Департамент образования города Москвы  
Государственное бюджетное общеобразовательное учреждение города Москвы «ГБОУ школа №1505 Преображенская»

**РЕФЕРАТ**

**на тему**

**Направление IT-безопасность в IT-классе**

Выполнил:  
 Манягин Иван Сергеевич  
Собин Александр Вадимович  
Руководитель:  
Барышев Юрий Николаевич  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись руководителя)

Москва  
2020/2021 уч.г.

**ОГЛАВЛЕНИЕ**

Оглавление

[Направление IT-безопасность в IT-классе 1](#_Toc65782772)

[ВВЕДЕНИЕ 3](#_Toc65782773)

[Цель проекта 3](#_Toc65782774)

[Задачи проекта 3](#_Toc65782775)

[Итоговый продукт 4](#_Toc65782776)

[Актуальность 4](#_Toc65782777)

[Наши роли в проекте 4](#_Toc65782778)

[Глава 1 5](#_Toc65782779)

[Глава 2 8](#_Toc65782780)

[ПРЕДИСЛОВИЕ 8](#_Toc65782781)

[БАЗОВАЯ ТЕРМИНОЛОГИЯ 8](#_Toc65782782)

[ОСНОВНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ 9](#_Toc65782783)

[ЦИФРОВЫЕ ПОДПИСИ 9](#_Toc65782784)

[ОБЕСПЕЧИВАЕМАЯ ШИФРОМ СТЕПЕНЬ ЗАЩИТЫ 10](#_Toc65782785)

[Глава 3 12](#_Toc65782786)

[КОМПЬЮТЕРНЫЙ ВИРУС 12](#_Toc65782787)

[ИСТОРИЯ ВИРУСОВ И ВСПЛЕСКИ КОМПЬЮТЕРНЫХ ВИРУСОВ 12](#_Toc65782788)

[ПРИЧИНЫ ПОЯВЛЕНИЯ ВИРУСОВ 13](#_Toc65782789)

[КЛАССИФИКАЦИЯ ВИРУСОВ 13](#_Toc65782790)

[КАК ОПРЕДЕЛИТЬ ВИРУС НА КОМПЬЮТЕРЕ 15](#_Toc65782791)

[ЗАКЛЮЧЕНИЕ 16](#_Toc65782792)

[Источники 17](#_Toc65782793)

# ВВЕДЕНИЕ

Значимость процесса обеспечения информационной безопасности в современном мире трудно переоценить. Пренебрежение информационной безопасностью – это не только материальный ущерб или удар по репутации, но и вред здоровью граждан, подрыв экологии, нарушение инфраструктуры, угроза государственной безопасности и тому подобное.

Проблемы защиты информации актуальны практически для всех видов деятельности: банковской сферы, энергетики, ВПК, политики, культуры, образования, транспорта и так далее. Профессионалы в области информационной безопасности всегда востребованы в государственных и коммерческих структурах. Если вы заинтересованы в том, чтобы ваша информация не разглашалась, всегда отличалась своей целостностью, подлинностью, доступностью, и, самое важное, конфиденциальностью, стоит всё-таки не упустить возможность и вовремя защитить необходимую вам информацию.

# Цель проекта

Разработать теоретический курс по направлению и донести его ученикам старшей школы, реализовать его в форме интерактивного урока в одном из классов нашей школы.

# Задачи проекта

* Определить тему проекта
* Сформулировать проблему**.**
* Выбрать консультанта проекта.
* Сформулировать цели и задачи.
* Сбор информации и создание текста.
* Анализ собранной информации.
* Создание анкеты для проверки знаний у учеников.
* Подготовка к предзащите темы проекта.
* Подготовка к уроку, который мы будем проводить
* Проведение урока
* Подготовка к защите проекта.

# Итоговый продукт

У нас много промежуточных продуктов, например: сценарий для проведения урока, анкета после проведенного урока для проверки эффективности нашей работы и многое другое, но 2 итоговых продукта:

Создание интерактивного урока по теме "Информационная безопасность" в IT-классе.

Сбор информации и создание реферата о данной теме

# Актуальность

Значимость процесса обеспечения информационной безопасности в современном мире трудно переоценить. Пренебрежение информационной безопасностью – это не только материальный ущерб или удар по репутации, но и вред здоровью граждан, подрыв экологии, нарушение инфраструктуры, угроза государственной безопасности и тому подобное.

# Наши роли в проекте

В данном проекте мы выполняем разные роли, а именно: Александр отвечает за сбор информации о нашей теме, Иван отвечает за проведение урока в нашей школе и подготовке к самому уроку. В конце мы получаем разные продукты: Саша подготавливает большой реферат на данную тему, Ваня продумывает сценарий урока и проводит сам урок. Цель и задачи проекта у нас одинаковые, но мы делаем разную работу для достижения этой цели.

