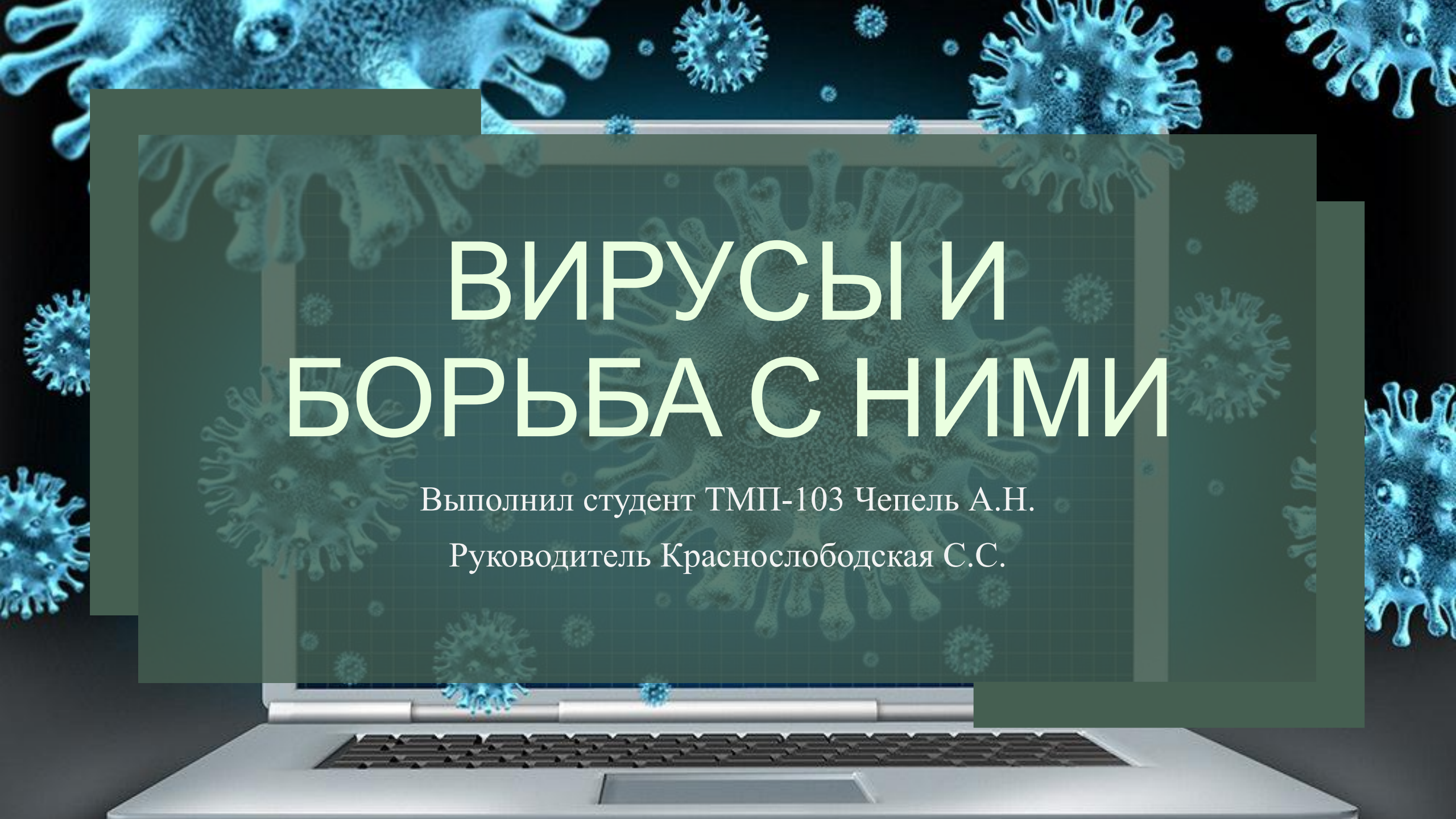


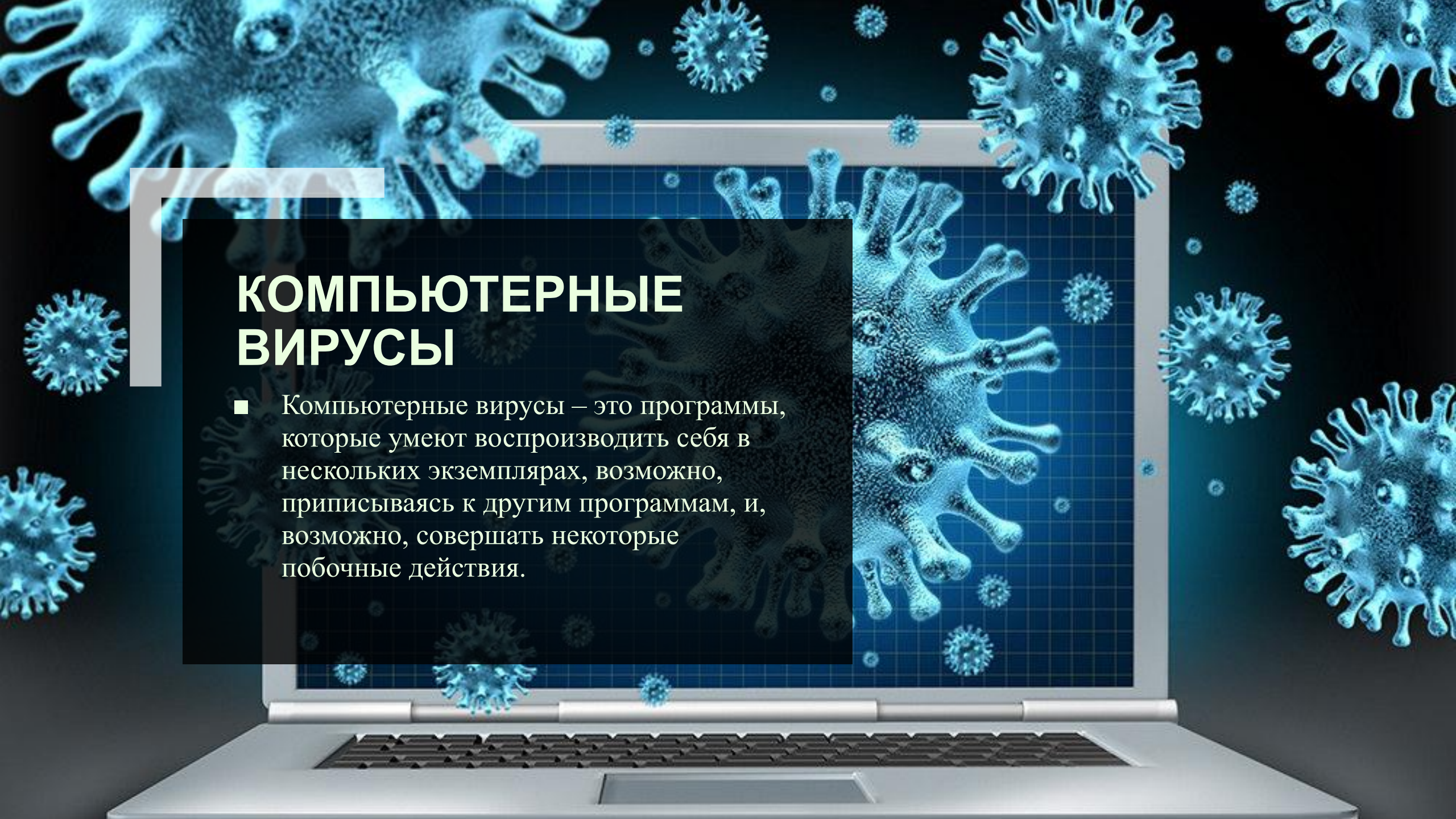
ВИРУСЫ И БОРЬБА С НИМИ

Выполнил студент ТМП-103 Чепель А.Н.

Руководитель Краснослободская С.С.

ВВЕДЕНИЕ

- Вирус один из самых важных врагов компьютера. Как и обычные вирусы, вирусы компьютера являются паразитами, чтобы размножаться, им нужен носитель - хозяин, программы или документа телом которого скрывают фрагменты кода программы. Вирусы, широко распространившиеся в области вычислительной техники, потрясли весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность...



КОМПЬЮТЕРНЫЕ ВИРУСЫ

- Компьютерные вирусы – это программы, которые умеют воспроизводить себя в нескольких экземплярах, возможно, приписываясь к другим программам, и, возможно, совершать некоторые побочные действия.

