrant blue and white digital theme. On the right, a globe is visible with labels for 'AFRICA', 'ERITREA', 'CHAD', and 'ARABIA'. The left side shows a computer keyboard and a screen displaying binary code (0s and 1s) and a search bar with a left-pointing arrow icon. A glowing white lightning bolt strikes down from the top left towards the keyboard. The overall aesthetic is high-tech and data-oriented.


Безопасность в информационном обществе

Выполнила : Бородина Е.С.

Существует информация
такая,
Которую должны беречь и
защищать,
Такая информация
значение имеет,
Нельзя ее из вида
упускать!

И в этот день, такой
секретный,
Желаю информацию
свою беречь,
Запретное, пусть будет
под запретом,
Нельзя, чтобы защита
дала течь!





Информация давно перестала быть лишь одним из источников познания окружающего мира. Это товар, который каждый день и час продается и покупается. Более того, информационные данные стали бесспорным и очень опасным оружием не только в узком кругу, но и в соблюдении и установлении мирового порядка.


Специалистам, которые занимаются защитой данных, даже посвятили отдельный праздник, именуемый **Днем защиты информации**. Ежегодно его отмечают 30 ноября.

История возникновения праздника

История возникновения праздника возвращает в 1988 год, когда была совершена первая масштабная атака на конфиденциальные информационные ресурсы. Тогда 2 ноября было зафиксировано появление и успешное распространение сетевого червя, который вывел из строя работу тысячи интернет-узлов в США. Вирус позднее нарекли червём Морриса, исходя из имени его "родителя". Роберт Моррис был на тот момент аспирантом факультета Вычислительной техники Корнельского университета. Хакеры в своих кругах прозвали его "великим червём".

Сложность обнаружения вируса состояла в том, что он использовал хорошую маскировку для сокрытия своего существования в операционной системе компьютера. "Червь" удалял свой исходный файл, ветвился каждые три минуты. Ущерб от вируса оценили более чем в 96 миллионов долларов. Этот случай наглядно указал, как опасно доверять компьютерным сетям.





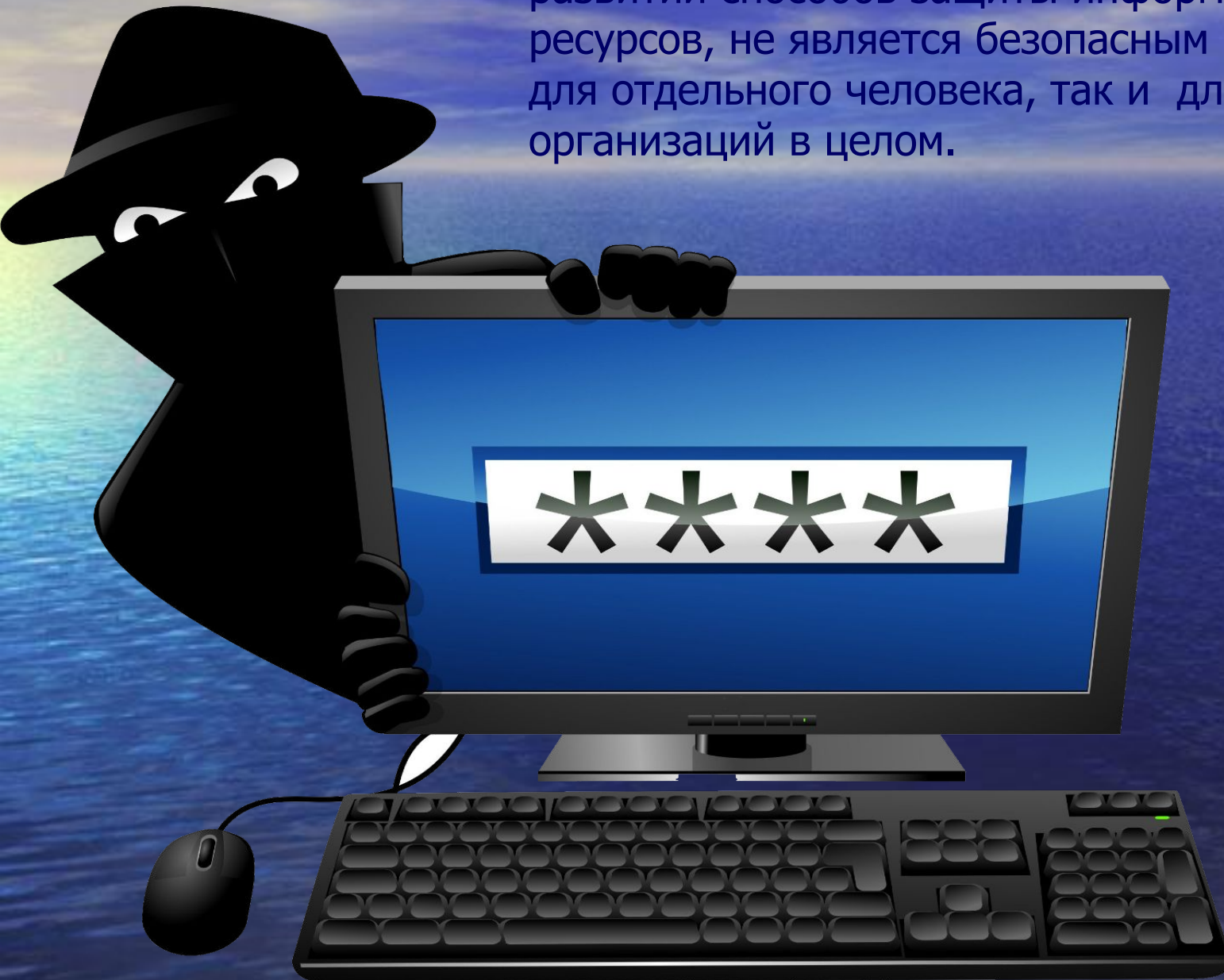
**Защита информационных
данных в первую
очередь
подразумевает:**