# Глава 1

Многие слышали словосочетание «***Информационная безопасность»***, но не все понимают, что это словосочетание обозначает. «Информационная безопасность» — это процесс обеспечения доступности (обеспечение доступа к информации), целостности (обеспечение достоверности и полноты информации) и конфиденциальности (обеспечение доступа к информации только авторизованным пользователям) информации. Чтобы найти необходимые и оптимальные средства защиты информации, нужно знать виды угроз информационной безопасности.

Компоненты, на которые угрозы нацелены:

1. Данные
2. Программы
3. Аппаратура
4. Поддерживающая инфраструктура

К основным угрозам **доступности** можно отнести:

1. Внутренний отказ информационной системы;
2. Отказ поддерживающей инфраструктуры.

Основными источниками внутренних отказов являются:

1. Нарушение (случайное или умышленное) от установленных правил эксплуатации
2. Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.)
3. Ошибки при (пере) конфигурировании системы
4. Вредоносное программное обеспечение
5. Отказы программного и аппаратного обеспечения
6. Разрушение данных
7. Разрушение или повреждение аппаратуры

К основным угрозам **целостности** можно отнести:

1. Угрозы статической целостности (злоумышленник может ввести неверные данные, изменить данные).
2. Угрозы динамической целостности (кража, дублирование данных).

К основным угрозам **конфиденциальности** можно отнести:

1. Злоупотребление полномочиями
2. Нанесение ущерба при сервисном обслуживании

Принимая все вышесказанное во внимание, можно приступить к выбору *средств защиты* информации.

*Средства защиты* информации принято делить: неформальные и формальные.

**Неформальными средствами защиты информации** – являются *законодательные, административные и морально-этические**средства*, к которым можно отнести: документы, правила, мероприятия.

* *Законодательные средства* информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, всевозможными разными федеральными законами и различными подзаконными актами. Также государство определят меру ответственности за нарушение положений законодательства в сфере информационной безопасности.
* *Административные мероприятия* играют огромную и очень важную роль в создании механизма защиты данных. Злоумышленник может действовать благодаря небрежности, халатности пользователей или охранников – персонала защиты. Чтобы предотвратить халатность пользователей, необходимы мероприятия, которые исключали бы или намного уменьшали возможность проникновения угрозы. Например: архитектурные и планировочные решения, которые позволяют защитить переговорные комнаты от утечки информации.
* *К морально-этическим средствам* можно отнести сложившиеся в обществе или данном коллективе моральные, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе. Грубо говоря, человек сам должен понимать, какую информацию ему можно рассказать, а какую нет. Не соблюдение этих правил не несет никакой ответственности, но, рассказав информацию, ты можешь подорвать свой статус или авторитет в обществе.

**Формальные средства защиты информации** – это специальные технические средства и программное обеспечение, которые можно разделить на *физические, аппаратные, программные и криптографические.*

* К *физическим средствам защиты информации* относятся: замки, жалюзи и занавески. Также это камеры и всевозможные видеорегистраторы.
* К *аппаратным средствам защиты информации* относятся: генераторы шума, сетевые фильтры и другие устройства, которые встраиваются в информационные системы.
* *Программные средства защиты информации*– это простые и комплексные программы, предназначенные для решения задач, связанных с обеспечением информационной безопасности. Примером комплексных решений служат DLP-системы и SIEM-системы. **DLP-системы** («*Data Leak Prevention*» дословно «предотвращение утечки данных») соответственно служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков. **SIEM-системы** («*Security Information and Event Management*», что в переводе означает «Управление событиями и информационной безопасностью») обеспечивают анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, приборами или услугами, и используется также для и генерации отчетов в целях совместимости с прочими бизнес данными. Программные средства требовательны к мощности аппаратных устройств, и при установке необходимо предусмотреть дополнительные резервы.
* *Криптографический метод защиты информации* - внедрение криптографических методов защиты данных для безопасной передачи по сети. Криптография считается одним из самых надежных способов защиты данных, ведь она охраняет саму информацию, а не доступ к ней. Внедрение криптографической защиты информации предусматривает создание программно-аппаратного комплекса, архитектура и состав которого определяется, исходя из потребностей конкретного заказчика, требований законодательства, поставленных задач и необходимых методов, и алгоритмов шифрования.