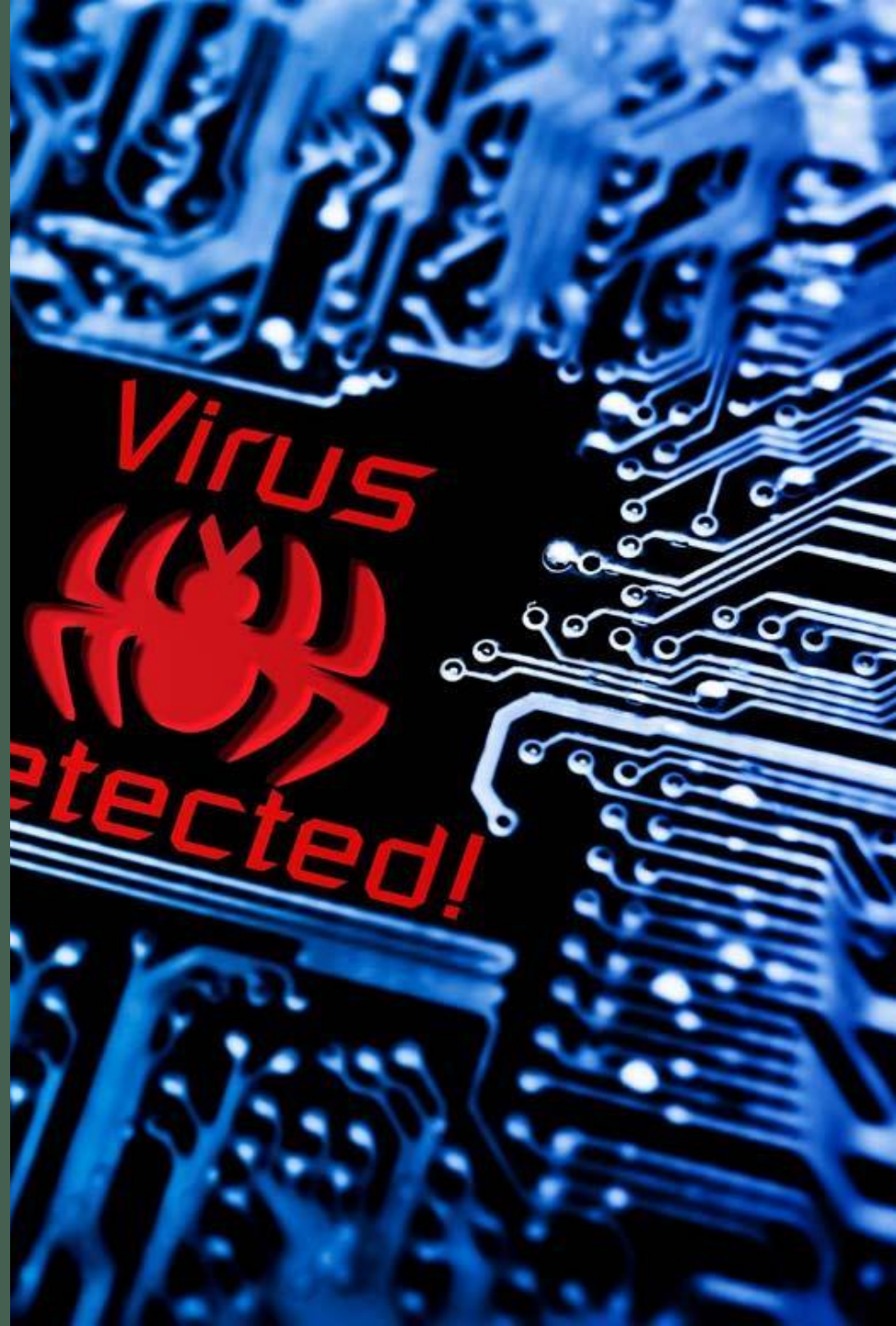
Классификация вирусов

- По масштабу вредных воздействий компьютерные вирусы делятся на:
- Безвредные – не влияют на работу ПК, лишь уменьшают объём свободной памяти на диске, в результате своего размножения.
- Неопасные – вирусы, влияние которых ограничивается уменьшением памяти на диске, графическими, звуковыми и другими внешними эффектами.

- Опасные– портят данные на дисках, порча данных происходит лишь эпизодически и не приводит к тяжёлым последствиям (например, портиться лишь COM-файлы при заражении, если длина этих файлов более 64000 байт). Приводят к сбоям и зависаниям при работе на ПК;
- Очень опасные – вирусы причиняют значительные разрушения, приводят к потере программ и данных (изменение, удаление), форматированию винчестера и т.д.

По среде обитания компьютерные вирусы бывают: сетевыми, файловыми, загрузочными.

- По среде обитания компьютерные вирусы бывают: сетевыми, файловыми, загрузочными.
- 1.Файловые вирусы размещаются в исполняемых файлах с расширением .com, .exe, создают файлы-двойники (компаньон-вирусы) или используют особенности организации файловой системы (link-вирусы).
- Способны внедряться в программы и активизируются при их запуске из оперативной памяти, вирусы заражают другие программные файлы, меняя их код вплоть до момента выключения ПК.