1. Обязательную установку антивирусных программ.
2. Использование хорошо защищенных и сложных паролей.
3. Физическую защиту информации. Соблюдение мер безопасности, правильное хранение информационных данных, соблюдение и поддержание порядка в хранении персональных данных – в интересах каждого отдельного пользователя сети.

ЗАЩИТА ЛИЧНОЙ ИНФОРМАЦИИ



Интернет, даже при невероятно быстром развитии способов защиты информационных ресурсов, не является безопасным местом как для отдельного человека, так и для мировых организаций в целом.



О профессии

Специалистам, которые занимаются защитой данных, даже посвятили отдельный праздник, именуемый

Днем защиты информации.

Ежегодно его отмечают 30 ноября.

Главная задача таких специалистов – обеспечение комплексной защиты информации. Представители данной профессии проводят информационное обследование и анализ, с целью обнаружения вероятного нарушителя.

Также они занимаются разработкой внутриорганизационных нормативно-технических документов. В их задачи входит руководство установкой и настройкой средств и механизмов защиты. Помимо этого, они обязаны поддерживать, модернизировать и обновлять существующую систему безопасности.



Правила общения в сети

1. Помните, что вы говорите с человеком.
2. Придерживайтесь тех же стандартов поведения, что и в реальной жизни.
3. Помните, что вы находитесь в киберпространстве.
4. Уважайте время и возможности других.
5. Сохраняйте лицо.
6. Помогайте другим там, где вы это можете делать.
7. Не ввязывайтесь в конфликты и не допускайте их.
8. Уважайте право на частную переписку.
9. Не злоупотребляйте своими возможностями.
10. Учитесь прощать другим их ошибки.

Чего делать нельзя в интернете без согласования со взрослыми:

- Никогда не оставляй встреченным в Интернете людям свой номер телефона, домашний адрес или фотографии.
- Никогда не договаривайся о встрече с интернет-знакомыми без сопровождения взрослых. Они не всегда являются теми, за кого себя выдают. Встречайся только в общественных местах.
- Никогда не открывай прикрепленные к электронному письму файлы, присланные от незнакомого человека. Файлы могут содержать вирусы или другие программы, которые могут повредить всю информацию или программное обеспечение компьютера.
- Никогда не отвечай на недоброжелательные сообщения или на сообщения с предложениями, всегда рассказывай родителям, если получил таковые.

Детям – безопасный Интернет