**Глава 2**

ПРЕДИСЛОВИЕ

Разные люди понимают под **КРИПТОГРАФИЕЙ** разные вещи. Дети играют в игрушечные шифры и секретные языки. Это, однако, не имеет ничего общего с настоящей криптографией. Настоящая криптография (*strong cryptography*) должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями, такими как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Сейчас, с становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

По мере образования информационного общества, крупным государствам становятся доступны технологические средства тотального надзора за миллионами людей. Поэтому криптография становится одним из основных инструментов обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

БАЗОВАЯ ТЕРМИНОЛОГИЯ

Представьте, что вам надо отправить сообщение адресату. Вы хотите, чтобы никто кроме адресата не смог прочитать отправленную информацию. Однако всегда есть вероятность, что кто-либо вскроет конверт или перехватит электронное послание.

В криптографической терминологии исходное послание именуют открытым текстом (**plaintext или cleartext**). Изменение исходного текста так, чтобы скрыть от прочих его содержание, называют шифрованием (**encryption**). Зашифрованное сообщение называют шифротекстом (**ciphertext**). Процесс, при котором из шифротекста извлекается открытый текст, называют дешифровкой (**decryption**). Обычно в процессе шифровки и дешифровки используется некий ключ (**key**) и алгоритм обеспечивает, что дешифрование можно сделать лишь зная этот ключ.

*Криптография* - это наука о том, как обеспечить секретность сообщения. *Криптоанализ* - это наука о том, как вскрыть шифрованное сообщение, то есть, как извлечь открытый текст не зная ключа. Криптографией занимаются криптографы, а криптоанализом занимаются криптоаналитики.

Метод шифровки/дешифровки называют шифром (**cipher**). Все современные алгоритмы используют ключ для управления шифровкой и дешифровкой.

ОСНОВНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Алгоритмы с использованием ключа делятся на два класса: *симметричные* (или алгоритмы секретным ключом) и *ассиметричные* (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки.

*Симметричные* алгоритмы подразделяют на потоковые шифры и блочные шифры. Потоковые позволяют шифровать информацию побитово, в то время как блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

*Ассиметричные* шифры (также именуемые алгоритмами с открытым ключом) допускают, чтобы открытый ключ был доступен всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют открытым ключом, а ключ для дешифрования называют закрытым ключом или секретным ключом. Таким образом, мы с вами можем понять, что симметричные алгоритмы работают быстрее, чем ассиметричные.

Многие качественные криптографические алгоритмы доступны в книжном магазине, библиотеке или в Интернете. К широко известным симметричным алгоритмам относятся DES и IDEA. Самым лучшим асимметричным алгоритмом является RSA.

ЦИФРОВЫЕ ПОДПИСИ

Некоторые из асимметричных алгоритмов могут использоваться для генерирования **цифровой подписи**. Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного пользователя. Цифровые подписи также можно использовать для удостоверения (сертификации) того, что документ принадлежит определенному лицу. Это делается так: открытый ключ и информация о том, кому он принадлежит, подписываются стороной, которой доверяем. При этом доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом, возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (то есть ему мы доверяем не потому, что он кем-то подписан, а потому, что мы верим, что ему можно доверять). В централизованной инфраструктуре ключей имеется очень небольшое количество корневых ключей сети (например, облеченные полномочиями государственные агентства, их также называют сертификационными агентствами - certification authorities). В распределенной инфраструктуре нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем своему собственному ключу и ключам, ею подписанным). Эта концепция носит название сети доверия (web of trust) и реализована, например, в PGP.

Цифровая подпись документа обычно создается так: из документа генерируется так называемый дайджест (message digest) и к нему добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель сначала решает для себя доверяет ли он тому, что открытый ключ принадлежит именно тому, кому должен принадлежать (с помощью сети доверия или априорного знания), и затем дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась, и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Свободно доступны несколько методов создания и проверки цифровых подписей. Наиболее известным является алгоритм RSA.

ОБЕСПЕЧИВАЕМАЯ ШИФРОМ СТЕПЕНЬ ЗАЩИТЫ

Хорошие криптографические системы создаются таким образом, чтобы сделать их вскрытие как можно более трудным делом. Можно построить системы, которые на практике невозможно вскрыть. При этом не требуется очень больших усилий для реализации. Единственное, что требуется - это аккуратность и базовые знания. Нет прощения разработчику, если он оставил возможность для вскрытия системы.