- Макровирусы - поражают документы, выполненные в некоторых прикладных программах (Word и Excel), имеющих средства для исполнения макрокоманд. Угроза заражения прекращается после закрытия приложения. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов и предлагается запретить их загрузку.

- Сетевыевирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. При открытии почтового сообщения обращайте внимание на вложенные файлы. К таким вирусам относятся троянские программы и почтовые вирусы - "сетевые черви".

Первые компьютерные вирусы

- Первый известный вирус был написан для компьютера Univac 1108 (конец 1960-х - начало 1970-х годов). Он назывался Pervading Animal и фактически представлял собой игру, написанную с ошибкой - с помощью наводящих вопросов программа пыталась определить имя животного, задуманного играющим. Ошибка заключалась в том, что при добавлении новых вопросов модифицированная игра записывалась поверх старой версии плюс копировалась в другие директории. Следовательно через некоторое время диск становился переполненным. Поскольку Pervading Animal не был настоящим вирусом, он не содержал процедуры самораспространения и передавался исключительно через пользователей, желающих по собственной воле переписать программу.

- В 1969 году в США была создана первая глобальная компьютерная сеть, прародитель современной Интернет, ARPANET (Advanced Research Projects Agency Network). Она объединяла четыре ведущих научных центра США и служила для быстрого обмена научной информацией. Не удивительно, что уже в начале 1970-х в ARPANET появился первый вирус, умеющий распространяться по сети. Он назывался Creeper и был способен самостоятельно выйти в сеть через модем и сохранить свою копию на удаленной машине. На зараженных компьютерах вирус обнаруживал себя сообщением: IM THE CREEPER: CATCH ME IF YOU CAN.

Мобильные угрозы

- Мир мобильных устройств относится к той сфере, где IT-безопасность развивается наиболее быстро. В 2013 году проблема безопасности мобильных устройств встала очень остро, и это связано и с количественным, и с качественным ростом мобильных угроз. Если 2011 год был годом становления мобильных зловредов, особенно в секторе Android-устройств, а 2012 — годом развития их многообразия, то 2013 год стал годом наступления их зрелости.

- Obad – пожалуй, наиболее заметное событие в сфере мобильных зловредов. Этот мобильный троянец распространяется разными способами, в том числе через уже существующий мобильный ботнет — смартфоны, зараженные Trojan-SMS.AndroidOS.Opfake.a, используются в качестве дополнительного вектора заражения. С них на все номера из списка контактов рассылаются сообщения, содержащие вредоносные ссылки. Такая практика широко распространена в сфере угроз для персональных компьютеров и популярна как сервис, предоставляемый ботоводами на теневом рынке киберпреступников.

БОРЬБА С ВИРУСАМИ

Основные методы защиты от компьютерных вирусов

- Для защиты от вирусов можно использовать:
- Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- Профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- Специализированные программы для защиты от вирусов.

- Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:
- Копирование информации — создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

История антивирусных программ

- Первые антивирусные программы появились еще зимой 1984 года (первый вирус для персональных компьютеров Apple появился в 1977 году, и только в 1981 году появились вирусы, представляющие какую-либо угрозу) под названиями CHK4BOMB и BOMBSQAD. Их написал американский программист Энди Хопкинс (Andy Hopkins). CHK4BOMB позволяла проанализировать текст загрузочного модуля и выявить все текстовые сообщения и «подозрительные» участки кода. Программа BOMBSQAD перехватывала операции записи и форматирования, выполняемые через BIOS. При выявлении запрещённой операции можно было разрешить или запретить её выполнение.

Методы обнаружения вирусов

- Обнаружение, основанное на сигнатурах - метод, когда антивирусная программа, просматривая файл, обращается к антивирусным базам, которые составлены производителем программы-антивируса.

- В случае соответствия, какого либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в базах, программа-антивирус может по запросу выполнить одно из следующих действий:
- Удалить инфицированный файл.
- Заблокировать доступ к инфицированному файлу.
- Отправить файл в карантин (то есть сделать его недоступным для выполнения с целью недопущения дальнейшего распространения вируса). Попытаться «вылечить» файл, удалив тело вируса из файла.
- В случае невозможности лечения/удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.

ЗАКЛЮЧЕНИЕ

- На сегодняшний день практически невозможно обойтись без компьютеров. И с этим невозможно не воспользоваться Интернетом и различных устройств для передачи и хранения информации. В этом смысле, существует высокая вероятность заражения вирусом. Таким образом, вам нужно установить несколько антивирусных программ на своих компьютерах. Но ни один антивирус не может дать стопроцентной гарантии, что вирус не прорежет в системе. Все это требует от владельцев ПК определенной культуры работы с компьютерами.


СПАСИБО ЗА
ВНИМАНИЕ!