Теоретически, любой шифровальный алгоритм с использованием ключа может быть вскрыт методом перебора всех значений ключа. Если ключ подбирается методом грубой силы (brute force), требуемая мощность компьютера растет экспоненциально с увеличением длины ключа. Ключ длиной в 32 бита требует 232 (около 109) шагов. Такая задача под силу любому дилетанту и решается на домашнем компьютере. Системы с 40-битным ключом требуют 240 шагов - такие компьютерные мощности имеются в большинстве университетов и даже в небольших компаниях. Системы с 56-битными ключами (DES) требуют для вскрытия заметных усилий, однако могут быть легко вскрыты с помощью специальной аппаратуры. Стоимость такой аппаратуры значительна, но доступна для мафии, крупных компаний и правительств. Ключи длиной 64 бита в настоящий момент, возможно, могут быть вскрыты крупными государствами и уже в ближайшие несколько лет будут доступны для вскрытия преступными организациями, крупными компаниями и небольшими государствами. Ключи длиной 80 бит могут в будущем стать уязвимыми. Ключи длиной 128 бит, вероятно, останутся недоступными для вскрытия методом грубой силы в обозримом будущем. Можно использовать и более длинные ключи. В пределе нетрудно добиться того, чтобы энергия, требуемая для вскрытия, превзойдет массу солнца.

Однако, длина ключа - это еще не все. Многие шифры можно вскрыть, не перебирая всех возможных комбинаций. Вообще говоря, очень трудно придумать шифр, который нельзя было бы вскрыть другим более эффективным способом. Разработка собственных шифров может стать приятным занятием, но для реальных приложений использовать самодельные шифры не рекомендуется, если вы не являетесь экспертом и не уверены на 100 процентов в том, что делаете.

В общем, следует держаться в стороне от неопубликованных или секретных алгоритмов. Часто разработчик такого алгоритма не уверен в его надежности, или же надежность зависит от секретности самого алгоритма. Вообще говоря, ни один алгоритм, секретность которого зависит от секретности самого алгоритма, не является надежным. В частности, имея шифрующую программу, можно нанять программиста, который восстановит алгоритм методом обратной инженерии. Опыт показывает, что большинство секретных алгоритмов, ставших впоследствии достоянием общественности, оказались ненадежными.

Длины ключей, используемых в криптографии с открытым ключом обычно значительно больше, чем в симметричных алгоритмах. Здесь проблема заключается не в подборе ключа, а в воссоздании секретного ключа по открытому. В случае RSA проблема эквивалентна разложению на множители большого целого числа, которое является произведением пары неизвестных простых чисел. В случае некоторых других криптосистем, проблема эквивалентна вычислению дискретного логарифма по модулю большого целого числа (такая задача считается примерно аналогичной по трудности задаче разложения на множители). Имеются криптосистемы, которые используют другие проблемы.

Важно подчеркнуть, что *степень надежности криптографической системы определяется ее слабейшим звеном*. Нельзя упускать из вида ни одного аспекта разработки системы - от выбора алгоритма до политики использования и распространения ключей.

**Глава 3**

КОМПЬЮТЕРНЫЙ ВИРУС

***Компьютерный вирус*** - это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам (т.е. «заражать» их), а также выполнять нежелательные различные действия на компьютере. Программа, внутри которой находится вирус, называется «заражённой». Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы, «засоряет» оперативную память и т.д.).

Для маскировки вируса, действия по заражению других программ и нанесению вреда могут выполняться не всегда, а скажем, при выполнении определённых условий. После того, как вирус выполнит нужные ему действия, он передаёт управление той программе, в которой он находится, и она работает так же, как обычная. Тем самым внешне работа заражённой программы выглядит так же, как и не заражённой.

Следует заметить, что тексты программ и документов, информационные файлы без данных, таблицы, табличные процессоры и другие аналогичные файлы не могут быть заражены вирусом, он может их только испортить.

ИСТОРИЯ ВИРУСОВ И ВСПЛЕСКИ КОМПЬЮТЕРНЫХ ВИРУСОВ

О появлении первого компьютерного вируса много разных мнений. Доподлинно только известно, что на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, его не было, а на Univax 1108 и IBM 360/370, в середине 1970-х годов они уже были. Среди тысяч вирусов лишь несколько десятков являются оригинальными разработками, использующими действительно принципиальные идеи. Все остальные - «вариации на тему». Но каждая оригинальная разработка заставляет создателей антивирусов приспосабливаться к новым условиям, *догонять вирусную технологию*. Например, в 1989 году американский студент сумел создать вирус, который вывел из строя около 6000 компьютеров Министерства обороны США. Или примером может быть эпидемия известного вируса Dir-II, разразившаяся в 1991 году. Вирус использовал действительно оригинальную, принципиально новую технологию и на первых порах сумел широко распространиться за счёт несовершенства традиционных антивирусных средств. Кристоферу Пайну удалось создать вирусы Pathogen и Queeq, а также вирус Smeg. Именно последний был самым опасным, его можно было накладывать на первые два вируса, и из-за этого после каждого прогона программы они меняли конфигурацию. Поэтому их было невозможно уничтожить. Чтобы распространить вирусы, Пайн скопировал компьютерные игры и программы, заразил их, а затем отправил обратно в сеть. Пользователи загружали в свои компьютеры, заражённые программы и инфицировали диски. Ситуация усугубилась тем, что Пайн умудрился занести вирусы и в программу, которая с ними борется. Запустив её, пользователи вместо уничтожения вирусов уничтожили файлы множества фирм, убытки составили миллионы фунтов стерлингов.

ПРИЧИНЫ ПОЯВЛЕНИЯ ВИРУСОВ

Причины появления и распространения компьютерных вирусов, с одной стороны, скрываются в психологии человеческой личности и её теневых сторонах (зависти, мести), с другой стороны, обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы персонального компьютера.

КЛАССИФИКАЦИЯ ВИРУСОВ

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

* среде обитания;
* способу заражения среды обитания;
* воздействию;
* особенностям алгоритма.

В зависимости от среды обитаниявирусы можно разделить на **сетевые, файлово-загрузочные, полиморфные, макровирусы и загрузочные.**

**Сетевые вирусы** распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, то есть в файлы, имеющие расширение COM и EXE.

**Файлово-загрузочные** вирусы могут внедряться в другие виды файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.

**Полиморфные вирусы** - это вирусы, модифицирующие свой код в заражённых программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

**Макро - вирусы** являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

**Загрузочные вирусы** внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска.

По способу заражения вирусы делятся на **резидентные и нерезидентные**.

**Резидентный вирус** при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

**Нерезидентные вирусы** не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вируса можно разделить на следующие виды:

* Неопасные, не мешающие работе компьютера, но уменьшающие объём свободной памяти и памяти на дисках. Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;
* Опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;
* Очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия.

**Простейшие вирусы** - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

**Вирусы - репликаторы**, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

**Вирусы-невидимки**, называемые стелс - вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращение операционной системы к поражённым файлом и секторам дисков и подставляют вместо своего тела незаражённые участки диска.

Наиболее трудно обнаружить **вирусы - мутанты**, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Имеются и так называемые **«троянские» программы**, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую структуру диска.

КАК ОПРЕДЕЛИТЬ ВИРУС НА КОМПЬЮТЕРЕ

Есть несколько признаков того, что на вашем компьютере завелся вирус:

1. Вас должно насторожить, если ваш *компьютер стал тормозить*. Если задачи выполняются дольше, чем обычно, то возможно, ваш компьютер заражен.
2. Будьте внимательны при появлении на компьютере *подозрительных приложений или программ*, о которых вы ничего не знаете. Если вы заметили, чтобы на компьютере появилось приложение или программа, которую вы не скачивали, будьте осторожны.
3. Еще один признак возможного заражения компьютера вирусом – это *странности в работе приложений или программ*. Если программы стали завершаться аварийно по непонятной причине, то, возможно, на вашем компьютере завелся вирус.
4. Зараженный компьютер может начать *перегреваться*. Если вы заметите такое, проверьте компьютер на вирусы, запустив антивирус.

**ЗАКЛЮЧЕНИЕ**

Данная работа может быть интересна выпускникам девятых классов, которые стоят перед выбором будущей профессии и направления обучения. Благодаря небольшой информации, которую ученики будут проходить в процессе обучения на профиле «ИТ-безопасность» в ИТ-классе, научная работа поможет школьникам определиться, действительно ли им интересен данный профиль.

Мы считаем, что ИТ-классы - это высокотехнологичные и оснащенные классы, направленные на обучение будущих специалистов в сфере ИТ. На профиле «ИТ-безопасность» обучаются будущие специалисты по защите информации в телекоммуникационных системах и сетях, будущие специалисты по безопасности компьютерных систем и сетей, у которых будет множество трудовых функций и знаний в целом.

# Источники

1. Перевод статьи Tatu Ylonen "Introduction to Cryptography"
2. Книга М.С.Наместникова. Книга называется "Информационная безопасность, или на расстоянии одного вируса". Книга предназначена для 7-9 классов. Также книга согласована с известнейшей компанией в своей сфере, с компанией "Kaspersky".
3. Основной интернет ресурс:  
   <https://habr.com/ru/company/vps_house/blog/343110/>
4. Основной сайт IT-класса:  
   <http://profil.mos.ru/it/?page_id=15>